

ΕΓΧΕΙΡΙΔΙΟ

Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων

Έκδοση 2018



Το χειρόγραφο ολοκληρώθηκε τον Απρίλιο του 2018.

Ενημερωμένες εκδόσεις θα διατίθενται στο μέλλον στον ιστότοπο του FRA, στη διεύθυνση fra.europa.eu, στον ιστότοπο του Συμβουλίου της Ευρώπης, στη διεύθυνση coe.int/dataprotection, και στον ιστότοπο του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου, στο μενού Νομολογία, στη διεύθυνση echr.coe.int, και στον ιστότοπο του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων, στη διεύθυνση edps.europa.eu.

Δικαιώματα φωτογραφίας (εξώφυλλο και εσωτερικό): © iStockphoto

© Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019

Η αναπαραγωγή επιτρέπεται εφόσον αναφέρεται η πηγή.

Για κάθε χρήση ή αναπαραγωγή φωτογραφιών ή άλλου υλικού τα οποία δεν καλύπτονται από δικαιώματα πνευματικής ιδιοκτησίας του Οργανισμού Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και του Συμβουλίου της Ευρώπης πρέπει να ζητείται απευθείας η άδεια των κατόχων των δικαιωμάτων πνευματικής ιδιοκτησίας.

Ούτε ο Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης/Συμβούλιο της Ευρώπης ούτε οποιοδήποτε πρόσωπο ενεργεί εξ ονόματός του ευθύνεται για ενδεχόμενη χρήση των παρακάτω πληροφοριών.

Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, 2019

ΣΤΕ: ISBN 978-92-871-9831-0

FRA – print: ISBN 978-92-9474-294-0

FRA – web: ISBN 978-92-9474-295-7

doi:10.2811/951028

doi:10.2811/631042

TK-05-17-225-EL-C

TK-05-17-225-EL-N

Το εγχειρίδιο συντάχθηκε στα αγγλικά. Το Συμβούλιο της Ευρώπης (ΣΤΕ) και το Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) δεν φέρουν ευθύνη για την ποιότητα της μετάφρασης του κειμένου σε άλλες γλώσσες. Οι απόψεις που εκφράζονται σε αυτό δεν δεσμεύουν το ΣΤΕ και το ΕΔΔΑ. Το εγχειρίδιο παραπέμπει σε επιλεγμένα υπομνηματιστικά έργα και εγχειρίδια. Το ΣΤΕ και το ΕΔΔΑ δεν φέρουν ευθύνη για το περιεχόμενό τους, και η επιλογή των συγκεκριμένων αναφορών στον βιβλιογραφικό κατάλογο δεν ισοδυναμεί με υιοθέτηση των απόψεων που εκφράζονται σε αυτά. Εκτενέστερη βιβλιογραφία διατίθεται στη διαδικτυακή σελίδα της βιβλιοθήκης του ΕΔΔΑ, στη διεύθυνση echr.coe.int/Library.

Το περιεχόμενο του παρόντος εγχειρίδιου δεν αντιπροσωπεύει την επίσημη θέση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) και δεν δεσμεύει τον ΕΕΠΔ κατά την άσκηση των αρμοδιοτήτων του. Ο ΕΕΠΔ δεν φέρει καμία ευθύνη για την ποιότητα των μεταφράσεων σε άλλες γλώσσες εκτός της αγγλικής.



Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων

Έκδοση 2018

Πρόλογος

Οι κοινωνίες μας ψηφιοποιούνται ολοένα και περισσότερο. Ο ρυθμός των τεχνολογικών εξελίξεων και ο τρόπος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα επηρεάζουν σε καθημερινή βάση τον καθένα από εμάς με πολλούς και διάφορους τρόπους. Πρόσφατα αναθεωρήθηκαν τα νομικά πλαίσια της Ευρωπαϊκής Ένωσης (ΕΕ) και του Συμβουλίου της Ευρώπης που διασφαλίζουν την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα.

Η Ευρώπη βρίσκεται στην πρώτη γραμμή της προστασίας δεδομένων παγκοσμίως. Τα πρότυπα της ΕΕ για την προστασία δεδομένων βασίζονται στη Σύμβαση 108 του Συμβουλίου της Ευρώπης, σε νομοθετικές πράξεις της ΕΕ – μεταξύ άλλων στον Γενικό Κανονισμό για την Προστασία Δεδομένων και στην Οδηγία για την Προστασία Δεδομένων που χρησιμοποιούνται από τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης– καθώς και στη σχετική νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου και του Δικαστηρίου της Ευρωπαϊκής Ένωσης.

Οι μεταρρυθμίσεις στον τομέα της προστασίας δεδομένων που πραγματοποιήθηκαν από την ΕΕ και το Συμβούλιο της Ευρώπης είναι εκτεταμένες και ενίοτε σύνθετες, με ποικίλα οφέλη και συνέπειες για τα άτομα και τις επιχειρήσεις. Στόχος του παρόντος εγχειριδίου είναι να ευαισθητοποιήσει και να ενισχύσει τη γνώση των κανόνων προστασίας δεδομένων, ιδίως για τους μη ειδικευμένους επαγγελματίες του νομικού κλάδου που καλούνται να χειριστούν ζητήματα προστασίας δεδομένων στο πλαίσιο της εργασίας τους.

Το παρόν εγχειρίδιο εκπονήθηκε από τον Οργανισμό Θεμελιωδών Δικαιωμάτων της ΕΕ (FRA), σε συνεργασία με το Συμβούλιο της Ευρώπης (από κοινού με τη Γραμματεία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου) και τον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων. Η παρούσα έκδοση, με την οποία επικαιροποιείται η έκδοση του 2014, αποτελεί μέρος μιας σειράς νομικών εγχειριδίων που εκδίδονται από κοινού από τον FRA και το Συμβούλιο της Ευρώπης.

Θα θέλαμε να εκφράσουμε τις ευχαριστίες μας στις αρχές προστασίας δεδομένων του Βελγίου, της Γαλλίας, της Γεωργίας, της Ελβετίας, της Εσθονίας, του Ηνωμένου Βασιλείου, της Ιρλανδίας, της Ιταλίας, του Μονακό και της Ουγγαρίας για τις χρήσιμες παρατηρήσεις τους σχετικά με το προσχέδιο του εγχειριδίου. Επιπλέον, θα θέλαμε να εκφράσουμε την εκτίμησή μας στη Μονάδα Προστασίας

Δεδομένων και στη Μονάδα Διεθνών Ροών Δεδομένων και Προστασίας Δεδομένων της Ευρωπαϊκής Επιτροπής. Ευχαριστούμε το Δικαστήριο της Ευρωπαϊκής Ένωσης για την υποστήριξη που μας παρείχε σε επίπεδο τεκμηρίωσης κατά τις προπαρασκευαστικές εργασίες της εκπόνησης του παρόντος εγχειριδίου. Τέλος, θα θέλαμε να εκφράσουμε τις ευχαριστίες μας στην Αρχή Προστασίας Δεδομένων της Ελλάδας και στο Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου για την υποστήριξή τους στην επικαιροποίηση της μετάφρασης του εγχειριδίου στα ελληνικά.

Χρήστος Γιακουμόπουλος Giovanni Buttarelli

Γενικός Διευθυντής
Δικαιωμάτων του
Ανθρώπου και Κράτους
Δικαίου του Συμβουλίου
της Ευρώπης

Ευρωπαίος Επόπτης
Προστασίας Δεδομένων

Michael O’Flaherty

Διευθυντής του
Οργανισμού Θεμελιωδών
Δικαιωμάτων της
Ευρωπαϊκής Ένωσης

Περιεχόμενα

ΠΡΟΛΟΓΟΣ	3
ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ ΚΑΙ ΑΚΡΩΝΥΜΙΑ	11
ΟΔΗΓΙΕΣ ΧΡΗΣΗΣ ΤΟΥ ΕΓΧΕΙΡΙΔΙΟΥ	13
1 ΠΛΑΙΣΙΟ ΚΑΙ ΙΣΤΟΡΙΚΟ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΔΙΚΑΙΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ	17
1.1. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα	20
Κύρια σημεία	20
1.1.1. Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα: σύντομη εισαγωγή	21
1.1.2. Διεθνές νομικό πλαίσιο: Ηνωμένα Έθνη	25
1.1.3. Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου	27
1.1.4. Σύμβαση 108 του Συμβουλίου της Ευρώπης	29
1.1.5. Το δίκαιο της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων	32
1.2. Περιορισμοί του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα	44
Κύρια σημεία	44
1.2.1. Προϋποθέσεις δικαιολογημένης επέμβασης βάσει της ΕΣΔΑ	45
1.2.2. Προϋποθέσεις νόμιμων περιορισμών βάσει του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ	52
1.3. Αλληλεπίδραση με άλλα δικαιώματα και θεμιτά συμφέροντα	65
Κύρια σημεία	65
1.3.1. Ελευθερία έκφρασης	67
1.3.2. Επαγγελματικό απόρρητο	86
1.3.3. Ελευθερία θρησκείας και πεποιθήσεων	90
1.3.4. Ελευθερία της τέχνης και της επιστήμης	92
1.3.5. Προστασία της διανοητικής ιδιοκτησίας	94
1.3.6. Προστασία δεδομένων και οικονομικά συμφέροντα	98
2 ΟΡΟΛΟΓΙΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ	103
2.1. Δεδομένα προσωπικού χαρακτήρα	105
Κύρια σημεία	105
2.1.1. Κύριες πτυχές της έννοιας των δεδομένων προσωπικού χαρακτήρα	106
2.1.2. Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα	123

2.2. Επεξεργασία δεδομένων	124
Κύρια σημεία	124
2.2.1. Η έννοια της επεξεργασίας δεδομένων	125
2.2.2. Αυτοματοποιημένη επεξεργασία δεδομένων	127
2.2.3. Μη αυτοματοποιημένη επεξεργασία δεδομένων	128
2.3. Χρήστες δεδομένων προσωπικού χαρακτήρα	129
Κύρια σημεία	129
2.3.1. Υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία	130
2.3.2. Αποδέκτες και τρίτοι	141
2.4. Συγκατάθεση	143
Κύρια σημεία	143

3 ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΔΙΚΑΙΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ

ΔΕΔΟΜΕΝΩΝ

3.1. Οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας της επεξεργασίας	149
Κύρια σημεία	149
3.1.1. Νομιμότητα της επεξεργασίας	150
3.1.2. Αντικειμενικότητα της επεξεργασίας	151
3.1.3. Διαφάνεια της επεξεργασίας	153
3.2. Η αρχή του περιορισμού του σκοπού	156
Κύρια σημεία	156
3.3. Η αρχή της ελαχιστοποίησης των δεδομένων	160
Κύρια σημεία	160
3.4. Η αρχή της ακρίβειας των δεδομένων	162
Κύρια σημεία	162
3.5. Η αρχή του περιορισμού της περιόδου αποθήκευσης	164
Κύρια σημεία	164
3.6. Η αρχή της ασφάλειας των δεδομένων	167
Κύρια σημεία	167
3.7. Η αρχή της λογοδοσίας	171
Κύρια σημεία	171

4 ΚΑΝΟΝΕΣ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΔΙΚΑΙΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

4.1. Κανόνες περί νόμιμης επεξεργασίας	178
Κύρια σημεία	178
4.1.1. Νόμιμοι λόγοι επεξεργασίας δεδομένων	178
4.1.2. Επεξεργασία ειδικών κατηγοριών δεδομένων (ευαίσθητα δεδομένα)	200

4.2.	Κανόνες περί ασφάλειας της επεξεργασίας	207
Κύρια σημεία		207
4.2.1.	Στοιχεία ασφάλειας δεδομένων	208
4.2.2.	Εμπιστευτικότητα	212
4.2.3.	Γνωστοποιήσεις παραβίασης δεδομένων προσωπικού χαρακτήρα	215
4.3.	Κανόνες περί λογοδοσίας και προώθησης της συμμόρφωσης	218
Κύρια σημεία		218
4.3.1.	Υπεύθυνοι προστασίας δεδομένων	219
4.3.2.	Αρχεία των δραστηριοτήτων επεξεργασίας	224
4.3.3.	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση	225
4.3.4.	Κώδικες δεοντολογίας	228
4.3.5.	Πιστοποίηση	230
4.4.	Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού	231
5	ΑΝΕΞΑΡΤΗΤΗ ΕΠΟΠΤΕΙΑ	235
Κύρια σημεία		236
5.1.	Ανεξαρτησία	240
5.2.	Αρμοδιότητα και εξουσίες	244
5.3.	Συνεργασία	248
5.4.	Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων	250
5.5.	Ο μηχανισμός συνεκτικότητας του ΓΚΠΔ	252
6	ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΥΠΟΚΕΙΜΕΝΩΝ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΕΠΙΒΟΛΗ ΤΟΥΣ	253
6.1.	Τα δικαιώματα των υποκειμένων των δεδομένων	257
Κύρια σημεία		257
6.1.1.	Δικαίωμα ενημέρωσης	258
6.1.2.	Δικαίωμα διόρθωσης	274
6.1.3.	Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)	277
6.1.4.	Δικαίωμα περιορισμού της επεξεργασίας	284
6.1.5.	Δικαίωμα στη φορητότητα των δεδομένων	285
6.1.6.	Δικαίωμα εναντίωσης	287
6.1.7.	Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ	292
6.2.	Προσφυγές, ευθύνη, κυρώσεις και αποζημίωση	296
Κύρια σημεία		296
6.2.1.	Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή	298
6.2.2.	Δικαίωμα πραγματικής δικαστικής προσφυγής	299
6.2.3.	Ευθύνη και δικαίωμα αποζημίωσης	308
6.2.4.	Κυρώσεις	310

7 ΔΙΕΘΝΕΙΣ ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΡΟΕΣ ΔΕΔΟΜΕΝΩΝ	
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	313
7.1. Φύση των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα	315
Κύρια σημεία	315
7.2. Ελεύθερη κυκλοφορία/ροή δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών ή συμβαλλόμενων μερών	316
Κύρια σημεία	316
7.3. Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες / μη συμβαλλόμενα μέρη ή σε διεθνείς οργανισμούς	318
Κύρια σημεία	318
7.3.1. Διαβιβάσεις βάσει απόφασης επάρκειας	319
7.3.2. Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις	325
7.3.3. Παρεκκλίσεις για ειδικές καταστάσεις	331
7.3.4. Διαβιβάσεις βάσει διεθνών συμφωνιών	334
8 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΑΣΤΥΝΟΜΙΚΟ ΤΟΜΕΑ ΚΑΙ ΤΟΝ ΤΟΜΕΑ ΤΗΣ ΠΟΙΝΙΚΗΣ ΔΙΚΑΙΟΣΥΝΗΣ	341
8.1. Το δίκαιο του Συμβουλίου της Ευρώπης για την προστασία των δεδομένων και την εθνική ασφάλεια, τον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης	343
Κύρια σημεία	343
8.1.1. Η σύσταση στον αστυνομικό τομέα	346
8.1.2. Η Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο	352
8.2. Το δίκαιο της ΕΕ για την προστασία των δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης	354
Κύρια σημεία	354
8.2.1. Η οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης	355
8.3. Άλλες ειδικές νομικές πράξεις σχετικά με την προστασία δεδομένων στον τομέα της επιβολής του νόμου	367
8.3.1. Προστασία δεδομένων στις δικαστικές υπηρεσίες και στις υπηρεσίες επιβολής του νόμου της ΕΕ	379
8.3.2. Προστασία δεδομένων στα κοινά συστήματα πληροφοριών σε επίπεδο ΕΕ	388

9	ΣΥΓΚΡΕΚΡΙΜΕΝΑ ΕΙΔΗ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΟΙ ΣΧΕΤΙΚΟΙ ΚΑΝΟΝΕΣ	
	ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΤΑ ΔΙΕΠΟΥΝ	411
9.1.	Ηλεκτρονικές επικοινωνίες	412
	Κύρια σημεία	412
9.2.	Δεδομένα στο πλαίσιο των εργασιακών σχέσεων	418
	Κύρια σημεία	418
9.3.	Δεδομένα υγείας	424
	Κύριο σημείο	424
9.4.	Επεξεργασία δεδομένων για ερευνητικούς και στατιστικούς σκοπούς	430
	Κύρια σημεία	430
9.5.	Χρηματοοικονομικά δεδομένα	434
	Κύρια σημεία	434
10	ΣΥΓΧΡΟΝΕΣ ΠΡΟΚΛΗΣΕΙΣ ΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ	
	ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ	439
10.1.	Μαζικά δεδομένα, αλγόριθμοι και τεχνητή νοημοσύνη	442
	Κύρια σημεία	442
	10.1.1. Ορισμός των μαζικών δεδομένων, των αλγόριθμων και της τεχνητής νοημοσύνης	443
	10.1.2. Στάθμιση των οφελών και των κινδύνων των μαζικών δεδομένων	446
	10.1.3. Ζητήματα προστασίας των δεδομένων	450
10.2.	Οι Ιστοί 2.0 και 3.0: κοινωνικά δίκτυα και διαδίκτυο των πραγμάτων	457
	Κύρια σημεία	457
	10.2.1. Ορισμός των Ιστών 2.0 και 3.0	458
	10.2.2. Στάθμιση των οφελών και των κινδύνων	461
	10.2.3. Ζητήματα προστασίας των δεδομένων	464
	ΕΠΙΠΡΟΣΘΕΤΗ ΒΙΒΛΙΟΓΡΑΦΙΑ	471
	ΝΟΜΟΛΟΓΙΑ	479
	Επιλεγμένη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου	479
	Επιλεγμένη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης	485
	ΕΥΡΕΤΗΡΙΟ	491

Συντομογραφίες και ακρωνύμια

CCTV	Κλειστό κύκλωμα τηλεόρασης
CETS	Σειρά Συνθηκών του Συμβουλίου της Ευρώπης
CRM	Διαχείριση σχέσεων με πελάτες
C-SIS	Κεντρικό Σύστημα Πληροφοριών Σένγκεν
EFSA	Ευρωπαϊκή Αρχή για την Ασφάλεια των Τροφίμων
ENISA	Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών
ENU	Εθνική Μονάδα Ευρώπης
ESMA	Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών
eu-LISA	Ευρωπαϊκός Οργανισμός για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης
EuroPriSe	Σφραγίδα Σεβασμού των Προσωπικών Δεδομένων (European Privacy Seal)
FRA	Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης
GPS	Παγκόσμιο Σύστημα Εντοπισμού Στίγματος (Global Positioning System)
ICCPR	Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα
ISP	Φορέας παροχής υπηρεσιών στο διαδίκτυο
N-SIS	Εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν
PIN	Προσωπικός αριθμός αναγνώρισης
PNR	Κατάσταση ονομάτων επιβατών
SCG	Συντονιστική Ομάδα Εποπτείας
SEPA	Ενιαίος Χώρος Πληρωμών σε Ευρώ (Single Euro Payments Area)
SIS	Σύστημα Πληροφοριών Σένγκεν
SWIFT	Εταιρεία Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (Society for Worldwide Interbank Financial Telecommunication)
VIS	Σύστημα πληροφοριών για τις θεωρήσεις
ΑΠΔ	Αρχή Προστασίας Δεδομένων
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Δεδομένων
ΔΕΔ-ΤΗΛΕ	Διερωπαϊκά δίκτυα στον τομέα των τηλεπικοινωνιών

ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης (καλούμενο έως τον Δεκέμβριο του 2009 ΔΕΚ, Δικαστήριο των Ευρωπαϊκών Κοινοτήτων)
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο των Δικαιωμάτων του Ανθρώπου
ΕΕ	Επίσημη Εφημερίδα
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΠΔ	Ευρωπαίος Επόπτης Προστασίας Δεδομένων
ΕΕΣ	Ευρωπαϊκό ένταλμα σύλληψης
ΕΖΕΣ	Ευρωπαϊκή Ζώνη Ελεύθερων Συναλλαγών
ΕΚ	Ευρωπαϊκή Κοινότητα
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος
ΕΣΔΑ	Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΚΕΑ	Κοινή Εποπτική Αρχή
ΜΚΟ	Μη κυβερνητική οργάνωση
ΟΔΔΑ	Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου
ΟΗΕ	Οργανισμός Ηνωμένων Εθνών
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
ΣΕΕ	Συνθήκη για την Ευρωπαϊκή Ένωση
ΣΛΕΕ	Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης
ΣτΕ	Συμβούλιο της Ευρώπης
Σύμβαση 108	Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (Συμβούλιο της Ευρώπης) Το τροποποιητικό πρωτόκολλο (CETS αριθ. 223) στη Σύμβαση 108 («Εκσυγχρονισμένη Σύμβαση 108») υιοθετήθηκε από την Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης στην 128η συνεδρίασή της, η οποία πραγματοποιήθηκε στο Elsinore, Δανία (17-18 Μαΐου 2018). Οι παραπομπές στην «Εκσυγχρονισμένη Σύμβαση 108» αναφέρονται στη Σύμβαση όπως αυτή τροποποιήθηκε από το Πρωτόκολλο CETS αριθ. 223.
ΤΠΕ	Τεχνολογία των πληροφοριών και των επικοινωνιών
ΤΣΠ	Τελωνειακό Σύστημα Πληροφοριών
ΥΠΔ	Υπεύθυνος προστασίας δεδομένων
Χάρτης	Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης

Οδηγίες χρήσης του εγχειριδίου

Στο παρόν εγχειρίδιο περιγράφονται οι νομικοί κανόνες σχετικά με την προστασία των δεδομένων οι οποίοι έχουν καθοριστεί από την Ευρωπαϊκή Ένωση (ΕΕ) και από το Συμβούλιο της Ευρώπης (ΣτΕ). Το εγχειρίδιο έχει σχεδιαστεί για να παρέχει βοήθεια σε νομικούς μη ειδικευμένους στον τομέα της προστασίας δεδομένων. Απευθύνεται σε δικηγόρους, δικαστές και άλλους ασκούντες νομικά επαγγέλματα, καθώς και σε πρόσωπα που εργάζονται σε άλλους φορείς, όπως μη κυβερνητικές οργανώσεις (ΜΚΟ), τα οποία μπορεί να αντιμετωπίζουν νομικά ζητήματα σχετικά με την προστασία δεδομένων.

Το παρόν εγχειρίδιο αποτελεί ένα πρώτο σημείο αναφοράς όσον αφορά το δίκαιο της ΕΕ, την Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), τη Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (Σύμβαση 108), καθώς και άλλες πράξεις του Συμβουλίου της Ευρώπης.

Κάθε κεφάλαιο ξεκινά με έναν πίνακα στον οποίο προσδιορίζονται οι νομικές διατάξεις που σχετίζονται με τα θέματα τα οποία εξετάζονται στο συγκεκριμένο κεφάλαιο. Οι πίνακες καλύπτουν το δίκαιο τόσο του Συμβουλίου της Ευρώπης, όσο και της ΕΕ και περιλαμβάνουν επιλεγμένη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) και του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ). Εν συνεχεία παρουσιάζονται διαδοχικά οι νομοθετικές ρυθμίσεις των δύο διαφορετικών ευρωπαϊκών έννομων τάξεων, όπως εφαρμόζονται στα υπό εξέταση θέματα. Με τον τρόπο αυτόν, ο αναγνώστης έχει τη δυνατότητα να παρατηρήσει τα σημεία στα οποία συγκλίνουν οι δύο έννομες τάξεις, αλλά και τις διαφορές τους. Ο πίνακας βοηθά επίσης τον αναγνώστη να βρει τις βασικές πληροφορίες που αφορούν την περίπτωση του, ιδίως εάν αυτή υπόκειται μόνο στο δίκαιο του Συμβουλίου της Ευρώπης. Σε μερικά κεφάλαια, όταν αυτό συμβάλλει στη συνοπτική παρουσίαση του περιεχομένου, η σειρά των θεμάτων στους πίνακες μπορεί να διαφέρει ελαφρώς από εκείνη εντός του ίδιου του κεφαλαίου. Το εγχειρίδιο παρέχει επίσης συνοπτική επισκόπηση του πλαισίου του Οργανισμού Ηνωμένων Εθνών.

Οι νομικοί σε κράτη εκτός της ΕΕ τα οποία είναι μέλη του Συμβουλίου της Ευρώπης και συμβαλλόμενα μέρη στην ΕΣΔΑ και στη Σύμβαση 108 μπορούν να βρουν τις πληροφορίες που αφορούν τη χώρα τους ανατρέχοντας απευθείας στις στήλες που αφορούν το Συμβούλιο της Ευρώπης. Οι νομικοί σε κράτη εκτός της ΕΕ πρέπει επίσης να λαμβάνουν υπόψη ότι, έπειτα από την έκδοση του Γενικού Κανονισμού

για την Προστασία Δεδομένων της ΕΕ, οι κανόνες της ΕΕ περί προστασίας δεδομένων εφαρμόζονται και σε οργανισμούς και άλλες οντότητες που δεν είναι εγκατεστημένοι στην ΕΕ εάν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα και προσφέρουν αγαθά και υπηρεσίες σε υποκείμενα δεδομένων στην Ένωση ή παρακολουθούν τη συμπεριφορά των εν λόγω υποκειμένων των δεδομένων.

Οι νομικοί σε κράτη μέλη της ΕΕ θα χρειάζεται να συμβουλευονται και τις δύο στήλες, δεδομένου ότι τα κράτη αυτά δεσμεύονται από αμφότερες τις έννομες τάξεις. Θα πρέπει να σημειωθεί ότι οι μεταρρυθμίσεις και ο εκσυγχρονισμός των κανόνων για την προστασία δεδομένων στην Ευρώπη, στο πλαίσιο τόσο του Συμβουλίου της Ευρώπης (Εκσυγχρονισμένη Σύμβαση 108 όπως αυτή τροποποιήθηκε από το Πρωτόκολλο CETS αριθ. 223) όσο και της ΕΕ (έκδοση του Γενικού Κανονισμού για την Προστασία Δεδομένων και της οδηγίας 2016/680/ΕΕ), υλοποιήθηκαν παράλληλα. Οι ρυθμιστικοί φορείς σε αμφότερα τα νομικά συστήματα επέδειξαν τη μέγιστη δυνατή προσοχή προκειμένου να διασφαλίζεται συνεκτικότητα και συμβατότητα μεταξύ των δύο νομικών πλαισίων. Επομένως, οι μεταρρυθμίσεις οδήγησαν σε μεγαλύτερη εναρμόνιση του δικαίου της προστασίας δεδομένων του Συμβουλίου της Ευρώπης και της ΕΕ. Όσοι επιθυμούν να εμβαθύνουν περισσότερο σε κάποιο συγκεκριμένο θέμα θα βρουν κατάλογο πιο εξειδικευμένων κειμένων στην ενότητα «Προτεινόμενη βιβλιογραφία». Για πληροφορίες σχετικά με τις διατάξεις του Πρωτοκόλλου 108 και του πρόσθετου Πρωτοκόλλου του 2001, τα οποία συνεχίζουν να εφαρμόζονται μέχρι τη θέση σε ισχύ του τροποποιητικού Πρωτοκόλλου, οι αναγνώστες πρέπει να ανατρέχουν στην έκδοση του 2014 του εγχειριδίου.

Το δίκαιο του Συμβουλίου της Ευρώπης παρουσιάζεται μέσω σύντομων παραπομπών σε επιλεγμένες υποθέσεις του ΕΔΔΑ. Αυτές επιλέχθηκαν από μεγάλο αριθμό αποφάσεων του ΕΔΔΑ οι οποίες αφορούν ζητήματα προστασίας των δεδομένων.

Το σχετικό δίκαιο της ΕΕ περιλαμβάνει εκδοθέντα νομοθετικά μέτρα, σχετικές διατάξεις των Συνθηκών και του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, όπως έχουν ερμηνευτεί στη νομολογία του ΔΕΕ. Επιπλέον, στο εγχειρίδιο παρουσιάζονται γνώμες και κατευθυντήριες γραμμές που έχουν εκδοθεί από την Ομάδα εργασίας του άρθρου 29, το συμβουλευτικό όργανο στο οποίο ανατέθηκε, βάσει της Οδηγίας για την Προστασία Δεδομένων, η παροχή εμπειρογνωσίας στα κράτη μέλη της ΕΕ, και το οποίο θα αντικατασταθεί από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) από τις 25 Μαΐου 2018 και έπειτα. Οι γνωμοδοτήσεις του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων παρέχουν επίσης σημαντικές πληροφορίες για την ερμηνεία του δικαίου της ΕΕ και, συνεπώς, περιλαμβάνονται στο παρόν εγχειρίδιο.

Οι υποθέσεις που περιγράφονται ή παρατίθενται στο παρόν εγχειρίδιο είναι ενδεικτικές σημαντικού όγκου νομολογίας τόσο του ΕΔΔΑ όσο και του ΔΕΕ. Στόχος των κατευθυντήριων γραμμών στο τέλος του εγχειριδίου είναι να βοηθήσουν τον αναγνώστη στην αναζήτηση νομολογίας μέσω διαδικτύου. Η νομολογία του ΔΕΕ που παρουσιάζεται αφορά την πρώην Οδηγία για την Προστασία Δεδομένων. Ωστόσο, οι ερμηνείες του ΔΕΕ εξακολουθούν να εφαρμόζονται στα αντίστοιχα δικαιώματα και στις αντίστοιχες υποχρεώσεις που καθιερώνει ο Γενικός Κανονισμός για την Προστασία Δεδομένων.

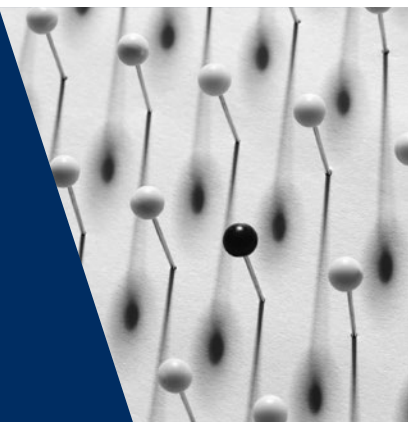
Επιπλέον, σε πλαίσια κειμένου με γαλάζιο φόντο παρέχονται πρακτικά παραδείγματα με υποθετικά σενάρια. Αυτά δίνουν μια σαφέστερη εικόνα για την εφαρμογή των ευρωπαϊκών κανόνων περί προστασίας δεδομένων στην πράξη, ιδίως όταν δεν υφίσταται συγκεκριμένη ειδική νομολογία του ΕΔΔΑ ή του ΔΕΕ. Σε άλλα πλαίσια κειμένου –με γκριζό φόντο– παρέχονται παραδείγματα τα οποία έχουν αντληθεί από διαφορετικές πηγές, πέραν της νομολογίας του ΕΔΔΑ και του ΔΕΕ, όπως νομοθεσία και γνώμες της Ομάδας εργασίας του άρθρου 29.

Το εγχειρίδιο ξεκινά με μια σύντομη περιγραφή του ρόλου των δύο νομικών συστημάτων όπως καθορίζεται στην ΕΣΔΑ και στο δίκαιο της ΕΕ (κεφάλαιο 1). Τα κεφάλαια 2 έως 10 καλύπτουν τα ακόλουθα ζητήματα:

- ορολογία στον τομέα της προστασίας δεδομένων·
- βασικές αρχές του ευρωπαϊκού δικαίου για την προστασία των δεδομένων·
- κανόνες του ευρωπαϊκού δικαίου για την προστασία των δεδομένων·
- ανεξάρτητη εποπτεία·
- δικαιώματα των υποκειμένων των δεδομένων και άσκηση αυτών·
- διασυννοιακές διαβιβάσεις και ροές δεδομένων προσωπικού χαρακτήρα·
- προστασία δεδομένων από μέρους της αστυνομίας και της ποινικής δικαιοσύνης·
- άλλοι ευρωπαϊκοί κανόνες περί προστασίας δεδομένων σε ειδικούς τομείς·
- σύγχρονες προκλήσεις της προστασίας των δεδομένων προσωπικού χαρακτήρα.

1

Πλαίσιο και ιστορικό του ευρωπαϊκού δικαίου για την προστασία των δεδομένων



ΕΕ

Ζητήματα
που
εξετάζονται

Συμβούλιο
της Ευρώπης

Το δικαίωμα στην προστασία των δεδομένων

Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, άρθρο 16.

Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ο Χάρτης), άρθρο 8 (δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα)

Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Οδηγία για την Προστασία Δεδομένων) (ΕΕ 1995, L 281, σ. 31) (σε ισχύ έως τον Μάιο του 2018)

Απόφαση-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις (ΕΕ 2008, L 350, σ. 60) (σε ισχύ έως τον Μάιο του 2018)

Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ 2016, L 119, σ. 1)

ΕΣΔΑ, άρθρο 8 (δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας)

Εκσυγχρονισμένη σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (Εκσυγχρονισμένη Σύμβαση 108)

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Οδηγία (ΕΕ) 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (προστασία δεδομένων για αστυνομικές και δικαστικές αρχές) (ΕΕ 2016, L 119, σ. 89) Οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ 2002, L 201, σ. 37) Κανονισμός (ΕΚ) αριθ. 45/2001 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (Κανονισμός για την προστασία δεδομένων από τα όργανα της ΕΕ) (ΕΕ 2001, L 8, σ. 1)		
Περιορισμοί του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα		
Ο Χάρτης, άρθρο 52 παράγραφος 1 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 23 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, <i>Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen</i> [τμήμα μείζονος συνθέσεως], 2010		ΕΣΔΑ, άρθρο 8 παράγραφος 2 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 11 ΕΔΔΑ, <i>S. και Marper κατά Ηνωμένου Βασιλείου</i> [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 2008
Εξισορρόπηση δικαιωμάτων		
ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, <i>Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen</i> [τμήμα μείζονος συνθέσεως], 2010	Γενικά	

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
ΔΕΕ, C-73/07, <i>Tietosuojavalvutettu</i> κατά <i>Satakunnan Markkinapörssi Oy</i> και <i>Satamedia Oy</i> [τμήμα μείζονος συνθέσεως], 2008 ΔΕΕ, C-131/12, <i>Google Spain SL, Google Inc.</i> κατά <i>Agencia Española de Protección de Datos (AEPD)</i> , <i>Mario Costeja González</i> [τμήμα μείζονος συνθέσεως], 2014	Ελευθερία έκφρασης	ΕΔΔΑ, <i>Axel Springer AG</i> κατά Γερμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 39954/08, 2012 ΕΔΔΑ, <i>Mosley</i> κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 48009/08, 2011 ΕΔΔΑ, <i>Bohlen</i> κατά Γερμανίας, προσφυγή αριθ. 53495/09, 2015
ΔΕΕ, C-28/08 P, <i>Ευρωπαϊκή Επιτροπή</i> κατά <i>The Bavarian Lager Co. Ltd</i> [τμήμα μείζονος συνθέσεως], 2010 ΔΕΕ, C-615/13 P, <i>ClientEarth, PAN Europe</i> κατά <i>EFSA</i> , 2015	Πρόσβαση σε έγγραφα	ΕΔΔΑ, <i>Magyar Helsinki Bizottság</i> κατά Ουγγαρίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 18030/11, 2016
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 90	Επαγγελματικό απόρρητο	ΕΔΔΑ, <i>Pruteanu</i> κατά Ρουμανίας, προσφυγή αριθ. 30181/05, 2015
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 91	Ελευθερία θρησκείας ή πεποιθήσεων	
	Ελευθερία της τέχνης και της επιστήμης	ΕΔΔΑ, <i>Vereinigung bildender Künstler</i> κατά Αυστρίας, προσφυγή αριθ. 68354/01, 2007
ΔΕΕ, C-275/06, <i>Productores de Música de España (Promusicae)</i> κατά <i>Telefónica de España SAU</i> [τμήμα μείζονος συνθέσεως], 2008	Προστασία της ιδιοκτησίας	
ΔΕΕ, C-131/12, <i>Google Spain SL, Google Inc.</i> κατά <i>Agencia Española de Protección de Datos (AEPD)</i> , <i>Mario Costeja González</i> [τμήμα μείζονος συνθέσεως], 2014 ΔΕΕ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce</i> κατά <i>Salvatore Manni</i> , 2017	Οικονομικά δικαιώματα	

1.1. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα

Κύρια σημεία

- Βάσει του άρθρου 8 της ΕΣΔΑ, το δικαίωμα προσώπου σε προστασία σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα περιλαμβάνεται στο δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας του.
- Η Σύμβαση 108 του Συμβουλίου της Ευρώπης είναι η πρώτη, και μέχρι στιγμής η μόνη, διεθνής νομικά δεσμευτική πράξη που αφορά την προστασία των δεδομένων. Η Σύμβαση υποβλήθηκε σε διαδικασία εκσυγχρονισμού, η οποία ολοκληρώθηκε με την υιοθέτηση του τροποποιητικού πρωτοκόλλου CETS αριθ. 223.
- Βάσει του δικαίου της ΕΕ, η προστασία δεδομένων αναγνωρίζεται ως διακριτό θεμελιώδες δικαίωμα. Προβλέπεται στο άρθρο 16 της Συνθήκης για τη λειτουργία της ΕΕ καθώς και στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.
- Στο πλαίσιο του δικαίου της ΕΕ, η προστασία δεδομένων ρυθμίστηκε για πρώτη φορά με την Οδηγία για την Προστασία Δεδομένων το 1995.
- Λαμβανομένων υπόψη των ραγδαίων τεχνολογικών εξελίξεων, η ΕΕ θέσπισε νέα νομοθεσία το 2016 για την προσαρμογή των κανόνων για την προστασία δεδομένων στην ψηφιακή εποχή. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων τέθηκε σε εφαρμογή τον Μάιο του 2018, καταργώντας την Οδηγία για την Προστασία Δεδομένων.
- Μαζί με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, η ΕΕ θέσπισε νομοθεσία για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από κρατικές αρχές για σκοπούς επιβολής του νόμου. Η οδηγία (ΕΕ) 2016/680 θεσπίζει τους κανόνες και τις αρχές προστασίας δεδομένων που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης και της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων.

1.1.1. Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα: σύντομη εισαγωγή

Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, παρότι συνδέονται στενά, είναι διακριτά δικαιώματα. Το δικαίωμα στην ιδιωτική ζωή –το οποίο αναφέρεται στο ευρωπαϊκό δίκαιο ως δικαίωμα στον σεβασμό της ιδιωτικής ζωής– έκανε την εμφάνισή του στο διεθνές δίκαιο ανθρωπίνων δικαιωμάτων στην Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (ΟΔΔΑ), η οποία εγκρίθηκε το 1948, ως ένα από τα θεμελιώδη προστατευόμενα ανθρώπινα δικαιώματα. Λίγο μετά την έγκριση της ΟΔΔΑ, η Ευρώπη κατοχύρωσε επίσης το δικαίωμα αυτό –στην Ευρωπαϊκή Σύμβαση των Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), συνθήκη η οποία είναι δεσμευτική για τα συμβαλλόμενα σε αυτή μέρη και η οποία καταρτίστηκε το 1950. Στην ΕΣΔΑ προβλέπεται ότι κάθε πρόσωπο έχει δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας του. Επέμβαση δημόσιας αρχής στην άσκηση του δικαιώματος αυτού δεν επιτρέπεται, εκτός εάν η επέμβαση προβλέπεται από τον νόμο, υπηρετεί σημαντικά και θεμιτά δημόσια συμφέροντα και είναι αναγκαία σε μια δημοκρατική κοινωνία.

Η ΟΔΔΑ και η ΕΣΔΑ εγκρίθηκαν πολύ πριν από την ανάπτυξη των ηλεκτρονικών υπολογιστών και του διαδικτύου και την ανάδυση της κοινωνίας των πληροφοριών. Οι εξελίξεις αυτές είχαν ως αποτέλεσμα σημαντικά πλεονεκτήματα για τα άτομα και την κοινωνία, βελτιώνοντας την ποιότητας ζωής, την αποδοτικότητα και την παραγωγικότητα. Ταυτόχρονα όμως, ενέχουν νέους κινδύνους για το δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Η αναγκαιότητα ειδικών κανόνων που να διέπουν τη συλλογή και τη χρήση προσωπικών πληροφοριών οδήγησε στην ανάδυση μιας νέας έννοιας της ιδιωτικής ζωής, που είναι γνωστή σε ορισμένες δικαιοδοσίες ως «πληροφοριακή ιδιωτικότητα» και σε άλλες ως «δικαίωμα στην πληροφοριακή αυτοδιάθεση»¹. Η έννοια αυτή οδήγησε στην

¹ Το γερμανικό Ομοσπονδιακό Συνταγματικό Δικαστήριο επιβεβαίωσε το δικαίωμα στην πληροφοριακή αυτοδιάθεση σε απόφαση του 1983 στην υπόθεση *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1 κ. επ. Το εν λόγω δικαστήριο έκρινε ότι η πληροφοριακή αυτοδιάθεση απορρέει από το θεμελιώδες δικαίωμα στον σεβασμό της προσωπικότητας, το οποίο κατοχυρώνεται στο γερμανικό Σύνταγμα. Σε απόφαση του 2017, το ΕΔΔΑ αναγνώρισε ότι το άρθρο 8 της ΕΣΔΑ «προβλέπει το δικαίωμα σε μορφή πληροφοριακής αυτοδιάθεσης». Βλ. ΕΔΔΑ, *Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας*, προσφυγή αριθ. 931/13, 27 Ιουνίου 2017, σκέψη 137.

ανάπτυξη ειδικών νομικών κανονισμών οι οποίοι εξασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα.

Η προστασία των δεδομένων στην Ευρώπη ξεκίνησε στη δεκαετία του 1970, με τη θέσπιση νομοθεσίας –από ορισμένα κράτη– για τον έλεγχο της επεξεργασίας προσωπικών πληροφοριών από δημόσιες αρχές και μεγάλες εταιρείες ². Εν συνεχεία θεσπίστηκαν πράξεις προστασίας των δεδομένων σε ευρωπαϊκό επίπεδο ³ και, με την πάροδο του χρόνου, η προστασία των δεδομένων εξελίχθηκε σε διακριτή αξία, η οποία δεν υπάγεται στο δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Στην έννομη τάξη της ΕΕ, η προστασία των δεδομένων αναγνωρίζεται ως θεμελιώδες δικαίωμα, διακριτό από το θεμελιώδες δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Ο διαχωρισμός αυτός εγείρει το ζήτημα της σχέσης και των διαφορών μεταξύ των δύο δικαιωμάτων.

Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα συνδέονται στενά. Αποσκοπούν αμφότερα στην προστασία παρόμοιων αξιών, δηλαδή της αυτονομίας και της ανθρωπίνης αξιοπρέπειας των προσώπων, παρέχοντάς τους μια σφαίρα στην οποία μπορούν να αναπτύσσουν ελεύθερα την προσωπικότητά τους, να σκέφτονται και να διαμορφώνουν τις απόψεις τους. Αποτελούν, επομένως, βασικό προαπαιτούμενο για την άσκηση άλλων θεμελιωδών ελευθεριών, όπως της ελευθερίας της έκφρασης, της ελευθερίας του συνέρχεσθαι και του συνεταιρίζεσθαι και της θρησκευτικής ελευθερίας.

Τα δύο δικαιώματα διαφέρουν ως προς τη διατύπωση και το πεδίο εφαρμογής τους. Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής συνίσταται σε γενική απαγόρευση των επεμβάσεων, με την επιφύλαξη ορισμένων κριτηρίων δημόσιου συμφέροντος τα οποία μπορούν να δικαιολογούν την επέμβαση σε ορισμένες περιπτώσεις. Η προστασία των δεδομένων προσωπικού χαρακτήρα γίνεται

2 Το γερμανικό κρατίδιο της Έσης εξέδωσε τον πρώτο νόμο για την προστασία των δεδομένων το 1970, ο οποίος ίσχυε μόνο στο συγκεκριμένο κρατίδιο. Το 1973 η Σουηδία εξέδωσε τον πρώτο παγκοσμίως εθνικό νόμο για την προστασία των δεδομένων. Έως τα τέλη της δεκαετίας του 1980, αρκετά ευρωπαϊκά κράτη (Γαλλία, Γερμανία, Ηνωμένο Βασίλειο και Κάτω Χώρες) είχαν επίσης θεσπίσει νομοθεσία για την προστασία των δεδομένων.

3 Η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (Σύμβαση 108) του Συμβουλίου της Ευρώπης εκδόθηκε το 1981. Η ΕΕ εξέδωσε την πρώτη της συνολική πράξη για την προστασία των δεδομένων το 1995: την οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

αντιληπτή ως σύγχρονο και ενεργό δικαίωμα ⁴, που απαιτεί την καθιέρωση ενός συστήματος ελέγχων και ισορροπιών για την προστασία των προσώπων κατά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Η επεξεργασία πρέπει να είναι σύμφωνη προς τις βασικές συνιστώσες της προστασίας των δεδομένων προσωπικού χαρακτήρα, ιδίως την ανεξάρτητη εποπτεία και τον σεβασμό των δικαιωμάτων του υποκειμένου των δεδομένων ⁵.

Το άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ (εφεξής ο Χάρτης) όχι μόνο αναγνωρίζει το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, αλλά επισημαίνει επίσης τις βασικές αξίες που συνδέονται με το δικαίωμα αυτό. Η εν λόγω διάταξη προβλέπει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από τον νόμο. Τα πρόσωπα πρέπει να έχουν δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν, καθώς και δικαίωμα δόρθωσης αυτών, η δε συμμόρφωση προς το δικαίωμα αυτό πρέπει να υπόκειται στον έλεγχο ανεξάρτητης αρχής.

Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα ενεργοποιείται κάθε φορά που πραγματοποιείται επεξεργασία τους επομένως, είναι ευρύτερο από το δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα υπόκειται σε κατάλληλη προστασία. Η προστασία αφορά όλα τα είδη δεδομένων προσωπικού χαρακτήρα και επεξεργασίας δεδομένων, ανεξάρτητα από τη σχέση και τον αντίκτυπο στην ιδιωτική ζωή. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα ενδέχεται επίσης να προσβάλλει το δικαίωμα στην ιδιωτική ζωή, όπως καταδεικνύεται στα παραδείγματα που παρατίθενται κατωτέρω. Ωστόσο, δεν είναι αναγκαίο να αποδεικνύεται προσβολή της ιδιωτικής ζωής προκειμένου να ενεργοποιηθούν οι κανόνες περί προστασίας δεδομένων.

Το δικαίωμα στην ιδιωτική ζωή αφορά καταστάσεις στις οποίες θίγεται ιδιωτικό συμφέρον, ή η «ιδιωτική ζωή», προσώπου. Όπως καταδεικνύεται στο παρόν εγχειρίδιο, η έννοια της «ιδιωτικής ζωής» έχει τύχει ευρείας ερμηνείας

4 Κατά τη γενική εισαγγελία E. Sharpston, η υπόθεση αφορούσε δύο διακριτά δικαιώματα: το «κλασικό» δικαίωμα στην προστασία της ιδιωτικής ζωής και ένα περισσότερο «σύγχρονο» δικαίωμα, το δικαίωμα στην προστασία δεδομένων. Βλ. ΔΕΕ, συνεκδικαζόμενες υποθέσεις C-92/09 και C-93/09, *Volkmer und Markus Schecke GbR κατά Land Hessen*, προτάσεις της γενικής εισαγγελέα *Eleanor Sharpston*, της 17ης Ιουνίου 2010, σημείο 71.

5 Hustinx, P., *EDPS Speeches & Articles, EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, Ιούλιος 2013.

στη νομολογία, ως καλύπτουσα προσωπικές καταστάσεις, ευαίσθητες ή εμπιστευτικές πληροφορίες, πληροφορίες οι οποίες θα μπορούσαν να επηρεάσουν αρνητικά την αντίληψη του κοινού για ένα πρόσωπο, αλλά ακόμη και πτυχές της επαγγελματικής ζωής και της δημόσιας συμπεριφοράς προσώπου. Ωστόσο, η αξιολόγηση της ύπαρξης, στο παρόν ή στο παρελθόν, επέμβασης στην «ιδιωτική ζωή» εξαρτάται από το πλαίσιο και τα πραγματικά περιστατικά κάθε επιμέρους περίπτωσης.

Από την άλλη πλευρά, οποιαδήποτε πράξη που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε να εμπίπτει στο πεδίο εφαρμογής των κανόνων περί προστασίας δεδομένων και να ενεργοποιήσει το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Για παράδειγμα, όταν ένας εργοδότης καταγράφει πληροφορίες που σχετίζονται με τα ονόματα και την αμοιβή των υπαλλήλων, η απλή καταγραφή των πληροφοριών αυτών δεν μπορεί να θεωρηθεί επέμβαση στην ιδιωτική ζωή. Τέτοια επέμβαση θα μπορούσε, ωστόσο, να στοιχειοθετηθεί, για παράδειγμα, εάν ο εργοδότης διαβίβαζε τις προσωπικές πληροφορίες των υπαλλήλων σε τρίτους. Εν πάση περιπτώσει, οι εργοδότες πρέπει να συμμορφώνονται προς τους κανόνες περί προστασίας δεδομένων, επειδή η καταχώριση πληροφοριών που αφορούν τους υπαλλήλους συνιστά επεξεργασία δεδομένων.

Παράδειγμα: Στην υπόθεση *Digital Rights Ireland*⁶, το ΔΕΕ κλήθηκε να αποφανθεί επί του κύρους της οδηγίας 2006/24/EK λαμβανομένων υπόψη των θεμελιωδών δικαιωμάτων στην προστασία των δεδομένων προσωπικού χαρακτήρα και στον σεβασμό της ιδιωτικής ζωής, τα οποία κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Η οδηγία υποχρέωνε τους παρόχους διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών να διατηρούν τα δεδομένα τηλεπικοινωνιών των πολιτών για μέγιστο διάστημα δύο ετών, προκειμένου τα δεδομένα να είναι διαθέσιμα για σκοπούς πρόληψης, διερεύνησης και δίωξης σοβαρών εγκλημάτων. Το μέτρο αφορούσε μόνο μεταδεδομένα, δεδομένα θέσης και δεδομένα αναγκαία για την αναγνώριση του συνδρομητή ή χρήστη. Δεν αφορούσε το περιεχόμενο των ηλεκτρονικών επικοινωνιών.

⁶ ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

Το ΔΕΕ έκρινε ότι η οδηγία συνιστούσε επέμβαση στο θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, «δεδομένου ότι προβλέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα» ⁷. Επιπλέον, διαπίστωσε ότι η οδηγία συνιστούσε επέμβαση στο δικαίωμα στον σεβασμό της ιδιωτικής ζωής ⁸. Θεωρούμενα στο σύνολό τους, τα δεδομένα προσωπικού χαρακτήρα που διατηρούνταν βάσει της οδηγίας, στα οποία μπορούσαν να έχουν πρόσβαση οι αρμόδιες αρχές, μπορούσαν να «παρέχουν τη δυνατότητα συναγωγής ιδιαίτερως ακριβών συμπερασμάτων σε σχέση με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα έχουν διατηρηθεί, όπως είναι οι καθημερινές συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των προσώπων αυτών και τα κοινωνικά περιβάλλοντα στα οποία τα πρόσωπα αυτά συχνάζουν» ⁹. Η επέμβαση στα δύο δικαιώματα ήταν τεράστιας έκτασης και ιδιαίτερα μεγάλης βαρύτητας.

Το ΔΕΕ κήρυξε την οδηγία 2006/24/EK ανίσχυρη, αποφαινόμενο ότι, παρότι επιδίωκε θεμιτό σκοπό, η επέμβαση στα δικαιώματα της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής ήταν σοβαρή και δεν περιοριζόταν στο απολύτως αναγκαίο μέτρο.

1.1.2. Διεθνές νομικό πλαίσιο: Ηνωμένα Έθνη

Το πλαίσιο των Ηνωμένων Εθνών δεν αναγνωρίζει την προστασία των δεδομένων προσωπικού χαρακτήρα ως θεμελιώδες δικαίωμα, παρότι το δικαίωμα στην ιδιωτική ζωή είναι από καιρό καθιερωμένο θεμελιώδες δικαίωμα στη διεθνή έννομη τάξη. Το άρθρο 12 της ΟΔΔΑ σχετικά με τον σεβασμό της ιδιωτικής και οικογενειακής ζωής ¹⁰ σηματοδοτεί την πρώτη φορά που διεθνής πράξη θεσπίζει το δικαίωμα στην προστασία της ιδιωτικής σφαίρας κατά επεμβάσεων τρίτων, και ιδίως του κράτους. Παρότι πρόκειται για μη δεσμευτική διακήρυξη, η ΟΔΔΑ περιβάλλεται με σημαντικό κύρος, ως η θεμελιακή πράξη του διεθνούς δικαίου ανθρωπίνων δικαιωμάτων, και έχει επηρεάσει την κατάρτιση άλλων πράξεων για τα ανθρώπινα δικαιώματα στην Ευρώπη. Το Διεθνές Σύμφωνο για

⁷ Ό.π., σκέψη 36.

⁸ Ό.π., σκέψεις 32-35.

⁹ Ό.π., σκέψη 27.

¹⁰ Οργανισμός Ηνωμένων Εθνών (ΟΗΕ), Οικουμενική Διακήρυξη των Δικαιωμάτων του Ανθρώπου (ΟΔΔΑ), 10 Δεκεμβρίου 1948.

τα Ατομικά και Πολιτικά Δικαιώματα (ICCPR) τέθηκε σε ισχύ το 1976. Διακηρύσσει ότι ουδείς υποβάλλεται σε αυθαίρετες ή παράνομες επεμβάσεις στην ιδιωτική ζωή, στην κατοικία ή στην αλληλογραφία του, ούτε σε παράνομες προσβολές της τιμής και της υπόληψής του. Το ICCPR είναι διεθνής συνθήκη η οποία δεσμεύει τα 169 συμβαλλόμενα μέρη της ώστε να σέβονται και να διασφαλίζουν την άσκηση των ατομικών δικαιωμάτων των φυσικών προσώπων, συμπεριλαμβανομένου του δικαιώματος στην ιδιωτική ζωή.

Από το 2013, ο Οργανισμός Ηνωμένων Εθνών έχει εκδώσει δύο αποφάσεις σχετικά με ζητήματα της ιδιωτικής ζωής με τίτλο «το δικαίωμα στην ιδιωτική ζωή στην ψηφιακή εποχή»¹¹ ως απάντηση στην ανάπτυξη νέων τεχνολογιών και στις αποκαλύψεις περί μαζικής παρακολούθησης που διενεργήθηκε σε ορισμένα κράτη (οι αποκαλύψεις Snowden). Σε αυτές καταδικάζεται έντονα η μαζική παρακολούθηση και τονίζεται ο αντίκτυπος που μπορεί να έχει αυτού του είδους η παρακολούθηση στα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και στην ελευθερία έκφρασης, καθώς και στη λειτουργία μιας σφύζουσας και δημοκρατικής κοινωνίας. Παρότι δεν είναι νομικά δεσμευτικές, οι αποφάσεις αυτές πυροδότησαν ευρύ διεθνή πολιτικό διάλογο υψηλού επιπέδου σχετικά με την ιδιωτική ζωή, τις νέες τεχνολογίες και την παρακολούθηση. Οδήγησαν επίσης στον διορισμό Ειδικού Εισηγητή για το δικαίωμα στην ιδιωτικότητα, με εντολή την προαγωγή και την προστασία του δικαιώματος αυτού. Στα ειδικά καθήκοντα του εισηγητή περιλαμβάνονται η συλλογή πληροφοριών σχετικά με τις εθνικές πρακτικές και εμπειρίες σε σχέση με την ιδιωτική ζωή και οι προκλήσεις που απορρέουν από τις νέες τεχνολογίες, η ανταλλαγή και η προώθηση βέλτιστων πρακτικών, καθώς και ο προσδιορισμός δυνητικών εμποδίων.

Ενώ προηγούμενες αποφάσεις επικεντρώνονταν στις αρνητικές συνέπειες της μαζικής παρακολούθησης και στην ευθύνη των κρατών να περιορίζουν τις εξουσίες των αρχών πληροφοριών, οι πιο πρόσφατες αποφάσεις αντικατοπτρίζουν μια βασική εξέλιξη στον διάλογο σχετικά με την ιδιωτική ζωή στα Ηνωμένα Έθνη¹². Στις αποφάσεις που εκδόθηκαν το 2016 και το 2017 επαναβεβαιώνεται η ανάγκη περιορισμού των εξουσιών των υπηρεσιών πληροφοριών και καταδικάζεται η μαζική παρακολούθηση. Ωστόσο, αναφέρεται επίσης ρητώς ότι «οι αυξανόμενες ικανότητες των επιχειρήσεων να συλλέγουν, να επεξεργάζονται

11 Βλ. ΟΗΕ, Γενική Συνέλευση, [Resolution on the right to privacy in the digital age](#), A/RES/68/167, Νέα Υόρκη, 18 Δεκεμβρίου 2013· και ΟΗΕ, Γενική Συνέλευση, [Revised draft resolution on the right to privacy in the digital age](#), A/C.3/69/L.26/Rev.1, Νέα Υόρκη, 19 Νοεμβρίου 2014.

12 ΟΗΕ, Γενική Συνέλευση, [Revised draft resolution on the right to privacy in the digital age](#), A/C.3/71/L.39/Rev.1, Νέα Υόρκη, 16 Νοεμβρίου 2016· ΟΗΕ, Συμβούλιο Ανθρωπίνων Δικαιωμάτων, [The right to privacy in the digital age](#), A/HRC/34/L.7/Rev.1, 22 Μαρτίου 2017.

και να χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα μπορεί να θέσουν σε κίνδυνο την άσκηση του δικαιώματος στην ιδιωτική ζωή στην ψηφιακή εποχή». Επομένως, πέραν της ευθύνης των κρατικών αρχών, στις αποφάσεις επισημαίνεται η ευθύνη του ιδιωτικού τομέα να σέβεται τα ανθρώπινα δικαιώματα και ζητείται από τις εταιρείες να ενημερώνουν τους χρήστες σχετικά με τη συλλογή, τη χρήση, την ανταλλαγή και τη διατήρηση δεδομένων προσωπικού χαρακτήρα, καθώς και να θεσπίζουν πολιτικές επεξεργασίας οι οποίες να χαρακτηρίζονται από διαφάνεια.

1.1.3. Η Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου

Το Συμβούλιο της Ευρώπης συστάθηκε μετά τον Β΄ Παγκόσμιο Πόλεμο με σκοπό να συνενώσει τα κράτη της Ευρώπης για την προαγωγή του κράτους δικαίου, της δημοκρατίας, των ανθρωπίνων δικαιωμάτων και της κοινωνικής ανάπτυξης. Για τον σκοπό αυτόν, το Συμβούλιο της Ευρώπης εξέδωσε το 1950 την ΕΣΔΑ, η οποία τέθηκε σε ισχύ το 1953.

Τα συμβαλλόμενα μέρη έχουν διεθνή υποχρέωση συμμόρφωσης με την ΕΣΔΑ. Όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης έχουν πλέον ενσωματώσει ή θέσει σε ισχύ την ΕΣΔΑ στο εθνικό τους δίκαιο, με αποτέλεσμα να υποχρεούνται να ενεργούν σύμφωνα με τις διατάξεις της. Τα συμβαλλόμενα μέρη οφείλουν να σέβονται τα δικαιώματα που προβλέπονται στη Σύμβαση κατά την άσκηση κάθε δραστηριότητας ή εξουσίας. Η υποχρέωση αυτή περιλαμβάνει τις δραστηριότητες που πραγματοποιούνται για την εθνική ασφάλεια. Αποφάσεις-ορόσημα του Ευρωπαϊκού Δικαστηρίου Δικαιωμάτων του Ανθρώπου (ΕΔΔΑ) αφορούν κρατικές δραστηριότητες στους ευαίσθητους τομείς της νομοθεσίας και της πρακτικής σε θέματα εθνικής ασφάλειας¹³. Το ΕΔΔΑ δεν δίστασε να επιβεβαιώσει ότι οι δραστηριότητες παρακολούθησης δεν συμβιβάζονται με τον σεβασμό της ιδιωτικής ζωής¹⁴.

Το ΕΔΔΑ συστάθηκε στο Στρασβούργο της Γαλλίας το 1959 προκειμένου να διασφαλίζεται η τήρηση των υποχρεώσεων των συμβαλλόμενων μερών στο πλαίσιο της ΕΣΔΑ. Το ΕΔΔΑ διασφαλίζει την τήρηση των υποχρεώσεων που υπέχουν τα κράτη βάσει της Σύμβασης εξετάζοντας προσφυγές φυσικών προσώπων,

13 Βλ., π.χ.: ΕΔΔΑ, *Klass κ.λπ. κατά Γερμανίας*, αριθ. 5029/71, 6 Σεπτεμβρίου 1978· ΕΔΔΑ, *Rotaru κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000 και ΕΔΔΑ, *Szabó και Vissy κατά Ουγγαρίας*, προσφυγή αριθ. 37138/14, 12 Ιανουαρίου 2016.

14 Ό.π.

ομάδων φυσικών προσώπων, ΜΚΟ ή νομικών προσώπων που προσφεύγουν κατά εικαζόμενων παραβιάσεων της Σύμβασης. Το ΕΔΔΑ μπορεί επίσης να εξετάζει υποθέσεις μεταξύ κρατών, όταν ένα ή περισσότερα κράτη μέλη του Συμβουλίου της Ευρώπης ασκούν προσφυγή κατά άλλου κράτους μέλους.

Από το 2018, το Συμβούλιο της Ευρώπης απαρτίζεται από 47 συμβαλλόμενα μέρη, εκ των οποίων 28 είναι επίσης κράτη μέλη της ΕΕ. Ο προσφεύγων ενώπιον του ΕΔΔΑ δεν είναι απαραίτητο να είναι πολίτης ενός εκ των συμβαλλόμενων μερών, παρότι οι εικαζόμενες παραβάσεις πρέπει να έχουν λάβει χώρα εντός της δικαιοδοσίας ενός εκ των συμβαλλόμενων μερών.

Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα περιλαμβάνεται στα δικαιώματα που προστατεύονται βάσει του άρθρου 8 της ΕΣΔΑ, στο οποίο κατοχυρώνεται το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και της αλληλογραφίας και καθορίζονται οι προϋποθέσεις υπό τις οποίες επιτρέπονται περιορισμοί του εν λόγω δικαιώματος¹⁵.

Το ΕΔΔΑ έχει εξετάσει πολλές περιπτώσεις που αφορούσαν ζητήματα προστασίας δεδομένων. Αυτές περιλαμβάνουν υποκλοπές επικοινωνιών¹⁶, διάφορες μορφές παρακολούθησης τόσο από τον ιδιωτικό, όσο και από τον δημόσιο τομέα¹⁷, καθώς και προστασία κατά της αποθήκευσης δεδομένων προσωπικού χαρακτήρα από δημόσιες αρχές¹⁸. Ο σεβασμός της ιδιωτικής ζωής δεν είναι απόλυτο δικαίωμα, καθώς η άσκηση του δικαιώματος στην ιδιωτική ζωή θα μπορούσε να θίγει άλλα δικαιώματα, όπως την ελευθερία έκφρασης και την πρόσβαση σε πληροφορίες και το αντίστροφο. Ως εκ τούτου, το ΕΔΔΑ προσπαθεί να επιτύχει ισορροπία μεταξύ των διαφόρων δικαιωμάτων που διακυβεύονται. Το ΕΔΔΑ έχει διευκρινίσει ότι το άρθρο 8 της ΕΣΔΑ όχι μόνο υποχρεώνει τα κράτη να απέχουν από οποιαδήποτε ενέργεια η οποία μπορεί να συνιστά παραβίαση του δικαιώματος αυτού που κατοχυρώνεται στη Σύμβαση, αλλά επιβάλλει επίσης, υπό ορισμένες συνθήκες, στα κράτη θετικές υποχρεώσεις, να διασφαλίζουν ενεργά τον

15 Συμβούλιο της Ευρώπης, Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, CETS αριθ. 005, 1950.

16 Βλ., για παράδειγμα: ΕΔΔΑ, *Malone κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 8691/79, 2 Αυγούστου 1984· ΕΔΔΑ, *Copland κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 62617/00, 3 Απριλίου 2007, ή ΕΔΔΑ, *Mustafa Sezgin Tanrikulu κατά Τουρκίας*, προσφυγή αριθ. 27473/06, 18 Ιουλίου 2017.

17 Βλ., για παράδειγμα: ΕΔΔΑ, *Klass κ.λπ. κατά Γερμανίας*, προσφυγή αριθ. 5029/71, 6 Σεπτεμβρίου 1978· ΕΔΔΑ, *Uzun κατά Γερμανίας*, προσφυγή αριθ. 35623/05, 2 Σεπτεμβρίου 2010.

18 Βλ., για παράδειγμα: ΕΔΔΑ, *Roman Zakharov κατά Ρωσίας*, προσφυγή αριθ. 47143/06, 4 Δεκεμβρίου 2015· ΕΔΔΑ, *Szabó και Vissy κατά Ουγγαρίας*, προσφυγή αριθ. 37138/14, 12 Ιανουαρίου 2016.

ουσιαστικό σεβασμό της ιδιωτικής και οικογενειακής ζωής¹⁹. Πολλές από τις υποθέσεις αυτές περιγράφονται αναλυτικά στα αντίστοιχα κεφάλαια.

1.1.4. Σύμβαση 108 του Συμβουλίου της Ευρώπης

Με την ανάπτυξη της τεχνολογίας των πληροφοριών στη δεκαετία του 1960, υπήρχε η αυξανόμενη ανάγκη για λεπτομερέστερους κανόνες προστασίας των φυσικών προσώπων μέσω της προστασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Έως τα μέσα της δεκαετίας του 1970, η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης εξέδωσε διάφορες αποφάσεις σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, παραπέμποντας στο άρθρο 8 της ΕΣΔΑ²⁰. Το 1981 άνοιξε προς υπογραφή η Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα (Σύμβαση 108)²¹. Η Σύμβαση 108 ήταν, και παραμένει, η μόνη νομικά δεσμευτική διεθνής πράξη στον τομέα της προστασίας δεδομένων.

Η Σύμβαση 108 εφαρμόζεται σε κάθε επεξεργασία δεδομένων η οποία εκτελείται τόσο από τον ιδιωτικό, όσο και από τον δημόσιο τομέα, συμπεριλαμβανομένης της επεξεργασίας δεδομένων από τις δικαστικές αρχές και τις αρχές επιβολής του νόμου. Προστατεύει τα πρόσωπα από τις καταχρήσεις οι οποίες ενδέχεται να συνοδεύουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και αποσκοπεί, ταυτόχρονα, στη ρύθμιση των διασυννοριακών ροών αυτών των δεδομένων. Όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι προβλεπόμενες στη Σύμβαση αρχές αφορούν, ιδίως, τη δίκαιη και νόμιμη συλλογή και αυτοματοποιημένη επεξεργασία, για συγκεκριμένους, θεμιτούς σκοπούς. Αυτό σημαίνει ότι τα δεδομένα δεν θα πρέπει να χρησιμοποιούνται για την επιδίωξη στόχων οι οποίοι δεν συνάδουν με τους σκοπούς αυτούς και δεν θα πρέπει να διατηρούνται για διάστημα μεγαλύτερο από το αναγκαίο. Οι αρχές αφορούν επίσης την ποιότητα των δεδομένων και ιδίως την ανάγκη να είναι κατάλληλα, συναφή και όχι υπερβολικά (αναλογικότητα), καθώς και ακριβή.

19 Βλ., για παράδειγμα: ΕΔΔΑ, *Ι κατά Φινλανδίας*, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008· ΕΔΔΑ, *Κ.Ι. κατά Φινλανδίας*, προσφυγή αριθ. 2872/02, 2 Δεκεμβρίου 2008.

20 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1973), Ψήφισμα (73) 22 για την προστασία της ιδιωτικής ζωής των φυσικών προσώπων έναντι των τραπεζών ηλεκτρονικών δεδομένων στον ιδιωτικό τομέα, 26 Σεπτεμβρίου 1973· Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1974), Ψήφισμα (74) 29 για την προστασία της ιδιωτικής ζωής των φυσικών προσώπων έναντι των τραπεζών ηλεκτρονικών δεδομένων στο δημόσιο τομέα, 20 Σεπτεμβρίου 1974.

21 Συμβούλιο της Ευρώπης, Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα, CETS αριθ. 108, 1981.

Επιπροσθέτως της παροχής εγγυήσεων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα και των υποχρεώσεων σε ό,τι αφορά την ασφάλεια των δεδομένων, η Σύμβαση απαγορεύει, απουσία κατάλληλων νομικών εγγυήσεων, την επεξεργασία «ευαίσθητων» δεδομένων –όπως αυτών που αναφέρονται στη φυλή, στις πολιτικές πεποιθήσεις, στην υγεία, στη θρησκεία, στη σεξουαλική ζωή ή στο ποινικό μητρώο ενός προσώπου.

Η Σύμβαση κατοχυρώνει επίσης το δικαίωμα του προσώπου να γνωρίζει ότι έχουν αποθηκευτεί πληροφορίες που το αφορούν και, εφόσον είναι αναγκαίο, να ζητεί τη διόρθωσή τους. Περιορισμοί των δικαιωμάτων που κατοχυρώνονται στη Σύμβαση μπορούν να τεθούν μόνον όταν διακυβεύεται υπέρτερο συμφέρον, όπως η εθνική ασφάλεια ή η εθνική άμυνα. Επιπλέον, η Σύμβαση προβλέπει την ελεύθερη ροή δεδομένων προσωπικού χαρακτήρα μεταξύ των συμβαλλόμενων μερών και επιβάλλει ορισμένους περιορισμούς στις ροές σε κράτη στα οποία η νομική ρύθμιση δεν προβλέπει ισοδύναμη προστασία.

Θα πρέπει να επισημανθεί ότι η Σύμβαση 108 είναι δεσμευτική για τα κράτη που την έχουν κυρώσει. Δεν υπόκειται στον δικαστικό έλεγχο του ΕΔΔΑ, αλλά έχει ληφθεί υπόψη στη νομολογία του ΕΔΔΑ στο πλαίσιο του άρθρου 8 της ΕΣΔΑ. Με την πάροδο των ετών, το ΕΔΔΑ έχει αποφανθεί ότι η προστασία των δεδομένων προσωπικού χαρακτήρα είναι μια σημαντική πτυχή του δικαιώματος στον σεβασμό της ιδιωτικής ζωής (άρθρο 8) και έχει χρησιμοποιήσει ως οδηγό τις αρχές της Σύμβασης 108 σε περιπτώσεις που έχει κληθεί να προσδιορίσει αν υπάρχει ή όχι επέμβαση στο θεμελιώδες αυτό δικαίωμα ²².

Για την περαιτέρω ανάπτυξη των γενικών αρχών και κανόνων που προβλέπονται στη Σύμβαση 108, η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης έχει εκδώσει αρκετές συστάσεις, οι οποίες δεν έχουν νομικά δεσμευτικό χαρακτήρα. Οι συστάσεις αυτές επηρέασαν την ανάπτυξη του δικαίου για την προστασία των δεδομένων στην Ευρώπη. Για παράδειγμα, επί σειρά ετών η μόνη πράξη στην Ευρώπη η οποία παρείχε καθοδήγηση σχετικά με τη χρήση των δεδομένων προσωπικού χαρακτήρα από την αστυνομία ήταν η σύσταση για την αστυνομία ²³. Οι αρχές που περιέχονται στη σύσταση, όπως οι τρόποι διατήρησης αρχείων δεδομένων και η αναγκαιότητα εφαρμογής σαφών κανόνων σχετικά με τα πρόσωπα που δικαιούνται πρόσβαση στα εν λόγω αρχεία, αναπτύχθηκαν περαιτέρω

22 Βλ., για παράδειγμα: ΕΔΔΑ, *Z κατά Φινλανδίας*, προσφυγή αριθ. 22009/93, 25 Φεβρουαρίου 1997.

23 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1987), Σύσταση Rec (87)15 προς τα κράτη μέλη για τη ρύθμιση της χρήσης δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα, Στρασβούργο, 17 Σεπτεμβρίου 1987.

και αντικατοπτρίζονται στην επακόλουθη νομοθεσία της ΕΕ ²⁴. Πιο πρόσφατες συστάσεις επιδιώκουν να αντιμετωπίσουν τις προκλήσεις της ψηφιακής εποχής –για παράδειγμα, θέματα που έχουν σχέση με την επεξεργασία δεδομένων στο πλαίσιο της απασχόλησης (βλ. κεφάλαιο 9).

Όλα τα κράτη μέλη της ΕΕ έχουν κυρώσει τη Σύμβαση 108. Το 1999 προτάθηκαν τροποποιήσεις της Σύμβασης 108 προκειμένου να μπορέσει η ΕΕ να γίνει συμβαλλόμενο μέρος της, αλλά ποτέ δεν τέθηκαν σε ισχύ ²⁵. Το 2001 εκδόθηκε πρόσθετο πρωτόκολλο στη Σύμβαση 108, το οποίο εισάγει διατάξεις σχετικά με τη διασυνοριακή ροή δεδομένων σε μη συμβαλλόμενα μέρη (δηλαδή στις αποκαλούμενες τρίτες χώρες) και με την υποχρεωτική σύσταση εθνικών εποπτικών αρχών προστασίας των δεδομένων ²⁶.

Η Σύμβαση 108 είναι ανοιχτή για προσχώρηση μη συμβαλλόμενων μερών του Συμβουλίου της Ευρώπης. Η δυνατότητα της Σύμβασης να αποτελέσει οικουμενικό πρότυπο, σε συνδυασμό με τον ανοιχτό χαρακτήρα της, αποτελεί τη βάση για την προαγωγή της προστασίας των δεδομένων σε παγκόσμιο επίπεδο. Έως σήμερα, 51 χώρες είναι συμβαλλόμενα μέρη στη Σύμβαση 108. Σε αυτά περιλαμβάνονται όλα τα κράτη μέλη του Συμβουλίου της Ευρώπης (47 χώρες)· η Ουρουγουάη, η πρώτη χώρα εκτός Ευρώπης η οποία προσχώρησε τον Αύγουστο του 2013· και ο Μαυρίκιος, η Σενεγάλη και η Τυνησία, χώρες οι οποίες προσχώρησαν το 2016 και το 2017.

Η Σύμβαση υποβλήθηκε πρόσφατα σε διαδικασία **εκσυγχρονισμού**. Δημόσια διαβούλευση η οποία διενεργήθηκε το 2011 επιβεβαίωσε τους δύο κύριους στόχους του έργου αυτού: ενίσχυση της προστασίας της ιδιωτικής ζωής στον ψηφιακό χώρο και ενδυνάμωση του μηχανισμού παρακολούθησης της Σύμβασης. Η διαδικασία εκσυγχρονισμού επικεντρώθηκε στους στόχους αυτούς και ολοκληρώθηκε με την υιοθέτηση ενός πρωτοκόλλου που τροποποιεί τη Σύμβαση 108

24 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 281 της 23.11.1995, σ. 31).

25 Συμβούλιο της Ευρώπης, Τροποποιήσεις στη Σύμβαση για την προστασία των προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα (CETS αριθ. 108) που υιοθετήθηκαν από την Επιτροπή Υπουργών, στο Στρασβούργο, στις 15 Ιουνίου 1999.

26 Συμβούλιο της Ευρώπης, Πρόσθετο Πρωτόκολλο στη Σύμβαση για την προστασία των προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχετικά με τις εποπτικές αρχές και τη διασυνοριακή ροή δεδομένων, CETS αριθ. 181, 2001. Με τον εκσυγχρονισμό της Σύμβασης 108, το Πρωτόκολλο αυτό δεν εφαρμόζεται πλέον, καθώς οι διατάξεις του επικαιροποιήθηκαν και ενσωματώθηκαν στην Εκσυγχρονισμένη Σύμβαση 108.

(Πρωτόκολλο CETS αριθ. 223). Ο εκσυγχρονισμός πραγματοποιήθηκε παράλληλα με άλλες μεταρρυθμίσεις διεθνών πράξεων για την προστασία δεδομένων και μαζί με τη μεταρρύθμιση των κανόνων της ΕΕ περί προστασίας δεδομένων, η οποία δρομολογήθηκε το 2012. Οι ρυθμιστικοί φορείς σε επίπεδο Συμβουλίου της Ευρώπης και σε επίπεδο ΕΕ επέδειξαν τη μέγιστη δυνατή προσοχή προκειμένου να διασφαλιστεί η συνεκτικότητα και συμβατότητα μεταξύ των δύο νομικών πλαισίων. Η διαδικασία εκσυγχρονισμού διαφυλάσσει τον γενικό και ευέλικτο χαρακτήρα της Σύμβασης και ενισχύει τη δυνατότητα να καταστεί η εν λόγω Σύμβαση οικουμενική πράξη του δικαίου για την προστασία των δεδομένων. Επιβεβαιώνει εκ νέου και παγιώνει σημαντικές αρχές, προβλέπει νέα δικαιώματα για τα φυσικά πρόσωπα, ενώ ταυτόχρονα αυξάνει τις ευθύνες των οντοτήτων που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα και διασφαλίζει μεγαλύτερη λογοδοσία. Για παράδειγμα, φυσικά πρόσωπα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία δικαιούνται να λαμβάνουν γνώση του σκεπτικού της επεξεργασίας και να αντιταχθούν σε αυτή. Για την αντιμετώπιση της αυξημένης χρήσης της κατάρτισης προφίλ στον διαδικτυακό χώρο, η Σύμβαση θεσπίζει επίσης το δικαίωμα του φυσικού προσώπου να μην υπόκειται σε αποφάσεις μόνο βάσει αυτοματοποιημένης επεξεργασίας, χωρίς να έχουν ληφθεί υπόψη οι απόψεις του. Η αποτελεσματική επιβολή των κανόνων περί προστασίας δεδομένων από ανεξάρτητες εποπτικές αρχές στα Συμβαλλόμενα Μέρη θεωρείται καθοριστικής σημασίας για την πρακτική εφαρμογή της Σύμβασης. Για τον σκοπό αυτόν, στην Εκσυγχρονισμένη Σύμβαση υπογραμμίζεται η αναγκαιότητα να ανατεθούν στις εποπτικές αρχές ουσιαστικές εξουσίες και καθήκοντα και να διαθέτουν οι εν λόγω αρχές ανεξαρτησία κατά την εκπλήρωση της αποστολής τους.

1.1.5. Το δίκαιο της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων

Το δίκαιο της ΕΕ περιλαμβάνει το πρωτογενές και το παράγωγο δίκαιο της ΕΕ. Οι Συνθήκες, και ειδικότερα η [Συνθήκη για την Ευρωπαϊκή Ένωση \(ΣΕΕ\)](#) και η Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), έχουν κυρωθεί από όλα τα κράτη μέλη της· αποτελούν το «πρωτογενές δίκαιο της ΕΕ». Οι κανονισμοί, οι οδηγίες και οι αποφάσεις της ΕΕ εκδόθηκαν από τα θεσμικά της όργανα στα οποία έχει δοθεί σχετική εξουσία βάσει των Συνθηκών· αποτελούν το «παράγωγο δίκαιο της ΕΕ».

Η προστασία δεδομένων στο πρωτογενές δίκαιο της ΕΕ

Οι αρχικές Συνθήκες των Ευρωπαϊκών Κοινοτήτων δεν περιείχαν καμία μνεία στα ανθρώπινα δικαιώματα ή στην προστασία τους, δεδομένου ότι η Ευρωπαϊκή Οικονομική Κοινότητα είχε αρχικά σχεδιαστεί ως περιφερειακός οργανισμός επικεντρωμένος στην οικονομική ολοκλήρωση και στην εγκαθίδρυση κοινής αγοράς. Θεμελιώδης αρχή στην οποία βασίζεται η δημιουργία και η ανάπτυξη των Ευρωπαϊκών Κοινοτήτων –και η οποία εξακολουθεί να ισχύει σήμερα– είναι η αρχή της δοτής αρμοδιότητας. Σύμφωνα με την αρχή αυτή, η ΕΕ ενεργεί μόνο εντός των ορίων των αρμοδιοτήτων που της αναθέτουν τα κράτη μέλη, όπως προβλέπεται στις Συνθήκες της. Εν αντιθέσει προς ό,τι συμβαίνει με το Συμβούλιο της Ευρώπης, οι Συνθήκες της ΕΕ δεν προβλέπουν καμία ρητή αρμοδιότητα σε θέματα θεμελιωδών δικαιωμάτων.

Οστόσο, δεδομένου ότι το ΔΕΕ κλήθηκε να επιληφθεί υποθέσεων εικαζόμενης παραβίασης των ανθρωπίνων δικαιωμάτων σε τομείς που εμπίπτουν στο πεδίο εφαρμογής του δικαίου της ΕΕ, το ΔΕΕ παρείχε σημαντική ερμηνεία των Συνθηκών. Προκειμένου να παράσχει προστασία στα φυσικά πρόσωπα, το ΔΕΕ ενέταξε τα θεμελιώδη δικαιώματα στις λεγόμενες γενικές αρχές του ευρωπαϊκού δικαίου. Κατά το ΔΕΕ, οι γενικές αυτές αρχές αντικατοπτρίζουν το περιεχόμενο της προστασίας των ανθρωπίνων δικαιωμάτων που προβλέπεται στα εθνικά συντάγματα και στις συμβάσεις για τα ανθρώπινα δικαιώματα, και ιδίως στην ΕΣΔΑ. Το ΔΕΕ διευκρίνισε ότι θα διασφαλίσει τη συμμόρφωση του δικαίου της ΕΕ με τις αρχές αυτές.

Αναγνωρίζοντας ότι οι πολιτικές της μπορούν να έχουν αντίκτυπο στα ανθρώπινα δικαιώματα και σε μια προσπάθεια να αισθανθούν οι πολίτες εγγύτερα στην ΕΕ, το 2000 η ΕΕ προέβη στη διακήρυξη του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (εφεξής Χάρτης). Ο Χάρτης ενσωματώνει ολόκληρο το φάσμα των ατομικών, πολιτικών, οικονομικών και κοινωνικών δικαιωμάτων των ευρωπαίων πολιτών, σε μια σύνθεση των κοινών συνταγματικών παραδόσεων και διεθνών υποχρεώσεων των κρατών μελών. Τα δικαιώματα που περιγράφονται στον Χάρτη υποδιαιρούνται σε έξι κατηγορίες: αξιοπρέπεια, ελευθερίες, ισότητα, αλληλεγγύη, δικαιώματα των πολιτών και δικαιοσύνη.

Αν και αρχικά ήταν μόνο ένα πολιτικό κείμενο, ο Χάρτης κατέστη νομικά δεσμευτικός ²⁷ ως πρωτογενές δίκαιο της ΕΕ (βλ. άρθρο 6 παράγραφος 1 της

²⁷ ΕΕ (2012), Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (ΕΕ C 326 της 26.10.2012, σ. 391).

ΣΕΕ) όταν η Συνθήκη της Λισαβόνας τέθηκε σε ισχύ την 1η Δεκεμβρίου 2009²⁸. Οι διατάξεις του Χάρτη απευθύνονται στα θεσμικά όργανα και στους οργανισμούς της ΕΕ και τους υποχρεώνουν να σέβονται τα δικαιώματα που απαριθμούνται σε αυτόν κατά την άσκηση των καθηκόντων τους. Οι διατάξεις του δεσμεύουν επίσης τα κράτη μέλη όταν εφαρμόζουν το δίκαιο της ΕΕ.

Ο Χάρτης όχι μόνον εγγυάται τον σεβασμό της ιδιωτικής και οικογενειακής ζωής (άρθρο 7), αλλά θεσπίζει επίσης το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα (άρθρο 8). Ο Χάρτης αναβάθμισε ρητώς το επίπεδο της προστασίας αυτής, ώστε το εν λόγω δικαίωμα να αναγνωρίζεται ως θεμελιώδες δικαίωμα βάσει του ενωσιακού δικαίου. Τα θεσμικά όργανα και οι οργανισμοί της ΕΕ οφείλουν να εγγυώνται και να σέβονται το δικαίωμα αυτό, όπως και τα κράτη μέλη όταν εφαρμόζουν το δίκαιο της Ένωσης (άρθρο 51 του Χάρτη). Το άρθρο 8 του Χάρτη, το οποίο διατυπώθηκε αρκετά χρόνια μετά την Οδηγία για την Προστασία Δεδομένων, πρέπει να θεωρείται ότι ενσωματώνει το προϊσχύσαν δίκαιο της ΕΕ για την προστασία των δεδομένων. Επομένως, ο Χάρτης όχι μόνον αναφέρει το δικαίωμα στην προστασία των δεδομένων στο άρθρο 8 παράγραφος 1, αλλά παραπέμπει επίσης σε βασικές αρχές προστασίας των δεδομένων στο άρθρο 8 παράγραφος 2. Τέλος, το άρθρο 8 παράγραφος 3 του Χάρτη απαιτεί την ύπαρξη ανεξάρτητης αρχής, η οποία ελέγχει την εφαρμογή των αρχών αυτών.

Η έγκριση της Συνθήκης της Λισαβόνας αποτελεί ορόσημο στην ανάπτυξη του δικαίου για την προστασία των δεδομένων, όχι μόνο επειδή αναβάθμισε τον Χάρτη προσδίδοντάς του καθεστώς νομικά δεσμευτικής πράξης στο επίπεδο του πρωτογενούς δικαίου, αλλά επίσης επειδή προέβλεψε το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Το δικαίωμα αυτό προβλέπεται ειδικώς στο άρθρο 16 της ΣΛΕΕ, στο μέρος της Συνθήκης που αφορά τις γενικές αρχές της ΕΕ. Το άρθρο 16 δημιουργεί επίσης νέα νομική βάση, η οποία παρέχει στην ΕΕ την αρμοδιότητα να νομοθετεί σε θέματα προστασίας δεδομένων. Αυτή είναι μια σημαντική εξέλιξη, επειδή οι κανόνες της ΕΕ περί προστασίας δεδομένων –ιδίως η Οδηγία για την Προστασία Δεδομένων– βασιζόνταν αρχικά στη νομική βάση για την εσωτερική αγορά και στην αναγκαιότητα προσέγγισης των εθνικών νομοθεσιών, ώστε να μην εμποδίζεται η ελεύθερη κυκλοφορία των δεδομένων εντός της ΕΕ. Το άρθρο 16 της ΣΛΕΕ παρέχει πλέον αυτοτελή νομική βάση για μια σύγχρονη, συνολική προσέγγιση της προστασίας δεδομένων, η οποία καλύπτει όλα τα θέματα αρμοδιότητας της ΕΕ, συμπεριλαμβανομένης

28 Βλ. ενοποιημένες αποδόσεις για: Ευρωπαϊκές Κοινότητες (2012), Συνθήκη για την Ευρωπαϊκή Ένωση (ΕΕ C 326 της 26.10.2012, σ. 1) και Ευρωπαϊκές Κοινότητες (2012), ΣΛΕΕ (ΕΕ C 326 της 26.10.2012, σ. 1).

της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. Στο άρθρο 16 της ΣΛΕΕ διευκρινίζεται επίσης ότι η τήρηση των κανόνων περί προστασίας δεδομένων που εκδίδονται βάσει του εν λόγω άρθρου πρέπει να υπόκειται στον έλεγχο ανεξάρτητων εποπτικών αρχών. Το άρθρο 16 αποτέλεσε τη νομική βάση για την έγκριση της συνολικής μεταρρύθμισης των κανόνων περί προστασίας δεδομένων το 2016, δηλαδή του Γενικού Κανονισμού για την Προστασία Δεδομένων και της οδηγίας για την προστασία δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης (βλ. κατωτέρω).

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων

Από το 1995 έως τον Μάιο του 2018 η κύρια νομική πράξη της ΕΕ σχετικά με την προστασία των δεδομένων ήταν η οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Οδηγία για την Προστασία Δεδομένων)²⁹. Η οδηγία εκδόθηκε το 1995, σε μια εποχή κατά την οποία αρκετά κράτη μέλη είχαν ήδη θεσπίσει εθνική νομοθεσία για την προστασία των δεδομένων³⁰, και ανέκυψε από την ανάγκη για εναρμόνιση των νομοθεσιών αυτών, ώστε να διασφαλίζεται υψηλό επίπεδο προστασίας και ελεύθερη ροή των δεδομένων προσωπικού χαρακτήρα μεταξύ των διαφόρων κρατών μελών. Η ελεύθερη κυκλοφορία των εμπορευμάτων, των κεφαλαίων, των υπηρεσιών και των προσώπων στην εσωτερική αγορά απαιτούσε ελεύθερη ροή των δεδομένων, η οποία μπορούσε να επιτευχθεί μόνον εάν τα κράτη μέλη μπορούσαν να στηρίζονται σε ομοιόμορφο υψηλό επίπεδο προστασίας των δεδομένων.

Η Οδηγία για την Προστασία Δεδομένων αντικατόπτριζε τις αρχές προστασίας των δεδομένων που ήδη περιείχονταν σε εθνικές νομοθεσίες και στη Σύμβαση 108, τις οποίες σε πολλές περιπτώσεις επέκτεινε. Αξιοποίησε τη δυνατότητα, η οποία προβλέπεται στο άρθρο 11 της Σύμβασης 108, περί προσθήκης μέσω προστασίας. Ειδικότερα, η θέσπιση στην οδηγία της ανεξάρτητης

29 Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 281 της 23.11.1995, σ. 31).

30 Το γερμανικό κρατίδιο της Έσης εξέδωσε τον πρώτο παγκοσμίως νόμο για την προστασία των δεδομένων το 1970, ο οποίος ίσχυε μόνο στο συγκεκριμένο κρατίδιο. Η Σουηδία εξέδωσε τον Datalagen το 1973· η Γερμανία εξέδωσε τον Bundesdatenschutzgesetz το 1976· και η Γαλλία εξέδωσε τον Loi relatif à l'informatique, aux fichiers et aux libertés το 1977. Στο Ηνωμένο Βασίλειο, ο Data Protection Act (νόμος περί προστασίας δεδομένων) εκδόθηκε το 1984. Τέλος, οι Κάτω Χώρες εξέδωσαν τον Wet Persoonregistraties το 1989.

εποπτείας ως μέσου για τη βελτίωση της τήρησης των κανόνων περί προστασίας δεδομένων αποδείχθηκε ότι είχε σημαντική συμβολή στην αποτελεσματική λειτουργία του ευρωπαϊκού δικαίου για την προστασία των δεδομένων. Επομένως, το χαρακτηριστικό αυτό ενσωματώθηκε στο δίκαιο του Συμβουλίου της Ευρώπης το 2001 με το πρόσθετο πρωτόκολλο στη Σύμβαση 108. Αυτό καταδεικνύει τη στενή αλληλεπίδραση και τη θετική επίδραση που είχε η μία πράξη στην άλλη με την πάροδο του χρόνου.

Η Οδηγία για την Προστασία Δεδομένων θέσπισε ένα ολοκληρωμένο και περιεκτικό σύστημα προστασίας των δεδομένων στην ΕΕ. Ωστόσο, σύμφωνα με το νομικό σύστημα της ΕΕ, οι οδηγίες δεν ισχύουν άμεσα και πρέπει να μεταφέρονται στην εθνική έννομη τάξη των κρατών μελών. Αναπόφευκτα, τα κράτη μέλη διαθέτουν περιθώριο διακριτικής ευχέρειας κατά τη μεταφορά των διατάξεων της οδηγίας. Παρότι η οδηγία απέβλεπε στην πλήρη εναρμόνιση³¹ (και σε ένα ύψιστο επίπεδο προστασίας), στην πράξη μεταφέρθηκε με διαφορετικό κάθε φορά τρόπο στην έννομη τάξη των κρατών μελών. Αυτό είχε ως αποτέλεσμα τη θέσπιση διαφορετικών κανόνων περί προστασίας των δεδομένων ανά την ΕΕ, με ορισμούς και κανόνες που ερμηνεύτηκαν διαφορετικά στις εθνικές νομοθεσίες. Τα επίπεδα επιβολής της νομοθεσίας και η βαρύτητα των κυρώσεων διέφεραν επίσης μεταξύ των κρατών μελών. Τέλος, από την κατάρτιση της οδηγίας στα μέσα της δεκαετίας του 1990, συντελέστηκαν σημαντικές αλλαγές στην τεχνολογία των πληροφοριών. Όλοι αυτοί οι λόγοι υπαγόρευσαν τη μεταρρύθμιση της νομοθεσίας της ΕΕ για την προστασία των δεδομένων.

Η μεταρρύθμιση είχε ως αποτέλεσμα την έκδοση του Γενικού Κανονισμού για την Προστασία Δεδομένων τον Απρίλιο του 2016, ύστερα από πολυετείς εντατικές συζητήσεις. Οι συζητήσεις σχετικά με την αναγκαιότητα εκσυγχρονισμού των κανόνων της ΕΕ περί προστασίας των δεδομένων ξεκίνησαν το 2009, όταν η Επιτροπή δρομολόγησε δημόσια διαβούλευση σχετικά με το μελλοντικό νομικό πλαίσιο για το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα. Η Επιτροπή δημοσίευσε την πρόταση κανονισμού τον Ιανουάριο του 2012, δρομολογώντας μια μακρά νομοθετική διαδικασία διαπραγματεύσεων μεταξύ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ. Μετά την έκδοσή του, ο Γενικός Κανονισμός για την Προστασία Δεδομένων προέβλεπε διετή μεταβατική περίοδο. Ο κανονισμός κατέστη πλήρως εφαρμοστέος στις 25 Μαΐου 2018, οπότε καταργήθηκε η Οδηγία για την Προστασία Δεδομένων.

31 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEDM) κατά Administración del Estado*, 24 Νοεμβρίου 2011, σκέψη 29.

Η έκδοση του Γενικού Κανονισμού για την Προστασία Δεδομένων το 2016 εκσυγχρόνισε τη νομοθεσία της ΕΕ για την προστασία δεδομένων, καθιστώντας την κατάλληλη για την προστασία των θεμελιωδών δικαιωμάτων στο πλαίσιο των οικονομικών και κοινωνικών προκλήσεων της ψηφιακής εποχής. Ο ΓΚΠΔ διαφυλάσσει και αναπτύσσει τις βασικές αρχές και τα δικαιώματα του υποκειμένου των δεδομένων που προβλέπονται στην Οδηγία για την Προστασία Δεδομένων. Επιπλέον, θέσπισε νέες υποχρεώσεις για τους οργανισμούς, οι οποίοι οφείλουν να εφαρμόζουν προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού· να διορίζουν υπεύθυνο προστασίας δεδομένων σε ορισμένες περιπτώσεις· να σέβονται το νέο δικαίωμα φορητότητας των δεδομένων· και να σέβονται την αρχή της λογοδοσίας. Βάσει του δικαίου της ΕΕ, οι κανονισμοί ισχύουν άμεσα· δεν απαιτούνται μέτρα μεταφοράς τους στην εθνική έννομη τάξη. Επομένως, ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει ενιαίο σύνολο κανόνων περί προστασίας δεδομένων σε ολόκληρη την ΕΕ. Με τον τρόπο αυτόν δημιουργούνται συνεκτικοί κανόνες περί προστασίας δεδομένων σε ολόκληρη την ΕΕ, θεσπίζοντας ένα περιβάλλον ασφάλειας δικαίου από το οποίο μπορούν να επωφεληθούν οι οικονομικοί φορείς και τα φυσικά πρόσωπα ως «υποκείμενα των δεδομένων».

Ωστόσο, παρότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων ισχύει άμεσα, τα κράτη μέλη θα πρέπει να επικαιροποιήσουν το ισχύον εθνικό τους δίκαιο για την προστασία των δεδομένων, ώστε να ευθυγραμμίζεται πλήρως με τον κανονισμό, αντικατοπτρίζοντας παράλληλα την ύπαρξη περιθωρίου διακριτικής ευχέρειας για τις ειδικότερες διατάξεις που μνημονεύονται στην αιτιολογική σκέψη 10. Οι κύριοι κανόνες και αρχές που θεσπίζονται στον κανονισμό, καθώς και τα ισχυρά δικαιώματα τα οποία αυτός παρέχει στα φυσικά πρόσωπα, καλύπτουν μεγάλο μέρος του παρόντος εγχειριδίου και παρουσιάζονται στα κεφάλαια που ακολουθούν. Ο κανονισμός προβλέπει συνολικούς κανόνες σχετικά με το εδαφικό πεδίο εφαρμογής. Εφαρμόζεται σε επιχειρήσεις εγκατεστημένες στην ΕΕ, καθώς επίσης και σε υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία μη εγκατεστημένους στην ΕΕ οι οποίοι παρέχουν αγαθά ή υπηρεσίες σε υποκείμενα των δεδομένων στην ΕΕ ή παρακολουθούν τη συμπεριφορά τους. Δεδομένου ότι αρκετές αλλοδαπές επιχειρήσεις στον τομέα της τεχνολογίας κατέχουν κρίσιμο μερίδιο στην ευρωπαϊκή αγορά και έχουν εκατομμύρια πελάτες στην ΕΕ, η υπαγωγή των οργανισμών αυτών στους κανόνες της ΕΕ περί προστασίας των δεδομένων είναι ιδιαίτερης σημασίας προκειμένου να διασφαλίζονται, αφενός, η προστασία των φυσικών προσώπων και, αφετέρου, ισότιμοι όροι ανταγωνισμού.

Η προστασία των δεδομένων στην επιβολή του νόμου – οδηγία 2016/680

Η καταργηθείσα Οδηγία για την Προστασία Δεδομένων προέβλεπε συνολικό καθεστώς προστασίας των δεδομένων. Το καθεστώς αυτό έχει πλέον ενισχυθεί περαιτέρω με την έκδοση του Γενικού Κανονισμού για την Προστασία Δεδομένων. Παρότι συνολικό, το πεδίο εφαρμογής της καταργηθείσας οδηγίας περιοριζόταν στις δραστηριότητες που ενέπιπταν στην εσωτερική αγορά, και στις δραστηριότητες των δημόσιων αρχών, πλην των αρχών επιβολής του νόμου. Επομένως, ήταν αναγκαία η θέσπιση ειδικών πράξεων για την επίτευξη της αναγκαίας σαφήνειας και ισορροπίας μεταξύ της προστασίας των δεδομένων και άλλων θεμιτών συμφερόντων, καθώς και για την αντιμετώπιση προκλήσεων που έχουν αυξημένη παρουσία σε συγκεκριμένους τομείς. Αυτό συμβαίνει στην περίπτωση των κανόνων που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρχές επιβολής του νόμου.

Η πρώτη νομική πράξη της ΕΕ η οποία ρύθμιζε το θέμα αυτό ήταν η απόφαση-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου για την προστασία των δεδομένων προσωπικού χαρακτήρα που τυγχάνουν επεξεργασίας στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας σε ποινικές υποθέσεις. Οι κανόνες της εφαρμόζονταν μόνο σε αστυνομικά και δικαστικά δεδομένα όταν αυτά ανταλλάσσονταν μεταξύ κρατών μελών. Η εγχώρια προστασία δεδομένων προσωπικού χαρακτήρα από τις αρχές επιβολής του νόμου εξαιρέθηκε από το πεδίο εφαρμογής της.

Η οδηγία 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών ³², γνωστή ως οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, κάλυψε το κενό αυτό. Η οδηγία εκδόθηκε παράλληλα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, κατάργησε την απόφαση-πλαίσιο 2008/977/ΔΕΥ και θέσπισε συνολικό σύστημα προστασίας των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της επιβολής του νόμου, αναγνωρίζοντας επίσης τις ιδιαιτερότητες

32 Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 119 της 4.5.2016, σ. 89).

της επεξεργασίας δεδομένων σχετικών με τη δημόσια ασφάλεια. Ενώ ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει γενικούς κανόνες για την προστασία των φυσικών προσώπων σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν και για τη διασφάλιση της ελεύθερης κυκλοφορίας των εν λόγω δεδομένων στην ΕΕ, η οδηγία θεσπίζει γενικούς κανόνες για την προστασία των δεδομένων στους τομείς της δικαστικής συνεργασίας σε ποινικές υποθέσεις και της αστυνομικής συνεργασίας. Όταν μια αρμόδια αρχή επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων, θα εφαρμόζεται η οδηγία 2016/680. Όταν οι αρμόδιες αρχές επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για άλλους σκοπούς πλην των προαναφερθέντων, θα εφαρμόζεται το γενικό καθεστώς που προβλέπεται στον Γενικό Κανονισμό για την Προστασία Δεδομένων. Εν αντιθέσει προς την προγενέστερη πράξη (απόφαση-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου), το πεδίο εφαρμογής της οδηγίας 2016/680 εκτείνεται στην εγχώρια επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρχές επιβολής του νόμου και δεν περιορίζεται στις ανταλλαγές των εν λόγω δεδομένων μεταξύ κρατών μελών. Επιπλέον, σκοπός της οδηγίας είναι να επιτύχει ισορροπία μεταξύ των δικαιωμάτων των φυσικών προσώπων και των θεμιτών σκοπών της σχετιζόμενης με την ασφάλεια επεξεργασίας.

Για τον σκοπό αυτόν, η οδηγία αναγνωρίζει το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα και τις βασικές αρχές οι οποίες θα πρέπει να διέπουν την επεξεργασία δεδομένων, εφαρμόζοντας προσεκτικά τους κανόνες και τις αρχές που κατοχυρώνονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων. Τα δικαιώματα των φυσικών προσώπων και οι υποχρεώσεις που προβλέπονται για τους υπευθύνους επεξεργασίας δεδομένων –για παράδειγμα, σε σχέση με την ασφάλεια των δεδομένων, την προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού και τις γνωστοποιήσεις παραβίασης δεδομένων– είναι παρόμοια με τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων. Η οδηγία λαμβάνει επίσης υπόψη και προσπαθεί να αντιμετωπίσει τις σοβαρές τεχνολογικές προκλήσεις που ανακύπτουν και οι οποίες μπορούν να έχουν ιδιαίτερα επαχθή αντίκτυπο στα φυσικά πρόσωπα, όπως τη χρήση τεχνικών κατάρτισης προφίλ από τις αρχές επιβολής του νόμου. Καταρχήν, αποφάσεις οι οποίες βασίζονται αποκλειστικά και μόνο σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, πρέπει να απαγορεύονται³³. Επιπλέον, οι αποφάσεις δεν

33 Οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, άρθρο 11 παράγραφος 1.

πρέπει να βασίζονται σε ευαίσθητα δεδομένα. Οι αρχές αυτές υπόκεινται σε ορισμένες εξαιρέσεις, οι οποίες προβλέπονται στην οδηγία. Επιπλέον, η εν λόγω επεξεργασία δεν πρέπει να έχει ως αποτέλεσμα διακρίσεις εις βάρος οποιουδήποτε προσώπου ³⁴.

Η οδηγία περιέχει επίσης κανόνες ώστε να διασφαλίζεται η λογοδοσία των υπευθύνων επεξεργασίας. Αυτοί πρέπει να ορίζουν υπεύθυνο προστασίας δεδομένων ο οποίος θα παρακολουθεί τη συμμόρφωση προς τους κανόνες περί προστασίας δεδομένων, θα ενημερώνει και θα συμβουλεύει την οντότητα και τους υπαλλήλους που εκτελούν την επεξεργασία σχετικά με τις υποχρεώσεις τους και θα συνεργάζεται με την εποπτική αρχή. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα της αστυνομίας και της ποινικής δικαιοσύνης υπόκειται πλέον στην εποπτεία ανεξάρτητων αρχών. Τόσο το γενικό νομικό καθεστώς περί προστασίας δεδομένων, όσο και το ειδικό καθεστώς περί προστασίας δεδομένων σε ό,τι αφορά την επιβολή του νόμου και ποινικές υποθέσεις πρέπει να συμμορφώνονται επίσης προς τις απαιτήσεις του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Το ειδικό καθεστώς για την επεξεργασία δεδομένων στο πλαίσιο της αστυνομικής και δικαστικής συνεργασίας, το οποίο θεσπίστηκε με την οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, περιγράφεται αναλυτικά στο [κεφάλαιο 8](#).

Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Η θέσπιση ειδικών κανόνων περί προστασίας δεδομένων κρίθηκε επίσης αναγκαία στον τομέα των ηλεκτρονικών επικοινωνιών. Με την ανάπτυξη του διαδικτύου και της σταθερής και κινητής τηλεφωνίας, ήταν σημαντικό να διασφαλιστεί ο σεβασμός των δικαιωμάτων των χρηστών στην ιδιωτική ζωή και στην εμπιστευτικότητα. Η οδηγία 2002/58/ΕΚ ³⁵ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες ή οδηγία e-Privacy) καθορίζει κανόνες για την ασφάλεια των δεδομένων προσωπικού χαρακτήρα στα δίκτυα αυτά, τη

³⁴ Ό.π., άρθρο 11 παράγραφοι 2 και 3.

³⁵ Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (ΕΕ L 201 της 31.7.2002, σ. 37) (οδηγία e-Privacy).

γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα και την εμπιστευτικότητα των επικοινωνιών.

Σε σχέση με την ασφάλεια, οι φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλουν, μεταξύ άλλων, να διασφαλίζουν ότι η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα επιτρέπεται μόνο σε εξουσιοδοτημένα πρόσωπα και να λαμβάνουν μέτρα για την πρόληψη της καταστροφής ή της απώλειας δεδομένων προσωπικού χαρακτήρα ή της τυχαίας πρόκλησης ζημίας σε αυτά ³⁶. Όταν υφίσταται ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δημόσιου δικτύου επικοινωνιών, οι φορείς παροχής υπηρεσιών οφείλουν να ενημερώνουν τους συνδρομητές σχετικά με τον κίνδυνο ³⁷. Εάν, παρά τη λήψη μέτρων ασφάλειας, υπάρξει παραβίαση της ασφάλειας, οι φορείς οφείλουν να ενημερώσουν την εθνική αρχή που είναι επιφορτισμένη με την εφαρμογή και την επιβολή της οδηγίας για την παραβίαση των δεδομένων προσωπικού χαρακτήρα. Ενίοτε οι φορείς υποχρεούνται επίσης να ενημερώνουν τα φυσικά πρόσωπα για παραβιάσεις των δεδομένων προσωπικού χαρακτήρα, ιδίως όταν η παραβίαση είναι πιθανό να επηρεάσει αρνητικά τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν ή την ιδιωτική ζωή τους ³⁸. Η εμπιστευτικότητα των επικοινωνιών απαιτεί την απαγόρευση, καταρχήν, της ακρόασης, της υποκλοπής, της αποθήκευσης ή άλλου είδους παρακολούθησης ή επιτήρησης των επικοινωνιών και των μεταδομένων. Η οδηγία απαγορεύει επίσης τα ανεπίκλητα ηλεκτρονικά μηνύματα (γνωστά και ως «spam»), εκτός εάν οι χρήστες έχουν δώσει τη συγκατάθεσή τους, και προβλέπει κανόνες για την αποθήκευση «cookies» σε ηλεκτρονικούς υπολογιστές και συσκευές. Οι βασικές αυτές αρνητικές υποχρεώσεις υποδεικνύουν σαφώς ότι η εμπιστευτικότητα των επικοινωνιών συνδέεται ρητώς με την προστασία του δικαιώματος στον σεβασμό της ιδιωτικής ζωής, το οποίο κατοχυρώνεται στο άρθρο 7 του Χάρτη, και του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, το οποίο κατοχυρώνεται στο άρθρο 8 του Χάρτη.

Τον Ιανουάριο του 2017 η Επιτροπή δημοσίευσε πρόταση κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες, ο οποίος προορίζεται να αντικαταστήσει την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές

36 Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, άρθρο 4 παράγραφος 1.

37 Ό.π., άρθρο 4 παράγραφος 2.

38 Ό.π., άρθρο 4 παράγραφος 3.

επικοινωνίες. Στόχος της μεταρρύθμισης είναι η ευθυγράμμιση των κανόνων που διέπουν τις ηλεκτρονικές επικοινωνίες με το νέο καθεστώς προστασίας δεδομένων το οποίο θεσπίστηκε με τον Γενικό Κανονισμό για την Προστασία Δεδομένων. Ο νέος κανονισμός θα ισχύει άμεσα σε ολόκληρη την ΕΕ- όλα τα φυσικά πρόσωπα θα απολαύουν του ίδιου επιπέδου προστασίας των ηλεκτρονικών επικοινωνιών τους, ενώ οι φορείς τηλεπικοινωνιών και οι επιχειρήσεις θα ωφεληθούν από τη σαφήνεια, την ασφάλεια δικαίου και την ύπαρξη ενιαίου συνόλου κανόνων ανά την ΕΕ. Οι προτεινόμενοι κανόνες περί της εμπιστευτικότητας των ηλεκτρονικών επικοινωνιών θα ισχύουν επίσης για τους νέους φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, οι οποίοι δεν καλύπτονται από την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Η οδηγία κάλυπτε μόνο τους παραδοσιακούς φορείς παροχής υπηρεσιών τηλεπικοινωνιών. Με τη μαζική διάδοση της χρήσης υπηρεσιών όπως Skype, WhatsApp, Facebook Messenger και Viber για την αποστολή μηνυμάτων ή την πραγματοποίηση κλήσεων, αυτές οι επιφυείς (over-the-top, OTT) υπηρεσίες θα εμπίπτουν πλέον στο πεδίο εφαρμογής του κανονισμού και θα πρέπει να συμμορφώνονται προς τις απαιτήσεις του όσον αφορά την προστασία, την ιδιωτικότητα και την ασφάλεια των δεδομένων. Κατά τον χρόνο δημοσίευσης του παρόντος εγχειριδίου, η νομοθετική διαδικασία σχετικά με τους κανόνες για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες βρισκόταν ακόμη σε εξέλιξη.

Κανονισμός αριθ. 45/2001

Καθώς η Οδηγία για την Προστασία Δεδομένων μπορούσε να εφαρμοστεί μόνο στα κράτη μέλη της ΕΕ, απαιτήθηκε πρόσθετη νομική πράξη για την καθιέρωση της προστασίας των δεδομένων στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από θεσμικά όργανα και οργανισμούς της ΕΕ. Το κενό αυτό συμπληρώνει ο κανονισμός (ΕΚ) αριθ. 45/2001 σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (κανονισμός για την προστασία δεδομένων από τα όργανα της ΕΕ)³⁹.

Ο κανονισμός αριθ. 45/2001 λαμβάνει υπόψη τις αρχές του γενικού καθεστώτος για την προστασία των δεδομένων στην ΕΕ και εφαρμόζει τις εν λόγω αρχές στην

³⁹ Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

επεξεργασία δεδομένων την οποία εκτελούν τα θεσμικά όργανα και οι οργανισμοί της ΕΕ κατά την άσκηση των δραστηριοτήτων τους. Επιπλέον, ο κανονισμός προβλέπει τη σύσταση ανεξάρτητης εποπτικής αρχής για την παρακολούθηση της εφαρμογής των διατάξεών του, τον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ). Στον ΕΕΠΔ ανατίθενται εποπτικές εξουσίες και το καθήκον να παρακολουθεί την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα και τους οργανισμούς της ΕΕ, καθώς και να εξετάζει και να διερευνά καταγγελίες για εικαζόμενες παραβάσεις των κανόνων περί προστασίας δεδομένων. Ο ΕΕΠΔ παρέχει επίσης συμβουλές στα θεσμικά όργανα και στους οργανισμούς της ΕΕ σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα, οι οποίες εκτείνονται από προτάσεις για νέα νομοθεσία έως την κατάρτιση εσωτερικών κανόνων όσον αφορά την επεξεργασία δεδομένων.

Τον Ιανουάριο του 2017 η Ευρωπαϊκή Επιτροπή παρουσίασε πρόταση νέου κανονισμού για την επεξεργασία δεδομένων από τα θεσμικά όργανα της ΕΕ, ο οποίος θα καταργήσει τον ισχύοντα. Όπως και η μεταρρύθμιση της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, η μεταρρύθμιση του κανονισμού αριθ. 45/2001 θα εκσυγχρονίσει και θα ευθυγραμμίσει τους κανόνες του με το νέο καθεστώς για την προστασία δεδομένων το οποίο θεσπίστηκε με τον Γενικό Κανονισμό για την Προστασία Δεδομένων.

Ο ρόλος του ΔΕΕ

Το ΔΕΕ είναι αρμόδιο να κρίνει αν ένα κράτος μέλος έχει εκπληρώσει τις υποχρεώσεις που υπέχει βάσει του δικαίου της ΕΕ για την προστασία των δεδομένων και να ερμηνεύει τη νομοθεσία της ΕΕ προκειμένου να διασφαλίζεται η αποτελεσματική και ομοιόμορφη εφαρμογή της σε όλα τα κράτη μέλη. Από την έκδοση της Οδηγίας για την Προστασία Δεδομένων το 1995, έχει συσσωρευτεί σημαντικός όγκος νομολογίας, στην οποία αποσαφηνίζονται το πεδίο εφαρμογής και η έννοια των αρχών της προστασίας δεδομένων, καθώς και του θεμελιώδους δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, όπως κατοχυρώνεται στο άρθρο 8 του Χάρτη. Παρότι η οδηγία καταργήθηκε και πλέον ισχύει νέα νομική πράξη, ο Γενικός Κανονισμός για την Προστασία Δεδομένων, η προϋφιστάμενη αυτή νομολογία παραμένει λυσιτελής και έγκυρη για την ερμηνεία και την εφαρμογή των αρχών της ΕΕ περί προστασίας δεδομένων, στο μέτρο που οι βασικές αρχές και έννοιες της Οδηγίας για την Προστασία Δεδομένων διατηρήθηκαν στον ΓΚΠΔ.

1.2. Περιορισμοί του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα

Κύρια σημεία

- Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο· μπορεί να περιοριστεί, εάν αυτό είναι αναγκαίο για στόχους γενικού συμφέροντος ή για την προστασία των δικαιωμάτων και των ελευθεριών των τρίτων.
- Οι προϋποθέσεις περιορισμού των δικαιωμάτων στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα απαριθμούνται στο άρθρο 8 της ΕΣΔΑ και στο άρθρο 52 παράγραφος 1 του Χάρτη. Έχουν αναπτυχθεί και αποτελέσει αντικείμενο ερμηνείας μέσω της νομολογίας του ΕΔΔΑ και του ΔΕΕ.
- Βάσει του δικαίου του Συμβουλίου της Ευρώπης για την προστασία των δεδομένων, η επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστά νόμιμη επέμβαση στο δικαίωμα στον σεβασμό της ιδιωτικής ζωής και μπορεί να πραγματοποιηθεί μόνο εάν:
 - προβλέπεται από τον νόμο·
 - επιδιώκει θεμιτό σκοπό·
 - σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών·
 - είναι αναγκαία και ανάλογη σε μια δημοκρατική κοινωνία για την επίτευξη θεμιτού σκοπού.
- Στην έννομη τάξη της ΕΕ προβλέπονται παρόμοιες προϋποθέσεις για τους περιορισμούς της άσκησης των θεμελιωδών δικαιωμάτων που προστατεύονται από τον Χάρτη. Κάθε περιορισμός οποιουδήποτε θεμελιώδους δικαιώματος, συμπεριλαμβανομένης της προστασίας των δεδομένων προσωπικού χαρακτήρα, μπορεί να είναι νόμιμος μόνο εάν:
 - προβλέπεται από τον νόμο·
 - σέβεται την ουσία του δικαιώματος·
 - είναι αναγκαίος, τηρουμένης της αρχής της αναλογικότητας, και
 - επιδιώκει στόχο γενικού συμφέροντος που αναγνωρίζει η ΕΕ ή ανταποκρίνεται στην ανάγκη προστασίας των δικαιωμάτων των τρίτων.

Το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα βάσει του άρθρου 8 του Χάρτη δεν είναι απόλυτο δικαίωμα, «αλλά πρέπει να λαμβάνεται υπόψη σε σχέση με τον ρόλο που επιτελεί στην κοινωνία»⁴⁰. Επομένως, στο άρθρο 52 παράγραφος 1 του Χάρτη αναγνωρίζεται ότι επιτρέπεται η επιβολή περιορισμών στην άσκηση δικαιωμάτων, όπως των δικαιωμάτων που προβλέπονται στα άρθρα 7 και 8 του Χάρτη, υπό την προϋπόθεση ότι οι περιορισμοί αυτοί προβλέπονται από τον νόμο, σέβονται την ουσία των εν λόγω δικαιωμάτων και ελευθεριών και, τηρουμένης της αρχής της αναλογικότητας, είναι αναγκαίοι και ανταποκρίνονται πραγματικά σε στόχους γενικού συμφέροντος που αναγνωρίζει η ΕΕ ή στην ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων⁴¹. Ομοίως, στο σύστημα της ΕΣΔΑ, η προστασία των δεδομένων κατοχυρώνεται στο άρθρο 8 και η άσκηση του δικαιώματος αυτού μπορεί να περιορίζεται όταν είναι αναγκαίο για την επιδίωξη θεμιτού σκοπού. Στην παρούσα ενότητα εξετάζονται οι προϋποθέσεις επέμβασης βάσει της ΕΣΔΑ, όπως ερμηνεύονται από τη νομολογία του ΕΔΔΑ, καθώς και οι προϋποθέσεις νόμιμων περιορισμών βάσει του άρθρου 52 του Χάρτη.

1.2.1. Προϋποθέσεις δικαιολογημένης επέμβασης βάσει της ΕΣΔΑ

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να συνιστά επέμβαση στο δικαίωμα του υποκειμένου των δεδομένων στον σεβασμό της ιδιωτικής ζωής του, το οποίο κατοχυρώνεται στο άρθρο 8 της ΕΣΔΑ⁴². Όπως εξηγείται ανωτέρω (βλ. [ενότητα 1.1.1](#) και [ενότητα 1.1.4.](#)), εν αντιθέσει προς ό,τι ισχύει στην έννομη τάξη της ΕΕ, η ΕΣΔΑ δεν προβλέπει την προστασία των δεδομένων προσωπικού χαρακτήρα ως διακριτό θεμελιώδες δικαίωμα. Αντιθέτως, η προστασία των δεδομένων προσωπικού χαρακτήρα εντάσσεται στην προστασία του δικαιώματος στον σεβασμό της ιδιωτικής ζωής. Επομένως, δεν θα μπορούσε να εμπίπτει στο πεδίο εφαρμογής του άρθρου 8 της ΕΣΔΑ κάθε πράξη που περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Για την ενεργοποίηση του άρθρου 8, πρέπει πρώτα να διαπιστωθεί αν θίγεται ιδιωτικό συμφέρον ή η ιδιωτική ζωή ενός προσώπου. Μέσω της νομολογίας του, το ΕΔΔΑ έχει αντιμετωπίσει

40 Βλ., για παράδειγμα, ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, *Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen* [τμήμα μείζονος συνθέσεως], 9 Νοεμβρίου 2010, σκέψη 48.

41 Ό.π., σκέψη 50.

42 ΕΔΔΑ, *S. και Marper κατά Ηνωμένου Βασιλείου* [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008, σκέψη 67.

την έννοια της «ιδιωτικής ζωής» ως ευρεία έννοια που καλύπτει ακόμη και πτυχές της επαγγελματικής ζωής και της δημόσιας συμπεριφοράς. Το ΕΔΔΑ αποφάνθηκε επίσης ότι η προστασία των δεδομένων προσωπικού χαρακτήρα αποτελεί σημαντικό μέρος του δικαιώματος στον σεβασμό της ιδιωτικής ζωής. Ωστόσο, παρά την ευρεία ερμηνεία της έννοιας της ιδιωτικής ζωής, δεν θίγουν όλα τα είδη επεξεργασίας, από μόνα τους, τα δικαιώματα που κατοχυρώνονται δυνάμει του άρθρου 8.

Όταν το ΕΔΔΑ εκτιμά ότι η επίμαχη πράξη επεξεργασίας θίγει το δικαίωμα των φυσικών προσώπων στον σεβασμό της ιδιωτικής ζωής, εξετάζει κατά πόσον η επέμβαση είναι δικαιολογημένη. Το δικαίωμα στον σεβασμό της ιδιωτικής ζωής δεν είναι απόλυτο, αλλά πρέπει να εξισορροπείται και να συμβιβάζεται με άλλα θεμιτά συμφέροντα και δικαιώματα, είτε αυτά αφορούν άλλα πρόσωπα (ιδιωτικά συμφέροντα) είτε αφορούν την κοινωνία στο σύνολό της (δημόσια συμφέροντα).

Οι προϋποθέσεις οι οποίες πρέπει να συντρέχουν σωρευτικά προκειμένου να δικαιολογείται η επέμβαση είναι οι εξής:

Η επέμβαση πρέπει να προβλέπεται από τον νόμο

Σύμφωνα με τη νομολογία του ΕΔΔΑ, η επέμβαση προβλέπεται από τον νόμο εάν βασίζεται σε διάταξη του εθνικού δικαίου η οποία έχει ορισμένες ιδιότητες. Ο νόμος πρέπει να είναι «προσβάσιμος σε όλους τους ενδιαφερομένους και προβλέψιμος ως προς τις συνέπειές του»⁴³. Ένας κανόνας είναι προβλέψιμος «εάν διατυπώνεται με επαρκή ακρίβεια ώστε να παρέχει τη δυνατότητα σε κάθε φυσικό πρόσωπο –εν ανάγκη, με τη συνδρομή διαφωτιστικών συμβουλών– να ρυθμίσει τη συμπεριφορά του»⁴⁴. Επιπλέον, «[ο] βαθμός ακρίβειας που απαιτείται συναφώς από τον “νόμο” θα εξαρτάται από το συγκεκριμένο θέμα»⁴⁵.

43 ΕΔΔΑ, *Amann κατά Ελβετίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000, σκέψη 50· βλ. επίσης ΕΔΔΑ, *Korpp κατά Ελβετίας*, προσφυγή αριθ. 23224/94, 25 Μαρτίου 1998, σκέψη 55 και ΕΔΔΑ, *lordachi κ.λπ. κατά Μολδαβίας*, προσφυγή αριθ. 25198/02, 10 Φεβρουαρίου 2009, σκέψη 50.

44 ΕΔΔΑ, *Amann κατά Ελβετίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000, σκέψη 56· βλ. επίσης ΕΔΔΑ, *Malone κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 8691/79, 2 Αυγούστου 1984, σκέψη 66· ΕΔΔΑ, *Silver κ.λπ. κατά Ηνωμένου Βασιλείου*, προσφυγές αριθ. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Μαρτίου 1983, σκέψη 88.

45 ΕΔΔΑ, *The Sunday Times κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 6538/74, 26 Απριλίου 1979, σκέψη 49· βλ. επίσης, *Silver κ.λπ. κατά Ηνωμένου Βασιλείου*, προσφυγές αριθ. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Μαρτίου 1983, σκέψη 88.

Παραδείγματα: Στην υπόθεση *Rotaru κατά Ρουμανίας*⁴⁶, ο προσφεύγων ισχυρίστηκε ότι υπήρξε παραβίαση του δικαιώματός του στον σεβασμό της ιδιωτικής ζωής του, επειδή η ρουμανική υπηρεσία πληροφοριών κατείχε και χρησιμοποιούσε φάκελο ο οποίος περιείχε πληροφορίες προσωπικού χαρακτήρα που τον αφορούσαν. Το ΕΔΔΑ διαπίστωσε ότι, παρότι το εθνικό δίκαιο επέτρεπε τη συλλογή, την καταγραφή και την αρχειοθέτηση σε μυστικούς φακέλους πληροφοριών που αφορούν την εθνική ασφάλεια, δεν προέβλεπε κανέναν περιορισμό στην άσκηση των εν λόγω εξουσιών, η οποία παρέμενε στη διακριτική ευχέρεια των αρχών. Για παράδειγμα, η εθνική νομοθεσία δεν όριζε το είδος των πληροφοριών που μπορούσαν να υποβληθούν σε επεξεργασία, τις κατηγορίες προσώπων κατά των οποίων μπορούσαν να ληφθούν μέτρα παρακολούθησης, τις περιστάσεις υπό τις οποίες μπορούσαν να ληφθούν τέτοια μέτρα ή τις διαδικασίες που έπρεπε να ακολουθούνται. Επομένως, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι η εθνική νομοθεσία δεν ήταν σύμφωνη προς την απαίτηση της προβλεψιμότητας βάσει του άρθρου 8 της ΕΣΔΑ και ότι παραβιάστηκε το εν λόγω άρθρο.

Στην υπόθεση *Taylor-Sabori κατά Ηνωμένου Βασιλείου*⁴⁷, ο προσφεύγων είχε αποτελέσει στόχο αστυνομικής παρακολούθησης. Χρησιμοποιώντας έναν «κλώνο» της συσκευής τηλειδιοποίησης του προσφεύγοντος, η αστυνομία ήταν σε θέση να υποκλέπτει τα εισερχόμενα μηνύματά του. Στη συνέχεια, ο προσφεύγων συνελήφθη και του απαγγέθηκαν κατηγορίες για συμμετοχή σε οργάνωση με σκοπό την προμήθεια ελεγχόμενης ναρκωτικής ουσίας. Το κατηγορητήριο βασιζόταν εν μέρει στα γραπτά μηνύματα του συστήματος τηλειδιοποίησης που είχαν απομαγνητοφωνηθεί από την αστυνομία κατά το ίδιο χρονικό διάστημα. Ωστόσο, κατά τον χρόνο της δίκης του προσφεύγοντος δεν υπήρχε στο βρετανικό δίκαιο διάταξη η οποία να διέπει την παρακολούθηση των επικοινωνιών που μεταδίδονται μέσω ιδιωτικού τηλεπικοινωνιακού συστήματος. Ως εκ τούτου, η παρέμβαση στα δικαιώματά του δεν ήταν «σύμφωνη με τον νόμο». Το ΕΔΔΑ αποφάνθηκε ότι παραβιάστηκε το άρθρο 8 ΕΣΔΑ.

46 ΕΔΔΑ, *Rotaru κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000, σκέψη 57· βλ. επίσης ΕΔΔΑ, *Association for European Integration and Human Rights και Ekinidzhiev κατά Βουλγαρίας*, προσφυγή αριθ. 62540/00, 28 Ιουνίου 2007· ΕΔΔΑ, *Shimovolos κατά Ρωσίας*, προσφυγή αριθ. 30194/09, 21 Ιουνίου 2011· και ΕΔΔΑ, *Vetter κατά Γαλλίας*, προσφυγή αριθ. 59842/00, 31 Μαΐου 2005.

47 ΕΔΔΑ, *Taylor-Sabori κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 47114/99, 22 Οκτωβρίου 2002.

Η υπόθεση *Vukota-Bojić κατά Ελβετίας*⁴⁸ αφορούσε μυστική παρακολούθηση μιας δικαιούχου παροχών κοινωνικής ασφάλισης από πράκτορες ιδιωτικών ερευνών τους οποίους προσέλαβε η ασφαλιστική εταιρεία της. Το ΕΔΔΑ αποφάνθηκε ότι, παρότι το επίμαχο στην προσφυγή μέτρο παρακολούθησης είχε διαταχθεί από ιδιωτική ασφαλιστική εταιρεία, η εν λόγω εταιρεία είχε εξουσιοδοτηθεί από το κράτος να χορηγεί παροχές οι οποίες προέκυπταν από υποχρεωτική ασφάλιση υγείας και να εισπράττει ασφάλιστρα. Το κράτος δεν μπορούσε να απεκδυθεί την ευθύνη που υπέχει βάσει της ΕΣΔΑ αναθέτοντας τις υποχρεώσεις του σε ιδιωτικούς φορείς ή φυσικά πρόσωπα. Η εθνική νομοθεσία έπρεπε να παρέχει επαρκείς εγγυήσεις κατά της κατάχρησης προκειμένου να «προβλέπεται από τον νόμο» η επέμβαση στα δικαιώματα βάσει του άρθρου 8 της ΕΣΔΑ. Στη συγκεκριμένη υπόθεση, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ, επειδή η εθνική νομοθεσία δεν υποδείκνυε με επαρκή σαφήνεια το πεδίο εφαρμογής και τον τρόπο άσκησης της διακριτικής ευχέρειας που αναγνωρίζεται στις ασφαλιστικές εταιρείες οι οποίες ενεργούν ως δημόσιες αρχές σε ασφαλιστικές διαφορές να διενεργούν μυστική παρακολούθηση ασφαλισμένων. Ειδικότερα, η νομοθεσία δεν περιλάμβανε επαρκείς εγγυήσεις κατά της κατάχρησης.

Η επέμβαση πρέπει να επιδιώκει θεμιτό σκοπό

Ο θεμιτός σκοπός μπορεί να είναι είτε ένα από τα αναφερόμενα δημόσια συμφέροντα είτε η προστασία των δικαιωμάτων και των ελευθεριών των τρίτων. Βάσει του άρθρου 8 παράγραφος 2 της ΕΣΔΑ, θεμιτοί σκοποί οι οποίοι θα μπορούσαν να δικαιολογούν επέμβαση είναι τα συμφέροντα της εθνικής ασφάλειας, της δημόσιας ασφάλειας ή της οικονομικής ευημερίας της χώρας, η προάσπιση της τάξης και η πρόληψη ποινικών παραβάσεων, η προστασία της υγείας ή της ηθικής και η προστασία των δικαιωμάτων και των ελευθεριών τρίτων.

Παράδειγμα: Στην υπόθεση *Peck κατά Ηνωμένου Βασιλείου*⁴⁹, ο προσφεύγων αποπειράθηκε να αυτοκτονήσει στον δρόμο κόβοντας τις φλέβες των καρπών του, μη γνωρίζοντας ότι μια κάμερα κλειστού κυκλώματος τηλεόρασης τον βιντεοσκοπούσε. Η αστυνομία, η οποία παρατηρούσε τις

48 ΕΔΔΑ, *Vukota-Bojić κατά Ελβετίας*, προσφυγή αριθ. 61838/10, 18 Οκτωβρίου 2016, σκέψη 77.

49 ΕΔΔΑ, *Peck κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 44647/98, 28 Ιανουαρίου 2003, σκέψη 85.

κάμερες της τηλεόρασης κλειστού κυκλώματος, τον έσωσε και ακολούθως διαβίβασε το υλικό που κατέγραψε η τηλεόραση κλειστού κυκλώματος στα μέσα ενημέρωσης, τα οποία το δημοσίευσαν χωρίς να αποκρύψουν το πρόσωπο του προσφεύγοντος. Το ΕΔΔΑ έκρινε ότι δεν υπήρχαν συναφείς ή επαρκείς λόγοι οι οποίοι δικαιολογούσαν την άμεση δημοσιοποίηση του υλικού από τις αρχές χωρίς τη συγκατάθεση του προσφεύγοντος ή την απόκρυψη της ταυτότητάς του. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Η επέμβαση να είναι αναγκαία σε μια δημοκρατική κοινωνία

Κατά το ΕΔΔΑ, «η έννοια της αναγκαιότητας σημαίνει ότι η επέμβαση ανταποκρίνεται σε επείγουσα κοινωνική ανάγκη και, ιδίως, ότι είναι ανάλογη προς τον επιδιωκόμενο θεμιτό σκοπό»⁵⁰. Όταν εκτιμά κατά πόσον ένα μέτρο είναι αναγκαίο για την αντιμετώπιση επείγουσας κοινωνικής ανάγκης, το ΕΔΔΑ εξετάζει αν αυτό είναι συναφές και κατάλληλο σε σχέση με τον επιδιωκόμενο σκοπό. Για τον σκοπό αυτόν, το ΕΔΔΑ μπορεί να εκτιμήσει κατά πόσον η επέμβαση επιχειρεί να αντιμετωπίσει ζήτημα το οποίο, εάν δεν αντιμετωπιστεί, θα μπορούσε να έχει επιζήμιες συνέπειες για την κοινωνία, εάν υπάρχουν στοιχεία που αποδεικνύουν ότι η επέμβαση αυτή μπορεί να μετριάσει τις εν λόγω επιζήμιες συνέπειες και ποιες είναι γενικά οι απόψεις της κοινωνίας επί του επίμαχου ζητήματος⁵¹. Για παράδειγμα, η συλλογή και η αποθήκευση δεδομένων προσωπικού χαρακτήρα από υπηρεσίες ασφάλειας για συγκεκριμένα φυσικά πρόσωπα τα οποία διαπιστώνεται ότι συνδέονται με τρομοκρατικά κινήματα συνιστούν επέμβαση στο δικαίωμα των φυσικών προσώπων στον σεβασμό της ιδιωτικής ζωής, η οποία εξυπηρετεί, παρ' όλα αυτά, σοβαρή, επείγουσα κοινωνική ανάγκη: την εθνική ασφάλεια και την καταπολέμηση της τρομοκρατίας. Προκειμένου να ανταποκρίνεται στο κριτήριο της αναγκαιότητας, η επέμβαση πρέπει επίσης να είναι ανάλογη. Στη νομολογία του ΕΔΔΑ, η αναλογικότητα εξετάζεται στο πλαίσιο της έννοιας της αναγκαιότητας. Η αναλογικότητα απαιτεί η επέμβαση στα δικαιώματα που προστατεύονται από την ΕΣΔΑ να μην υπερβαίνει το μέτρο που είναι αναγκαίο για την εκπλήρωση του επιδιωκόμενου θεμιτού σκοπού. Σημαντικοί παράγοντες οι οποίοι πρέπει να λαμβάνονται υπόψη κατά την εφαρμογή του

50 ΕΔΔΑ, *Leander κατά Σουηδίας*, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987, σκέψη 58.

51 Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (Ομάδα εργασίας του άρθρου 29) (2014), *Γνώμη σχετικά με την εφαρμογή των εννοιών της αναγκαιότητας και της αναλογικότητας και την προστασία των δεδομένων στον τομέα της επιβολής της νομοθεσίας*, WP 211, Βρυξέλλες, 27 Φεβρουαρίου 2014, σ. 7-8.

κριτηρίου της αναλογικότητας είναι η έκταση της επέμβασης, ιδίως το πλήθος των θιγόμενων προσώπων, και οι εγγυήσεις ή προειδοποιήσεις που έχουν θεσπιστεί για τον περιορισμό της έκτασης ή των επιζήμιων συνεπειών της στα δικαιώματα των φυσικών προσώπων ⁵².

Παράδειγμα: Στην υπόθεση *Khelili κατά Ελβετίας* ⁵³, κατά τη διάρκεια ελέγχου για εξακρίβωση στοιχείων η αστυνομία διαπίστωσε ότι η προσφεύγουσα έφερε πάνω της καρτ βισίτ, στις οποίες αναγράφονταν τα εξής: «Ευγενική, όμορφη γυναίκα, κοντά στα 40, επιθυμεί να γνωρίσει άνδρα για να πουν μαζί ένα ποτό ή για περιστασιακή συντροφιά. Τηλεφωνήστε στο [...]». Η προσφεύγουσα ισχυρίστηκε ότι, μετά την ανακάλυψη αυτή, η αστυνομία την καταχώρισε στα αρχεία της ως «εκδιδόμενη», επάγγελμα το οποίο αυτή αρνήθηκε συστηματικά ότι ασκεί. Η προσφεύγουσα ζήτησε τη διαγραφή της λέξης «εκδιδόμενη» από τα ηλεκτρονικά αρχεία της αστυνομίας. Το ΕΔΔΑ έκανε δεκτό, καταρχήν, ότι η διατήρηση των δεδομένων προσωπικού χαρακτήρα φυσικού προσώπου με την αιτιολογία ότι το εν λόγω πρόσωπο θα μπορούσε να διαπράξει άλλο αδίκημα μπορεί υπό ορισμένες περιστάσεις να συνιστά αναλογικό μέτρο. Ωστόσο, στην περίπτωση της προσφεύγουσας, ο ισχυρισμός περί παράνομης πορνείας φαινόταν υπερβολικά αόριστος και γενικός, δεν υποστηριζόταν από συγκεκριμένα πραγματικά περιστατικά, δεδομένου ότι η προσφεύγουσα δεν είχε ποτέ καταδικαστεί για παράνομη πορνεία και, επομένως, δεν μπορούσε να θεωρηθεί ότι ανταποκρίνεται σε «επιτακτική κοινωνική ανάγκη» κατά την έννοια του άρθρου 8 της ΕΣΔΑ. Εκτιμώντας ότι εναπόκειται στις αρχές να αποδείξουν την ακρίβεια των αποθηκευμένων δεδομένων που αφορούν την προσφεύγουσα και λαμβανομένης υπόψη της σοβαρότητας της επέμβασης στα δικαιώματα της προσφεύγουσας, το ΕΔΔΑ αποφάνθηκε ότι η διατήρηση της λέξης «εκδιδόμενη» στα αστυνομικά αρχεία επί σειρά ετών δεν ήταν αναγκαία σε μια δημοκρατική κοινωνία. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

⁵² Ό.π., σ. 9-11.

⁵³ ΕΔΔΑ, *Khelili κατά Ελβετίας*, προσφυγή αριθ. 16188/07, 18 Οκτωβρίου 2011.

Παράδειγμα: Στην υπόθεση *S. και Marger κατά Ηνωμένου Βασιλείου*⁵⁴, οι δύο προσφεύγοντες συνελήφθησαν και κατηγορήθηκαν για ποινικά αδικήματα. Η αστυνομία έλαβε τα δακτυλικά τους αποτυπώματα και δείγματα DNA, όπως προβλέπεται στον περί Αστυνομίας και Ποινικών Αποδεικτικών Στοιχείων νόμο. Οι προσφεύγοντες δεν καταδικάστηκαν ποτέ για τα αδικήματα: ο πρώτος αθωώθηκε από το δικαστήριο, ενώ η διαδικασία κατά του δεύτερου προσφεύγοντος δεν ολοκληρώθηκε. Παρ' όλα αυτά, τα δακτυλικά αποτυπώματα, το προφίλ DNA και βιολογικό υλικό διατηρήθηκαν και αποθηκεύτηκαν από την αστυνομία σε βάση δεδομένων, και η εθνική νομοθεσία επέτρεπε τη διατήρησή τους χωρίς χρονικούς περιορισμούς. Παρότι το Ηνωμένο Βασίλειο υποστήριξε ότι η διατήρηση βοηθά στην ταυτοποίηση μελλοντικών δραστών αδικημάτων και, επομένως, επιδιώκει τον θεμιτό σκοπό της πρόληψης και της ανίχνευσης του εγκλήματος, το ΕΔΔΑ έκρινε αδικαιολόγητη την επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής των προσφευγόντων. Υπενθύμισε ότι οι βασικές αρχές της προστασίας δεδομένων απαιτούν η διατήρηση των δεδομένων προσωπικού χαρακτήρα να είναι ανάλογη προς τον σκοπό της συλλογής και οι περίοδοι διατήρησης να είναι περιορισμένες. Το ΕΔΔΑ δέχθηκε ότι η επέκταση της βάσης δεδομένων ώστε να περιλαμβάνει προφίλ DNA όχι μόνο καταδικασθέντων προσώπων αλλά και φυσικών προσώπων που θεωρήθηκαν ύποπτα αλλά δεν καταδικάστηκαν μπορεί να συνέβαλε στην ανίχνευση και στην πρόληψη της εγκληματικότητας στο Ηνωμένο Βασίλειο. Ωστόσο, το ΕΔΔΑ «εξεπλάγη από την εξουσία διατήρησης αδιακρίτως όλων των δακτυλικών αποτυπωμάτων, κυτταρικών δειγμάτων και προφίλ DNA»⁵⁵.

Λαμβανομένου υπόψη του πλούτου των γενετικών πληροφοριών και πληροφοριών σχετικά με την υγεία που περιέχονται στα κυτταρικά δείγματα, η επέμβαση στο δικαίωμα στον σεβασμό της ιδιωτικής ζωής των προσφευγόντων ήταν ιδιαίτερα μεγάλη. Τα δακτυλικά αποτυπώματα και τα δείγματα μπορούσαν να λαμβάνονται από συλληφθέντες και να διατηρούνται επ' αόριστον στη βάση δεδομένων της αστυνομίας ανεξάρτητα από τη φύση και τη σοβαρότητα του αδικήματος, ακόμη και για ήσσονος σημασίας αδικήματα τα οποία δεν τιμωρούνται με ποινή φυλάκισης. Επιπλέον, οι δυνατότητες των απαλλαχθέντων προσώπων

54 ΕΔΔΑ, *S. και Marger κατά Ηνωμένου Βασιλείου* [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008.

55 Ό.π., σκέψη 119.

να επιτύχουν την διαγραφή των δεδομένων που τα αφορούσαν από τη βάση δεδομένων ήταν περιορισμένες. Τέλος, το ΕΔΔΑ έλαβε ιδιαίτερα υπόψη το γεγονός ότι ένας εκ των προσφευγόντων ήταν έντεκα ετών όταν συνελήφθη. Η διατήρηση των δεδομένων προσωπικού χαρακτήρα ανηλίκου ο οποίος δεν καταδικάστηκε μπορεί να είναι ιδιαίτερα επιζήμια, λαμβανομένης υπόψη της ευπάθειας των ανηλίκων και της σημασίας της ανάπτυξης και της ένταξής τους στην κοινωνία ⁵⁶. Το ΕΔΔΑ αποφάνθηκε ομόφωνα ότι η διατήρηση συνιστούσε δυσανάλογη επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής, η οποία δεν μπορούσε να θεωρηθεί αναγκαία σε μια δημοκρατική κοινωνία.

Παράδειγμα: Στην υπόθεση *Leander κατά Σουηδίας* ⁵⁷, το ΕΔΔΑ έκρινε ότι η διενέργεια μυστικού ελέγχου σχετικά με πρόσωπα που υπέβαλαν αίτηση για απασχόληση σε σημαντικές θέσεις στην εθνική ασφάλεια δεν αντέβαινε, αυτή καθαυτή, στην απαίτηση της αναγκαιότητας σε μια δημοκρατική κοινωνία. Οι ειδικές εγγυήσεις που θεσπίζονται στην εθνική νομοθεσία για την προστασία των συμφερόντων του υποκειμένου των δεδομένων –για παράδειγμα, έλεγχοι από το Κοινοβούλιο και τον υπουργό Δικαιοσύνης– οδήγησαν το ΕΔΔΑ στο συμπέρασμα ότι το σουηδικό σύστημα ελέγχου του προσωπικού πληρούσε τις προϋποθέσεις του άρθρου 8 παράγραφος 2 της ΕΣΔΑ. Λαμβάνοντας υπόψη το ευρύ περιθώριο εκτίμησης του καθού κράτους, ήταν δικαίωμά του να θεωρήσει ότι, στην περίπτωση του προσφεύγοντος, τα συμφέροντα της εθνικής ασφάλειας υπερίσχυαν των ατομικών συμφερόντων. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι δεν παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

1.2.2. Προϋποθέσεις νόμιμων περιορισμών βάσει του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ

Η δομή και η διατύπωση του Χάρτη διαφέρουν από της ΕΣΔΑ. Ο Χάρτης δεν κάνει λόγο για επεμβάσεις σε κατοχυρωμένα δικαιώματα, πλην όμως περιέχει διάταξη σχετικά με περιορισμούς στην άσκηση των δικαιωμάτων και ελευθεριών που αναγνωρίζονται στον Χάρτη.

⁵⁶ Ό.π., σκέψη 124.

⁵⁷ ΕΔΔΑ, *Leander κατά Σουηδίας*, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987, σκέψεις 59 και 67.

Σύμφωνα με το άρθρο 52 παράγραφος 1, περιορισμοί στην άσκηση των δικαιωμάτων και των ελευθεριών που αναγνωρίζονται στον Χάρτη και, επομένως, στην άσκηση του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα επιτρέπονται μόνο εάν:

- προβλέπονται από τον νόμο και
- σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και
- είναι αναγκαίοι, τηρουμένης της αρχής της αναλογικότητας⁵⁸, και
- εξυπηρετούν στόχους γενικού συμφέροντος που αναγνωρίζει η Ένωση ή την ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων.

Δεδομένου ότι η προστασία των δεδομένων προσωπικού χαρακτήρα είναι διακριτό και αυτοτελές θεμελιώδες δικαίωμα στην έννομη τάξη της ΕΕ, το οποίο κατοχυρώνεται στο άρθρο 8 του Χάρτη, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστά, αυτή καθαυτή, επέμβαση στο εν λόγω δικαίωμα. Είναι αδιάφορο το κατά πόσον τα επίμαχα δεδομένα προσωπικού χαρακτήρα σχετίζονται με την ιδιωτική ζωή του προσώπου ή είναι ευαίσθητα, ή κατά πόσον τα υποκείμενα των δεδομένων ενοχλήθηκαν με οποιονδήποτε τρόπο. Προκειμένου να είναι νόμιμη, η επέμβαση πρέπει να πληροί όλες τις προϋποθέσεις που απαριθμούνται στο άρθρο 52 παράγραφος 1 του Χάρτη.

Ο περιορισμός πρέπει να προβλέπεται από τον νόμο

Οι περιορισμοί του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα πρέπει να προβλέπονται από τον νόμο. Η προϋπόθεση αυτή σημαίνει ότι οι περιορισμοί πρέπει να θεμελιώνονται σε νομική βάση η οποία είναι αρκούντως προσβάσιμη και προβλέψιμη και έχει διατυπωθεί με επαρκή ακρίβεια ώστε να παρέχει στα φυσικά πρόσωπα τη δυνατότητα να κατανοήσουν τις υποχρεώσεις τους και να ρυθμίσουν τη συμπεριφορά τους. Η νομική βάση πρέπει επίσης να ορίζει σαφώς την έκταση και τον τρόπο άσκησης της εξουσίας των αρμόδιων αρχών, ώστε τα φυσικά πρόσωπα να προστατεύονται από τυχόν αυθαίρετη επέμβαση. Η ερμηνεία αυτή ομοιάζει με την προϋπόθεση της «νόμιμης

⁵⁸ Σχετικά με την εκτίμηση της αναγκαιότητας μέτρων που περιορίζουν το θεμελιώδες δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, βλ. ΕΕΠΔ (2017), *Necessity Toolkit*, Βρυξέλλες, 11 Απριλίου 2017.

επέμβασης» που διατυπώνεται στη νομολογία του ΕΔΔΑ ⁵⁹ και έχει υποστηριχθεί ότι η έννοια της έκφρασης «προβλέπεται από τον νόμο», η οποία χρησιμοποιείται στον Χάρτη, θα πρέπει να είναι ίδια με εκείνη που αποδίδεται σε σχέση με την ΕΣΔΑ ⁶⁰. Η νομολογία του ΕΔΔΑ, και ιδίως η έννοια της «ύπαρξης νόμου» την οποία αυτό έχει αναπτύξει με την πάροδο του χρόνου, αποτελεί συναφή παράγοντα τον οποίο πρέπει να λαμβάνει υπόψη το ΔΕΕ κατά την ερμηνεία του πεδίου εφαρμογής του άρθρου 52 παράγραφος 1 του Χάρτη ⁶¹.

Ο περιορισμός πρέπει να σέβεται την ουσία του δικαιώματος

Στην έννομη τάξη της ΕΕ, κάθε περιορισμός των θεμελιωδών δικαιωμάτων που προστατεύονται βάσει του Χάρτη πρέπει να σέβεται την ουσία των εν λόγω δικαιωμάτων. Αυτό σημαίνει ότι περιορισμοί οι οποίοι είναι τόσο εκτενείς και τόσο παρεμβατικοί ώστε να στερούν από ένα θεμελιώδες δικαίωμα την ουσία του δεν μπορούν να δικαιολογηθούν. Εάν θίγεται η ουσία του δικαιώματος, ο περιορισμός πρέπει να θεωρηθεί παράνομος, χωρίς να χρειάζεται να εκτιμηθεί περαιτέρω αν εξυπηρετεί στόχο γενικού συμφέροντος και αν πληροί τα κριτήρια της αναγκαιότητας και της αναλογικότητας.

Παράδειγμα: Η υπόθεση *Schrems* ⁶² αφορούσε την προστασία φυσικών προσώπων σε σχέση με τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα που τα αφορούσαν σε τρίτες χώρες –στην περίπτωση αυτή, στις ΗΠΑ. Ο Μ. Schrems, αυστριακός πολίτης και χρήστης του Facebook επί αρκετά χρόνια, κατέθεσε καταγγελία στην ιρλανδική εποπτική αρχή προστασίας των δεδομένων παραπονούμενος για τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα που τον αφορούσαν από την ιρλανδική θυγατρική εταιρεία της Facebook στη Facebook Inc. και στους εγκατεστημένους στις ΗΠΑ διακομιστές, όπου αυτά υποβλήθηκαν σε επεξεργασία. Υποστήριξε ότι, λαμβανομένων υπόψη των αποκαλύψεων

59 ΕΕΠΑ (2017), *Necessity Toolkit*, Βρυξέλλες, 11 Απριλίου 2017, σ. 4· βλ. επίσης ΔΕΕ, *Γνωμοδότηση 1/15 του Δικαστηρίου* [τμήμα μείζονος συνθέσεως], της 26ης Ιουλίου 2017.

60 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, *Tele2 Sverige AB κατά Post- och telestyrelsen* και *Secretary of State for the Home Department κατά Tom Watson, Peter Brice, Geoffrey Lewis* [τμήμα μείζονος συνθέσεως], προτάσεις του γενικού εισαγγελέα Η. Saugmandsgaard Øe, της 19ης Ιουλίου 2016, σημείο 140.

61 ΔΕΕ, C-70/10, *Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs (SABAM)*, προτάσεις του γενικού εισαγγελέα P. Cruz Villalón, της 14ης Απριλίου 2011, σημείο 100.

62 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015.

που έγιναν το 2013 από τον αμερικανό πληροφοριοδότη Edward Snowden σχετικά με τις δραστηριότητες των υπηρεσιών παρακολούθησης των ΗΠΑ, το δίκαιο και η πρακτική των ΗΠΑ δεν παρείχαν επαρκή προστασία για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονταν στο έδαφός τους. Ο E. Snowden είχε αποκαλύψει ότι η National Security Agency (NSA) παρακολουθούσε απευθείας τους διακομιστές επιχειρήσεων, όπως η Facebook, και μπορούσε να διαβάσει το περιεχόμενο συνομιλιών και ιδιωτικών μηνυμάτων.

Οι διαβιβάσεις δεδομένων στις ΗΠΑ βασιζόνταν σε απόφαση επάρκειας που εκδόθηκε από την Επιτροπή το 2000, η οποία επέτρεπε τις διαβιβάσεις σε αυτοπιστοποιημένες αμερικανικές εταιρείες που βεβαίωναν ότι θα προστάτευαν τα δεδομένα προσωπικού χαρακτήρα τα οποία διαβιβάζονταν από την ΕΕ και θα τηρούσαν τις λεγόμενες «αρχές ασφαλούς λιμένα». Όταν επιλήφθηκε της υπόθεσης, το ΔΕΕ εξέτασε το κύρος της απόφασης της Επιτροπής υπό το πρίσμα του Χάρτη. Το ΔΕΕ υπενθύμισε ότι η προστασία των θεμελιωδών δικαιωμάτων στην ΕΕ απαιτεί οι αποκλίσεις και οι περιορισμοί των εν λόγω δικαιωμάτων να μην υπερβαίνουν τα όρια του απολύτως αναγκαίου. Το ΔΕΕ έκρινε ότι νομοθεσία η οποία επιτρέπει σε δημόσιες αρχές να έχουν πρόσβαση, γενικά, στο περιεχόμενο ηλεκτρονικών επικοινωνιών «προσβάλλει το ουσιαστικό περιεχόμενο του θεμελιώδους δικαιώματος του σεβασμού της ιδιωτικής ζωής, όπως αυτό κατοχυρώνεται από το άρθρο 7 του Χάρτη». Το δικαίωμα αυτό θα καθίστατο κενό περιεχομένου εάν οι αμερικανικές δημόσιες αρχές μπορούσαν να έχουν πρόσβαση σε επικοινωνίες, κατά τρόπο τυχαίο, χωρίς καμία αντικειμενική δικαιολογία στηριζόμενη σε λόγους εθνικής ασφάλειας ή πρόληψης της εγκληματικότητας οι οποίοι να συνδέονται ειδικώς με τα οικεία άτομα, και χωρίς οι εν λόγω πρακτικές παρακολούθησης να συνοδεύονται από κατάλληλες εγγυήσεις κατά της κατάχρησης εξουσίας.

Επιπλέον, το ΔΕΕ επισήμανε ότι «ρύθμιση που δεν προβλέπει ένδικα μέσα προκειμένου ο ενδιαφερόμενος να αποκτήσει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τον αφορούν ή να επιτύχει την τροποποίηση ή την κατάργηση τέτοιων δεδομένων» δεν συνάδει με το θεμελιώδες δικαίωμα σε αποτελεσματική δικαστική προστασία (άρθρο 47 του Χάρτη). Επομένως, η απόφαση για τον ασφαλή λιμένα δεν διασφάλισε επίπεδο

προστασίας των θεμελιωδών δικαιωμάτων από τις ΗΠΑ ουσιαστικά ισοδύναμο με εκείνο που διασφαλίζεται στην ΕΕ βάσει της οδηγίας, υπό το πρίσμα του Χάρτη. Ως εκ τούτου, το ΔΕΕ κήρυξε ανίσχυρη την απόφαση ⁶³.

Παράδειγμα: Στην υπόθεση *Digital Rights Ireland* ⁶⁴, το ΔΕΕ εξέτασε τη συμβατότητα της οδηγίας 2006/24/ΕΚ (οδηγία για τη διατήρηση δεδομένων) με τα άρθρα 7 και 8 του Χάρτη. Η οδηγία υποχρέωνε τους φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν δεδομένα κίνησης και δεδομένα θέσης για τουλάχιστον έξι μήνες και για μέγιστο διάστημα 24 μηνών, καθώς και να επιτρέπουν στις αρμόδιες εθνικές αρχές να έχουν πρόσβαση στα εν λόγω δεδομένα για τον σκοπό της πρόληψης, της διερεύνησης, της διαπίστωσης και της δίωξης σοβαρών εγκλημάτων. Η οδηγία δεν επέτρεπε τη διατήρηση του περιεχομένου των ηλεκτρονικών επικοινωνιών. Το ΔΕΕ επισήμανε ότι τα δεδομένα τα οποία έπρεπε να διατηρούν οι φορείς παροχής των υπηρεσιών βάσει της οδηγίας περιλάμβαναν δεδομένα αναγκαία για την ανίχνευση και τον προσδιορισμό της πηγής και του προορισμού της επικοινωνίας, τον αριθμό τηλεφώνου του καλούντος και τους αριθμούς των καλουμένων, καθώς και τις διευθύνσεις IP. Τα δεδομένα αυτά, «λαμβάνόμενα στο σύνολό τους, παρέχουν τη δυνατότητα συναγωγής ιδιαίτερως ακριβών συμπερασμάτων σε σχέση με την ιδιωτική ζωή των προσώπων των οποίων τα δεδομένα έχουν διατηρηθεί, όπως είναι οι καθημερινές συνήθειες, οι μόνιμοι ή οι προσωρινοί τόποι διαμονής, οι καθημερινές και άλλες μετακινήσεις, οι ασκούμενες δραστηριότητες, οι κοινωνικές σχέσεις των προσώπων αυτών και τα κοινωνικά περιβάλλοντα στα οποία τα πρόσωπα αυτά συχνάζουν».

Επομένως, η διατήρηση δεδομένων προσωπικού χαρακτήρα βάσει της οδηγίας συνιστούσε ιδιαίτερα σοβαρή επέμβαση στα δικαιώματα στην ιδιωτική ζωή και στην προστασία των δεδομένων προσωπικού χαρακτήρα.

63 Η απόφαση του ΔΕΕ να κηρύξει ανίσχυρη την απόφαση 520/2000/ΕΚ της Επιτροπής βασιζόταν και σε πρόσθετους λόγους που θα εξεταστούν σε άλλες ενότητες του παρόντος εγχειριδίου. Ειδικότερα, το ΔΕΕ έκρινε ότι η απόφαση περιόρισε παράνομα τις εξουσίες των εθνικών εποπτικών αρχών προστασίας των δεδομένων. Επιπλέον, βάσει του καθεστώτος του ασφαλούς λιμένα, δεν υπήρχαν διαθέσιμα ένδικο βοηθήματα για τα φυσικά πρόσωπα στην περίπτωση που επιθυμούσαν να έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τα αφορούσαν και/ή να εξασφαλίσουν τη διόρθωση ή τη διαγραφή τους. Επομένως, εθίγη επίσης το ουσιαστικό περιεχόμενο του θεμελιώδους δικαιώματος σε αποτελεσματική δικαστική προστασία, το οποίο κατοχυρώνεται στο άρθρο 47 του Χάρτη.

64 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

Ωστόσο, το ΔΕΕ έκρινε ότι η επέμβαση δεν έθιγε το ουσιαστικό περιεχόμενο των εν λόγω δικαιωμάτων. Όσον αφορά το δικαίωμα στην ιδιωτική ζωή, δεν εθίγη η ουσία του, επειδή η οδηγία δεν επέτρεπε την ανάκτηση του ίδιου του περιεχομένου των ηλεκτρονικών επικοινωνιών. Ομοίως, η ουσία του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν εθίγη, καθώς η οδηγία υποχρέωνε τους φορείς παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών να τηρούν ορισμένες αρχές προστασίας των δεδομένων και ασφάλειας των δεδομένων και να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για τον σκοπό αυτόν.

Αναγκαιότητα και αναλογικότητα

Το άρθρο 52 παράγραφος 1 του Χάρτη προβλέπει ότι, τηρουμένης της αρχής της αναλογικότητας, περιορισμοί στην άσκηση των θεμελιωδών δικαιωμάτων και ελευθεριών που αναγνωρίζει ο Χάρτης επιτρέπεται να επιβάλλονται μόνον εφόσον είναι αναγκαίοι.

Ο περιορισμός μπορεί να είναι **αναγκαίος** εάν υφίσταται ανάγκη λήψης μέτρων για τον επιδιωκόμενο σκοπό δημόσιου συμφέροντος, αλλά η αναγκαιότητα, όπως ερμηνεύεται από το ΔΕΕ, σημαίνει επίσης ότι τα ληφθέντα μέτρα πρέπει να είναι λιγότερο επεμβατικά σε σύγκριση με άλλες εναλλακτικές δυνατότητες για την επίτευξη του ίδιου σκοπού. Για τους περιορισμούς των δικαιωμάτων στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα, το ΔΕΕ εφαρμόζει κριτήριο απόλυτης αναγκαιότητας, έχοντας αποφανθεί ότι οι «αποκλίσεις και οι περιορισμοί δεν πρέπει να υπερβαίνουν τα όρια του απολύτως αναγκαίου». Εφόσον ο περιορισμός κριθεί απολύτως αναγκαίος, πρέπει επίσης να εκτιμηθεί αν είναι ανάλογος.

Αναλογικότητα σημαίνει ότι τα πλεονεκτήματα από τον περιορισμό θα πρέπει να υπερτερούν σε σύγκριση με τα μειονεκτήματα που αυτός συνεπάγεται σε ό,τι αφορά την άσκηση των διακυβευόμενων θεμελιωδών δικαιωμάτων⁶⁵. Για τη μείωση των μειονεκτημάτων και των κινδύνων όσον αφορά την απόλαυση των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων, είναι σημαντικό οι περιορισμοί να εμπεριέχουν κατάλληλες εγγυήσεις.

65 ΕΕΠΔ (2017), *Necessity Toolkit*, σ. 5.

Παράδειγμα: Στην υπόθεση *Volker und Markus Schecke* ⁶⁶, το ΔΕΕ κατέληξε στο συμπέρασμα ότι, με τη θέσπιση της υποχρέωσης δημοσιοποίησης των δεδομένων όλων των προσώπων που είναι δικαιούχοι ενισχύσεων από ορισμένα γεωργικά ταμεία, χωρίς να γίνεται διάκριση ανάλογα με τα σχετικά κριτήρια, όπως οι περίοδοι κατά τις οποίες τα εν λόγω πρόσωπα έλαβαν τη σχετική ενίσχυση, η συχνότητα των ενισχύσεων ή το είδος και το ποσό αυτών, το Συμβούλιο και η Επιτροπή είχαν υπερβεί τα όρια που επιβάλλει η τήρηση της αρχής της αναλογικότητας.

Ως εκ τούτου, το ΔΕΕ έκρινε αναγκαίο να κηρύξει ανίσχυρες ορισμένες διατάξεις του κανονισμού (ΕΚ) αριθ. 1290/2005 του Συμβουλίου και τον κανονισμό αριθ. 259/2008 στο σύνολό του ⁶⁷.

Παράδειγμα: Στην υπόθεση *Digital Rights Ireland* ⁶⁸, το ΔΕΕ αποφάνθηκε ότι η επέμβαση στο δικαίωμα στην ιδιωτική ζωή λόγω της οδηγίας για τη διατήρηση δεδομένων δεν έθιγε την ουσία του εν λόγω δικαιώματος δεδομένου ότι απαγόρευε τη διατήρηση του περιεχομένου των ηλεκτρονικών επικοινωνιών. Ωστόσο, κατέληξε στο συμπέρασμα ότι η οδηγία δεν ήταν συμβατή προς τα άρθρα 7 και 8 του Χάρτη και την κήρυξε ανίσχυρη. Επειδή τα δεδομένα κίνησης και θέσης, λαμβανόμενα στο σύνολό τους, μπορούσαν να αναλυθούν και να αποτυπώσουν λεπτομερή εικόνα της ιδιωτικής ζωής των φυσικών προσώπων, η οδηγία συνιστούσε σοβαρή επέμβαση στα εν λόγω δικαιώματα. Το ΔΕΕ έλαβε υπόψη ότι η οδηγία απαιτούσε τη διατήρηση όλων των μεταδεδομένων που αφορούσαν σταθερή τηλεφωνία, κινητή τηλεφωνία, πρόσβαση στο διαδίκτυο, ηλεκτρονικό ταχυδρομείο και τηλεφωνία μέσω του διαδικτύου και εφαρμοζόταν σε όλα τα μέσα ηλεκτρονικής επικοινωνίας –των οποίων η χρήση είναι ευρύτατα διαδεδομένη στην καθημερινή ζωή των ανθρώπων. Ουσιαστικά, συνεπαγόταν επέμβαση που επηρέαζε το σύνολο

66 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, *Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen* [τμήμα μείζονος συνθέσεως], 9 Νοεμβρίου 2010, σκέψεις 89 και 86.

67 Κανονισμός (ΕΚ) αριθ. 1290/2005 του Συμβουλίου, της 21ης Ιουνίου 2005, για τη χρηματοδότηση της κοινής γεωργικής πολιτικής (ΕΕ L 209 της 11.8.2005, σ. 1)· κανονισμός (ΕΚ) αριθ. 259/2008 της Επιτροπής, της 18ης Μαρτίου 2008, για τη θέσπιση λεπτομερών κανόνων εφαρμογής του κανονισμού (ΕΚ) αριθ. 1290/2005 του Συμβουλίου σχετικά με τη δημοσιοποίηση πληροφοριών για τους δικαιούχους κονδυλίων προερχόμενων από το Ευρωπαϊκό Γεωργικό Ταμείο Εγγυήσεων (ΕΓΤΕ) και το Ευρωπαϊκό Γεωργικό Ταμείο Αγροτικής Ανάπτυξης (ΕΓΤΑΑ) (ΕΕ L 76 της 19.3.2008, σ. 28).

68 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014, σκέψη 39.

του ευρωπαϊκού πληθυσμού. Λαμβανομένων υπόψη της έκτασης και της σοβαρότητας της επέμβασης αυτής, η διατήρηση των δεδομένων κίνησης και θέσης μπορούσε, κατά το ΔΕΕ, να είναι δικαιολογημένη μόνο για τον σκοπό της καταπολέμησης του σοβαρού εγκλήματος. Επιπλέον, η οδηγία δεν προέβλεπε κανένα αντικειμενικό κριτήριο το οποίο θα διασφάλιζε ότι η πρόσβαση των αρμόδιων εθνικών αρχών στα διατηρούμενα δεδομένα θα περιοριζόταν στο απολύτως αναγκαίο μέτρο. Εξάλλου, η οδηγία δεν περιείχε ουσιαστικές και διαδικαστικές προϋποθέσεις που να διέπουν την πρόσβαση στα διατηρούμενα δεδομένα και τη χρήση αυτών από τις εθνικές αρχές, καθώς η πρόσβαση και η χρήση δεν εξαρτιόνταν από προηγούμενο έλεγχο δικαστηρίου ή άλλου ανεξάρτητου οργάνου.

Το ΔΕΕ κατέληξε σε παρόμοιο συμπέρασμα στις συνεκδικασθείσες υποθέσεις *Tele2 Sverige AB κατά Post- och telestyrelsen* και *Secretary of State for the Home Department κατά Tom Watson κ.λπ.*⁶⁹ Οι υποθέσεις αυτές αφορούσαν τη διατήρηση δεδομένων κίνησης και θέσης για «όλους τους συνδρομητές και τους εγγεγραμμένους χρήστες και όλα τα μέσα ηλεκτρονικής επικοινωνίας, καθώς και όλα τα μεταδεδομένα» χωρίς «διαφοροποίηση, περιορισμό ή εξαίρεση σε σχέση προς τον επιδιωκόμενο σκοπό»⁷⁰. Στην περίπτωση αυτή, το κατά πόσον ένα πρόσωπο εμπλεκόταν, άμεσα ή έμμεσα, σε σοβαρά ποινικά αδικήματα ή κατά πόσον οι επικοινωνίες του είχαν σημασία για την εθνική ασφάλεια δεν αποτελούσε προϋπόθεση για τη διατήρηση των δεδομένων του. Λαμβανομένης υπόψη της απουσίας είτε του απαιτούμενου συνδέσμου μεταξύ των διατηρούμενων δεδομένων και απειλής για τη δημόσια ασφάλεια είτε χρονικών ή γεωγραφικών περιορισμών, το ΔΕΕ κατέληξε στο συμπέρασμα ότι η εθνική νομοθεσία υπερέβαινε τα όρια του απολύτως αναγκαίου μέτρου για τον σκοπό της καταπολέμησης του σοβαρού εγκλήματος⁷¹.

Παρόμοια προσέγγιση όσον αφορά την αναγκαιότητα εφάρμοσε και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων στο έγγραφο με τίτλο *Necessity Toolkit*⁷². Στόχος της εργαλειοθήκης που περιέχει το έγγραφο είναι να

69 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, *Tele2 Sverige AB κατά Post- och telestyrelsen* και *Secretary of State for the Home Department κατά Tom Watson κ.λπ.* [τμήμα μείζονος συνθέσεως], 21 Δεκεμβρίου 2016, σκέψεις 105-106.

70 Ό.π., σκέψη 105.

71 Ό.π., σκέψη 107.

72 ΕΕΠΑ (2017), *Necessity Toolkit*, Βρυξέλλες, 11 Απριλίου 2017.

διευκολυνθεί η αξιολόγηση της συμμόρφωσης προτεινόμενων μέτρων με το δίκαιο της ΕΕ για την προστασία δεδομένων. Καταρτίστηκε για να παρέχει καλύτερα εφόδια στους υπεύθυνους χάραξης πολιτικής και στους νομοθέτες της ΕΕ οι οποίοι είναι αρμόδιοι για την κατάρτιση ή τον έλεγχο μέτρων που συνεπάγονται επεξεργασία δεδομένων προσωπικού χαρακτήρα και περιορίζουν το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς και άλλα δικαιώματα και ελευθερίες που προβλέπονται στον Χάρτη.

Στόχοι γενικού συμφέροντος

Προκειμένου να είναι δικαιολογημένος, κάθε περιορισμός στην άσκηση των δικαιωμάτων που αναγνωρίζονται στον Χάρτη πρέπει επίσης να εξυπηρετεί πραγματικά στόχους γενικού συμφέροντος που αναγνωρίζει η Ένωση ή την ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων. Όσον αφορά την ανάγκη προστασίας των δικαιωμάτων και των ελευθεριών των τρίτων, το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα αλληλεπιδρά συχνά με άλλα θεμελιώδη δικαιώματα. Στην [ενότητα 1.3](#) αναλύονται λεπτομερώς οι εν λόγω αλληλεπιδράσεις. Όσον αφορά τους στόχους γενικού συμφέροντος, σε αυτούς περιλαμβάνονται οι γενικοί στόχοι της ΕΕ, οι οποίοι επιβεβαιώνονται στο άρθρο 3 της Συνθήκης για την Ευρωπαϊκή Ένωση (ΣΕΕ), όπως η προαγωγή της ειρήνης και της ευημερίας των λαών της, η κοινωνική δικαιοσύνη και προστασία και η εγκαθίδρυση ενός χώρου ελευθερίας, ασφάλειας και δικαιοσύνης, στον οποίο διασφαλίζεται η ελεύθερη κυκλοφορία των προσώπων, σε συνδυασμό με κατάλληλα μέτρα για την πρόληψη και την καταπολέμηση της εγκληματικότητας, καθώς και άλλοι στόχοι και συμφέροντα που προστατεύονται από ειδικές διατάξεις των Συνθηκών ⁷³. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων προσδιορίζει περαιτέρω το άρθρο 52 παράγραφος 1 του Χάρτη συναφώς: Το άρθρο 23 παράγραφος 1 του κανονισμού απαριθμεί σειρά στόχων γενικού συμφέροντος οι οποίοι θεωρούνται θεμιτοί για τον περιορισμό των δικαιωμάτων των φυσικών προσώπων, εφόσον ο περιορισμός σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα και είναι αναγκαίος και ανάλογος. Η εθνική ασφάλεια και άμυνα, η πρόληψη του εγκλήματος, η προστασία σημαντικών οικονομικών και χρηματοοικονομικών συμφερόντων της ΕΕ ή των κρατών μελών, η δημόσια υγεία και η κοινωνική ασφάλιση συγκαταλέγονται στους στόχους δημόσιου συμφέροντος που αναφέρονται στο εν λόγω άρθρο.

⁷³ Επεξηγήσεις σχετικά με τον Χάρτη των Θεμελιωδών Δικαιωμάτων (2007/C 303/02) (ΕΕ C 303 της 14.12.2007, σ.17).

Είναι σημαντικό να ορίζεται και να εξηγείται, με επαρκή βαθμό λεπτομέρειας, ο στόχος γενικού συμφέροντος που επιδιώκεται με τον περιορισμό, καθώς η αναγκαιότητα του περιορισμού θα αξιολογηθεί σε σχέση με το πλαίσιο αυτό. Η σαφής και λεπτομερής περιγραφή του σκοπού του περιορισμού και των προτεινόμενων μέτρων είναι κρίσιμης σημασίας προκειμένου να καταστεί εφικτή η αξιολόγηση της αναγκαιότητάς του ⁷⁴. Ο επιδιωκόμενος σκοπός και η αναγκαιότητα και η αναλογικότητα του περιορισμού συνδέονται στενά.

Παράδειγμα: Η υπόθεση *Schwarz κατά Stadt Bochum* ⁷⁵ αφορούσε περιορισμούς στο δικαίωμα στον σεβασμό της ιδιωτικής ζωής και στο δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα ως αποτέλεσμα της λήψης και της αποθήκευσης δακτυλικών αποτυπωμάτων κατά τη χορήγηση διαβατηρίων από τις αρχές κράτους μέλους ⁷⁶. Ο προσφεύγων υπέβαλε αίτηση χορήγησης διαβατηρίου στον Stadt Bochum (Δήμο Bochum), αλλά αρνήθηκε να υποβληθεί σε λήψη δακτυλικών αποτυπωμάτων· κατόπιν τούτου, ο Stadt Bochum απέρριψε την αίτηση χορήγησης διαβατηρίου. Εν συνεχεία άσκησε προσφυγή ενώπιον γερμανικού δικαστηρίου με αίτημα να του χορηγηθεί διαβατήριο χωρίς να υποβληθεί σε λήψη δακτυλικών αποτυπωμάτων. Το γερμανικό δικαστήριο παρέπεμψε το ζήτημα στο ΔΕΕ, ζητώντας να διευκρινιστεί αν πρέπει να θεωρηθεί έγκυρο το άρθρο 1 παράγραφος 2 του κανονισμού 2252/2004 σχετικά με την καθιέρωση προτύπων για τα χαρακτηριστικά ασφαλείας και τη χρήση βιομετρικών στοιχείων στα διαβατήρια και τα ταξιδιωτικά έγγραφα των κρατών μελών.

Το ΔΕΕ επισήμανε ότι τα δακτυλικά αποτυπώματα **συνιστούν δεδομένα προσωπικού χαρακτήρα**, στο μέτρο που περιέχουν αντικειμενικώς εξατομικευμένες πληροφορίες σχετικά με φυσικά πρόσωπα και καθιστούν δυνατή την εξακρίβωση της ταυτότητάς τους, ενώ η λήψη και η αποθήκευση δακτυλικών αποτυπωμάτων συνιστά επεξεργασία. Η επεξεργασία αυτή, η οποία ρυθμίζεται από το άρθρο 1 παράγραφος 2 του κανονισμού αριθ. 2252/2004, συνιστά απειλή για τα δικαιώματα στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα ⁷⁷. Ωστόσο, το άρθρο 52 παράγραφος 1 του Χάρτη

74 ΕΕΠΔ (2017), *Necessity Toolkit*, Βρυξέλλες, 11 Απριλίου 2017, σ. 4.

75 ΔΕΕ, C-291/12, *Michael Schwarz κατά Stadt Bochum*, 17 Οκτωβρίου 2013.

76 Ό.π., σκέψεις 33-36.

77 Ό.π., σκέψεις 27-30.

επιτρέπει περιορισμούς στην άσκηση των εν λόγω δικαιωμάτων εφόσον οι περιορισμοί αυτοί προβλέπονται από τον νόμο, σέβονται το βασικό περιεχόμενο των εν λόγω δικαιωμάτων, είναι αναγκαίοι, τηρουμένης της αρχής της αναλογικότητας, και εξυπηρετούν πραγματικά στόχους γενικού συμφέροντος που αναγνωρίζει η Ένωση ή την ανάγκη προστασίας των δικαιωμάτων και ελευθεριών των τρίτων.

Στην προκειμένη περίπτωση, το ΔΕΕ επισήμανε, κατ' αρχάς, ότι ο περιορισμός που προκύπτει από τη λήψη και την αποθήκευση δακτυλικών αποτυπωμάτων κατά την έκδοση διαβατηρίων πρέπει να θεωρηθεί ότι **προβλέπεται από τον νόμο**, δεδομένου ότι οι πράξεις αυτές προβλέπονται στο άρθρο 1 παράγραφος 2 του κανονισμού αριθ. 2252/2004. Δεύτερον, ο κανονισμός αυτός εκδόθηκε με σκοπό την πρόληψη της πλαστογράφησης των διαβατηρίων και της δόλιας χρήσης αυτών. Επομένως, το άρθρο 1 παράγραφος 2 θεσπίστηκε για την πρόληψη, μεταξύ άλλων, της παράνομης εισόδου στην ΕΕ και, ως εκ τούτου, επιδιώκει στόχο γενικού ενδιαφέροντος που αναγνωρίζεται από την Ένωση. Τρίτον, δεν προέκυπτε από τα στοιχεία που είχε στη διάθεσή του το ΔΕΕ, ούτε άλλωστε υποστηρίχθηκε, ότι οι περιορισμοί στην άσκηση των εν λόγω δικαιωμάτων στην υπόθεση αυτή δεν σέβονταν την ουσία των εν λόγω δικαιωμάτων. Τέταρτον, η αποθήκευση δακτυλικών αποτυπωμάτων σε μέσο αποθήκευσης υψηλής ασφάλειας, όπως προβλέπεται στη διάταξη αυτή, προϋποθέτει υπερσύγχρονη τεχνολογία. Η αποθήκευση αυτή είναι ικανή να μειώσει τον κίνδυνο πλαστογράφησης των διαβατηρίων και να διευκολύνει το έργο των αρχών που είναι επιφορτισμένες με τον έλεγχο της γνησιότητάς τους κατά τη διέλευση των συνόρων της ΕΕ. Το γεγονός ότι η μέθοδος δεν είναι απολύτως αξιόπιστη δεν είναι αποφασιστικής σημασίας. Μολονότι δεν αποκλείει εντελώς το ενδεχόμενο εσφαλμένης έγκρισης διέλευσης των συνόρων από πρόσωπα στα οποία δεν επιτρέπεται η είσοδος στο έδαφος της Ένωσης, η μέθοδος αυτή μειώνει σημαντικά τον κίνδυνο τέτοιων εσφαλμένων εγκρίσεων εισόδου. Λαμβανομένων υπόψη των προεκτεθέντων, το ΔΕΕ αποφάνθηκε ότι η λήψη και η αποθήκευση δακτυλικών αποτυπωμάτων, η οποία αναφέρεται στο άρθρο 1 παράγραφος 2 του κανονισμού αριθ. 2252/2004, ενδείκνυται για την εκπλήρωση των σκοπών που επιδιώκονται με τον εν λόγω κανονισμό και, κατ' επέκταση, του σκοπού της πρόληψης της παράνομης εισόδου στην ΕΕ ⁷⁸.

78 Ό.π., σκέψεις 35-45.

Εν συνεχεία, το ΔΕΕ εκτίμησε κατά πόσον η επεξεργασία αυτή είναι **αναγκαία**, επισημαίνοντας ότι η επίμαχη διαδικασία αφορούσε μόνο τη λήψη των αποτυπωμάτων δύο δακτύλων, τα οποία επιπλέον είναι συνήθως εκτεθειμένα σε κοινή θέα, και ότι δεν επρόκειτο για κατ' ιδίαν πράξη. Επιπλέον, η εν λόγω διαδικασία, όπως και η διαδικασία λήψης φωτογραφίας προσώπου, δεν είναι ιδιαίτερα δυσάρεστη σωματικά ή ψυχολογικά. Επισημαίνεται ότι η μοναδική πραγματική εναλλακτική της λήψης δακτυλικών αποτυπωμάτων λύση που προτάθηκε κατά την ενώπιον του ΔΕΕ διαδικασία είναι η λήψη εικόνας της ίριδας του ματιού. Από κανένα στοιχείο της υποβληθείσας στο ΔΕΕ δικογραφίας δεν προκύπτει ότι η διαδικασία αυτή θα έθιγε τα προστατευόμενα από τα άρθρα 7 και 8 του Χάρτη δικαιώματα λιγότερο από τη λήψη δακτυλικών αποτυπωμάτων. Επιπλέον, όσον αφορά την αποτελεσματικότητα των δύο αυτών μεθόδων, είναι γνωστό ότι το τεχνολογικό επίπεδο της μεθόδου που στηρίζεται στην αναγνώριση της ίριδας δεν είναι εξίσου υψηλό με εκείνο της μεθόδου που στηρίζεται στη λήψη δακτυλικών αποτυπωμάτων, και η αναγνώριση της ίριδας αποτελεί σήμερα διαδικασία με σαφώς υψηλότερο κόστος έναντι της σύγκρισης των δακτυλικών αποτυπωμάτων και, ως εκ τούτου, ενδείκνυται λιγότερο για γενικευμένη χρήση. Επομένως, δεν έχει περιέλθει σε γνώση του ΔΕΕ η ύπαρξη μέτρων τα οποία θα μπορούσαν να συμβάλουν αρκούντως αποφασιστικά στον σκοπό της προστασίας των διαβατηρίων από δόλια χρήση και συγχρόνως θα έθιγαν τα δικαιώματα που κατοχυρώνονται στα άρθρα 7 και 8 του Χάρτη σε μικρότερο βαθμό έναντι της μεθόδου που στηρίζεται στη λήψη δακτυλικών αποτυπωμάτων ⁷⁹.

Το ΔΕΕ επισήμανε ότι το άρθρο 4 παράγραφος 3 του κανονισμού αριθ. 2252/2004 ορίζει ρητώς ότι τα δακτυλικά αποτυπώματα χρησιμοποιούνται με μοναδικό σκοπό την εξακρίβωση της γνησιότητας του διαβατηρίου και της ταυτότητας του κατόχου του, ενώ το άρθρο 1 παράγραφος 2 του κανονισμού προβλέπει την αποθήκευση των δακτυλικών αποτυπωμάτων μόνο στο ίδιο το διαβατήριό, το οποίο ανήκει μόνο στον κάτοχό του. Επομένως, ο κανονισμός δεν παρείχε νομική βάση για την ενδεχόμενη συγκεντρωτική επεξεργασία των δεδομένων που συλλέγονται βάσει των διατάξεών του ή για χρήση των δεδομένων αυτών με άλλο σκοπό πλην αυτού της αποτροπής της παράνομης εισόδου

79 ΔΕΕ, C-291/12, *Michael Schwarz κατά Stadt Bochum*, 17 Οκτωβρίου 2013, σκέψεις 46-53.

προσώπων στο έδαφος της Ένωσης ⁸⁰. Λαμβανομένων υπόψη των ως άνω σκέψεων, το ΔΕΕ κατέληξε στο συμπέρασμα ότι από την εξέταση του προδικαστικού ερωτήματος δεν προέκυψαν στοιχεία δυνάμενα να θίξουν το κύρος του άρθρου 1 παράγραφος 2 του κανονισμού αριθ. 2252/2004.

Σχέση μεταξύ του Χάρτη και της ΕΣΔΑ

Παρά τη διαφορετική διατύπωση, οι προϋποθέσεις των νόμιμων περιορισμών των δικαιωμάτων, οι οποίες προβλέπονται στο άρθρο 52 παράγραφος 1 του Χάρτη, θυμίζουν το άρθρο 8 παράγραφος 2 της ΕΣΔΑ σχετικά με το δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Στη νομολογία τους, το ΔΕΕ και το ΕΔΔΑ παραπέμπουν συχνά το ένα στις αποφάσεις του άλλου, στο πλαίσιο του συνεχούς διαλόγου μεταξύ των δύο δικαστηρίων και της επιδίωξης εναρμονισμένης ερμηνείας των κανόνων περί προστασίας δεδομένων. Το άρθρο 52 παράγραφος 3 του Χάρτη ορίζει ότι «στον βαθμό που ο παρών Χάρτης περιλαμβάνει δικαιώματα που αντιστοιχούν σε δικαιώματα τα οποία διασφαλίζονται στην Ευρωπαϊκή Σύμβαση για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών, η έννοια και η εμβέλειά τους είναι ίδιες με εκείνες που τους αποδίδει η εν λόγω Σύμβαση». Ωστόσο, το άρθρο 8 του Χάρτη δεν αντιστοιχεί άμεσα σε άρθρο της ΕΣΔΑ ⁸¹. Το άρθρο 52 παράγραφος 3 του Χάρτη αφορά μάλλον το περιεχόμενο και την εμβέλεια των δικαιωμάτων που προστατεύονται σε κάθε έννομη τάξη, παρά τις προϋποθέσεις του περιορισμού τους. Ωστόσο, δεδομένου του ευρύτερου πλαισίου διαλόγου και συνεργασίας μεταξύ των δύο δικαστηρίων, το ΔΕΕ μπορεί να λαμβάνει υπόψη στις αναλύσεις του τα κριτήρια του νόμιμου περιορισμού τα οποία προβλέπονται στο άρθρο 8 της ΕΣΔΑ, όπως ερμηνεύονται από το ΕΔΔΑ. Το αντίθετο σενάριο, κατά το οποίο το ΕΔΔΑ μπορεί να παραπέμψει στις προϋποθέσεις νόμιμου περιορισμού βάσει του Χάρτη, είναι επίσης δυνατό. Εν πάση περιπτώσει, πρέπει επίσης να λαμβάνεται υπόψη ότι στην ΕΣΔΑ δεν υπάρχει απολύτως αντίστοιχη διάταξη του άρθρου 8 του Χάρτη η οποία να παραπέμπει στην προστασία των δικαιωμάτων προσωπικού χαρακτήρα και ιδίως στα δικαιώματα του υποκειμένου των δεδομένων, στους θεμιτούς λόγους επεξεργασίας και στην εποπτεία ανεξάρτητης αρχής. Ορισμένα στοιχεία του άρθρου 8 του Χάρτη απαντούν στη νομολογία του ΕΔΔΑ η οποία αναπτύχθηκε στο πλαίσιο του άρθρου 8 της ΕΣΔΑ και σχετίζεται με τη Σύμβαση 108 ⁸². Ο σύνδεσμος αυτός διασφαλίζει ότι το ΔΕΕ και το ΕΔΔΑ λαμβάνουν αμοιβαίως

80 Ό.π., σκέψεις 56-61.

81 ΕΕΠΑ (2017), *Necessity Toolkit*, Βρυξέλλες, 11 Απριλίου 2017, σ. 6.

82 Επεξηγήσεις σχετικά με τον Χάρτη των Θεμελιωδών Δικαιωμάτων (2007/C 303/02), άρθρο 8.

υπόψη τις αντίστοιχες νομολογίες τους σε υποθέσεις που έχουν ως αντικείμενο την προστασία δεδομένων.

1.3. Αλληλεπίδραση με άλλα δικαιώματα και θεμιτά συμφέροντα

Κύρια σημεία

- Το δικαίωμα στην προστασία των δεδομένων αλληλεπιδρά συχνά με άλλα δικαιώματα, όπως είναι η ελευθερία της έκφρασης και το δικαίωμα λήψης και μετάδοσης πληροφοριών.
- Η αλληλεπίδραση αυτή είναι συχνά αμφίσημη: παρότι υπάρχουν περιπτώσεις στις οποίες το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα αντιτίθεται σε συγκεκριμένο δικαίωμα, υπάρχουν επίσης περιπτώσεις στις οποίες το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα διασφαλίζει αποτελεσματικά τον σεβασμό του ίδιου συγκεκριμένου δικαιώματος. Για παράδειγμα, αυτό συμβαίνει στην περίπτωση της ελευθερίας της έκφρασης, δεδομένου ότι το επαγγελματικό απόρρητο είναι στοιχείο του δικαιώματος στον σεβασμό της ιδιωτικής ζωής.
- Η ανάγκη προστασίας των δικαιωμάτων και των ελευθεριών των τρίτων είναι ένα από τα κριτήρια που χρησιμοποιούνται για την αξιολόγηση της νομιμότητας του περιορισμού του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα.
- Όταν διακυβεύονται διαφορετικά δικαιώματα, τα δικαστήρια οφείλουν να τα σταθμίζουν και να τα συμβιβάζουν.
- Ο Γενικός Κανονισμός για την Προστασία Δεδομένων υποχρεώνει τα κράτη μέλη να συμβιβάζουν το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με την ελευθερία έκφρασης και πληροφόρησης.
- Τα κράτη μέλη μπορούν επίσης να θεσπίζουν ειδικούς κανόνες στο εθνικό δικαιοπρόκειμένου να συμβιβάζουν το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα πρόσβασης του κοινού σε επίσημα έγγραφα και τις υποχρεώσεις επαγγελματικού απορρήτου.

Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο· οι προϋποθέσεις του νόμιμου περιορισμού του δικαιώματος αυτού περιγράφονται αναλυτικά ανωτέρω. Ένα από τα κριτήρια επιβολής νόμιμων περιορισμών σε δικαιώματα, το οποίο αναγνωρίζεται τόσο βάσει του δικαίου του

Συμβουλίου της Ευρώπης όσο και βάσει του δικαίου της ΕΕ, είναι το αν η επέμβαση στην προστασία των δικαιωμάτων είναι αναγκαία για την προστασία των δικαιωμάτων και των ελευθεριών των τρίτων. Όταν η προστασία των δεδομένων αλληλεπιδρά με άλλα δικαιώματα, τόσο το ΕΔΔΑ όσο και το ΔΕΕ έχουν αποφανθεί επανειλημμένως ότι, κατά την εφαρμογή και την ερμηνεία του άρθρου 8 της ΕΣΔΑ και του άρθρου 8 του Χάρτη, είναι αναγκαία η στάθμιση με άλλα δικαιώματα⁸³. Με μια σειρά χαρακτηριστικά παραδείγματα καταδεικνύεται κατωτέρω με ποιον τρόπο πραγματοποιείται η στάθμιση αυτή.

Επιπροσθέτως της στάθμισης που διενεργούν τα δικαστήρια αυτά, τα κράτη μπορούν, εάν απαιτείται, να θεσπίζουν νομοθεσία για τον συμβιβασμό του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα με άλλα δικαιώματα. Για τον λόγο αυτόν, ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει ορισμένους τομείς στους οποίους μπορούν να εφαρμοστούν παρεκκλίσεις σε εθνικό επίπεδο.

Όσον αφορά την ελευθερία έκφρασης, ο ΓΚΠΔ απαιτεί τα κράτη μέλη να συμβιβάζουν, διά νόμου, «το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δυνάμει του παρόντος κανονισμού με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς και για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης»⁸⁴. Τα κράτη μέλη μπορούν επίσης να θεσπίσουν νομοθεσία για τον συμβιβασμό της προστασίας των δεδομένων με το δικαίωμα πρόσβασης του κοινού σε επίσημα έγγραφα και τις υποχρεώσεις επαγγελματικού απορρήτου που προστατεύονται ως έκφραση του δικαιώματος στον σεβασμό της ιδιωτικής ζωής⁸⁵.

83 ΕΔΔΑ, *Von Hannover κατά Γερμανίας* (αριθ. 2) [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 40660/08 και 60641/08, 7 Φεβρουαρίου 2012· ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECMD) κατά Administración del Estado*, 24 Νοεμβρίου 2011, σκέψη 48· ΔΕΕ, C-275/06, *Productores de Música de España (Promusicae) κατά Telefónica de España SAU* [τμήμα μείζονος συνθέσεως], 29 Ιανουαρίου 2008, σκέψη 68.

84 Γενικός Κανονισμός Προστασίας Δεδομένων, άρθρο 85.

85 Ό.π., άρθρα 86 και 90.

1.3.1. Ελευθερία έκφρασης

Ένα από τα δικαιώματα που αλληλεπιδρά σε πολύ σημαντικό βαθμό με το δικαίωμα στην προστασία των δεδομένων είναι αυτό της ελευθερίας της έκφρασης.

Η ελευθερία της έκφρασης κατοχυρώνεται στο άρθρο 11 του Χάρτη («Ελευθερία έκφρασης και πληροφόρησης»). Το δικαίωμα αυτό περιλαμβάνει την «ελευθερία γνώμης και την ελευθερία λήψης ή μετάδοσης πληροφοριών ή ιδεών, χωρίς την ανάμειξη δημοσίων αρχών και αδιακρίτως συνόρων». Σύμφωνα τόσο με το άρθρο 11 του Χάρτη όσο και με το άρθρο 10 της ΕΣΔΑ, η ελευθερία πληροφόρησης προστατεύει το δικαίωμα όχι μόνο της μετάδοσης αλλά και της λήψης πληροφοριών.

Οι περιορισμοί της ελευθερίας της έκφρασης πρέπει να είναι σύμφωνοι προς τα κριτήρια που προβλέπονται στο άρθρο 52 παράγραφος 1 του Χάρτη, τα οποία περιγράφονται ανωτέρω. Επιπλέον, το άρθρο 11 του Χάρτη αντιστοιχεί στο άρθρο 10 της ΕΣΔΑ. Βάσει του άρθρου 52 παράγραφος 3 του Χάρτη, στον βαθμό που ο Χάρτης περιλαμβάνει δικαιώματα που αντιστοιχούν σε δικαιώματα τα οποία διασφαλίζονται στην ΕΣΔΑ, «η έννοια και η εμβέλειά τους είναι ίδιες με εκείνες που τους αποδίδει η εν λόγω Σύμβαση». Επομένως, οι περιορισμοί που μπορούν να επιβληθούν νομίμως στο δικαίωμα που κατοχυρώνεται στο άρθρο 11 του Χάρτη δεν επιτρέπεται να υπερβαίνουν τους προβλεπόμενους στο άρθρο 10 παράγραφος 2 της ΕΣΔΑ –δηλαδή, πρέπει να προβλέπονται από τον νόμο και να είναι αναγκαίοι σε μια δημοκρατική κοινωνία για «την προστασία της υπολήψεως ή των δικαιωμάτων των τρίτων». Τα δικαιώματα αυτά περιλαμβάνουν, ιδίως, το δικαίωμα στον σεβασμό της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Η σχέση μεταξύ της προστασίας των δεδομένων προσωπικού χαρακτήρα και της ελευθερίας της έκφρασης διέπεται από το άρθρο 85 του Γενικού Κανονισμού για την Προστασία Δεδομένων, με τίτλο «Επεξεργασία και ελευθερία έκφρασης και πληροφόρησης». Κατά το άρθρο αυτό, τα κράτη μέλη συμβιβάζουν το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία της έκφρασης και πληροφόρησης. Ειδικότερα, εξαιρέσεις και παρεκκλίσεις από συγκεκριμένα κεφάλαια του Γενικού Κανονισμού για την Προστασία Δεδομένων προβλέπονται για δημοσιογραφικούς σκοπούς ή για σκοπούς πανεπιστημιακής, καλλιτεχνικής ή λογοτεχνικής έκφρασης, στο μέτρο που είναι αναγκαίες για τον συμβιβασμό του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα με την ελευθερία της έκφρασης και πληροφόρησης.

Παράδειγμα: Στην υπόθεση *Tietosuojavalvuttettu κατά Satakunnan Markkinapörssi Oy και Satamedia Oy*⁸⁶, το ΔΕΕ κλήθηκε να ορίσει τη σχέση μεταξύ της προστασίας των δεδομένων και της ελευθερίας του Τύπου⁸⁷. Συγκεκριμένα, κλήθηκε να εξετάσει τη δημοσιοποίηση εκ μέρους εταιρείας, μέσω υπηρεσίας SMS, των φορολογικών στοιχείων περίπου 1,2 εκατομμυρίων φυσικών προσώπων, τα οποία είχαν αποκτηθεί νομίμως από τις φινλανδικές φορολογικές αρχές. Η φινλανδική εποπτική αρχή προστασίας των δεδομένων είχε εκδώσει απόφαση με την οποία υποχρέωνε την εταιρεία να παύσει τη δημοσιοποίηση των στοιχείων αυτών. Η εταιρεία προσέβαλε την απόφαση αυτή ενώπιον εθνικού δικαστηρίου, το οποίο ζήτησε από το ΔΕΕ διευκρινίσεις σχετικά με την ερμηνεία της Οδηγίας για την Προστασία Δεδομένων. Ειδικότερα, το ΔΕΕ έπρεπε να εξακριβώσει αν η επεξεργασία δεδομένων προσωπικού χαρακτήρα, τα οποία είχαν διαθέσει οι φορολογικές αρχές προκειμένου οι χρήστες κινητών τηλεφώνων να λαμβάνουν φορολογικά στοιχεία που αφορούν άλλα φυσικά πρόσωπα, πρέπει να θεωρείται δραστηριότητα η οποία ασκείται «αποκλειστικά για δημοσιογραφικούς σκοπούς». Αφού διαπίστωσε ότι οι δραστηριότητες της εταιρείας συνιστούσαν «επεξεργασία δεδομένων προσωπικού χαρακτήρα» κατά την έννοια του άρθρου 3 παράγραφος 1 της οδηγίας για την προστασία δεδομένων, το ΔΕΕ ερμήνευσε το άρθρο 9 της οδηγίας (για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ελευθερία έκφρασης). Το ΔΕΕ επισήμανε κατ' αρχάς τη σημασία του δικαιώματος της ελευθερίας της έκφρασης σε κάθε δημοκρατική κοινωνία και έκρινε ότι οι σχετικές έννοιες, όπως εκείνη του δημοσιογραφικού σκοπού, πρέπει να ερμηνεύονται ευρέως. Εν συνεχεία, επισήμανε ότι, για την επίτευξη ισόρροπης στάθμισης μεταξύ των δύο θεμελιωδών δικαιωμάτων, οι παρεκκλίσεις και οι περιορισμοί του δικαιώματος στην προστασία των δεδομένων δεν πρέπει να υπερβαίνουν τα όρια του απολύτως αναγκαίου. Υπό τις περιστάσεις αυτές, το ΔΕΕ αποφάνθηκε ότι δραστηριότητες όπως αυτές που ασκούν οι εταιρείες

86 ΔΕΕ, C-73/07, *Tietosuojavalvuttettu κατά Satakunnan Markkinapörssi Oy και Satamedia Oy* [τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008, σκέψεις 56, 61 και 62.

87 Η υπόθεση αφορούσε την ερμηνεία της Οδηγίας για την Προστασία Δεδομένων και ιδίως το άρθρο 9, το οποίο έχει πλέον αντικατασταθεί από το άρθρο 85 του Γενικού Κανονισμού για την Προστασία Δεδομένων, που προέβλεπε τα εξής: «Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται αποκλειστικώς για δημοσιογραφικούς σκοπούς ή στο πλαίσιο καλλιτεχνικής ή λογοτεχνικής έκφρασης, τα κράτη μέλη προβλέπουν τις εξαιρέσεις ή παρεκκλίσεις από τις διατάξεις του παρόντος κεφαλαίου, του κεφαλαίου IV και του κεφαλαίου VI μόνο στο βαθμό που είναι αναγκαίες ώστε το δικαίωμα της ιδιωτικής ζωής να συμβιβάζεται με τους κανόνες που διέπουν την ελευθερία έκφρασης».

στην υπόθεση της κύριας δίκης, οι οποίες αφορούν δεδομένα που προέρχονται από δημόσια έγγραφα κατά την εθνική νομοθεσία, μπορούν να χαρακτηρίζονται ως δημοσιογραφικές αν με αυτές σκοπείται να ανακοινώνονται στο κοινό πληροφορίες, απόψεις ή ιδέες, με οποιονδήποτε τρόπο. Το ΔΕΕ αποφάνθηκε επίσης ότι οι δραστηριότητες αυτές δεν απαιτείται να συνδέονται αποκλειστικά με επιχειρήσεις μέσω μαζικής ενημέρωσης και μπορούν να ασκούνται με σκοπό το κέρδος. Ωστόσο, το ΔΕΕ έκρινε ότι εναπόκειται στο εθνικό δικαστήριο να εκτιμήσει αν συμβαίνει κάτι τέτοιο με βάση τα ιδιαίτερα πραγματικά περιστατικά της συγκεκριμένης υπόθεσης.

Η ίδια υπόθεση εξετάστηκε επίσης από το ΕΔΔΑ, αφού το εθνικό δικαστήριο έκρινε, με την καθοδήγηση του ΔΕΕ, ότι η εντολή της εποπτικής αρχής περί παύσης της δημοσιοποίησης όλων των φορολογικών στοιχείων συνιστούσε δικαιολογημένη επέμβαση στην ελευθερία έκφρασης της εταιρείας. Το ΕΔΔΑ επικύρωσε την προσέγγιση αυτή⁸⁸. Έκρινε ότι, παρότι υπήρξε επέμβαση στο δικαίωμα των εταιρειών να μεταδίδουν πληροφορίες, η επέμβαση προβλεπόταν από τον νόμο, επιδίωκε θεμιτό σκοπό και ήταν αναγκαία σε μια δημοκρατική κοινωνία.

Το ΕΔΔΑ υπενθύμισε τα νομολογιακά κριτήρια τα οποία θα πρέπει να καθοδηγούν τις εθνικές αρχές και το ίδιο το ΕΔΔΑ όταν σταθμίζουν την ελευθερία της έκφρασης με το δικαίωμα στον σεβασμό της ιδιωτικής ζωής. Όταν απειλείται ο πολιτικός λόγος ή ο διάλογος σχετικά με θέμα δημόσιου συμφέροντος, είναι μικρό το περιθώριο περιορισμού του δικαιώματος λήψης και μετάδοσης πληροφοριών, καθώς το κοινό έχει δικαίωμα ενημέρωσης, «και αυτό είναι ουσιώδες δικαίωμα σε μια δημοκρατική κοινωνία»⁸⁹. Ωστόσο, άρθρα στον Τύπο τα οποία στοχεύουν μόνο στην ικανοποίηση της περιέργειας συγκεκριμένου αναγνωστικού κοινού σχετικά με λεπτομέρειες της ιδιωτικής ζωής ενός προσώπου δεν μπορεί να θεωρηθεί ότι συμβάλλουν σε διάλογο σχετικά με θέμα δημόσιου συμφέροντος. Η παρέκκλιση από τους κανόνες περί προστασίας δεδομένων για δημοσιογραφικούς σκοπούς προβλέπεται ώστε να παρέχεται στους δημοσιογράφους η δυνατότητα να έχουν πρόσβαση σε δεδομένα, καθώς και να συλλέγουν και να επεξεργάζονται δεδομένα,

⁸⁸ ΕΔΔΑ, *Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 931/13, 27 Ιουνίου 2017.

⁸⁹ Ό.π., σκέψη 169.

ώστε να είναι σε θέση να ασκούν τις επαγγελματικές τους δραστηριότητες. Επομένως, εξυπηρετούσε όντως δημόσιο συμφέρον η παροχή πρόσβασης στον μεγάλο όγκο των επίμαχων φορολογικών στοιχείων και η αναγνώριση του δικαιώματος των προσφευγουσών εταιρειών να συλλέξουν και να επεξεργαστούν τα στοιχεία αυτά. Αντιθέτως, το ΕΔΔΑ έκρινε ότι δεν υπήρχε δημόσιο συμφέρον όσον αφορά τη μαζική μετάδοση από τις εφημερίδες τέτοιων μη επεξεργασμένων δεδομένων, αυτούσιων και χωρίς καμία ανάλυση. Οι πληροφορίες σχετικά με τη φορολόγηση μπορεί να επέτρεψαν σε μέρος του κοινού να ικανοποιήσει την περιέργειά του, να κατηγοριοποιήσει διάφορα πρόσωπα ανάλογα με την οικονομική τους κατάσταση και να κορέσει τη δίψα του για πληροφορίες σχετικά με την ιδιωτική ζωή τρίτων. Αυτό δεν μπορούσε να θεωρηθεί ότι συνέβαλλε σε διάλογο για θέμα δημόσιου συμφέροντος.

Παράδειγμα: Στην υπόθεση *Google Spain*⁹⁰, το ΔΕΕ εξέτασε αν η Google ήταν υποχρεωμένη να διαγράψει παρωχημένες πληροφορίες σχετικά με τις οικονομικές δυσκολίες του προσφεύγοντος από τον κατάλογο αποτελεσμάτων των αναζητήσεων. Κατά την αναζήτηση με χρήση του ονόματος του προσφεύγοντος στη μηχανή αναζήτησης της Google, τα αποτελέσματα παρείχαν συνδέσμους προς παλαιά άρθρα εφημερίδων τα οποία τον συνέδεαν με διαδικασίες πτώχευσης. Ο προσφεύγων θεώρησε ότι αυτό συνιστά παραβίαση των δικαιωμάτων του στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα, καθώς οι διαδικασίες είχαν ολοκληρωθεί πριν από χρόνια με αποτέλεσμα οι παραπομπές αυτές να είναι άνευ σημασίας.

Το ΔΕΕ αποσαφήνισε, κατ' αρχάς, ότι οι μηχανές αναζήτησης στο διαδίκτυο και τα αποτελέσματα αναζητήσεων τα οποία παρέχουν δεδομένα προσωπικού χαρακτήρα παρέχουν τη δυνατότητα κατάρτισης λεπτομερούς προφίλ φυσικού προσώπου. Σε μια ολοένα και περισσότερο ψηφιοποιημένη κοινωνία, η απαίτηση, αφενός, να είναι τα δεδομένα προσωπικού χαρακτήρα ακριβή και, αφετέρου, να μην υπερβαίνει η δημοσιοποίησή τους τα όρια του αναγκαίου, δηλαδή της παροχής πληροφοριών στο κοινό, είναι θεμελιώδους σημασίας προκειμένου να διασφαλίζεται υψηλό επίπεδο προστασίας των δεδομένων για τα φυσικά πρόσωπα. Ο «υπεύθυνος της επεξεργασίας αυτής πρέπει να διασφαλίζει,

90 ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014, σκέψεις 81-83.

στο πλαίσιο των ευθυνών, των ικανοτήτων και των δυνατοτήτων του, ότι η εν λόγω δραστηριότητα ανταποκρίνεται στις απαιτήσεις» της νομοθεσίας της ΕΕ, προκειμένου οι προβλεπόμενες νόμιμες εγγυήσεις να μπορούν να παράγουν πλήρως τα αποτελέσματά τους. Αυτό σημαίνει ότι το δικαίωμα προσώπου στη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν όταν η επεξεργασία δεν είναι πλέον αναγκαία ή είναι παρωχημένη καλύπτει επίσης τις μηχανές αναζήτησης, οι οποίες διαπιστώθηκε ότι είναι υπεύθυνοι επεξεργασίας, όχι απλώς εκτελούντες (βλ. ενότητα 2.3.1).

Όταν εξέτασε αν η Google ήταν υποχρεωμένη να αφαιρέσει τους σχετικούς με τον προσφεύγοντα συνδέσμους, το ΔΕΕ αποφάνθηκε ότι, υπό ορισμένες προϋποθέσεις, τα φυσικά πρόσωπα έχουν το δικαίωμα να εξασφαλίζουν τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που τα αφορούν από τα αποτελέσματα μηχανής αναζήτησης στο διαδίκτυο. Το δικαίωμα αυτό μπορεί να προβληθεί όταν οι πληροφορίες που αφορούν το φυσικό πρόσωπο είναι ανακριβείς, ακατάλληλες, άσχετες ή υπερβολικές για τους σκοπούς της επεξεργασίας δεδομένων. Το ΔΕΕ αναγνώρισε ότι το δικαίωμα αυτό δεν είναι απόλυτο· πρέπει να σταθμίζεται με άλλα, ιδίως δε με το συμφέρον και το δικαίωμα του ευρύτερου κοινού να έχει πρόσβαση στις πληροφορίες. Κάθε αίτημα διαγραφής πρέπει να αξιολογείται κατά περίπτωση ώστε να επιδιώκεται η ισορροπία μεταξύ, αφενός, των θεμελιωδών δικαιωμάτων στην προστασία των δεδομένων προσωπικού χαρακτήρα και στον σεβασμό της ιδιωτικής ζωής του υποκειμένου των δεδομένων και, αφετέρου, των θεμιτών συμφερόντων όλων των χρηστών του διαδικτύου. Το ΔΕΕ παρείχε καθοδήγηση σχετικά με τους παράγοντες που πρέπει να λαμβάνονται υπόψη κατά την εν λόγω στάθμιση. Η φύση των επίμαχων πληροφοριών είναι ιδιαίτερα σημαντικός παράγοντας. Εάν οι πληροφορίες για την ιδιωτική ζωή του φυσικού προσώπου είναι ευαίσθητες και δεν υπηρετείται το δημόσιο συμφέρον από τη διαθεσιμότητα των πληροφοριών, η προστασία των δεδομένων και η ιδιωτική ζωή υπερισχύουν του δικαιώματος του ευρύτερου κοινού να έχει πρόσβαση στις πληροφορίες. Εάν, αντιθέτως, φαίνεται ότι το υποκείμενο των δεδομένων είναι δημόσιο πρόσωπο ή ότι οι πληροφορίες είναι τέτοιας φύσης ώστε να δικαιολογούν την παροχή στο ευρύτερο κοινό της δυνατότητας πρόσβασης σε αυτές, η επέμβαση στα θεμελιώδη δικαιώματα της προστασίας δεδομένων και της ιδιωτικής ζωής είναι δικαιολογημένη.

Μετά την έκδοση της απόφασης αυτής, η Ομάδα εργασίας του άρθρου 29 εξέδωσε κατευθυντήριες γραμμές σχετικά με την εφαρμογή της. Οι κατευθυντήριες γραμμές περιλαμβάνουν κατάλογο κοινών κριτηρίων προς χρήση από τις εποπτικές αρχές κατά τον χειρισμό καταγγελιών που αφορούν αιτήματα διαγραφής φυσικών προσώπων, καθώς και για την καθοδήγησή τους κατά την εν λόγω διαδικασία στάθμισης των δικαιωμάτων⁹¹.

Όσον αφορά τον συμβιβασμό του δικαιώματος στην προστασία δεδομένων και του δικαιώματος στην ελευθερία της έκφρασης, το ΕΔΔΑ έχει εκδώσει αρκετές αποφάσεις-ορόσημα.

Παράδειγμα: Στην υπόθεση *Axel Springer AG κατά Γερμανίας*⁹², το ΕΔΔΑ έκρινε ότι η απαγόρευση που είχε επιβάλει εθνικό δικαστήριο στην προσφεύγουσα εταιρεία να δημοσιεύσει άρθρο σχετικά με τη σύλληψη και την καταδίκη διάσημου ηθοποιού συνιστούσε παράβαση του άρθρου 10 της ΕΣΔΑ. Το ΕΔΔΑ επανέλαβε τα κριτήρια τα οποία πρέπει να λαμβάνονται υπόψη κατά τη στάθμιση του δικαιώματος στην ελευθερία της έκφρασης και του δικαιώματος στον σεβασμό της ιδιωτικής ζωής, όπως καθορίζονται στη νομολογία του:

- αν το γεγονός που πραγματευόταν το επίμαχο δημοσιευθέν άρθρο ήταν γενικού ενδιαφέροντος·
- αν ο θιγόμενος ήταν δημόσιο πρόσωπο· και
- με ποιον τρόπο αποκτήθηκαν οι πληροφορίες και αν ήταν αξιόπιστες.

Το ΕΔΔΑ αποφάνθηκε ότι η σύλληψη και η καταδίκη του ηθοποιού ήταν δημόσιο δικαστικό γεγονός και, επομένως, αφορούσε το δημόσιο συμφέρον· ότι ο ηθοποιός ήταν αρκούντως γνωστός ώστε να μπορεί να χαρακτηριστεί δημόσιο πρόσωπο· και ότι οι πληροφορίες είχαν παρασχεθεί από την εισαγγελική αρχή και η ακρίβειά τους δεν τέθηκε

91 Ομάδα εργασίας του άρθρου 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12, WP 225, Βρυξέλλες, 26 Νοεμβρίου 2014.

92 ΕΔΔΑ, *Axel Springer AG κατά Γερμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 39954/08, 7 Φεβρουαρίου 2012, σκέψεις 90 και 91.

υπό αμφισβήτηση από τους διαδίκους. Επομένως, οι περιορισμοί στη δημοσίευση οι οποίοι επιβλήθηκαν στην εταιρεία δεν ήταν ευλόγως ανάλογοι προς τον θεμιτό σκοπό της προστασίας της ιδιωτικής ζωής του προσφεύγοντος. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι υπήρξε παράβαση του άρθρου 10 της ΕΣΔΑ.

Παράδειγμα: Η υπόθεση *Couderc και Hachette Filipacchi Associés κατά Γαλλίας*⁹³ αφορούσε τη δημοσίευση σε γαλλικό εβδομαδιαίο περιοδικό της συνέντευξης της N. Coste, η οποία ισχυριζόταν ότι ο πρίγκιπας Αλβέρτος του Μονακό ήταν ο πατέρας του υιού της. Η συνέντευξη περιέγραφε επίσης τη σχέση της N. Coste με τον πρίγκιπα και τον τρόπο με τον οποίο αυτός αντέδρασε στη γέννηση του παιδιού, και συνοδευόταν από φωτογραφίες του πρίγκιπα με το παιδί. Ο πρίγκιπας Αλβέρτος προσέφυγε κατά του εκδότη του περιοδικού για παραβίαση του δικαιώματός του στην προστασία της ιδιωτικής ζωής του. Τα γαλλικά δικαστήρια αποφάνθηκαν ότι η δημοσίευση του άρθρου προκάλεσε ανήκεστο βλάβη στον πρίγκιπα Αλβέρτο και διέταξε τον εκδότη να καταβάλει αποζημίωση και να δημοσιεύσει τις λεπτομέρειες της απόφασης στο εξώφυλλο του περιοδικού.

Οι εκδότες του περιοδικού προσέφυγαν ενώπιον του ΕΔΔΑ, υποστηρίζοντας ότι η απόφαση των γαλλικών δικαστηρίων συνιστούσε αδικαιολόγητη επέμβαση στο δικαίωμά τους στην ελευθερία της έκφρασης. Το ΕΔΔΑ έπρεπε να σταθμίσει, αφενός, το δικαίωμα στον σεβασμό της ιδιωτικής ζωής του πρίγκιπα Αλβέρτου και, αφετέρου, το δικαίωμα στην ελευθερία έκφρασης του εκδότη και το δικαίωμα ενημέρωσης του ευρύτερου κοινού. Το δικαίωμα της N. Coste να γνωστοποιήσει την ιστορία της στο κοινό και το συμφέρον του παιδιού να επισημοποιηθεί η σχέση πατέρα-τέκνου ήταν επίσης σημαντικοί παράγοντες που συνεκτιμήθηκαν.

Το ΕΔΔΑ αποφάνθηκε ότι η δημοσίευση της συνέντευξης συνιστούσε επέμβαση στην ιδιωτική ζωή του πρίγκιπα και εξέτασε, ακολούθως, αν η επέμβαση ήταν αναγκαία. Έκρινε ότι η δημοσίευση αφορούσε δημόσιο πρόσωπο και θέμα δημόσιου συμφέροντος, δεδομένου ότι οι πολίτες του Μονακό είχαν συμφέρον να γνωρίζουν την ύπαρξη τέκνου του πρίγκιπα, καθώς το μέλλον ενός κληρονομικού μονάρχη «συνδέεται αναπόσπαστα με την ύπαρξη διαδόχων» και αποτελεί, επομένως, θέμα

93 ΕΔΔΑ, *Couderc και Hachette Filipacchi Associés κατά Γαλλίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 40454/07, 10 Νοεμβρίου 2015.

το οποίο ενδιαφέρει το κοινό⁹⁴. Το ΕΔΔΑ επισήμανε επίσης ότι το άρθρο είχε παράσχει στη N. Coste και στο παιδί της τη δυνατότητα να ασκήσουν το δικαίωμά τους στην ελευθερία της έκφρασης. Τα εθνικά δικαστήρια δεν είχαν λάβει δεόντως υπόψη τις αρχές και τα κριτήρια που έχουν αναπτυχθεί από τη νομολογία του ΕΔΔΑ για τη στάθμιση του δικαιώματος στον σεβασμό της ιδιωτικής ζωής και του δικαιώματος στην ελευθερία της έκφρασης. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι η Γαλλία παρέβη το άρθρο 10 της ΕΣΔΑ σχετικά με την ελευθερία έκφρασης.

Στη νομολογία του ΕΔΔΑ, ένα από το κρίσιμα κριτήρια για τη στάθμιση των δικαιωμάτων αυτών είναι αν η επίμαχη έκφραση συμβάλλει ή όχι σε διάλογο για θέμα γενικού δημόσιου συμφέροντος.

Παράδειγμα: Στην υπόθεση *Mosley κατά Ηνωμένου Βασιλείου*⁹⁵, πανεθνικής κυκλοφορίας εβδομαδιαία εφημερίδα δημοσίευσε φωτογραφίες του προσφεύγοντος, γνωστού προσώπου, σε άκρως ιδιωτικές στιγμές, και εκείνος στη συνέχεια άσκησε αγωγή κατά του εκδότη, η οποία έγινε δεκτή, με αποτέλεσμα να του επιδικαστεί αποζημίωση. Παρά τη χρηματική αποζημίωση που του επιδικάστηκε, ο προσφεύγων παραπονέθηκε ότι παρέμενε θύμα παραβίασης του δικαιώματός του στην ιδιωτική ζωή, καθώς στερήθηκε τη δυνατότητα να υποβάλει αίτηση ασφαλιστικών μέτρων για την έκδοση απαγόρευσης πριν από τη δημοσίευση των επίμαχων φωτογραφιών λόγω της ανυπαρξίας νομικής υποχρέωσης της εφημερίδας να τον ενημερώσει εκ των προτέρων για την επικείμενη δημοσίευση.

Το ΕΔΔΑ επισήμανε ότι, παρότι το υλικό αυτό δημοσιεύθηκε κυρίως για ψυχαγωγικούς και όχι εκπαιδευτικούς σκοπούς, η δημοσίευσή του έχαιρε αναμφίβολα της προστασίας που προβλέπεται στο άρθρο 10 της ΕΣΔΑ, η οποία ενδέχεται να υποχωρεί εάν πληρούνται οι προϋποθέσεις του άρθρου 8 της ΕΣΔΑ, όταν οι πληροφορίες είναι ιδιωτικής και προσωπικής φύσης και η δημοσίευσή τους δεν εξυπηρετεί δημόσιο συμφέρον. Ωστόσο, απαιτείται να εξετάζονται με ιδιαίτερη προσοχή περιορισμοί οι οποίοι ενδέχεται να λειτουργούν ως μορφή λογοκρισίας προ της δημοσίευσης.

94 Ό.π., σκέψεις 104-116.

95 ΕΔΔΑ, *Mosley κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 48009/08, 10 Μαΐου 2011, σκέψεις 129 και 130.

Λαμβάνοντας υπόψη το αποτρεπτικό αποτέλεσμα (chilling effect) που θα μπορούσε να έχει η απαίτηση εκ των προτέρων γνωστοποίησης, τις αμφιβολίες σχετικά με την αποτελεσματικότητά της και το ευρύ περιθώριο εκτίμησης στον τομέα αυτόν, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι δεν απαιτείται δυνάμει του άρθρου 8 η ύπαρξη νομικά δεσμευτικής υποχρέωσης εκ των προτέρων γνωστοποίησης. Κατά συνέπεια, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι δεν υπήρξε παράβαση του άρθρου 8.

Παράδειγμα: Στην υπόθεση *Bohlen κατά Γερμανίας*⁹⁶, ο προσφεύγων, γνωστός τραγουδιστής και καλλιτεχνικός παραγωγός, είχε δημοσιεύσει την αυτοβιογραφία του και αναγκάστηκε, ακολούθως, να αφαιρέσει ορισμένα αποσπάσματα από το βιβλίο κατόπιν δικαστικών αποφάσεων. Η υπόθεση καλύφθηκε ευρέως από τα εθνικά μέσα ενημέρωσης και μια καπνοβιομηχανία παρουσίασε χιουμοριστική διαφημιστική εκστρατεία η οποία παρέπεμπε στο γεγονός αυτό, κάνοντας χρήση του ονόματος του προσφεύγοντος χωρίς τη συγκατάθεσή του. Ο προσφεύγων άσκησε, ανεπιτυχώς, αγωγή αποζημίωσης κατά της διαφημιστικής εταιρείας, επικαλούμενος παραβίαση των δικαιωμάτων του που απορρέουν από το άρθρο 8 της ΕΣΔΑ. Το ΕΔΔΑ επανέλαβε τα κριτήρια που εφαρμόζονται για τη στάθμιση του δικαιώματος στον σεβασμό της ιδιωτικής ζωής με το δικαίωμα στην ελευθερία της έκφρασης και αποφάνθηκε ότι δεν υπήρξε παράβαση του άρθρου 8. Ο προσφεύγων ήταν δημόσιο πρόσωπο και η διαφήμιση δεν παρέπεμπε σε λεπτομέρειες της ιδιωτικής ζωής του, αλλά σε ευρέως γνωστό γεγονός το οποίο είχε ήδη καλυφθεί από τα μέσα ενημέρωσης και αποτελούσε μέρος δημόσιου διαλόγου. Επιπλέον, η διαφήμιση είχε χιουμοριστικό χαρακτήρα και δεν περιείχε κανένα προσβλητικό ή αρνητικό στοιχείο όσον αφορά τον προσφεύγοντα.

Παράδειγμα: Στην υπόθεση *Biriuk κατά Λιθουανίας*⁹⁷, η προσφεύγουσα υποστήριξε ενώπιον του ΕΔΔΑ ότι η Λιθουανία παρέβη την υποχρέωσή της να διασφαλίσει τον σεβασμό του δικαιώματός της στην ιδιωτική ζωή, επειδή, παρότι διαπράχθηκε σοβαρή παραβίαση της ιδιωτικής της ζωής από μεγάλη εφημερίδα, τα εθνικά δικαστήρια που επιλήφθηκαν της υπόθεσης της επιδίκασαν ασήμαντη χρηματική αποζημίωση. Κατά την επιδίκαση της αποζημίωσης για ηθική βλάβη, τα εθνικά δικαστήρια είχαν εφαρμόσει τις διατάξεις της εθνικής νομοθεσίας περί παροχής

96 ΕΔΔΑ, *Bohlen κατά Γερμανίας*, προσφυγή αριθ. 53495/09, 19 Φεβρουαρίου 2015, σκέψεις 45-60.

97 ΕΔΔΑ, *Biriuk κατά Λιθουανίας*, προσφυγή αριθ. 23373/03, 25 Νοεμβρίου 2008.

πληροφοριών στο κοινό, η οποία προέβλεπε χαμηλό ανώτατο όριο αποζημίωσης για ηθική βλάβη προκληθείσα λόγω της παράνομης δημοσιοποίησης από τα μέσα ενημέρωσης πληροφοριών σχετικά με την ιδιωτική ζωή προσώπου. Η υπόθεση ανέκυψε λόγω της δημοσίευσης από τη μεγαλύτερη ημερήσια εφημερίδα της Λιθουανίας πρωτοσέλιδου άρθρου στο οποίο αναφερόταν ότι η προσφεύγουσα είχε προσβληθεί από τον ιό HIV. Το άρθρο επέκρινε επίσης τη συμπεριφορά της προσφεύγουσας και ήγγειρε αμφιβολίες όσον αφορά την ηθική της.

Το ΕΔΔΑ υπενθύμισε ότι η προστασία των δεδομένων προσωπικού χαρακτήρα, και κυρίως των ιατρικών δεδομένων, είναι θεμελιώδους σημασίας για τη διαφύλαξη του δικαιώματος στον σεβασμό της ιδιωτικής ζωής βάσει της ΕΣΔΑ. Ο εμπιστευτικός χαρακτήρας των δεδομένων που αφορούν την υγεία είναι ιδιαίτερα σημαντικό να γίνεται σεβαστός, δεδομένου ότι η δημοσιοποίηση ιατρικών δεδομένων (εν προκειμένω, του γεγονότος ότι η προσφεύγουσα είχε προσβληθεί από τον HIV) μπορεί να επηρεάσει σημαντικά την ιδιωτική και οικογενειακή ζωή του προσώπου, την επαγγελματική του κατάσταση και την ένταξή του στην κοινωνία. Το ΕΔΔΑ απέδωσε ιδιαίτερη σημασία στο γεγονός ότι, σύμφωνα με το άρθρο της εφημερίδας, το ιατρικό προσωπικό του νοσοκομείου είχε παράσχει πληροφορίες σχετικά με το γεγονός ότι η προσφεύγουσα είχε προσβληθεί από τον HIV κατά πρόδηλη παράβαση της υποχρέωσής του να τηρεί το ιατρικό απόρρητο. Επομένως, η επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής της προσφεύγουσας δεν ήταν θεμιτή.

Το άρθρο είχε δημοσιευθεί στον Τύπο, και η ελευθερία της έκφρασης είναι επίσης θεμελιώδες δικαίωμα βάσει της ΕΣΔΑ. Ωστόσο, όταν εξέτασε αν η ύπαρξη δημόσιου συμφέροντος δικαιολογούσε τη δημοσίευση τέτοιου είδους πληροφοριών σχετικά με την προσφεύγουσα, το ΕΔΔΑ διαπίστωσε ότι ο κύριος σκοπός της δημοσίευσης ήταν η αύξηση των πωλήσεων της εφημερίδας ικανοποιώντας την περιέργεια των αναγνωστών. Ένας τέτοιος σκοπός δεν θα μπορούσε να θεωρηθεί ότι συμβάλλει σε οποιονδήποτε διάλογο γενικού ενδιαφέροντος χρήσιμο για την κοινωνία. Καθώς επρόκειτο για περίπτωση «απαράδεκτης κατάχρησης της ελευθερίας του Τύπου», οι σοβαροί περιορισμοί στην αποκατάσταση της ζημίας και το χαμηλό ποσό της αποζημίωσης για ηθική βλάβη που προβλέπονταν στην εθνική νομοθεσία σήμαιναν ότι η Λιθουανία παρέβη τη θετική υποχρέωσή της να προστατεύσει το δικαίωμα της προσφεύγουσας στον σεβασμό της ιδιωτικής ζωής της. Το ΕΔΔΑ έκρινε ότι υπήρξε παράβαση του άρθρου 8 της ΕΣΔΑ.

Το δικαίωμα στην ελευθερία της έκφρασης και το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν αντιτίθενται πάντοτε το ένα στο άλλο. Υπάρχουν περιπτώσεις στις οποίες η αποτελεσματική προστασία των δεδομένων προσωπικού χαρακτήρα διασφαλίζει την ελευθερία της έκφρασης.

Παράδειγμα: Το ΔΕΕ στην υπόθεση *Tele2 Sverige* έκρινε ότι η επέμβαση με βάση την οδηγία 2006/24 (οδηγία για τη διατήρηση δεδομένων) στα θεμελιώδη δικαιώματα που καθιερώνουν τα άρθρα 7 και 8 του Χάρτη έχει «τεράστιο εύρος και πρέπει να θεωρηθεί ως ιδιαίτερως σοβαρή. Πέραν τούτου, το γεγονός ότι η διατήρηση δεδομένων και η εν συνεχεία χρήση τους πραγματοποιούνται χωρίς ο συνδρομητής ή ο εγγεγραμμένος χρήστης να ενημερώνονται σχετικώς μπορεί να προκαλέσει στα οικεία πρόσωπα την αίσθηση ότι η ιδιωτική τους ζωή αποτελεί το αντικείμενο διαρκούς παρακολούθησής τους». Το ΔΕΕ αποφάνθηκε επίσης ότι η γενικευμένη διατήρηση δεδομένων κίνησης και θέσης θα μπορούσε να επηρεάσει τη χρήση των μέσων ηλεκτρονικής επικοινωνίας και, «ως εκ τούτου, την άσκηση από τους χρήστες των εν λόγω μέσων της ελευθερίας τους εκφράσεως την οποία κατοχυρώνει το άρθρο 11 του Χάρτη»⁹⁸. Υπ' αυτή την έννοια, απαιτώντας αυστηρές εγγυήσεις προκειμένου τα δεδομένα να μη διατηρούνται κατά γενικό τρόπο, οι κανόνες περί προστασίας δεδομένων συμβάλλουν εντέλει στην άσκηση της ελευθερίας της έκφρασης.

Όσον αφορά το δικαίωμα λήψης πληροφοριών, το οποίο αποτελεί επίσης μέρος της ελευθερίας της έκφρασης, η συνειδητοποίηση της σημασίας της διαφάνειας στο κράτος για τη λειτουργία μιας δημοκρατικής κοινωνίας αυξάνεται. Η διαφάνεια αποτελεί στόχο γενικού ενδιαφέροντος ο οποίος θα μπορούσε, επομένως, να δικαιολογήσει επέμβαση στο δικαίωμα στην προστασία των δεδομένων, εάν αυτή είναι αναγκαία και ανάλογη, όπως εξηγείται στην [ενότητα 1.2](#). Επομένως, κατά την τελευταία εικοσαετία η πρόσβαση σε έγγραφα που κατέχουν δημόσιες αρχές έχει αναγνωριστεί ως σημαντικό δικαίωμα κάθε πολίτη της ΕΕ καθώς και

⁹⁸ ΔΕΕ, συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, *Tele2 Sverige AB κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson κ.λπ.* [τμήμα μείζονος συνθέσεως], 21 Δεκεμβρίου 2016, σκέψεις 37 και 101· ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014, σκέψη 28.

κάθε φυσικού ή νομικού προσώπου που κατοικεί ή έχει την καταστατική έδρα του σε κράτος μέλος.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, μπορεί να γίνεται παραπομπή στις αρχές που κατοχυρώνονται στη σύσταση για την πρόσβαση σε επίσημα έγγραφα, που αποτέλεσε πηγή έμπνευσης για τους συντάκτες της Σύμβασης για την πρόσβαση σε επίσημα έγγραφα (Σύμβαση 205)⁹⁹.

Βάσει του δικαίου της ΕΕ, το δικαίωμα πρόσβασης στα έγγραφα κατοχυρώνεται στον κανονισμό αριθ. 1049/2001 για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής (κανονισμός για την πρόσβαση στα έγγραφα)¹⁰⁰. Το άρθρο 42 του Χάρτη και το άρθρο 15 παράγραφος 3 της ΣΛΕΕ επέκτειναν αυτό το δικαίωμα πρόσβασης «στα έγγραφα των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, ανεξαρτήτως υποθέματος».

Το δικαίωμα αυτό μπορεί να έρχεται σε σύγκρουση με το δικαίωμα στην προστασία των δεδομένων εάν η πρόσβαση σε έγγραφο αποκαλύπτει τα δεδομένα προσωπικού χαρακτήρα τρίτων. Το άρθρο 86 του Γενικού Κανονισμού για την Προστασία Δεδομένων ορίζει σαφώς ότι τα δεδομένα προσωπικού χαρακτήρα που περιέχονται σε επίσημα έγγραφα τα οποία κατέχει δημόσια αρχή ή δημόσιος φορέας μπορούν να κοινοποιούνται από την εν λόγω αρχή ή φορέα σύμφωνα με το δίκαιο της Ένωσης¹⁰¹ ή του κράτους μέλους, προκειμένου να συμβιβάζεται η πρόσβαση του κοινού σε επίσημα έγγραφα με το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού.

Επομένως, τα αιτήματα πρόσβασης σε έγγραφα ή πληροφορίες που κατέχουν δημόσιες αρχές ενδέχεται να χρειάζεται να σταθμιστούν με το δικαίωμα στην προστασία δεδομένων των προσώπων των οποίων τα δεδομένα περιέχονται στα ζητούμενα έγγραφα.

99 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2002), Σύσταση αριθ. R (81)19 και σύσταση αριθ. R (2002)2 στα κράτη μέλη σχετικά με την πρόσβαση σε επίσημα έγγραφα, 21 Φεβρουαρίου 2002· Συμβούλιο της Ευρώπης, Σύμβαση για την πρόσβαση σε επίσημα έγγραφα, CETS No. 205, 18 Ιουνίου 2009. Η εν λόγω Σύμβαση δεν έχει τεθεί ακόμη σε ισχύ.

100 Κανονισμός (ΕΚ) αριθ. 1049/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 30ής Μαΐου 2001, για την πρόσβαση του κοινού στα έγγραφα του Ευρωπαϊκού Κοινοβουλίου, του Συμβουλίου και της Επιτροπής (ΕΕ L 145 της 31.5.2001, σ. 43).

101 Άρθρο 42 του Χάρτη, άρθρο 15 παράγραφος 3 της ΣΛΕΕ και κανονισμός αριθ. 1049/2009.

Παράδειγμα: Στην υπόθεση *Volker und Markus Schecke και Hartmut Eifert κατά Land Hessen*¹⁰², το ΔΕΕ κλήθηκε να αξιολογήσει την αναλογικότητα της δημοσίευσης, η οποία επιβάλλεται από τη νομοθεσία της ΕΕ, του ονόματος των δικαιούχων γεωργικών επιδοτήσεων της ΕΕ και των ποσών που έλαβαν. Σκοπός της δημοσιοποίησης ήταν να βελτιώσει τη διαφάνεια και να συμβάλει στον δημόσιο έλεγχο της κατάλληλης χρήσης των δημόσιων πόρων από τη διοίκηση. Αρκετοί δικαιούχοι αμφισβήτησαν την αναλογικότητα της δημοσιοποίησης αυτής.

Επισημαίνοντας ότι το δικαίωμα στην προστασία των δεδομένων δεν είναι απόλυτο, το ΔΕΕ διευκρίνισε ότι η δημοσιοποίηση, σε ισότοπο, δεδομένων στα οποία κατονομάζονται οι δικαιούχοι δύο ταμείων γεωργικών ενισχύσεων της ΕΕ και των ακριβών ποσών που έλαβαν συνιστά επέμβαση στην ιδιωτική ζωή τους, γενικά, και στην προστασία των δεδομένων προσωπικού χαρακτήρα που τους αφορούν, ειδικότερα.

Το Δικαστήριο έκανε δεκτό ότι η εν λόγω παρέμβαση στα δικαιώματα των άρθρων 7 και 8 του Χάρτη προβλέπεται από τον νόμο και ανταποκρίνεται σε σκοπό γενικού συμφέροντος που αναγνωρίζει η ΕΕ, δηλαδή αποσκοπεί μεταξύ άλλων στην αύξηση της διαφάνειας όσον αφορά τη χρήση των κοινοτικών κονδυλίων. Το ΔΕΕ, πάντως, έκρινε ότι η δημοσιοποίηση των ονομάτων των φυσικών προσώπων που είναι δικαιούχοι γεωργικών ενισχύσεων από τα δύο ταμεία της ΕΕ και των συγκεκριμένων ποσών που λαμβάνουν είναι μέτρο που υπερβαίνει τα όρια της αναλογικότητας και δεν δικαιολογείται κατά το άρθρο 52 παράγραφος 1 του Χάρτη. Το ΔΕΕ αναγνώρισε τη σημασία, σε μια δημοκρατική κοινωνία, της ενημέρωσης των φορολογουμένων σχετικά με τη χρήση των δημόσιων πόρων. Ωστόσο, δεδομένου ότι «[δ]εν αναγνωρίζεται [...] αυτομάτως, υπεροχή του σκοπού της διαφάνειας έναντι του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα»¹⁰³, τα θεσμικά όργανα της ΕΕ οφείλουν να σταθμίζουν το συμφέρον της Ένωσης για διασφάλιση διαφάνειας και τον περιορισμό της άσκησης των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων τον οποίο υφίστανται οι δικαιούχοι ως αποτέλεσμα της δημοσιοποίησης.

¹⁰² ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, *Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen* [τμήμα μείζονος συνθέσεως], 9 Νοεμβρίου 2010, σκέψεις 47-52, 58, 66-67, 75, 86 και 92.

¹⁰³ Ό.π., σκέψη 85.

Το ΔΕΕ έκρινε ότι τα θεσμικά όργανα της ΕΕ δεν προέβησαν δεόντως στην ισόρροπη αυτή στάθμιση, δεδομένου ότι ήταν δυνατόν να προβλεφθούν μέτρα που θα έθιγαν σε μικρότερο βαθμό τα θεμελιώδη δικαιώματα των φυσικών προσώπων, συμβάλλοντας ταυτόχρονα κατά τρόπο αποτελεσματικό στον σκοπό της διαφάνειας που επιδιώκεται με τη δημοσιοποίηση. Για παράδειγμα, αντί της γενικής δημοσιοποίησης που επηρεάζει όλους τους δικαιούχους, η οποία παρέχει το όνομα και τα ακριβή ποσά που έλαβε έκαστος εξ αυτών, θα μπορούσε να γίνει διάκριση βάσει σχετικών κριτηρίων, όπως οι περίοδοι κατά τις οποίες τα εν λόγω πρόσωπα έλαβαν την ενίσχυση, η συχνότητα της ενίσχυσης ή το ύψος και το είδος της ¹⁰⁴. Επομένως, το ΔΕΕ κήρυξε εν μέρει ανίσχυρη τη νομοθεσία της ΕΕ σχετικά με τη δημοσιοποίηση πληροφοριών που αφορούν τους δικαιούχους ευρωπαϊκών γεωργικών ταμείων.

Παράδειγμα: Στην υπόθεση *Rechnungshof κατά Österreichischer Rundfunk κ.λπ.* ¹⁰⁵, το ΔΕΕ έλεγξε τη συμβατότητα ορισμένων αυστριακών νομοθετικών πράξεων με το δίκαιο της ΕΕ για την προστασία των δεδομένων. Η νομοθεσία υποχρέωνε κρατικό φορέα να συλλέγει και να διαβιβάζει δεδομένα σχετικά με το εισόδημα για σκοπούς δημοσιοποίησης του ονόματος και του εισοδήματος των υπαλλήλων διαφόρων δημόσιων οντοτήτων σε ετήσια έκθεση που επρόκειτο να καταστεί διαθέσιμη στο ευρύτερο κοινό. Ορισμένα φυσικά πρόσωπα αρνήθηκαν να γνωστοποιήσουν τα δεδομένα που τα αφορούσαν, επικαλούμενα την προστασία των δεδομένων.

Στην απόφασή του, το ΔΕΕ επικαλέστηκε την προστασία των θεμελιωδών δικαιωμάτων ως γενική αρχή του δικαίου της ΕΕ και το άρθρο 8 της ΕΣΔΑ, υπενθυμίζοντας ότι ο Χάρτης δεν είχε τότε δεσμευτικό χαρακτήρα. Αποφάνθηκε ότι η συλλογή δεδομένων σχετικά με τα εισοδήματα ενός ατόμου από άσκηση επαγγέλματος, και ιδίως η γνωστοποίησή τους σε τρίτους, εμπίπτει στο πεδίο του δικαιώματος στον σεβασμό της ιδιωτικής ζωής και συνιστά παραβίαση του δικαιώματος αυτού. Η επέμβαση θα μπορούσε να είναι δικαιολογημένη εάν προβλεπόταν από τον νόμο, επιδίωκε θεμιτό σκοπό και ήταν αναγκαία σε μια δημοκρατική κοινωνία για την επίτευξη του σκοπού αυτού. Το ΔΕΕ επισήμανε ότι η αυστριακή

104 Ό.π., σκέψη 89.

105 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-465/00, C-138/01 και C-139/01, *Rechnungshof κατά Österreichischer Rundfunk κ.λπ.* και *Christa Neukomm και Joseph Laueremann κατά Österreichischer Rundfunk*, 20 Μαΐου 2003.

νομοθεσία επιδίωκε θεμιτό σκοπό, καθώς αποσκοπούσε στη διατήρηση των αποδοχών των δημόσιων υπαλλήλων εντός εύλογων ορίων –μέτρο το οποίο συνδέεται επίσης με την οικονομική ευημερία της χώρας. Ωστόσο, το ενδιαφέρον της Αυστρίας να διασφαλίσει τη βέλτιστη χρήση των δημόσιων πόρων έπρεπε να σταθμιστεί με τη σοβαρότητα της επέμβασης στο δικαίωμα των ενδιαφερόμενων προσώπων στον σεβασμό της ιδιωτικής ζωής τους.

Μολονότι διευκρίνισε ότι εναπόκειται στο εθνικό δικαστήριο να διαπιστώσει αν η δημοσιοποίηση των δεδομένων σχετικά με τα εισοδήματα φυσικών προσώπων ήταν αναγκαίο και ανάλογο μέτρο για τον επιδιωκόμενο από τη νομοθεσία σκοπό, το ΔΕΕ ζήτησε από το εθνικό δικαστήριο να εξετάσει αν ένας τέτοιος σκοπός θα μπορούσε να είχε υπηρετηθεί εξίσου αποτελεσματικά με λιγότερο παρεμβατικό τρόπο. Παράδειγμα θα μπορούσε να αποτελέσει η διαβίβαση των δεδομένων προσωπικού χαρακτήρα μόνο στα αρμόδια όργανα ελέγχου και όχι στο ευρύτερο κοινό.

Σε μεταγενέστερες υποθέσεις, κατέστη πρόδηλο ότι η στάθμιση της προστασίας των δεδομένων και της πρόσβασης σε έγγραφα απαιτεί λεπτομερή κατά περίπτωση ανάλυση. Κανένα από τα δικαιώματα δεν υπερισχύει αυτομάτως του άλλου. Το ΔΕΕ είχε την ευκαιρία να ερμηνεύσει το δικαίωμα πρόσβασης σε έγγραφα που περιείχαν δεδομένα προσωπικού χαρακτήρα σε δύο υποθέσεις.

Παράδειγμα: Στην υπόθεση *Ευρωπαϊκή Επιτροπή κατά Bavarian Lager* ¹⁰⁶, το ΔΕΕ καθόρισε την εμβέλεια της προστασίας των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της πρόσβασης σε έγγραφα των θεσμικών οργάνων της ΕΕ και τη σχέση μεταξύ του κανονισμού αριθ. 1049/2001 (κανονισμός για την πρόσβαση στα έγγραφα) και του κανονισμού αριθ. 45/2001 (κανονισμός για την προστασία δεδομένων από τα όργανα της ΕΕ). Η Bavarian Lager, η οποία ιδρύθηκε το 1992, εισάγει εμφιαλωμένο γερμανικό ζύθο στο Ηνωμένο Βασίλειο, κυρίως για ποτοπωλεία. Ωστόσο, αντιμετώπισε δυσκολίες επειδή η βρετανική νομοθεσία ευνοούσε εκ των πραγμάτων τους εθνικούς παραγωγούς. Κατόπιν καταγγελίας της Bavarian Lager, η Ευρωπαϊκή Επιτροπή κίνησε κατά του Ηνωμένου

¹⁰⁶ ΔΕΕ, C-28/08 Ρ, *Ευρωπαϊκή Επιτροπή κατά The Bavarian Lager Co. Ltd.* [τμήμα μείζονος συνθέσεως], 29 Ιουνίου 2010.

Βασιλείου διαδικασία παράβασης, η οποία είχε ως αποτέλεσμα την τροποποίηση των επίμαχων διατάξεων και την ευθυγράμμισή τους με το δίκαιο της ΕΕ. Η Bavarian Lager ζήτησε ακολούθως από την Επιτροπή, μεταξύ άλλων εγγράφων, αντίγραφο των πρακτικών συνεδρίασης στην οποία έλαβαν μέρος εκπρόσωποι της Επιτροπής, των βρετανικών αρχών και της Confédération des Brasseurs du Marché Commun (CBMC). Η Επιτροπή δέχθηκε να γνωστοποιήσει ορισμένα έγγραφα σχετικά με τη συνεδρίαση, αλλά παρέλειψε πέντε ονόματα τα οποία περιείχονταν στα πρακτικά –καθώς δύο πρόσωπα αντιτάχθηκαν ρητώς στη γνωστοποίηση της ταυτότητάς τους, η δε Επιτροπή δεν μπόρεσε να επικοινωνήσει με τα τρία άλλα πρόσωπα. Με απόφαση της 18ης Μαρτίου 2004, η Επιτροπή απέρριψε νέο αίτημα της Bavarian Lager για τη γνωστοποίηση των πλήρων πρακτικών της συνεδρίασης, επικαλούμενη ιδίως την προστασία της ιδιωτικής ζωής των εν λόγω προσώπων, όπως διασφαλίζεται από τον κανονισμός για την προστασία δεδομένων από τα όργανα της ΕΕ.

Δυσανεστημένη από την απόφαση αυτή, η Bavarian Lager προσέφυγε ενώπιον του Πρωτοδικείου. Το Πρωτοδικείο ακύρωσε την απόφαση της Επιτροπής, με την απόφασή του της 8ης Νοεμβρίου 2007 (υπόθεση T-194/04, *The Bavarian Lager Co. Ltd κατά Επιτροπής των Ευρωπαϊκών Κοινοτήτων*), κρίνοντας ότι η απλή αναγραφή των επίμαχων ονομάτων των προσώπων που έλαβαν μέρος σε συνεδρίαση για λογαριασμό του φορέα που εκπροσωπούσαν ουδόλως προσέβαλλε τον σεβασμό της ιδιωτικής ζωής τους, ούτε την έθιγε.

Κατόπιν άσκησης αίτησης αναίρεσης από την Επιτροπή, το ΔΕΕ αναίρεσε την απόφαση του Πρωτοδικείου. Το ΔΕΕ αποφάνθηκε ότι ο κανονισμός για την πρόσβαση στα έγγραφα καθιερώνει «ειδικό καθεστώς ενισχυμένης προστασίας των προσώπων, τα δεδομένα προσωπικού χαρακτήρα των οποίων είναι δυνατόν, κατά περίπτωση, να γνωστοποιηθούν στο κοινό». Κατά το ΔΕΕ, όταν αίτηση η οποία βασίζεται στον κανονισμό για την πρόσβαση στα έγγραφα αποσκοπεί στην πρόσβαση σε έγγραφα που περιέχουν δεδομένα προσωπικού χαρακτήρα, οι διατάξεις του κανονισμού για την προστασία δεδομένων από τα όργανα της ΕΕ εφαρμόζονται πλήρως. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι ορθώς η Επιτροπή είχε απορρίψει την αίτηση πρόσβασης στα πλήρη πρακτικά της συνεδρίασης του Οκτωβρίου του 1996. Απουσία της συγκατάθεσης των πέντε συμμετεχόντων στην εν λόγω συνεδρίαση, η Επιτροπή συμμορφώθηκε επαρκώς με την υποχρέωση διαφάνειας που υπέχει παρέχοντας έκδοση του επίμαχου εγγράφου στην οποία είχαν παραλειφθεί τα ονόματά τους.

Επιπλέον, κατά το ΔΕΕ, «δεδομένου ότι η Bavarian Lager δεν προέβαλε καμία ρητή και θεμιτή δικαιολογία ούτε κάποιο πειστικό επιχειρήμα προκειμένου να αποδείξει την αναγκαιότητα διαβίβασης των εν λόγω δεδομένων προσωπικού χαρακτήρα, η Επιτροπή δεν μπόρεσε να σταθμίσει τα διάφορα διακυβευόμενα συμφέροντα των διαδίκων. Δεν μπορούσε ακόμη να ελέγξει αν συνέτρεχε λόγος να γίνει δεκτό ότι η διαβίβαση αυτή μπορούσε να θίξει τα έννομα συμφέροντα των υποκειμένων των δεδομένων», όπως ορίζεται στον κανονισμό για την προστασία δεδομένων από τα όργανα της ΕΕ.

Παράδειγμα: Στην υπόθεση *Client Earth και PAN Europe κατά EFSA* ¹⁰⁷, το ΔΕΕ εξέτασε αν η απόφαση της Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων (EFSA) να αρνηθεί την πλήρη πρόσβαση των αιτούντων σε έγγραφα ήταν αναγκαία για την προστασία των δικαιωμάτων στην ιδιωτική ζωή και στην προστασία των δεδομένων των προσώπων στα οποία αναφέρονταν τα εν λόγω έγγραφα. Τα έγγραφα αφορούσαν σχέδιο κατευθυντήριας οδηγίας το οποίο είχε εκπονήσει ομάδα εργασίας της EFSA σε συνεργασία με εξωτερικούς πραγματογνώμονες σχετικά με τη διάθεση προϊόντων φυτοπροστασίας στην αγορά. Αρχικά, η EFSA επέτρεψε την πρόσβαση των αιτούντων σε μέρος των εγγράφων, ενώ αρνήθηκε την πρόσβαση σε διαδοχικά κείμενα του σχεδίου κατευθυντήριας οδηγίας. Ακολούθως, επέτρεψε την πρόσβαση στο σχέδιο το οποίο περιλάμβανε τις ατομικές παρατηρήσεις των εξωτερικών πραγματογνωμόνων. Ωστόσο, δεν γνωστοποίησε τα ονόματα των πραγματογνωμόνων επικαλούμενη το άρθρο 4 παράγραφος 1 στοιχείο β) του κανονισμού αριθ. 45/2001 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα και τους οργανισμούς της ΕΕ και την ανάγκη προστασίας της ιδιωτικής ζωής των εξωτερικών πραγματογνωμόνων. Σε πρώτο βαθμό, το Γενικό Δικαστήριο της ΕΕ επικύρωσε την απόφαση της EFSA.

Κατόπιν άσκησης αίτησης αναίρεσης από τους προσφεύγοντες, το ΔΕΕ αναίρεσε την πρωτόδικη απόφαση. Κατέληξε στο συμπέρασμα ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα στη συγκεκριμένη υπόθεση ήταν αναγκαία προκειμένου να διαπιστωθεί η αμεροληψία καθενός εκ των εξωτερικών εμπειρογνομήνων κατά την εκτέλεση των καθηκόντων τους ως επιστημόνων και να διασφαλισθεί η διαφάνεια της διαδικασίας λήψης αποφάσεων της EFSA. Κατά το ΔΕΕ, η EFSA

¹⁰⁷ ΔΕΕ, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) κατά Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων (EFSA)*, Ευρωπαϊκή Επιτροπή, 16 Ιουλίου 2015.

δεν διευκρίνισε με ποιον τρόπο η γνωστοποίηση των ονομάτων των εξωτερικών εμπειρογνομόνων που είχαν διατυπώσει συγκεκριμένες παρατηρήσεις επί του σχεδίου κατευθυντήριας οδηγίας θα έθιγε τα νόμιμα συμφέροντα των εμπειρογνομόνων. Το γενικό επιχείρημα ότι η γνωστοποίηση ενδέχεται να θίγει την ιδιωτική ζωή δεν αρκεί εάν δεν υποστηρίζεται από συγκεκριμένες αποδείξεις που αφορούν ειδικά κάθε περίπτωση.

Σύμφωνα με τις αποφάσεις αυτές, η επέμβαση στο δικαίωμα στην προστασία δεδομένων στο πλαίσιο της πρόσβασης σε έγγραφα πρέπει να στηρίζεται σε ειδικούς και αιτιολογημένους λόγους. Το δικαίωμα πρόσβασης σε έγγραφα δεν μπορεί να υπερισχύει αυτομάτως του δικαιώματος στην προστασία δεδομένων ¹⁰⁸.

Η **προσέγγιση** αυτή είναι παρόμοια με εκείνη την οποία εφαρμόζει το ΕΔΔΑ σε σχέση με την ιδιωτική ζωή και την πρόσβαση στα έγγραφα, όπως καταδεικνύεται από την ακόλουθη απόφαση. Στην απόφαση *Magyar Helsinki*, το ΕΔΔΑ αποφάνθηκε ότι το άρθρο 10 δεν αναγνωρίζει στο φυσικό πρόσωπο δικαίωμα πρόσβασης σε πληροφορίες τις οποίες κατέχει δημόσια αρχή ούτε υποχρεώνει την κυβέρνηση να μεταδίδει τέτοιες πληροφορίες στο φυσικό πρόσωπο. Ωστόσο, τέτοιο δικαίωμα ή υποχρέωση θα μπορούσε να ανακύψει: πρώτον, όταν η γνωστοποίηση των πληροφοριών επιβάλλεται με δικαστική διαταγή η οποία απέκτησε νομική ισχύ· δεύτερον, όταν η πρόσβαση στις πληροφορίες είναι καθοριστικής σημασίας για την άσκηση από το φυσικό πρόσωπο του δικαιώματός του στην ελευθερία της έκφρασης –ιδίως στην ελευθερία της λήψης και της παροχής πληροφοριών– και όταν η άρνηση πρόσβασης θα συνιστούσε επέμβαση στο εν λόγω δικαίωμα ¹⁰⁹. Το κατά πόσον, και σε ποια έκταση, η άρνηση πρόσβασης σε πληροφορίες συνιστά επέμβαση στην ελευθερία της έκφρασης προσφεύγοντος πρέπει να εκτιμάται σε κάθε μεμονωμένη περίπτωση και λαμβανομένων υπόψη των ιδιαίτερων περιστάσεων αυτής, συμπεριλαμβανομένων των εξής: i) του σκοπού του αιτήματος παροχής πληροφοριών· ii) του χαρακτήρα των ζητούμενων πληροφοριών· iii) του ρόλου του προσφεύγοντος· και iv) του κατά πόσον οι πληροφορίες είναι έτοιμες και διαθέσιμες.

¹⁰⁸ Βλ., ωστόσο, τη λεπτομερή ανάλυση του ΕΕΠΔ (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Βρυξέλλες, 24 Μαρτίου 2011.

¹⁰⁹ ΕΔΔΑ, *Magyar Helsinki Bizottság κατά Ουγγαρίας* [Τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 18030/11, 8 Νοεμβρίου 2016, σκέψη 148.

Παράδειγμα: Στην υπόθεση *Magyar Helsinki Bizottság κατά Ουγγαρίας*¹¹⁰, η προσφεύγουσα, ΜΚΟ στον τομέα των ανθρωπίνων δικαιωμάτων, ζήτησε από την αστυνομία πληροφορίες σχετικά με το έργο του αυτεπαγγέλτως ορισθέντος συνηγόρου υπεράσπισης, με σκοπό τη συμπλήρωση μελέτης σχετικά με τη λειτουργία του συστήματος του δημόσιου συνηγόρου στην Ουγγαρία. Η αστυνομία αρνήθηκε να παράσχει τις πληροφορίες, με το επιχείρημα ότι επρόκειτο για δεδομένα προσωπικού χαρακτήρα τα οποία δεν μπορούσαν να δημοσιοποιηθούν. Εφαρμόζοντας τα ανωτέρω κριτήρια, το ΕΔΔΑ αποφάνθηκε ότι υπήρξε επέμβαση στο προστατευόμενο βάσει του άρθρου 10 δικαίωμα. Ειδικότερα, η προσφεύγουσα επιθυμούσε να ασκήσει το δικαίωμα μετάδοσης πληροφοριών σχετικά με θέμα δημόσιου συμφέροντος, είχε ζητήσει πρόσβαση σε πληροφορίες για τον σκοπό αυτόν και οι πληροφορίες ήταν αναγκαίες για την άσκηση του δικαιώματος της προσφεύγουσας στην ελευθερία της έκφρασης. Οι πληροφορίες σχετικά με τον διορισμό δημόσιων συνηγόρων ενδιέφεραν το κοινό. Δεν υπήρχε λόγος να αμφισβητηθεί ότι η επίμαχη μελέτη περιείχε πληροφορίες τις οποίες η προσφεύγουσα αναλάμβανε να μεταδώσει στο κοινό και τις οποίες το κοινό είχε το δικαίωμα να λάβει. Επομένως, το ΕΔΔΑ πείστηκε ότι η πρόσβαση στις ζητηθείσες πληροφορίες ήταν αναγκαία για να μπορέσει η προσφεύγουσα να επιτελέσει το έργο της. Τέλος, οι πληροφορίες ήταν έτοιμες και διαθέσιμες.

Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι η άρνηση πρόσβασης σε πληροφορίες στην υπόθεση αυτή είχε θίξει την ουσία της ελευθερίας λήψης πληροφοριών αυτή καθαυτή. Για να καταλήξει στο συμπέρασμα αυτό, το ΕΔΔΑ εξέτασε ιδίως τον σκοπό των πληροφοριών που ζητήθηκαν και τη συμβολή τους σε σημαντικό δημόσιο διάλογο, τον χαρακτήρα των εν λόγω πληροφοριών και το κατά πόσον εξυπηρετούσαν το δημόσιο συμφέρον και τον ρόλο τον οποίο διαδραμάτιζε στην κοινωνία η προσφεύγουσα στην υπόθεση.

Στο σκεπτικό του, το ΕΔΔΑ επισήμανε ότι η μελέτη της ΜΚΟ αφορούσε τη λειτουργία της δικαιοσύνης και το δικαίωμα σε δίκαιη δίκη, δικαίωμα θεμελιώδους σημασίας στο πλαίσιο της ΕΣΔΑ. Δεδομένου ότι οι ζητηθείσες πληροφορίες δεν αφορούσαν δεδομένα τα οποία δεν ήταν δημοσίως γνωστά, τα δικαιώματα στην ιδιωτική ζωή των ενδιαφερόμενων υποκειμένων των δεδομένων (των αυτεπαγγέλτως

¹¹⁰ Ό.π., σκέψεις 181, 187-200.

οριζόμενων δημόσιων συνηγόρων υπεράσπισης) δεν θα θίγονταν εάν η αστυνομία επρόκειτο να παράσχει στην προσφεύγουσα πρόσβαση στις πληροφορίες. Οι πληροφορίες τις οποίες ζήτησε η προσφεύγουσα ήταν στατιστικού χαρακτήρα, αφορούσαν τον αριθμό των περιπτώσεων στις οποίες είχαν οριστεί αυτεπαγγέλτως συνήγοροι για να εκπροσωπήσουν κατηγορούμενους σε ποινικές δίκες.

Κατά το ΕΔΔΑ, δεδομένου ότι σκοπός της μελέτης ήταν να συμβάλει σε σημαντικό διάλογο σχετικά με ζήτημα γενικού ενδιαφέροντος, κάθε περιορισμός στη σχεδιαζόμενη δημοσίευση της ΜΚΟ έπρεπε να είχε ελεγχθεί διεξοδικά. Οι πληροφορίες που διακυβεύονταν ήταν δημόσιου συμφέροντος, δεδομένου ότι το δημόσιο συμφέρον περιλαμβάνει «θέματα τα οποία είναι ικανά να προκαλέσουν σοβαρές αντιπαραθέσεις, τα οποία αφορούν σημαντικό κοινωνικό ζήτημα ή τα οποία αφορούν πρόβλημα για το οποίο υφίσταται συμφέρον του κοινού να ενημερωθεί»¹¹¹. Επομένως, το δημόσιο συμφέρον θα περιλάμβανε αναμφίβολα συζήτηση σχετικά με την απονομή της δικαιοσύνης και τις δίκαιες δίκες, που ήταν και το αντικείμενο της μελέτης της προσφεύγουσας. Σταθμίζοντας τα διαφορετικά δικαιώματα που διακυβεύονταν και εφαρμόζοντας την αρχή της αναλογικότητας, το ΕΔΔΑ αποφάνθηκε ότι υπήρξε αδικαιολόγητη παραβίαση των δικαιωμάτων της προσφεύγουσας βάσει του άρθρου 10 της ΕΣΔΑ.

1.3.2. Επαγγελματικό απόρρητο

Βάσει του εθνικού δικαίου, ορισμένες επικοινωνίες μπορεί να υπόκεινται σε υποχρέωση επαγγελματικού απορρήτου. Ως επαγγελματικό απόρρητο νοείται ειδικό δεοντολογικό καθήκον το οποίο συνεπάγεται έννομη υποχρέωση εγγενή σε ορισμένα επαγγέλματα και καθήκοντα, τα οποία βασίζονται στην πίστη και στην εμπιστοσύνη. Τα πρόσωπα και τα όργανα που επιτελούν τα καθήκοντα αυτά υποχρεούνται να μη γνωστοποιούν τις εμπιστευτικές πληροφορίες τις οποίες λαμβάνουν κατά την άσκηση των καθηκόντων τους. Το επαγγελματικό απόρρητο ισχύει ιδίως στο ιατρικό και στο δικηγορικό επάγγελμα, ενώ πολλές δικαιοδοσίες αναγνωρίζουν επίσης την υποχρέωση τήρησης επαγγελματικού απορρήτου στον χρηματοπιστωτικό τομέα. Το επαγγελματικό απόρρητο δεν είναι θεμελιώδες δικαίωμα, αλλά προστατεύεται ως έκφανση του δικαιώματος στον

¹¹¹ Ό.π., σκέψη 156.

σεβασμό της ιδιωτικής ζωής. Για παράδειγμα, το ΔΕΕ έχει αποφανθεί ότι, σε ορισμένες περιπτώσεις, «μπορεί να είναι αναγκαίο να απαγορευθεί η δημοσιοποίηση ορισμένων πληροφοριών που χαρακτηρίζονται ως εμπιστευτικές, προκειμένου να προστατευθεί το θεμελιώδες δικαίωμα μιας επιχείρησης στον σεβασμό της ιδιωτικής ζωής, το οποίο κατοχυρώνεται από το άρθρο 8 της ΕΣΔΑ, και από το άρθρο 7 του Χάρτη»¹¹². Το ΕΔΔΑ κλήθηκε επίσης να αποφανθεί αν η επιβολή περιορισμών του επαγγελματικού απορρήτου συνιστά παράβαση του άρθρου 8 της ΕΣΔΑ, όπως φαίνεται στα ακόλουθα χαρακτηριστικά παραδείγματα.

Παράδειγμα: Στην υπόθεση *Pruteanu κατά Roumanίας*¹¹³, ο προσφεύγων ήταν δικηγόρος εμπορικής εταιρείας στην οποία είχε επιβληθεί απαγόρευση διεξαγωγής τραπεζικών συναλλαγών κατόπιν ισχυρισμών περί απάτης. Κατά τη διερεύνηση της υπόθεσης, τα ρουμανικά δικαστήρια επέτρεψαν στις εισαγγελικές αρχές να παρακολουθήσουν και να καταγράψουν τις τηλεφωνικές συνομιλίες εταίρου της εταιρείας για ορισμένο χρονικό διάστημα. Οι καταγραφές και οι παρακολουθήσεις αφορούσαν και τις επικοινωνίες του με τον δικηγόρο του.

Ο κ. Pruteanu ισχυρίστηκε ότι αυτό συνιστούσε επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής και της αλληλογραφίας του. Στην απόφασή του, το ΕΔΔΑ τόνισε το καθεστώς και τη σημασία της σχέσης του δικηγόρου με τον πελάτη του. Η παρακολούθηση των συνομιλιών δικηγόρου με τον πελάτη του αναμφίβολα συνιστούσε παραβίαση του επαγγελματικού απορρήτου, το οποίο αποτελεί τη βάση της σχέσης μεταξύ των δύο αυτών προσώπων. Σε μια τέτοια περίπτωση, ο δικηγόρος μπορούσε επίσης να καταγγείλει επέμβαση στο δικαίωμά του στον σεβασμό της ιδιωτικής ζωής και της αλληλογραφίας του. Το ΔΕΕ έκρινε ότι υπήρξε παράβαση του άρθρου 8 της ΕΣΔΑ.

Παράδειγμα: Στην υπόθεση *Brito Ferrinho Bexiga Villa-Nova κατά Πορτογαλίας*¹¹⁴, η προσφεύγουσα, δικηγόρος, αρνήθηκε να γνωστοποιήσει τα αντίγραφα των προσωπικών τραπεζικών λογαριασμών της στις φορολογικές αρχές επικαλούμενη το επαγγελματικό και τραπεζικό

¹¹² ΔΕΕ, υπόθεση T-462/12 R, *Pilkington Group Ltd κατά Ευρωπαϊκής Επιτροπής*, διάταξη του Προέδρου του Γενικού Δικαστηρίου, 11 Μαρτίου 2013, σκέψη 44.

¹¹³ ΕΔΔΑ, *Pruteanu κατά Roumanίας*, προσφυγή αριθ. 30181/05, 3 Φεβρουαρίου 2015.

¹¹⁴ ΕΔΔΑ, *Brito Ferrinho Bexiga Villa-Nova κατά Πορτογαλίας*, προσφυγή αριθ. 69436/10, 1 Δεκεμβρίου 2015.

απόρρητο. Η εισαγγελική αρχή κίνησε διαδικασία έρευνας για φορολογική απάτη και ζήτησε άδεια αναστολής του επαγγελματικού απορρήτου. Τα εθνικά δικαστήρια διέταξαν την αναστολή των κανόνων περί επαγγελματικού και τραπεζικού απορρήτου, εκτιμώντας ότι το δημόσιο συμφέρον θα πρέπει να υπερισχύσει των ιδιωτικών συμφερόντων της προσφεύγουσας.

Όταν η υπόθεση υποβλήθηκε στο ΕΔΔΑ, αυτό αποφάνθηκε ότι η πρόσβαση στα αντίγραφα τραπεζικών λογαριασμών της προσφεύγουσας συνιστά επέμβαση στο δικαίωμά της στον σεβασμό του επαγγελματικού απορρήτου, το οποίο εμπίπτει στο πεδίο της ιδιωτικής ζωής. Η επέμβαση προβλεπόταν από τον νόμο, δεδομένου ότι βασιζόταν στον κώδικα ποινικής δικονομίας, και επιδίωκε θεμιτό σκοπό. Ωστόσο, εξετάζοντας την αναγκαιότητα και την αναλογικότητα της επέμβασης, το ΕΔΔΑ επισήμανε ότι η διαδικασία άρσης του απορρήτου έλαβε χώρα χωρίς τη συμμετοχή και εν αγνοία της προσφεύγουσας. Επομένως, η προσφεύγουσα δεν μπόρεσε να εκθέσει τα επιχειρήματά της. Επιπλέον, παρότι το εθνικό δίκαιο προέβλεπε ότι στη διαδικασία αυτή έπρεπε να ζητηθεί η γνώμη του δικηγορικού συλλόγου, κάτι τέτοιο δεν είχε συμβεί. Τέλος, η προσφεύγουσα δεν είχε τη δυνατότητα να προσβάλει αποτελεσματικά την άρση του απορρήτου ούτε διέθετε οποιοδήποτε ένδικο βοήθημα με το οποίο να αμφισβητήσει το μέτρο. Λόγω της έλλειψης δικονομικών εγγυήσεων και αποτελεσματικού δικαστικού ελέγχου επί του μέτρου αναστολής του επαγγελματικού απορρήτου, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι υπήρξε παράβαση του άρθρου 8 της ΕΣΔΑ.

Η αλληλεπίδραση μεταξύ του επαγγελματικού απορρήτου και της προστασίας δεδομένων είναι συχνά αμφίσημη. Αφενός, οι κανόνες και οι εγγυήσεις της προστασίας δεδομένων που προβλέπονται στη νομοθεσία συμβάλλουν στη διασφάλιση του επαγγελματικού απορρήτου. Για παράδειγμα, κανόνες οι οποίοι υποχρεώνουν τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να εφαρμόζουν αξιόπιστα μέτρα ασφάλειας των δεδομένων στοχεύουν στην πρόληψη, μεταξύ άλλων, της απώλειας του εμπιστευτικού χαρακτήρα των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από το επαγγελματικό απόρρητο. Επιπλέον, ο Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ παρέχει τη δυνατότητα επεξεργασίας δεδομένων που αφορούν την υγεία, τα οποία αποτελούν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που χρήζουν ισχυρότερης προστασίας, αλλά την εξαρτά από την ύπαρξη

κατάλληλων και συγκεκριμένων μέτρων για τη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων, και ιδίως του επαγγελματικού απορρήτου ¹¹⁵.

Αφετέρου, οι υποχρεώσεις επαγγελματικού απορρήτου που επιβάλλονται στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία σε σχέση με ορισμένα δεδομένα προσωπικού χαρακτήρα ενδέχεται να περιορίζουν τα δικαιώματα των υποκειμένων των δεδομένων, και ιδίως το δικαίωμα λήψης πληροφοριών. Παρότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων περιέχει εκτενή κατάλογο πληροφοριών οι οποίες πρέπει, καταρχήν, να παρέχονται στο υποκείμενο των δεδομένων σε περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα δεν αποκτήθηκαν από το ίδιο, αυτή η απαίτηση γνωστοποίησης δεν ισχύει όταν τα δεδομένα προσωπικού χαρακτήρα πρέπει να παραμείνουν εμπιστευτικά λόγω υποχρέωσης επαγγελματικού απορρήτου η οποία επιβάλλεται είτε από το εθνικό είτε από το ενωσιακό δίκαιο ¹¹⁶.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) προβλέπει τη δυνατότητα των κρατών μελών να θεσπίζουν διά νόμου ειδικούς κανόνες προκειμένου να διαφυλάσσονται οι υποχρεώσεις επαγγελματικού απορρήτου ή άλλες αντίστοιχες υποχρεώσεις απορρήτου, στον βαθμό που αυτό είναι αναγκαίο για τον συμβιβασμό του δικαιώματος στην προστασία δεδομένων προσωπικού χαρακτήρα με την υποχρέωση επαγγελματικού απορρήτου ¹¹⁷.

Ο ΓΚΠΔ προβλέπει ότι τα κράτη μέλη μπορούν να θεσπίσουν ειδικούς κανόνες σχετικά με τις εξουσίες των εποπτικών αρχών ως προς τους υπευθύνους της επεξεργασίας και τους εκτελούντες την επεξεργασία που υπέχουν υποχρέωση επαγγελματικού απορρήτου. Οι ειδικοί αυτοί κανόνες αφορούν την εξουσία εξασφάλισης πρόσβασης στις εγκαταστάσεις υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, στον εξοπλισμό του για την επεξεργασία δεδομένων και στα δεδομένα προσωπικού χαρακτήρα τα οποία κατέχει, όταν τα εν λόγω δεδομένα έχουν ληφθεί στο πλαίσιο δραστηριότητας που καλύπτεται από την υποχρέωση τήρησης απορρήτου. Επομένως, οι εποπτικές αρχές στις οποίες έχει ανατεθεί η προστασία των δεδομένων οφείλουν να σέβονται τις υποχρεώσεις επαγγελματικού απορρήτου που δεσμεύουν τους υπευθύνους της επεξεργασίας και τους εκτελούντες την επεξεργασία. Επιπλέον, τα ίδια τα μέλη των εποπτικών

115 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2 στοιχείο η) και άρθρο 9 παράγραφος 3.

116 Ό.π., άρθρο 14 παράγραφος 5 στοιχείο δ).

117 Ό.π., αιτιολογική σκέψη 164 και άρθρο 90.

αρχών υπέχουν καθήκον τήρησης του επαγγελματικού απορρήτου κατά τη διάρκεια και μετά τη λήξη της θητείας τους. Κατά τη διάρκεια της άσκησης των καθηκόντων τους, τα μέλη και το προσωπικό των εποπτικών αρχών ενδέχεται να λάβουν γνώση εμπιστευτικών πληροφοριών. Το άρθρο 54 παράγραφος 2 του κανονισμού προβλέπει ρητώς ότι έχουν υποχρέωση τήρησης επαγγελματικού απορρήτου σε σχέση με τέτοιες εμπιστευτικές πληροφορίες.

Ο ΓΚΠΔ υποχρεώνει τα κράτη μέλη να κοινοποιούν στην Επιτροπή τούς κανόνες τους οποίους θεσπίζουν για τον συμβιβασμό της προστασίας των δεδομένων και των αρχών που καθορίζει ο κανονισμός με την υποχρέωση επαγγελματικού απορρήτου.

1.3.3. Ελευθερία θρησκείας και πεποιθήσεων

Η ελευθερία θρησκείας και πεποιθήσεων κατοχυρώνεται στο άρθρο 9 της ΕΣΔΑ (Ελευθερία σκέψης, συνείδησης και θρησκείας) και στο άρθρο 10 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν θρησκευτικές ή φιλοσοφικές πεποιθήσεις θεωρούνται «ευαίσθητα δεδομένα» τόσο βάσει του δικαίου της ΕΕ, όσο και βάσει του δικαίου του Συμβουλίου της Ευρώπης, η δε επεξεργασία και χρήση τους αποτελεί αντικείμενο ενισχυμένης προστασίας.

Παράδειγμα: Στην υπόθεση *Sinan Isik κατά Τουρκίας*¹¹⁸, ο προσφεύγων ήταν μέλος της θρησκευτικής κοινότητας των αλεβιτών, των οποίων η πίστη έχει δεχθεί επιρροές από τον σουφισμό και άλλες προϊσλαμικές πεποιθήσεις και θεωρείται από ορισμένους μελετητές χωριστή θρησκεία και από άλλους μέρος της μουσουλμανικής θρησκείας. Ο προσφεύγων κατήγγειλε ότι, παρά τη θέλησή του, το δελτίο ταυτότητάς του περιλάμβανε ένα πεδίο στο οποίο η θρησκεία του αναφερόταν ως «μουσουλμανική» και όχι ως «αλεβιτική». Τα εθνικά δικαστήρια απέρριψαν το αίτημά του για αλλαγή της θρησκείας στο δελτίο ταυτότητάς του σε «αλεβιτική», με την αιτιολογία ότι η λέξη υποδηλώνει υποομάδα του ισλάμ και όχι χωριστή θρησκεία. Εν συνεχεία, ο προσφεύγων κατήγγειλε στο ΕΔΔΑ ότι υποχρεώθηκε να αποκαλύψει την πίστη του, χωρίς τη συγκατάθεσή του, επειδή ήταν υποχρεωτικό να αναγράφεται η θρησκεία ενός προσώπου στο δελτίο

¹¹⁸ ΕΔΔΑ, *Sinan Isik κατά Τουρκίας*, προσφυγή αριθ. 21924/05, 2 Φεβρουαρίου 2010.

ταυτότητάς του και ότι αυτό συνιστούσε παραβίαση του δικαιώματός του στην ελευθερία θρησκείας και συνείδησης, δεδομένου μάλιστα ότι η αναφορά του ισλάμ στο δελτίο ταυτότητάς του ήταν ανακριβής.

Το ΕΔΔΑ επανέλαβε ότι η θρησκευτική ελευθερία συνεπάγεται την ελευθερία του προσώπου να εκδηλώνει τη θρησκεία του από κοινού με άλλους, δημόσια και στον κύκλο προσώπων που συμμερίζονται την ίδια πίστη, αλλά και κατά μόνας και κατ' ιδίαν. Η τότε ισχύουσα εθνική νομοθεσία υποχρέωνε τα φυσικά πρόσωπα να έχουν δελτίο ταυτότητας, έγγραφο το οποίο έπρεπε να επιδεικνύεται κατόπιν αιτήματος κάθε δημόσιας αρχής ή ιδιωτικής επιχείρησης και στο οποίο αναγραφόταν η θρησκεία τους. Η υποχρέωση αυτή δεν αναγνώριζε ότι το δικαίωμα ενός προσώπου να εκδηλώνει τη θρησκεία του εμπεριέχει και το αντίστροφο, δηλαδή το δικαίωμα ενός προσώπου να μην αποκαλύψει τις πεποιθήσεις του. Παρότι η κυβέρνηση υποστήριξε ότι η εθνική νομοθεσία είχε τροποποιηθεί ώστε τα φυσικά πρόσωπα να μπορούν να ζητούν να μη συμπληρωθεί το πεδίο της θρησκείας στο δελτίο ταυτότητάς τους, το ΕΔΔΑ έκρινε ότι και μόνο το γεγονός ότι τα φυσικά πρόσωπα υποχρεούνταν να ζητήσουν την απαλοιφή της αναφοράς σε θρησκεία μπορούσε να συνιστά γνωστοποίηση πληροφοριών σχετικά με τη στάση τους απέναντι στη θρησκεία. Επιπλέον, όταν το δελτίο ταυτότητας έχει πεδίο για τη θρησκεία, η μη συμπλήρωσή του έχει ειδική σημασία, καθώς οι κάτοχοι δελτίου ταυτότητας χωρίς πληροφορίες σχετικά με τη θρησκεία τους θα διακρίνονται από εκείνους που έχουν δελτίο ταυτότητας στο οποίο αναγράφονται οι πεποιθήσεις τους. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι η εθνική νομοθεσία συνιστούσε παράβαση του άρθρου 9 της ΕΣΔΑ.

Ωστόσο, η λειτουργία Εκκλησιών και θρησκευτικών ενώσεων ή κοινοτήτων μπορεί να απαιτεί την επεξεργασία των προσωπικών πληροφοριών των μελών τους, ώστε να καθίσταται εφικτή η επικοινωνία μεταξύ των μελών του εκκλησιασματος και η οργάνωση των δραστηριοτήτων τους. Επομένως, οι Εκκλησίες και οι θρησκευτικές ενώσεις εφαρμόζουν συχνά κανόνες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Κατά το άρθρο 91 του Γενικού Κανονισμού για την Προστασία Δεδομένων, όταν οι κανόνες αυτοί είναι ολοκληρωμένοι, μπορούν να συνεχίσουν να εφαρμόζονται, εφόσον ευθυγραμμίζονται με τις διατάξεις του κανονισμού. Οι Εκκλησίες και οι θρησκευτικές ενώσεις που εφαρμόζουν τέτοιους κανόνες πρέπει να υπόκεινται στον έλεγχο ανεξάρτητης εποπτικής αρχής, που μπορεί να είναι εξειδικευμένη, υπό τον όρο ότι πληροί τις

προϋποθέσεις του Γενικού Κανονισμού για την Προστασία Δεδομένων για τις εν λόγω αρχές ¹¹⁹.

Οι θρησκευτικές οργανώσεις ενδέχεται να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για διάφορους λόγους –για παράδειγμα, για να διατηρούν επαφή με τα μέλη τους ή για να ανακοινώνουν πληροφορίες σχετικά με θρησκευτικές ή φιλανθρωπικές και εορταστικές εκδηλώσεις τις οποίες οργανώνουν. Σε ορισμένα κράτη, οι Εκκλησίες πρέπει να τηρούν αρχεία των μελών τους για φορολογικούς σκοπούς, καθώς η συμμετοχή σε θρησκευτικά ιδρύματα μπορεί να έχει αντίκτυπο στους φόρους τους οποίους πληρώνουν τα φυσικά πρόσωπα. Εν πάση περιπτώσει, βάσει του ευρωπαϊκού δικαίου, τα δεδομένα που αποκάλυπτουν θρησκευτικές πεποιθήσεις είναι ευαίσθητα δεδομένα και οι Εκκλησίες πρέπει να λογοδοτούν για τον χειρισμό και την επεξεργασία τέτοιων δεδομένων, εφόσον μάλιστα οι πληροφορίες τις οποίες επεξεργάζονται οι θρησκευτικές οργανώσεις αφορούν συχνά παιδιά, ηλικιωμένους και άλλα ευάλωτα μέλη της κοινωνίας.

1.3.4. Ελευθερία της τέχνης και της επιστήμης

Ένα άλλο δικαίωμα το οποίο πρέπει να σταθμίζεται με τα δικαιώματα στον σεβασμό της ιδιωτικής ζωής και της προστασίας των δεδομένων είναι η ελευθερία της τέχνης και της επιστήμης, η οποία προστατεύεται ρητώς δυνάμει του άρθρου 13 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Το δικαίωμα αυτό προκύπτει πρωτίστως από το δικαίωμα στην ελευθερία της σκέψης και της έκφρασης και πρέπει να ασκείται λαμβανομένου υπόψη του άρθρου 1 του Χάρτη (ανθρώπινη αξιοπρέπεια). Το ΕΔΔΑ εκτιμά ότι η ελευθερία των τεχνών προστατεύεται στο πλαίσιο του άρθρου 10 της ΕΣΔΑ ¹²⁰. Το δικαίωμα που κατοχυρώνεται στο άρθρο 13 του Χάρτη μπορεί επίσης να υπόκειται σε περιορισμούς σύμφωνα με το άρθρο 52 παράγραφος 1 του Χάρτη, το οποίο μπορεί επίσης να ερμηνεύεται υπό το πρίσμα του άρθρου 10 παράγραφος 2 της ΕΣΔΑ ¹²¹.

¹¹⁹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 91 παράγραφος 2.

¹²⁰ ΕΔΔΑ, *Müller κ.λπ. κατά Ελβετίας*, προσφυγή αριθ. 10737/84, 24 Μαΐου 1988.

¹²¹ Επεξηγήσεις σχετικά με τον Χάρτη των Θεμελιωδών Δικαιωμάτων (ΕΕ 2007 C 303).

Παράδειγμα: Στην υπόθεση *Vereinigung bildender Künstler κατά Αυστρίας*¹²², τα αυστριακά δικαστήρια απαγόρευσαν στην προσφεύγουσα ένωση να συνεχίσει να εκθέτει πίνακα ο οποίος περιείχε φωτογραφίες του κεφαλιού διαφόρων δημόσιων προσώπων σε ερωτικές περιπτώσεις. Αυστριακός βουλευτής, του οποίου η φωτογραφία είχε χρησιμοποιηθεί στον πίνακα, είχε κινηθεί δικαστικά κατά της προσφεύγουσας ένωσης ζητώντας την έκδοση διαταγής για την απαγόρευση της έκθεσης του πίνακα. Το εθνικό δικαστήριο έκανε δεκτό το αίτημά του και διέταξε την απαγόρευση. Το ΕΔΔΑ επανέλαβε ότι το άρθρο 10 της ΕΣΔΑ εφαρμόζεται και για ιδέες οι οποίες προσβάλλουν, σοκάρουν ή ενοχλούν το κράτος ή οποιοδήποτε τμήμα του πληθυσμού. Όσοι δημιουργούν, εκτελούν, διανέμουν ή εκθέτουν έργα τέχνης συμβάλλουν στην ανταλλαγή ιδεών και απόψεων, και το κράτος έχει υποχρέωση να μην καταπατά αδικαιολόγητα την ελευθερία έκφρασής τους. Δεδομένου ότι ο πίνακας ήταν κολάζ και χρησιμοποιούσε φωτογραφίες μόνο του κεφαλιού προσώπων, και ότι τα σώματά τους ήταν ζωγραφισμένα με μη ρεαλιστικό και υπερβολικό τρόπο, ο οποίος προδήλως δεν αποσκοπούσε στο να αντικατοπτρίσει ή ακόμη και να υποδηλώσει την πραγματικότητα, το ΕΔΔΑ επισήμανε περαιτέρω ότι «μετά δυσκολίας θα μπορούσε να θεωρηθεί πως ο πίνακας αναφέρεται σε λεπτομέρειες της ιδιωτικής ζωής του [απεικονιζόμενου], αλλά σχετίζεται μάλλον με τη δημόσια θέση του ως πολιτικού» και ότι «με την ιδιότητά του αυτή [ο απεικονιζόμενος] οφείλει να επιδεικνύει μεγαλύτερη ανεκτικότητα απέναντι στην κριτική». Σταθμίζοντας τα διαφορετικά συμφέροντα που διακυβεύονταν, το ΕΔΔΑ αποφάνθηκε ότι η απεριόριστη απαγόρευση της περαιτέρω έκθεσης του πίνακα ήταν υπερβολικό μέτρο. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 10 της ΕΣΔΑ.

Το ευρωπαϊκό δίκαιο για την προστασία των δεδομένων προσωπικού χαρακτήρα αναγνωρίζει επίσης την ιδιαίτερη αξία της επιστήμης στην κοινωνία. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων και η Εκσυγχρονισμένη Σύμβαση 108 επιτρέπουν τη διατήρηση δεδομένων προσωπικού χαρακτήρα για μεγαλύτερο χρονικό διάστημα εφόσον αυτά θα υποβληθούν σε επεξεργασία μόνο για σκοπούς επιστημονικής ή ιστορικής έρευνας. Επιπλέον, και ανεξάρτητα από τον αρχικό σκοπό της συγκεκριμένης επεξεργασίας, η επακόλουθη χρήση δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας δεν θεωρείται

122 ΕΔΔΑ, *Vereinigung bildender Künstler κατά Αυστρίας*, προσφυγή αριθ. 68354/01, 25 Ιανουαρίου 2007, σκέψεις 26 και 34.

ασύμβατος σκοπός¹²³. Ταυτόχρονα, πρέπει να εφαρμόζονται κατάλληλες εγγυήσεις για την εν λόγω επεξεργασία με σκοπό την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων. Το δίκαιο της ΕΕ ή των κρατών μελών μπορεί να προβλέπει παρεκκλίσεις σε σχέση με τα δικαιώματα των υποκειμένων των δεδομένων, για παράδειγμα το δικαίωμα στην πρόσβαση, στη διόρθωση, στον περιορισμό της επεξεργασίας, καθώς και το δικαίωμα εναντίωσης όταν πρόκειται για επεξεργασία των δεδομένων προσωπικού χαρακτήρα τους για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς (βλ. επίσης [ενότητα 6.1](#) και [ενότητα 9.4](#)).

1.3.5. Προστασία της διανοητικής ιδιοκτησίας

Το δικαίωμα στην προστασία της ιδιοκτησίας κατοχυρώνεται στο άρθρο 1 του πρώτου πρωτοκόλλου της ΕΣΔΑ, καθώς επίσης και στο άρθρο 17 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Μια σημαντική πτυχή του δικαιώματος ιδιοκτησίας η οποία έχει ιδιαίτερη σημασία για την προστασία των δεδομένων είναι η προστασία της διανοητικής ιδιοκτησίας, η οποία αναφέρεται ρητώς στο άρθρο 17 παράγραφος 2 του Χάρτη. Αρκετές οδηγίες στην έννομη τάξη της ΕΕ στοχεύουν στην αποτελεσματική προστασία της διανοητικής ιδιοκτησίας, και ιδίως του δικαιώματος του δημιουργού. Η διανοητική ιδιοκτησία δεν περιλαμβάνει μόνο τη λογοτεχνική και την καλλιτεχνική ιδιοκτησία, αλλά και τα διπλώματα ευρεσιτεχνίας, τα εμπορικά σήματα και τα συγγενικά δικαιώματα.

Όπως έχει καταστεί σαφές στη νομολογία του ΔΕΕ, η προστασία του θεμελιώδους δικαιώματος στην ιδιοκτησία πρέπει να σταθμίζεται με την προστασία άλλων θεμελιωδών δικαιωμάτων, και ιδίως με το δικαίωμα στην προστασία δεδομένων¹²⁴. Σε ορισμένες περιπτώσεις, οργανισμοί προστασίας του δικαιώματος του δημιουργού ζήτησαν από φορείς παροχής πρόσβασης στο διαδίκτυο να γνωστοποιήσουν την ταυτότητα χρηστών πλατφορμών για την ανταλλαγή αρχείων στο διαδίκτυο. Τέτοιες πλατφόρμες παρέχουν συχνά τη δυνατότητα στους χρήστες του διαδικτύου να καταφορτώνουν μουσικούς τίτλους δωρεάν, παρότι οι τίτλοι αυτοί προστατεύονται με δικαίωμα δημιουργού.

¹²³ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο β), και Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο β).

¹²⁴ ΔΕΕ, C-275/06, *Productores de Música de España (Promusicae) κατά Telefónica de España SAU* [τμήμα μείζονος συνθέσεως], 29 Ιανουαρίου 2008, σκέψεις 62-68.

Παράδειγμα: Η υπόθεση *Promusicae κατά Telefónica de España*¹²⁵ αφορούσε την άρνηση ισπανικού φορέα παροχής πρόσβασης στο διαδίκτυο, της Telefónica, να γνωστοποιήσει στην Promusicae, μη κερδοσκοπική ένωση μουσικών παραγωγών και εκδοτών μουσικών και οπτικοακουστικών έργων, τα δεδομένα προσωπικού χαρακτήρα ορισμένων ατόμων στα οποία παρείχε υπηρεσίες πρόσβασης στο διαδίκτυο. Η Promusicae ζήτησε τη γνωστοποίηση των πληροφοριών ώστε να μπορέσει να ασκήσει αγωγή κατά των προσώπων αυτών, τα οποία, κατά τους ισχυρισμούς της, χρησιμοποιούσαν πρόγραμμα ανταλλαγής αρχείων το οποίο παρείχε πρόσβαση σε φωνογραφήματα των οποίων τα δικαιώματα εκμετάλλευσης ανήκαν σε μέλη της Promusicae.

Το ισπανικό δικαστήριο παρέπεμψε το ζήτημα στο ΔΕΕ, με το αίτημα να διευκρινιστεί αν, βάσει του κοινοτικού δικαίου, τα εν λόγω δεδομένα προσωπικού χαρακτήρα πρέπει να γνωστοποιηθούν, στο πλαίσιο αστικής δίκης με σκοπό τη διασφάλιση της αποτελεσματικής προστασίας του δικαιώματος του δημιουργού. Το ισπανικό δικαστήριο παρέπεμψε στις οδηγίες 2000/31, 2001/29 και 2004/48, σε συνδυασμό με τα άρθρα 17 και 47 του Χάρτη. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι οι τρεις αυτές οδηγίες, καθώς και η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (οδηγία 2002/58), δεν αποκλείουν τη δυνατότητα των κρατών μελών να θεσπίσουν υποχρέωση δημοσιοποίησης δεδομένων προσωπικού χαρακτήρα στο πλαίσιο αστικής δίκης για τη διασφάλιση αποτελεσματικής προστασίας του δικαιώματος του δημιουργού.

Το ΔΕΕ σημείωσε ότι, ως εκ τούτου, στη συγκεκριμένη υπόθεση τέθηκε το θέμα του αναγκαίου συμβιβασμού μεταξύ των επιταγών που συνδέονται με την προστασία διαφόρων θεμελιωδών δικαιωμάτων –δηλαδή, του δικαιώματος στον σεβασμό της ιδιωτικής ζωής και των δικαιωμάτων προστασίας της ιδιοκτησίας και ασκήσεως αποτελεσματικής προσφυγής.

Κατέληξε στο συμπέρασμα ότι «τα κράτη μέλη οφείλουν, κατά τη μεταφορά των προαναφερθεισών οδηγιών στο εσωτερικό δίκαιο, να μεριμνούν ώστε να βασίζονται σε ερμηνεία των οδηγιών αυτών που καθιστά δυνατή τη διασφάλιση της ορθής ισορροπίας μεταξύ των διαφόρων θεμελιωδών δικαιωμάτων που προστατεύει η κοινοτική έννομη

¹²⁵ Ό.π., σκέψεις 54 και 60.

τάξη. Περαιτέρω, κατά την εφαρμογή των μέτρων μεταφοράς των οδηγιών αυτών στο εσωτερικό δίκαιο, οι αρχές και τα δικαστήρια των κρατών μελών οφείλουν όχι μόνο να ερμηνεύουν το εθνικό τους δίκαιο κατά τρόπο σύμφωνο προς τις εν λόγω οδηγίες, αλλά και να μεριμνούν ώστε να μη βασίζονται σε ερμηνεία αυτών που θα μπορούσε να έλθει σε σύγκρουση με τα εν λόγω θεμελιώδη δικαιώματα ή με τις λοιπές γενικές αρχές του κοινοτικού δικαίου, όπως η αρχή της αναλογικότητας»¹²⁶.

Παράδειγμα: Η υπόθεση *Bonnier Audio AB κ.λπ. κατά Perfect Communication Sweden AB*¹²⁷ αφορούσε τη στάθμιση των δικαιωμάτων διανοητικής ιδιοκτησίας και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Οι προσφεύγουσες –πέντε εκδοτικές εταιρείες με δικαιώματα δημιουργού σε 27 ακουστικά βιβλία– προσέφυγαν ενώπιον σουηδικού δικαστηρίου υποστηρίζοντας ότι τα εν λόγω δικαιώματα δημιουργού προσβάλλονταν μέσω διακομιστή FTP (πρωτοκόλλου μεταφοράς αρχείων, το οποίο επιτρέπει την ανταλλαγή αρχείων και τη μεταφορά δεδομένων μέσω του διαδικτύου). Οι προσφεύγουσες ζήτησαν από τον φορέα παροχής υπηρεσιών στο διαδίκτυο (ISP) να κοινοποιήσει το όνομα και τη διεύθυνση του προσώπου που χρησιμοποιούσε τη διεύθυνση IP από την οποία αποστέλλονταν τα αρχεία. Η ePhone, ο φορέας παροχής υπηρεσιών στο διαδίκτυο, απέρριψε το αίτημα, υποστηρίζοντας ότι αυτή η κοινοποίηση συνιστά παράβαση της οδηγίας 2006/24 (οδηγία για τη διατήρηση δεδομένων –κηρύχθηκε ανίσχυρη το 2014).

Το σουηδικό δικαστήριο παρέπεμψε το ζήτημα στο ΔΕΕ, ζητώντας να διευκρινιστεί αν η οδηγία 2006/24 αποκλείει την εφαρμογή εθνικής διάταξης που βασίζεται στο άρθρο 8 της οδηγίας 2004/48 (οδηγία για την επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας), η οποία επιτρέπει την έκδοση διαταγής προς τους φορείς παροχής υπηρεσιών στο διαδίκτυο (ISP) ώστε να διαβιβάσουν στους δικαιούχους των δικαιωμάτων δημιουργού πληροφορίες σχετικά με τους συνδρομητές των οποίων οι διευθύνσεις IP εικάζεται ότι χρησιμοποιήθηκαν για τις παραβιάσεις των δικαιωμάτων. Το ερώτημα βασιζόταν στην παραδοχή ότι οι προσφεύγουσες έχουν

126 Ό.π., σκέψεις 65 και 68· βλ. επίσης ΔΕΕ, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) κατά Netlog NV*, 16 Φεβρουαρίου 2012.

127 ΔΕΕ, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB κατά Perfect Communication Sweden AB*, 19 Απριλίου 2012.

προσκομίσει αποχρώσεις ενδείξεις για το υποστατό της προσβολής ορισμένου δικαιώματος πνευματικής ιδιοκτησίας και ότι το μέτρο είναι ανάλογο προς τον επιδιωκόμενο σκοπό.

Το ΔΕΕ επισήμανε ότι η οδηγία 2006/24 αφορά αποκλειστικά τον χειρισμό και τη διατήρηση δεδομένων που παράγουν οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών για τον σκοπό της διερεύνησης, της διαπίστωσης και της δίωξης σοβαρών αδικημάτων, καθώς και τη διαβίβαση των δεδομένων αυτών στις αρμόδιες εθνικές αρχές. Επομένως, εθνική διάταξη μεταφοράς της οδηγίας για την επιβολή των δικαιωμάτων διανοητικής ιδιοκτησίας στο εθνικό δίκαιο δεν εμπίπτει στο πεδίο εφαρμογής της οδηγίας 2006/24 και, ως εκ τούτου, δεν αποκλείεται από την εν λόγω οδηγία ¹²⁸.

Όσον αφορά την επίμαχη κοινοποίηση του ονόματος και της διεύθυνσης, την οποία ζήτησαν οι προσφεύγουσες, το ΔΕΕ αποφάνθηκε ότι η πράξη αυτή συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα και εμπίπτει στο πεδίο εφαρμογής της οδηγίας 2002/58 (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες). Επισήμανε επίσης ότι η κοινοποίηση των δεδομένων αυτών απαιτείται στο πλαίσιο αστικής διαδικασίας προς όφελος του δικαιούχου δικαιώματος του δημιουργού ώστε να διασφαλιστεί η αποτελεσματική προστασία του δικαιώματος του δημιουργού και, ως εκ τούτου, εμπίπτει εκ του αντικειμένου της στο πεδίο εφαρμογής της οδηγίας 2004/48 ¹²⁹.

Το ΔΕΕ κατέληξε στο συμπέρασμα ότι οι οδηγίες 2002/58 και 2004/48 πρέπει να θεωρηθεί ότι δεν απαγορεύουν την εθνική νομοθεσία, όπως η επίμαχη στην κύρια δίκη, στον βαθμό που η νομοθεσία αυτή επιτρέπει στο εθνικό δικαστήριο ενώπιον του οποίου υποβλήθηκε αίτηση έκδοσης διαταγής περί κοινοποίησης δεδομένων προσωπικού χαρακτήρα να σταθμίσει, με βάση τις περιστάσεις κάθε συγκεκριμένης περίπτωσης και λαμβάνοντας δεόντως υπόψη τις απαιτήσεις που απορρέουν από την αρχή της αναλογικότητας, τα αντιτιθέμενα εν προκειμένω συμφέροντα.

¹²⁸ Ό.π., σκέψη 40-41.

¹²⁹ Ό.π., σκέψεις 52-54. Βλ. επίσης ΔΕΕ, C-275/06, *Productores de Música de España (Promusicae) κατά Telefónica de España SAU* [Τμήμα μείζονος συνθέσεως], 29 Ιανουαρίου 2008, σκέψη 58.

1.3.6. Προστασία δεδομένων και οικονομικά συμφέροντα

Στην ψηφιακή εποχή ή εποχή των μαζικών δεδομένων, τα δεδομένα έχουν χαρακτηριστεί «το νέο πετρέλαιο» της οικονομίας για την τόνωση της καινοτομίας και της δημιουργικότητας ¹³⁰. Πολλές εταιρείες έχουν οικοδομήσει εύρωστα επιχειρηματικά πρότυπα γύρω από την επεξεργασία δεδομένων, και η εν λόγω επεξεργασία συχνά περιλαμβάνει δεδομένα προσωπικού χαρακτήρα. Ορισμένες εταιρείες μπορεί να θεωρούν ότι ειδικοί κανόνες που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα ενδέχεται, στην πράξη, να έχουν ως αποτέλεσμα υπερβολικά επαχθείς υποχρεώσεις οι οποίες θα μπορούσαν να θίξουν τα οικονομικά συμφέροντά τους. Επομένως, τίθεται το ερώτημα αν τα οικονομικά συμφέροντα των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία, ή του ευρύτερου κοινού, θα μπορούσαν να δικαιολογήσουν τον περιορισμό του δικαιώματος στην προστασία των δεδομένων.

Παράδειγμα: Στην υπόθεση *Google Spain* ¹³¹, το ΔΕΕ αποφάνθηκε ότι, υπό ορισμένες προϋποθέσεις, τα φυσικά πρόσωπα δικαιούνται να ζητούν από φορείς εκμετάλλευσης μηχανών αναζήτησης να διαγράψουν αποτελέσματα από το ευρετήριο αναζητήσεών τους. Στο σκεπτικό του, το ΔΕΕ επισήμανε ότι η χρήση μηχανών αναζήτησης και ο κατάλογος των αποτελεσμάτων της αναζήτησης μπορούν να χρησιμοποιηθούν για την κατάρτιση λεπτομερούς προφίλ ενός φυσικού προσώπου. Οι πληροφορίες αυτές μπορεί να αφορούν διάφορες πτυχές της ιδιωτικής ζωής του φυσικού προσώπου και δεν θα μπορούσαν να ανευρεθούν ή να διασταυρωθούν χωρίς μηχανή αναζήτησης. Επομένως, συνιστούν δυνητικά σοβαρή επέμβαση στα θεμελιώδη δικαιώματα των υποκειμένων των δεδομένων στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Το ΔΕΕ εξέτασε ακολούθως αν η επέμβαση θα μπορούσε να είναι δικαιολογημένη. Όσον αφορά το οικονομικό συμφέρον της εταιρείας της μηχανής αναζήτησης από τη διενέργεια της επεξεργασίας, το ΔΕΕ διευκρίνισε ότι «επιβάλλεται η διαπίστωση ότι η επέμβαση αυτή [...] δεν

¹³⁰ Βλ., για παράδειγμα, *Financial Times* (2016), «Data is the new oil... who's going to own it?», 16 Νοεμβρίου 2016.

¹³¹ ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD)*, *Mario Costeja González* [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014.

μπορεί να δικαιολογείται μόνο με βάση το οικονομικό συμφέρον του φορέα εκμετάλλευσης της μηχανής αναζήτησης στην ως άνω επεξεργασία» και ότι «καταρχήν» τα θεμελιώδη δικαιώματα που απορρέουν από τα άρθρα 7 και 8 του Χάρτη υπερισχύουν του οικονομικού αυτού συμφέροντος και του συμφέροντος του κοινού να αποκτήσει την πληροφορία αυτή στο πλαίσιο αναζήτησης με βάση το ονοματεπώνυμο του υποκειμένου των δεδομένων ¹³².

Ένα από τα βασικά μελήματα του ευρωπαϊκού δικαίου προστασίας των δεδομένων είναι η παροχή στα φυσικά πρόσωπα μεγαλύτερου ελέγχου επί των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Στην ψηφιακή μάλιστα εποχή, υπάρχει ανισορροπία μεταξύ της ισχύος των επιχειρήσεων που επεξεργάζονται και έχουν πρόσβαση σε μεγάλες ποσότητες δεδομένων προσωπικού χαρακτήρα και της δυνατότητας των φυσικών προσώπων στα οποία ανήκουν τα δεδομένα προσωπικού χαρακτήρα να ελέγχουν τις πληροφορίες που τα αφορούν. Το ΔΕΕ εφαρμόζει την κατά περίπτωση προσέγγιση όταν σταθμίζει την προστασία των δεδομένων και τα οικονομικά συμφέροντα –όπως τα συμφέροντα τρίτων που συνδέονται με μετοχικές εταιρείες και εταιρείες περιορισμένης ευθύνης, όπως καταδεικνύεται στην απόφαση *Mannl*.

Παράδειγμα: Η υπόθεση *Mannl* ¹³³ αφορούσε τη συμπερίληψη των δεδομένων προσωπικού χαρακτήρα φυσικού προσώπου σε δημόσιο εμπορικό μητρώο. Ο S. Mannl είχε ζητήσει από το Εμπορικό Επιμελητήριο του Λέτσε να διαγράψει από το οικείο μητρώο τα δεδομένα προσωπικού χαρακτήρα που τον αφορούσαν, καθώς ανακάλυψε ότι δυνητικοί πελάτες συμβουλευόνταν το μητρώο και διαπίστωναν ότι είχε διατελέσει διαχειριστής εταιρείας η οποία είχε κηρύξει πτώχευση πριν από περισσότερο από μια δεκαετία. Οι πληροφορίες αυτές επηρέαζαν αρνητικά τους δυνητικούς πελάτες του και μπορούσαν να έχουν αρνητικό αντίκτυπο στα εμπορικά συμφέροντά του.

Το ΔΕΕ κλήθηκε να κρίνει αν το δίκαιο της ΕΕ αναγνώριζε δικαίωμα διαγραφής στην περίπτωση αυτή. Για να καταλήξει στο συμπέρασμά του, στάθμισε τους κανόνες της ΕΕ περί προστασίας δεδομένων και

¹³² Ό.π., σκέψεις 81 και 97.

¹³³ ΔΕΕ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*, 9 Μαρτίου 2017.

το εμπορικό συμφέρον του S. Μαννί που απαιτούσε να διαγραφούν οι πληροφορίες σχετικά με την πτώχευση της πρώην εταιρείας του με το δημόσιο συμφέρον πρόσβασης στις πληροφορίες. Έλαβε δεόντως υπόψη το γεγονός ότι η υποχρέωση δημοσιότητας στο δημόσιο μητρώο εταιρειών προβλεπόταν από τον νόμο και ιδίως από οδηγία της ΕΕ η οποία αποσκοπεί στη διευκόλυνση της πρόσβασης τρίτων σε εταιρικές πληροφορίες. Η δημοσιότητα συμβάλλει σημαντικά στην προστασία των δικαιωμάτων τρίτων που ενδέχεται να επιθυμούν να συναλλαχθούν με συγκεκριμένη εταιρεία, επειδή οι μόνες εγγυήσεις που παρέχουν οι μετοχικές εταιρείες και οι εταιρείες περιορισμένης ευθύνης έναντι των τρίτων είναι η εταιρική τους περιουσία. Ως εκ τούτου, «η δημοσιότητα πρέπει να παρέχει στους τρίτους τη δυνατότητα να γνωρίζουν τις ουσιώδεις καταστατικές πράξεις της οικείας εταιρείας καθώς και ορισμένα στοιχεία που την αφορούν, ιδίως δε τα στοιχεία ταυτότητας των ατόμων που έχουν την εξουσία να τη δεσμεύουν»¹³⁴.

Λόγω της σημασίας του θεμιτού σκοπού που επιδιώκει το μητρώο, το ΔΕΕ αποφάνθηκε ότι ο S. Μαννί δεν είχε δικαίωμα στη διαγραφή των δεδομένων προσωπικού χαρακτήρα που τον αφορούσαν, καθώς η ανάγκη να προστατευθούν τα συμφέροντα των τρίτων που συνδέονται με μετοχικές εταιρείες και εταιρείες περιορισμένης ευθύνης και να διασφαλιστεί η ασφάλεια δικαίου, η εντιμότητα των εμπορικών συναλλαγών και, με τον τρόπο αυτόν, η εύρυθμη λειτουργία της εσωτερικής αγοράς υπερίσχυε των δικαιωμάτων του βάσει της νομοθεσίας για την προστασία των δεδομένων. Λαμβανομένου μάλιστα υπόψη ότι τα φυσικά πρόσωπα που αποφασίζουν να ασκήσουν οικονομική δραστηριότητα μέσω μετοχικής εταιρείας ή εταιρείας περιορισμένης ευθύνης γνωρίζουν ότι υποχρεούνται να δημοσιοποιούν πληροφορίες σχετικά με την ταυτότητα και τις αρμοδιότητές τους.

Παρότι αποφάνθηκε ότι δεν συνέτρεχε λόγος εξασφάλισης της διαγραφής στην περίπτωση αυτή, το ΔΕΕ αναγνώρισε την ύπαρξη του δικαιώματος του ενδιαφερομένου να αντισταχθεί στην επεξεργασία, επισημαίνοντας τα εξής: «όταν έχει παρέλθει ένα αρκούντως μακρύ χρονικό διάστημα [...], δεν μπορεί να αποκλείεται το ενδεχόμενο να υπάρξουν ιδιαίτερες καταστάσεις στις οποίες επιτακτικοί και θεμιτοί λόγοι συνδεόμενοι με τη συγκεκριμένη περίπτωση του ενδιαφερομένου να δικαιολογούν όλως

134 Ό.π., σκέψη 49.

εξαιρετικώς να περιορίζεται η πρόσβαση στα καταχωρισμένα στο μητρώο δεδομένα προσωπικού χαρακτήρα που τον αφορούν εκ μέρους τρίτων οι οποίοι έχουν ειδικό συμφέρον να λάβουν γνώση των δεδομένων αυτών»¹³⁵.

Το ΔΕΕ επισήμανε ότι εναπόκειται στα εθνικά δικαστήρια να εκτιμήσουν σε κάθε περίπτωση, και λαμβανομένων υπόψη όλων των σχετικών περιστάσεων του φυσικού προσώπου, την ύπαρξη ή απουσία θεμιτών και επιτακτικών λόγων οι οποίοι θα μπορούσαν να δικαιολογούν κατ' εξαίρεση τον περιορισμό της πρόσβασης τρίτων σε δεδομένα προσωπικού χαρακτήρα τα οποία περιέχονται σε μητρώα εταιρειών. Ωστόσο, το ΔΕΕ διευκρίνισε ότι στην περίπτωση του *S. Μαννί* το γεγονός και μόνον ότι η δημοσιοποίηση των δεδομένων προσωπικού χαρακτήρα που τον αφορούν στο μητρώο επηρεάζει, κατά τους ισχυρισμούς του, την πελατεία του δεν θα μπορούσε να θεωρηθεί τέτοιος θεμιτός και επιτακτικός λόγος. Οι δυνητικοί πελάτες του *S. Μαννί* έχουν έννομο συμφέρον να μάθουν τις πληροφορίες που αφορούν την πτώχευση της προηγούμενης εταιρείας του.

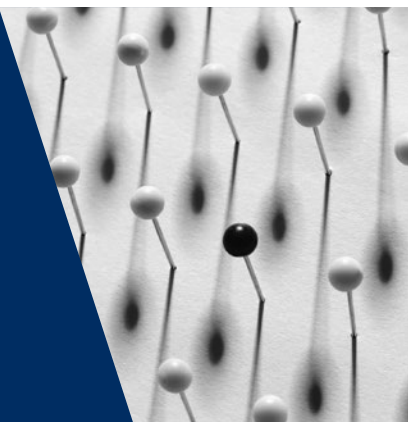
Η επέμβαση στα θεμελιώδη δικαιώματα του *S. Μαννί*, και άλλων προσώπων που περιλαμβάνονται στο μητρώο, στον σεβασμό της ιδιωτικής ζωής και στην προστασία των δεδομένων προσωπικού χαρακτήρα, όπως κατοχυρώνονται από τα άρθρα 7 και 8 του Χάρτη, εξυπηρετούσε στόχο γενικού συμφέροντος και ήταν αναγκαία και ανάλογη.

Επομένως, στην υπόθεση *Μαννί* το ΔΕΕ αποφάνθηκε ότι τα δικαιώματα στην προστασία των δεδομένων και στον σεβασμό της ιδιωτικής ζωής δεν υπερισχύουν του συμφέροντος τρίτων από την πρόσβαση σε πληροφορίες του μητρώου εταιρειών σχετικά με μετοχικές εταιρείες και εταιρείες περιορισμένης ευθύνης.

¹³⁵ Ό.π., σκέψη 60.

2

Ορολογία για την προστασία δεδομένων



ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Δεδομένα προσωπικού χαρακτήρα		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 1	Νομικός ορισμός της προστασίας δεδομένων	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο α)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 5 και άρθρο 5 παράγραφος 1 στοιχείο ε)		ΕΔΔΑ, <i>Bernh Larsen Holding AS κ.λπ. κατά Νορβηγίας</i> , προσφυγή αριθ. 24117/08, 2013
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9		ΕΔΔΑ, <i>Uzun κατά Γερμανίας</i> , προσφυγή αριθ. 35623/05, 2010
ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, <i>Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen</i> [τμήμα μείζονος συνθέσεως], 2010		ΕΔΔΑ, <i>Amann κατά Ελλάδας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 2000
ΔΕΕ, C-275/06, <i>Productores de Música de España (Promusicae) κατά Telefónica de España SAU</i> [τμήμα μείζονος συνθέσεως], 2008		
ΔΕΕ, C-70/10, <i>Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)</i> , 2011		
ΔΕΕ, C-582/14, <i>Patrick Breyer κατά Bundesrepublik Deutschland</i> , 2016		
ΔΕΕ, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, <i>YS κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S</i> , 2014		

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
ΔΕΕ, C-101/01, <i>Ποινική δίκη κατά Bodil Lindqvist</i> , 2003	Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα δεδομένα)	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 6 παράγραφος 1
ΔΕΕ, C-434/16, <i>Peter Nowak κατά Data Protection Commissioner</i> , 2017	Ανωνυμοποιημένα και ψευδωνυμοποιημένα δεδομένα προσωπικού χαρακτήρα	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο ε) Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, παράγραφος 50
Επεξεργασία δεδομένων		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 2 ΔΕΕ, C-212/13, <i>František Ryneš κατά Úřad pro ochranu osobních údajů</i> , 2014 ΔΕΕ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni</i> , 2017 ΔΕΕ, C-101/01, <i>Ποινική δίκη κατά Bodil Lindqvist</i> , 2003 ΔΕΕ, C-131/12, <i>Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [τμήμα μείζονος συνθέσεως], 2014	Ορισμοί	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχεία β) και γ)
Χρήστες δεδομένων		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 7 ΔΕΕ, C-212/13, <i>František Ryneš κατά Úřad pro ochranu osobních údajů</i> , 2014 ΔΕΕ, C-1318/12, <i>Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [τμήμα μείζονος συνθέσεως], 2014	Υπεύθυνος επεξεργασίας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο δ) Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 1 στοιχείο ζ)*

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 8	Εκτελών την επεξεργασία	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο στ) Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 1 στοιχείο η)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 9	Αποδέκτης	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο ε)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 10	Τρίτος	
Συγκατάθεση		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 11 και άρθρο 7 ΔΕΕ, C-543/09, <i>Deutsche Telekom AG κατά Bundesrepublik Deutschland</i> , 2011 ΔΕΕ, C-536/15, <i>Tele2 (Netherlands) BV κ.λπ. κατά Autoriteit Consument en Markt (ACM)</i> , 2017	Ορισμός και προϋποθέσεις έγκυρης συγκατάθεσης	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 2 Σύσταση για τα ιατρικά δεδομένα, άρθρο 6, και διάφορες μεταγενέστερες συστάσεις ΕΔΔΑ, <i>Elberte κατά Λετονίας</i> , προσφυγή αριθ. 61243/08, 2015

Σημείωση: * Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2010), Σύσταση CM/Rec (2010)13 της Επιτροπής των Υπουργών προς τα κράτη μέλη σχετικά με την προστασία των φυσικών προσώπων έναντι της αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της κατάρτισης προφίλ (σύσταση για την κατάρτιση προφίλ), 23 Νοεμβρίου 2010.

2.1. Δεδομένα προσωπικού χαρακτήρα

Κύρια σημεία

- Τα δεδομένα είναι δεδομένα προσωπικού χαρακτήρα εάν αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, το «υποκείμενο των δεδομένων».
- Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, θα πρέπει να λαμβάνονται υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν είτε από τον υπεύθυνο επεξεργασίας είτε από τρίτο, όπως για παράδειγμα ο διαχωρισμός του, για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου.

- Η επαλήθευση της ταυτότητας συνίσταται στην απόδειξη ότι ένα ορισμένο πρόσωπο διαθέτει ορισμένη ταυτότητα και/ή είναι εξουσιοδοτημένο να ασκεί ορισμένες δραστηριότητες.
- Υπάρχουν ειδικές κατηγορίες δεδομένων, τα λεγόμενα ευαίσθητα δεδομένα, τα οποία απαριθμούνται στην Εκσυγχρονισμένη Σύμβαση 108 και στο δίκαιο της ΕΕ για την προστασία των δεδομένων, απαιτούν ενισχυμένη προστασία και, επομένως, υπόκεινται σε ειδικό νομικό καθεστώς.
- Τα δεδομένα είναι ανωνυμοποιημένα εάν δεν συνδέονται πλέον με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.
- Η ψευδωνυμοποίηση είναι μέτρο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν να αποδοθούν στο υποκείμενο των δεδομένων χωρίς πρόσθετες πληροφορίες, οι οποίες διατηρούνται χωριστά. Το «κλειδί» που καθιστά εφικτή την εκ νέου εξακρίβωση της ταυτότητας των υποκειμένων των δεδομένων πρέπει να διατηρείται χωριστά και υπό ασφαλείς συνθήκες. Τα δεδομένα τα οποία αποτέλεσαν αντικείμενο ψευδωνυμοποίησης παραμένουν δεδομένα προσωπικού χαρακτήρα. Η έννοια των «ψευδωνυμοποιημένων δεδομένων» δεν υφίσταται στο δίκαιο της ΕΕ.
- Οι αρχές και οι κανόνες της προστασίας δεδομένων δεν εφαρμόζονται στις ανωνυμοποιημένες πληροφορίες. Ωστόσο, εφαρμόζονται στα ψευδωνυμοποιημένα δεδομένα.

2.1.1. Κύριες πτυχές της έννοιας των δεδομένων προσωπικού χαρακτήρα

Βάσει του δικαίου της ΕΕ, καθώς και **βάσει του δικαίου του Συμβουλίου της Ευρώπης**, ως «δεδομένα προσωπικού χαρακτήρα» νοούνται οι πληροφορίες που αφορούν ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο ¹³⁶. Πρόκειται για πληροφορίες σχετικά με πρόσωπο του οποίου η ταυτότητα είτε είναι προδήλως σαφής είτε μπορεί να εξακριβωθεί με συμπληρωματικές πληροφορίες. Για να κριθεί κατά πόσον ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο, ο υπεύθυνος επεξεργασίας ή άλλος τρίτος πρέπει να λαμβάνει υπόψη όλα τα μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την άμεση ή έμμεση εξακρίβωση της ταυτότητας του φυσικού προσώπου, όπως για παράδειγμα ο διαχωρισμός του, με αποτέλεσμα να καθίσταται εφικτή η διαφορετική μεταχείριση ενός προσώπου από άλλο ¹³⁷.

¹³⁶ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 1· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο α).

¹³⁷ Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 26.

Εάν υποβάλλονται σε επεξεργασία δεδομένα σχετικά με ένα πρόσωπο, το πρόσωπο αυτό καλείται «υποκείμενο των δεδομένων».

Το υποκείμενο των δεδομένων

Βάσει του δικαίου της ΕΕ, οι κανόνες περί προστασίας δεδομένων ισχύουν μόνο για τα φυσικά πρόσωπα ¹³⁸, και το ευρωπαϊκό δίκαιο για την προστασία των δεδομένων προστατεύει μόνο ζώντα πρόσωπα ¹³⁹. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) ορίζει ως «δεδομένα προσωπικού χαρακτήρα» κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Το δίκαιο του Συμβουλίου της Ευρώπης, και ιδίως η Εκσυγχρονισμένη Σύμβαση 108, αναφέρεται επίσης στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Και στην περίπτωση αυτή, ως «δεδομένο προσωπικού χαρακτήρα» νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Το φυσικό πρόσωπο ή πρόσωπο, όπως αναφέρεται στον ΓΚΠΔ και στην Εκσυγχρονισμένη Σύμβαση 108, αντίστοιχα, είναι γνωστό στο δίκαιο για την προστασία των δεδομένων ως το «υποκείμενο των δεδομένων».

Τα νομικά πρόσωπα τυγχάνουν επίσης κάποιας προστασίας. Στη νομολογία του ΕΔΔΑ περιλαμβάνονται αποφάσεις που έχουν εκδοθεί επί προσφυγών νομικών προσώπων που κατήγγειλαν παραβίαση του δικαιώματός τους για προστασία κατά της χρήσης των δεδομένων τους βάσει του άρθρου 8 της ΕΣΔΑ. Το άρθρο 8 της ΕΣΔΑ αναγνωρίζει τόσο το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, όσο και το δικαίωμα στον σεβασμό της κατοικίας και της αλληλογραφίας. Επομένως, το ΕΔΔΑ μπορεί να επιληφθεί υποθέσεων που αφορούν τον σεβασμό της κατοικίας και της αλληλογραφίας αντί του σεβασμού της ιδιωτικής ζωής.

¹³⁸ Ό.π., άρθρο 1.

¹³⁹ Ό.π., αιτιολογική σκέψη 27. Βλ. επίσης Ομάδα εργασίας του άρθρου 29 (2007), *Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα»*, WP 136, 20 Ιουνίου 2007, σ. 22.

Παράδειγμα: Η υπόθεση *Bernh Larsen Holding AS κ.λπ. κατά Νορβηγίας*¹⁴⁰ αφορούσε καταγγελία τριών νορβηγικών εταιρειών κατά απόφασης φορολογικής αρχής με την οποία είχαν διαταχθεί να παράσχουν στους φορολογικούς ελεγκτές αντίγραφο όλων των δεδομένων που διατηρούνταν σε διακομιστή ηλεκτρονικού υπολογιστή τον οποίο χρησιμοποιούσαν από κοινού.

Το ΕΔΔΑ αποφάνθηκε ότι η εν λόγω υποχρέωση που επιβλήθηκε στις προσφεύγουσες εταιρείες συνιστούσε επέμβαση στα δικαιώματά τους στον σεβασμό της «κατοικίας» και της «αλληλογραφίας» τους βάσει του άρθρου 8 της ΕΣΔΑ. Ωστόσο, το ΕΔΔΑ αποφάνθηκε ότι οι φορολογικές αρχές διέθεταν αποτελεσματικές και κατάλληλες εγγυήσεις κατά των καταχρήσεων: οι προσφεύγουσες εταιρείες είχαν ειδοποιηθεί εγκαίρως ήταν παρούσες και μπόρεσαν να υποβάλουν προτάσεις κατά τη διάρκεια της επιτόπιας παρέμβασης και το υλικό επρόκειτο να καταστραφεί μετά το πέρας του φορολογικού ελέγχου. Υπό τις περιστάσεις αυτές είχε επιτευχθεί ορθή ισορροπία μεταξύ, αφενός, του δικαιώματος των προσφευγουσών εταιρειών στον σεβασμό της «κατοικίας» και της «αλληλογραφίας» τους και του συμφέροντός τους που απέρρεε από την προστασία της ιδιωτικής ζωής των προσώπων που εργάζονταν σε αυτές και, αφετέρου, του δημόσιου συμφέροντος που υπηρετούνταν από τη διασφάλιση αποτελεσματικού ελέγχου για σκοπούς βεβαίωσης φόρων. Επομένως, το ΕΔΔΑ αποφάνθηκε ότι δεν υπήρξε παράβαση του άρθρου 8 της ΕΣΔΑ.

Σύμφωνα με την Εκσυγχρονισμένη Σύμβαση 108, η προστασία των δεδομένων αφορά, πρωτίστως, την προστασία φυσικών προσώπων· ωστόσο, τα συμβαλλόμενα μέρη μπορούν να επεκτείνουν την προστασία των δεδομένων σε νομικά πρόσωπα, όπως επιχειρήσεις και ενώσεις, στο εθνικό τους δίκαιο. Σύμφωνα με την Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης, το εθνικό δίκαιο μπορεί να προστατεύει τα θεμιτά συμφέροντα νομικών προσώπων επεκτείνοντας το πεδίο εφαρμογής της Σύμβασης στους φορείς αυτούς¹⁴¹. **Το δίκαιο της ΕΕ για την προστασία των δεδομένων** δεν καλύπτει την επεξεργασία δεδομένων που αφορούν νομικά πρόσωπα και ιδίως επιχειρήσεις συσταθείσες ως νομικά πρόσωπα, περιλαμβανομένων της επωνυμίας και του τύπου του νομικού προσώπου, καθώς

¹⁴⁰ ΕΔΔΑ, *Bernh Larsen Holding AS κ.λπ. κατά Νορβηγίας*, προσφυγή αριθ. 24117/08, 14 Μαρτίου 2013. Ωστόσο, βλ. επίσης, ΕΔΔΑ, *Liberty κ.λπ. κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 58243/00, 1 Ιουλίου 2008.

¹⁴¹ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σκέψη 30.

και των στοιχείων επικοινωνίας αυτού ¹⁴². Ωστόσο, η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες προστατεύει την εμπιστευτικότητα των επικοινωνιών και τα θεμιτά συμφέροντα νομικών προσώπων έναντι των αυξανόμενων δυνατοτήτων αυτόματης αποθήκευσης και επεξεργασίας δεδομένων που αφορούν συνδρομητές και χρήστες ¹⁴³. Ομοίως, το σχέδιο κανονισμού για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες επεκτείνει την προστασία στα νομικά πρόσωπα.

Παράδειγμα: Στην υπόθεση *Volker und Markus Schecke και Hartmut Eifert κατά Land Hessen* ¹⁴⁴, το ΔΕΕ, παραπέμποντας στη δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα που αφορούσαν δικαιούχους γεωργικών ενισχύσεων, αποφάνθηκε ότι «τα νομικά πρόσωπα δεν μπορούν να επικαλούνται την κατά τα άρθρα 7 και 8 του Χάρτη προστασία έναντι μιας τέτοιας αναφοράς παρά μόνο στο μέτρο που η επωνυμία του νομικού προσώπου προσδιορίζει ένα ή περισσότερα φυσικά πρόσωπα. [...] Ο σεβασμός του δικαιώματος στην ιδιωτική ζωή ενόψει της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ο οποίος αναγνωρίζεται στα άρθρα 7 και 8 του Χάρτη, αφορά κάθε πληροφορία σχετικά με φυσικό πρόσωπο η ταυτότητα του οποίου είναι γνωστή ή μπορεί να εξακριβωθεί [...]» ¹⁴⁵.

Σταθμίζοντας, αφενός, το συμφέρον της ΕΕ σε ό,τι αφορά τη διασφάλιση διαφάνειας κατά την κατανομή ενισχύσεων και, αφετέρου, τα θεμελιώδη δικαιώματα στην ιδιωτική ζωή και στην προστασία των δεδομένων των φυσικών προσώπων που έλαβαν ενίσχυση, το ΔΕΕ εκτίμησε ότι η επέμβαση στα εν λόγω θεμελιώδη δικαιώματα ήταν δυσανάλογη. Το ΔΕΕ έκρινε ότι ο στόχος της διαφάνειας θα μπορούσε να είχε επιτευχθεί αποτελεσματικά με μέτρα τα οποία είναι λιγότερο παρεμβατικά όσον αφορά τα δικαιώματα των ενδιαφερόμενων φυσικών προσώπων. Ωστόσο, όταν εξέτασε την αναλογικότητα της δημοσιοποίησης πληροφοριών σχετικά με τα νομικά πρόσωπα που έλαβαν ενίσχυση, το ΔΕΕ κατέληξε σε διαφορετικό συμπέρασμα, αποφαινόμενο ότι η εν λόγω δημοσιοποίηση δεν υπερέβαινε τα όρια της αρχής της αναλογικότητας. Διευκρίνισε ότι

¹⁴² Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 14.

¹⁴³ Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, αιτιολογική σκέψη 7 και άρθρο 1 παράγραφος 2.

¹⁴⁴ ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, *Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen* [τμήμα μείζονος συνθέσεως], 9 Νοεμβρίου 2010, σκέψη 53.

¹⁴⁵ Ό.π., σκέψεις 52-53.

«συγκεκριμένα, η σοβαρότητα της προσβολής του δικαιώματος στην προστασία δεδομένων προσωπικού χαρακτήρα είναι διαφορετική για τα νομικά πρόσωπα σε σχέση με τα φυσικά πρόσωπα»¹⁴⁶. Τα νομικά πρόσωπα έχουν αυξημένες υποχρεώσεις όσον αφορά τη δημοσιοποίηση πληροφοριών που τα αφορούν. Το ΔΕΕ έκρινε ότι η επιβολή στις εθνικές αρχές της υποχρέωσης να εξετάζουν, πριν από τη δημοσιοποίηση των δεδομένων, αν τα δεδομένα κάθε δικαιούχου νομικού προσώπου προσδιορίζουν οποιαδήποτε συνδεδεμένα φυσικά πρόσωπα θα συνεπαγόταν δυσανάλογο διοικητικό φόρτο για τις εν λόγω αρχές. Επομένως, η νομοθεσία που απαιτούσε γενικευμένη δημοσιοποίηση των δεδομένων σχετικά με τα νομικά πρόσωπα είχε επιτύχει ορθή ισορροπία μεταξύ των διακυβευόμενων ανταγωνιστικών συμφερόντων.

Φύση των δεδομένων

Κάθε είδους πληροφορία μπορεί να συνιστά δεδομένο προσωπικού χαρακτήρα εφόσον αφορά ταυτοποιημένο ή ταυτοποιήσιμο πρόσωπο.

Παράδειγμα: Η αξιολόγηση από προϊστάμενο των εργασιακών επιδόσεων υπαλλήλου, η οποία αποθηκεύεται στον προσωπικό φάκελο του υπαλλήλου, συνιστά δεδομένο προσωπικού χαρακτήρα που αφορά τον υπάλληλο. Αυτό ισχύει παρότι μπορεί να αντικατοπτρίζει απλώς, εν όλω ή εν μέρει, την προσωπική άποψη του προϊσταμένου, όπως «ο/η υπάλληλος δεν είναι προσηλωμένος/-η στην εργασία του/της», και όχι αναμφισβήτητα πραγματικά περιστατικά, όπως «ο/η υπάλληλος απουσίασε από την εργασία επί πέντε εβδομάδες στη διάρκεια των τελευταίων έξι μηνών».

Τα δεδομένα προσωπικού χαρακτήρα περιλαμβάνουν πληροφορίες που αφορούν την ιδιωτική ζωή ενός προσώπου, συμπεριλαμβανομένων και των επαγγελματικών δραστηριοτήτων, καθώς και πληροφορίες σχετικά με τη δημόσια ζωή του.

Στην υπόθεση *Amann*¹⁴⁷, το ΕΔΔΑ έκρινε ότι ο όρος «δεδομένα προσωπικού χαρακτήρα» δεν περιορίζεται σε θέματα που εμπίπτουν στην ιδιωτική σφαίρα

¹⁴⁶ Ό.π., σκέψη 87.

¹⁴⁷ Βλ. ΕΔΔΑ, *Amann κατά Ελβετίας*, προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000, σκέψη 65.

φυσικού προσώπου. Αυτή η έννοια του όρου «δεδομένα προσωπικού χαρακτήρα» είναι επίσης λυσιτελής για τον ΓΚΠΔ.

Παράδειγμα: Στην υπόθεση *Volker und Markus Schecke και Hartmut Eifert κατά Land Hessen*¹⁴⁸, το ΔΕΕ διευκρίνισε ότι «δεν ασκεί, συναφώς, επιρροή το γεγονός ότι οι δημοσιοποιούμενες πληροφορίες αφορούν επαγγελματικές δραστηριότητες [...]. Το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων έκρινε συναφώς, ως προς την ερμηνεία του άρθρου 8 της Σύμβασης (ΕΣΔΑ), ότι ο όρος “ιδιωτική ζωή” δεν πρέπει να ερμηνεύεται συσταλτικά και ότι δεν υφίσταται κανένας λόγος αρχής για τον αποκλεισμό των επαγγελματικών δραστηριοτήτων [...] από την έννοια της “ιδιωτικής ζωής”».

Παράδειγμα: Στις συνεκδικασθείσες υποθέσεις *YS κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S*¹⁴⁹, το ΔΕΕ έκρινε ότι η νομική ανάλυση την οποία περιείχε το σχέδιο απόφασης της υπηρεσίας μετανάστευσης και πολιτογράφησης σχετικά με αιτήσεις άδειας παραμονής δεν συνιστά αυτή καθαυτή δεδομένο προσωπικού χαρακτήρα, παρότι ενδέχεται να περιέχει ορισμένα δεδομένα προσωπικού χαρακτήρα.

Η νομολογία του ΕΔΔΑ σχετικά με το άρθρο 8 της ΕΣΔΑ επιβεβαιώνει ότι ο πλήρης διαχωρισμός των θεμάτων της ιδιωτικής και της επαγγελματικής ζωής μπορεί να είναι δυσχερές¹⁵⁰.

Παράδειγμα: Στην υπόθεση *Bărbulescu κατά Ρουμανίας*¹⁵¹, ο προσφεύγων είχε απολυθεί επειδή χρησιμοποίησε τη σύνδεση στο διαδίκτυο του εργοδότη του στη διάρκεια του ωραρίου εργασίας κατά παράβαση των εσωτερικών κανονισμών. Ο εργοδότης του είχε παρακολουθήσει

148 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, *Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen* [τμήμα μείζονος συνθέσεως], 9 Νοεμβρίου 2010, σκέψη 59.

149 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, *YS κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S*, 17 Ιουλίου 2014, σκέψη 39.

150 Βλ., για παράδειγμα, ΕΔΔΑ, *Rotaru κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000, σκέψη 43· ΕΔΔΑ, *Niemietz κατά Γερμανίας*, προσφυγή αριθ. 13710/88, 16 Δεκεμβρίου 1992, σκέψη 29.

151 ΕΔΔΑ, *Bărbulescu κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 61496/08, 5 Σεπτεμβρίου 2017, σκέψη 121.

τις επικοινωνίες του, ενώ και τα σχετικά αρχεία, τα οποία περιείχαν μηνύματα αμιγώς προσωπικής φύσης, προσκομίστηκαν στην εθνική διαδικασία. Δεδομένου ότι έκρινε ότι το άρθρο 8 τυγχάνει εφαρμογής, το ΕΔΔΑ δεν εξέτασε αν οι περιοριστικοί κανονισμοί του εργοδότη παρείχαν στον προσφεύγοντα εύλογη προσδοκία όσον αφορά την προστασία της ιδιωτικής ζωής, αλλά αποφάνθηκε, εν πάση περιπτώσει, ότι οι οδηγίες εκ μέρους εργοδότη δεν μπορούν να εκμηδενίζουν την ιδιωτική κοινωνική ζωή στον χώρο εργασίας. Επί της ουσίας, πρέπει να αναγνωρίζεται στα συμβαλλόμενα κράτη ευρύ περιθώριο εκτίμησης κατά την αξιολόγηση της ανάγκης θέσπισης νομικού πλαισίου που θα διέπει τις προϋποθέσεις υπό τις οποίες ένας εργοδότης μπορεί να ρυθμίζει τις –ηλεκτρονικές ή άλλης μορφής– μη επαγγελματικές επικοινωνίες των υπαλλήλων του στον χώρο εργασίας. Παρ’ όλα αυτά, οι εθνικές αρχές πρέπει να διασφαλίσουν ότι η θέσπιση από τον εργοδότη μέτρων παρακολούθησης της αλληλογραφίας και άλλων επικοινωνιών, ανεξάρτητα από την έκταση και τη διάρκεια των εν λόγω μέτρων, θα συνοδεύεται από κατάλληλες και επαρκείς εγγυήσεις κατά των καταχρήσεων. Η αναλογικότητα και οι διαδικαστικές εγγυήσεις έναντι της αυθαιρεσίας ήταν καθοριστικής σημασίας, και το ΕΔΔΑ προσδιόρισε ορισμένους παράγοντες οι οποίοι ήταν συναφείς υπό τις συγκεκριμένες περιστάσεις. Στους παράγοντες αυτούς συγκαταλέγονταν, για παράδειγμα, η έκταση της παρακολούθησης των υπαλλήλων από τον εργοδότη και ο βαθμός επέμβασης στην ιδιωτική ζωή του υπαλλήλου, οι συνέπειες για τον υπάλληλο και η πρόβλεψη ή μη κατάλληλων εγγυήσεων. Επιπλέον, οι εθνικές αρχές έπρεπε να διασφαλίσουν ότι υπάλληλος του οποίου οι επικοινωνίες είχαν υποβληθεί σε παρακολούθηση θα είχε πρόσβαση σε ένδικο βοήθημα ενώπιον δικαστηρίου με δικαιοδοσία να καθορίσει, τουλάχιστον επί της ουσίας, τον τρόπο τήρησης των περιγραφέντων κριτηρίων και αν τα προσβαλλόμενα μέτρα ήταν νόμιμα. Στην προκειμένη περίπτωση, το ΕΔΔΑ διαπίστωσε παράβαση του άρθρου 8, επειδή οι εθνικές αρχές δεν είχαν προστατεύσει κατάλληλα το δικαίωμα του προσφεύγοντος στον σεβασμό της ιδιωτικής ζωής και της αλληλογραφίας του και, ως εκ τούτου, δεν είχαν επιτύχει ορθή ισορροπία μεταξύ των διακυβευόμενων συμφερόντων.

Βάσει του δικαίου της ΕΕ καθώς και **βάσει του δικαίου του Συμβουλίου της Ευρώπης**, οι πληροφορίες περιέχουν δεδομένα σχετικά με ένα πρόσωπο εάν:

- ένα φυσικό πρόσωπο ταυτοποιείται ή είναι ταυτοποιήσιμο με τις πληροφορίες αυτές ή
- ένα φυσικό πρόσωπο, μολονότι δεν ταυτοποιείται, μπορεί να διαχωριστεί με τις πληροφορίες αυτές κατά τρόπο που να καθιστά εφικτό να εξακριβωθεί ποιο είναι το υποκείμενο των δεδομένων με τη διενέργεια περαιτέρω έρευνας.

Αμφότερα τα είδη πληροφοριών προστατεύονται με τον ίδιο τρόπο βάσει του ευρωπαϊκού δικαίου για την προστασία των δεδομένων. Η άμεση ή έμμεση δυνατότητα εξακρίβωσης της ταυτότητας φυσικών προσώπων απαιτεί συνεχή αξιολόγηση, «λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας»¹⁵². Το ΕΔΔΑ έχει αποφανθεί κατ' επανάληψη ότι η έννοια των «δεδομένων προσωπικού χαρακτήρα» στο πλαίσιο της ΕΣΔΑ είναι ίδια με τη χρησιμοποιούμενη στη Σύμβαση 108, ιδίως αναφορικά με την προϋπόθεση που αφορά τα ταυτοποιημένα ή ταυτοποιήσιμα πρόσωπα¹⁵³.

Στον ΓΚΠΔ ορίζεται ότι ένα φυσικό πρόσωπο είναι ταυτοποιήσιμο όταν «η ταυτότητά [του] μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου»¹⁵⁴. Επομένως, η εξακρίβωση της ταυτότητας απαιτεί στοιχεία τα οποία περιγράφουν ένα πρόσωπο κατά τρόπο που αυτό να διακρίνεται από άλλα πρόσωπα και να μπορεί να αναγνωριστεί ως φυσικό πρόσωπο. Το όνομα είναι χαρακτηριστικό παράδειγμα τέτοιων περιγραφικών στοιχείων και μπορεί να προσδιορίσει άμεσα ένα πρόσωπο. Σε ορισμένες περιπτώσεις, άλλα χαρακτηριστικά μπορεί να έχουν παρόμοιες συνέπειες με το όνομα, καθιστώντας ένα πρόσωπο έμμεσα ταυτοποιήσιμο. Ο αριθμός τηλεφώνου, ο αριθμός κοινωνικής

152 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 26.

153 Βλ. ΕΔΔΑ, *Amann κατά Ελβετίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000, σκέψη 65.

154 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 1.

ασφάλισης και ο αριθμός κυκλοφορίας οχήματος είναι παραδείγματα πληροφοριών οι οποίες μπορεί να καθιστούν ταυτοποιήσιμο ένα φυσικό πρόσωπο. Ιδιοχαρακτηριστικά –όπως ηλεκτρονικά αρχεία, cookies και εργαλεία παρακολούθησης της κίνησης στον Παγκόσμιο Ιστό– μπορούν επίσης να χρησιμοποιηθούν για τον διαχωρισμό φυσικών προσώπων προσδιορίζοντας τη συμπεριφορά και τις συνήθειές τους. Όπως εξηγείται σε γνώμη της Ομάδας εργασίας του άρθρου 29, «χωρίς ούτε καν να ερευνηθεί το όνομα και η διεύθυνση του ατόμου, το άτομο αυτό είναι δυνατόν να ενταχθεί σε μια κατηγορία με βάση κοινωνικοοικονομικά, ψυχολογικά, φιλοσοφικά ή άλλα κριτήρια και να αποδοθούν σε αυτό ορισμένες αποφάσεις, δεδομένου ότι το σημείο επαφής του ατόμου (ο ηλεκτρονικός υπολογιστής) δεν απαιτεί πλέον την αποκάλυψη της ταυτότητάς του σε στενή έννοια»¹⁵⁵. Ο ορισμός των δεδομένων προσωπικού χαρακτήρα, στο πλαίσιο τόσο του Συμβουλίου της Ευρώπης όσο και της ΕΕ, είναι αρκετά ευρύς ώστε να καλύπτει όλες τις δυνατότητες εξακρίβωσης της ταυτότητας (και, επομένως, όλους τους βαθμούς αναγνωρισιμότητας).

Παράδειγμα: Στην υπόθεση *Promusicae κατά Telefónica de España*¹⁵⁶, το ΔΕΕ έκρινε ότι «δεν αμφισβητείται ότι η ζητούμενη από την Promusicae ανακοίνωση των ονομάτων και των διευθύνσεων ορισμένων χρηστών [ορισμένης διαδικτυακής πλατφόρμας ανταλλαγής αρχείων] συνεπάγεται τη διάθεση δεδομένων προσωπικού χαρακτήρα, δηλαδή πληροφοριών για φυσικά πρόσωπα των οποίων η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, σύμφωνα με τον ορισμό του άρθρου 2, στοιχείο α', της οδηγίας 95/46 [νυν άρθρο 4 σημείο 1 του ΓΚΠΔ]. Αυτή η ανακοίνωση πληροφοριών τις οποίες, κατά την Promusicae, έχει αποθηκεύσει η Telefónica –πράγμα το οποίο δεν αμφισβητεί η τελευταία– συνιστά επεξεργασία δεδομένων προσωπικού χαρακτήρα»¹⁵⁷.

Παράδειγμα: Η υπόθεση *Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*¹⁵⁸ αφορούσε την άρνηση του φορέα παροχής υπηρεσιών διαδικτύου Scarlet να εγκαταστήσει σύστημα χρήσης

155 Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, *Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα»*, WP 136, 20 Ιουνίου 2007, σ. 15.

156 ΔΕΕ, C-275/06, *Productores de Música de España (Promusicae) κατά Telefónica de España SAU* [τμήμα μείζονος συνθέσεως], 29 Ιανουαρίου 2008, σκέψη 45.

157 Πρώην οδηγία 95/46, άρθρο 2 στοιχείο β), νυν Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 2.

158 ΔΕΕ, C-70/10, *Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Νοεμβρίου 2011, σκέψη 51.

φίλτρου στις ηλεκτρονικές επικοινωνίες που χρησιμοποιούν λογισμικό ανταλλαγής αρχείων για την πρόληψη της ανταλλαγής αρχείων, σύστημα το οποίο προσβάλλει τα δικαιώματα δημιουργού που προστατεύει η SABAM, εταιρεία διαχείρισης η οποία εκπροσωπεί δημιουργούς, συνθέτες και παραγωγούς μουσικών έργων. Το ΔΕΕ έκρινε ότι οι διευθύνσεις IP των χρηστών «συνιστούν δεδομένα προσωπικού χαρακτήρα καθόσον καθιστούν δυνατή την πλήρη αναγνώριση των εν λόγω χρηστών».

Δεδομένου ότι πολλά ονόματα δεν είναι μοναδικά, η εξακρίβωση της ταυτότητας ενός προσώπου μπορεί να απαιτεί πρόσθετα χαρακτηριστικά ώστε να διασφαλίζεται ότι δεν υπάρχει σύγχυση μεταξύ προσώπων. Ενίοτε, ενδέχεται να πρέπει να συνδυαστούν άμεσα και έμμεσα χαρακτηριστικά προκειμένου να προσδιοριστεί το φυσικό πρόσωπο το οποίο αφορούν οι πληροφορίες. Συχνά χρησιμοποιούνται η ημερομηνία και ο τόπος γέννησης. Επιπλέον, σε κάποιες χώρες έχουν θεσπιστεί εξατομικευμένοι αριθμοί για την καλύτερη διαφοροποίηση των πολιτών. Διαβιβασθέντα φορολογικά δεδομένα ¹⁵⁹, δεδομένα που αφορούν αιτούντα άδεια παραμονής τα οποία περιέχονται σε διοικητικό έγγραφο ¹⁶⁰, καθώς και έγγραφα που αφορούν τραπεζικές σχέσεις και σχέσεις θεματοφυλακής ¹⁶¹ ενδέχεται να αποτελούν δεδομένα προσωπικού χαρακτήρα. Βιομετρικά δεδομένα, όπως δακτυλικά αποτυπώματα, ψηφιακές φωτογραφίες ή ιριδοσκόπηση, δεδομένα θέσης και επιγραμμικά ιδιοχαρακτηριστικά χρησιμοποιούνται ολοένα και περισσότερο για την εξακρίβωση της ταυτότητας προσώπων στην τεχνολογική εποχή.

Ωστόσο, σε ό,τι αφορά τη δυνατότητα εφαρμογής του ευρωπαϊκού δικαίου για την προστασία των δεδομένων, δεν απαιτείται να εξακριβωθεί πραγματικά η ταυτότητα του υποκειμένου των δεδομένων· αρκεί να είναι ταυτοποιήσιμο το ενδιαφερόμενο πρόσωπο. Ένα πρόσωπο θεωρείται ταυτοποιήσιμο εάν υπάρχουν αρκετά διαθέσιμα στοιχεία μέσω των οποίων η ταυτότητά του μπορεί να εξακριβωθεί άμεσα ή έμμεσα ¹⁶². Σύμφωνα με την αιτιολογική σκέψη 26 του ΓΚΠΔ, το κριτήριο αναφοράς είναι κατά πόσον είναι πιθανό οι προβλέψιμοι χρήστες των πληροφοριών να διαθέτουν και να διαχειρίζονται μέσα τα οποία είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας,

¹⁵⁹ ΔΕΕ, C-201/14, *Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ.*, 1 Οκτωβρίου 2015.

¹⁶⁰ ΔΕΕ, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, *YS κατά Minister voor Immigratie, Integratie en Asiel* και *Minister voor Immigratie, Integratie en Asiel κατά M και S*, 17 Ιουλίου 2014.

¹⁶¹ ΕΔΔΑ, *M.N. κ.λπ. κατά Αγίου Μαρίνου*, προσφυγή αριθ. 28005/12, 7 Ιουλίου 2015.

¹⁶² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 1.

συμπεριλαμβανομένων των πληροφοριών που κατέχουν τρίτοι αποδέκτες (βλ. ενότητα 2.3.2).

Παράδειγμα: Αρχή τοπικής αυτοδιοίκησης αποφασίζει να συλλέγει δεδομένα σχετικά με τα αυτοκίνητα που υπερβαίνουν το όριο ταχύτητας στους δρόμους της κοινότητας. Φωτογραφίζει τα αυτοκίνητα, καταγράφοντας αυτομάτως την ώρα και τον τόπο, προκειμένου να διαβιβάσει τα δεδομένα στην αρμόδια αρχή, ώστε αυτή να μπορέσει να επιβάλει πρόστιμο σε εκείνους που παραβίασαν τα όρια ταχύτητας. Υποκείμενο των δεδομένων υποβάλλει καταγγελία, υποστηρίζοντας ότι η αρχή τοπικής αυτοδιοίκησης δεν διαθέτει νομική βάση, κατά το δίκαιο περί προστασίας δεδομένων, για τέτοια συλλογή δεδομένων. Η αρχή τοπικής αυτοδιοίκησης υποστηρίζει ότι δεν συλλέγει δεδομένα προσωπικού χαρακτήρα. Διατείνεται ότι οι πινακίδες κυκλοφορίας είναι ανώνυμες πληροφορίες. Η αρχή τοπικής αυτοδιοίκησης δεν διαθέτει εξουσιοδότηση βάσει του νόμου για να αποκτήσει πρόσβαση στο γενικό μητρώο οχημάτων ώστε να εξακριβώσει την ταυτότητα του ιδιοκτήτη ή του οδηγού του αυτοκινήτου.

Η συλλογιστική αυτή δεν συνάδει με την αιτιολογική σκέψη 26 του ΓΚΠΔ. Δεδομένου ότι ο σκοπός της συλλογής δεδομένων είναι σαφώς η εξακρίβωση της ταυτότητας των παραβατών του ορίου ταχύτητας και η επιβολή προστίμου σε αυτούς, μπορεί να προβλεφθεί ότι θα επιχειρηθεί εξακρίβωση της ταυτότητας. Παρότι η αρχή τοπικής αυτοδιοίκησης δεν έχει άμεσα στη διάθεσή της κάποιο μέσο εξακρίβωσης της ταυτότητας, θα διαβιβάσει τα δεδομένα στην αρμόδια αρχή, την αστυνομία, η οποία διαθέτει τέτοια μέσα. Επίσης, στην αιτιολογική σκέψη 26 αναφέρεται ρητώς σενάριο στο οποίο μπορεί να προβλεφθεί ότι περαιτέρω αποδέκτες των δεδομένων, πέραν του άμεσου χρήστη τους, ενδέχεται να επιχειρήσουν να εξακριβώσουν την ταυτότητα του φυσικού προσώπου. Λαμβανομένης υπόψη της αιτιολογικής σκέψης 26, η ενέργεια της αρχής τοπικής αυτοδιοίκησης ισοδυναμεί με συλλογή δεδομένων σχετικά με ταυτοποιήσιμα πρόσωπα και, επομένως, απαιτεί νομική βάση σύμφωνα με το δίκαιο για την προστασία των δεδομένων.

«Για να διαπιστωθεί κατά πόσον κάποια μέσα είναι ευλόγως πιθανό ότι θα χρησιμοποιηθούν για την εξακρίβωση της ταυτότητας του φυσικού προσώπου, θα πρέπει να λαμβάνονται υπόψη όλοι οι αντικειμενικοί παράγοντες, όπως τα έξοδα

και ο χρόνος που απαιτούνται για την ταυτοποίηση, λαμβανομένων υπόψη της τεχνολογίας που είναι διαθέσιμη κατά τον χρόνο της επεξεργασίας και των εξελίξεων της τεχνολογίας»¹⁶³.

Παράδειγμα: Στην υπόθεση *Breyer κατά Bundesrepublik Deutschland*¹⁶⁴, το ΔΕΕ εξέτασε την έννοια της έμμεσης δυνατότητας εξακρίβωσης της ταυτότητας των υποκειμένων των δεδομένων. Η υπόθεση αφορούσε δυναμικές διευθύνσεις IP, οι οποίες αλλάζουν κάθε φορά που πραγματοποιείται νέα σύνδεση στο διαδίκτυο. Οι ιστότοποι των γερμανικών ομοσπονδιακών υπηρεσιών κατέγραφαν και αποθήκευαν δυναμικές διευθύνσεις IP για την πρόληψη των επιθέσεων στον κυβερνοχώρο και την κίνηση ποινικής διαδικασίας, εφόσον ήταν αναγκαίο. Μόνο ο φορέας παροχής υπηρεσιών διαδικτύου που χρησιμοποιούσε ο P. Breyer διέθετε τις συμπληρωματικές πληροφορίες που ήταν αναγκαίες για την εξακρίβωση της ταυτότητάς του.

Το ΔΕΕ έκρινε ότι μια δυναμική διεύθυνση IP, την οποία αποθηκεύει φορέας παροχής υπηρεσιών τηλεμέσων όταν ένα πρόσωπο επισκέπτεται ιστότοπο τον οποίο ο φορέας έχει καταστήσει προσβάσιμο στο κοινό, συνιστά δεδομένο προσωπικού χαρακτήρα όταν μόνο ένας τρίτος –εν προκειμένω ο φορέας παροχής υπηρεσιών διαδικτύου– διαθέτει τις αναγκαίες πρόσθετες πληροφορίες για την εξακρίβωση της ταυτότητας του προσώπου¹⁶⁵. Αποφάνθηκε ότι «δεν απαιτείται όλες οι πληροφορίες που καθιστούν δυνατή την εξακρίβωση του εμπλεκόμενου προσώπου να βρίσκονται στη διάθεση ενός μόνον προσώπου» για να συνιστούν δεδομένα προσωπικού χαρακτήρα. Η ταυτότητα των χρηστών δυναμικής διεύθυνσης IP που καταγράφεται από φορέα παροχής υπηρεσιών διαδικτύου ενδέχεται να εξακριβωθεί σε ορισμένες περιπτώσεις, για παράδειγμα στο πλαίσιο ποινικής διαδικασίας σε περίπτωση επιθέσεων στον κυβερνοχώρο, με τη βοήθεια άλλων προσώπων¹⁶⁶. Κατά το ΔΕΕ, όταν ο φορέας «έχει στη διάθεσή του νόμιμα μέσα βάσει των οποίων

¹⁶³ Ό.π., αιτιολογική σκέψη 26.

¹⁶⁴ ΔΕΕ, C-582/14, *Patrick Breyer κατά Bundesrepublik Deutschland*, 19 Οκτωβρίου 2016, σκέψη 43.

¹⁶⁵ Πρώην οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, άρθρο 2 στοιχείο α).

¹⁶⁶ ΔΕΕ, C-70/10, *Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Νοεμβρίου 2011, σκέψεις 47-48.

μπορεί να εξακριβωθεί η ταυτότητα του οικείου προσώπου χάρη στις πρόσθετες πληροφορίες που έχει στη διάθεσή του ο πάροχος υπηρεσιών προσβάσεως στο διαδίκτυο του εν λόγω προσώπου», αυτό συνιστά «μέσο που μπορεί ευλόγως να χρησιμοποιηθεί για να εξακριβωθεί η ταυτότητα του οικείου προσώπου». Επομένως, τέτοια δεδομένα θεωρούνται δεδομένα προσωπικού χαρακτήρα.

Στο πλαίσιο του δικαίου του Συμβουλίου της Ευρώπης, η αναγνωρισιμότητα γίνεται αντιληπτή με παρόμοιο τρόπο. Στην αιτιολογική έκθεση της Εκσυγχρονισμένης Σύμβασης 108 περιλαμβάνεται παρόμοια περιγραφή: η έννοια του «ταυτοποιήσιμου» δεν αναφέρεται μόνο στην αστική ή νομική ταυτότητα του φυσικού προσώπου αυτή καθαυτή, αλλά και στα στοιχεία που ενδέχεται να καθιστούν εφικτή την «εξατομίκευση» ή τον διαχωρισμό ενός προσώπου από άλλα και, ως εκ τούτου, τη δυνητικά διαφορετική μεταχείρισή του. Η «εξατομίκευση» αυτή θα μπορούσε, για παράδειγμα, να επιτευχθεί με τη συγκεκριμένη αναφορά στο συγκεκριμένο πρόσωπο ή σε συσκευή ή συνδυασμό συσκευών (ηλεκτρονικό υπολογιστή, κινητό τηλέφωνο, συσκευές παιχνιδιών κ.λπ.) που συνδέονται με αναγνωριστικό αριθμό, ψευδώνυμο, βιομετρικά ή γενετικά δεδομένα, δεδομένα θέσης, διεύθυνση IP ή άλλο αναγνωριστικό στοιχείο ταυτότητας ¹⁶⁷. Ένα φυσικό πρόσωπο δεν θεωρείται «ταυτοποιήσιμο» εάν η εξακρίβωση της ταυτότητάς του απαιτεί χρόνο, προσπάθεια ή πόρους που δεν είναι εύλογοι. Αυτό συμβαίνει, για παράδειγμα, όταν η εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων απαιτεί υπερβολικά πολύπλοκες, χρονοβόρες και δαπανηρές ενέργειες. Ο μη εύλογος χαρακτήρας του χρόνου, της προσπάθειας ή των πόρων πρέπει να εκτιμάται κατά περίπτωση, λαμβάνοντας υπόψη παράγοντες όπως τον σκοπό της επεξεργασίας, το κόστος και τα οφέλη της εξακρίβωσης της ταυτότητας, το είδος του υπευθύνου επεξεργασίας και τη χρησιμοποιούμενη τεχνολογία ¹⁶⁸.

Όσον αφορά τη μορφή αποθήκευσης ή χρήσης των δεδομένων προσωπικού χαρακτήρα, είναι σημαντικό να επισημανθεί ότι αυτή δεν έχει σημασία για τη δυνατότητα εφαρμογής του δικαίου για την προστασία των δεδομένων. Γραπτές ή προφορικές επικοινωνίες μπορεί να περιέχουν δεδομένα προσωπικού χαρακτήρα όπως εικόνες ¹⁶⁹, συμπεριλαμβανομένου υλικού από κλειστό κύκλωμα

¹⁶⁷ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σκέψη 18.

¹⁶⁸ Ό.π., σκέψη 17.

¹⁶⁹ ΕΔΔΑ, *Von Hannover κατά Γερμανίας*, προσφυγή αριθ. 59320/00, 24 Ιουνίου 2004· ΕΔΔΑ, *Sciaccia κατά Ιταλίας*, προσφυγή αριθ. 50774/99, 11 Ιανουαρίου 2005· ΔΕΕ, C-212/13, *František Ryneš κατά Úřad pro ochranu osobních údajů*, 11 Δεκεμβρίου 2014.

τηλεόρασης (CCTV) ¹⁷⁰, ή ήχο ¹⁷¹. Ηλεκτρονικά καταγεγραμμένες πληροφορίες και πληροφορίες σε έντυπη μορφή μπορεί επίσης να είναι δεδομένα προσωπικού χαρακτήρα. Ακόμη και κυτταρικά δείγματα ανθρώπινου ιστού –στα οποία καταγράφεται το DNA ενός προσώπου– μπορεί να είναι πηγές από τις οποίες μπορούν να εξαχθούν βιομετρικά δεδομένα ¹⁷², εφόσον τα δεδομένα αφορούν τα κληρονομικά ή επίκτητα γενετικά χαρακτηριστικά του προσώπου, παρέχουν μοναδικές πληροφορίες σχετικά με την υγεία ή τη φυσιολογία του και προκύπτουν από ανάλυση βιολογικού δείγματος του συγκεκριμένου προσώπου ¹⁷³.

Ανωνυμοποίηση

Σύμφωνα με την αρχή του περιορισμού της αποθήκευσης, η οποία προβλέπεται τόσο στον ΓΚΠΔ όσο και στην Εκσυγχρονισμένη Σύμβαση 108 (εξετάζεται λεπτομερέστερα στο [κεφάλαιο 3](#)), τα δεδομένα πρέπει να διατηρούνται «υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα» ¹⁷⁴. Επομένως, τα δεδομένα θα πρέπει να διαγραφούν ή να ανωνυμοποιηθούν εάν ο υπεύθυνος επεξεργασίας επιθυμεί να τα αποθηκεύσει όταν δεν είναι πλέον αναγκαία και δεν εξυπηρετούν πλέον τον αρχικό σκοπό τους.

Η διαδικασία ανωνυμοποίησης των δεδομένων σημαίνει ότι όλα τα αναγνωριστικά στοιχεία απαλείφονται από ένα σύνολο δεδομένων προσωπικού χαρακτήρα έτσι ώστε το υποκείμενο των δεδομένων να μην είναι πλέον ταυτοποιήσιμο ¹⁷⁵. Στη γνώμη 05/2014 που εξέδωσε, η Ομάδα εργασίας του άρθρου 29 αναλύει την αποτελεσματικότητα και τα όρια των διαφόρων τεχνικών

170 ΕΔΔΑ, *Peck κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 44647/98, 28 Ιανουαρίου 2003· ΕΔΔΑ, *Körke κατά Γερμανίας* (διάταξη), προσφυγή αριθ. 420/07, 5 Οκτωβρίου 2010· ΕΕΠΔ (2010), *The EDPS video-surveillance guidelines*, 17 Μαρτίου 2010.

171 ΕΔΔΑ, *P.G. και J.H. κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 44787/98, 25 Σεπτεμβρίου 2001, σκέψεις 59-60· ΕΔΔΑ, *Wisse κατά Γαλλίας*, προσφυγή αριθ. 71611/01, 20 Δεκεμβρίου 2005 (έκδοση στη γαλλική γλώσσα).

172 Βλ. Ομάδα εργασίας του άρθρου 29 (2007), *Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα»*, WP 136, 20 Ιουνίου 2007, σ. 9· Συμβούλιο της Ευρώπης, Σύσταση Rec (2006)4 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την έρευνα επί βιολογικού υλικού ανθρώπινης προέλευσης, 15 Μαρτίου 2006.

173 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 13.

174 Ο.π., άρθρο 5 παράγραφος 1 στοιχείο ε)· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο ε).

175 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 26.

ανωνυμοποίησης¹⁷⁶. Η δυνητική αξία των τεχνικών αυτών αναγνωρίζεται, αλλά επισημαίνεται ότι ορισμένες τεχνικές δεν είναι κατ' ανάγκη αποτελεσματικές σε όλες τις περιπτώσεις. Για την εξεύρεση της βέλτιστης λύσης σε μια δεδομένη κατάσταση, η κατάλληλη διαδικασία ανωνυμοποίησης θα πρέπει να αποφασίζεται κατά περίπτωση. Ανεξάρτητα από τη χρησιμοποιηθείσα τεχνική, η εξακρίβωση της ταυτότητας πρέπει να παρεμποδίζεται με μη αναστρέψιμο τρόπο. Αυτό σημαίνει ότι, για να ανωνυμοποιηθούν τα δεδομένα, δεν πρέπει να παραμείνει στις πληροφορίες κανένα στοιχείο το οποίο θα μπορούσε να χρησιμοποιηθεί, με εύλογη προσπάθεια, για την εκ νέου εξακρίβωση της ταυτότητας του ενδιαφερόμενου προσώπου¹⁷⁷. Ο κίνδυνος εκ νέου εξακρίβωσης της ταυτότητας μπορεί να αξιολογηθεί συνεκτιμώντας «τον χρόνο, την προσπάθεια ή τους πόρους που θα απαιτούνταν, λαμβανομένων υπόψη της φύσης των δεδομένων, του πλαισίου της χρήσης τους, των διαθέσιμων τεχνολογιών εκ νέου εξακρίβωσης της ταυτότητας και του σχετικού κόστους»¹⁷⁸.

Όταν τα δεδομένα έχουν ανωνυμοποιηθεί επιτυχώς, δεν είναι πλέον δεδομένα προσωπικού χαρακτήρα και δεν εφαρμόζεται πλέον σε αυτά η νομοθεσία για την προστασία δεδομένων.

Ο ΓΚΠΔ προβλέπει ότι το πρόσωπο ή ο οργανισμός που ελέγχει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα δεν μπορεί να υποχρεούται να διατηρεί, να αποκτά ή να επεξεργάζεται συμπληρωματικές πληροφορίες για την εξακρίβωση της ταυτότητας του υποκειμένου των δεδομένων αποκλειστικά και μόνο για τον σκοπό της συμμόρφωσης προς τον κανονισμό. Ωστόσο, ο κανόνας αυτός συνοδεύεται από μια σημαντική εξαίρεση: οσάκις το υποκείμενο των δεδομένων παρέχει στον υπεύθυνο της επεξεργασίας, για τον σκοπό της άσκησης των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής, περιορισμού της επεξεργασίας και της φορητότητας των δεδομένων, συμπληρωματικές πληροφορίες που επιτρέπουν την εξακρίβωση της ταυτότητάς του, τα δεδομένα αυτά, τα οποία είχαν ανωνυμοποιηθεί προηγουμένως, καθίστανται εκ νέου δεδομένα προσωπικού χαρακτήρα¹⁷⁹.

176 Ομάδα εργασίας του άρθρου 29 (2014), *Γνώμη 05/2014 σχετικά με τις τεχνικές ανωνυμοποίησης*, WP 216, 10 Απριλίου 2014.

177 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 26.

178 Συμβούλιο της Ευρώπης (2017), Συμβουλευτική Επιτροπή στο πλαίσιο της Σύμβασης 108 (2017), *Κατευθυντήριες γραμμές για την προστασία των ατόμων σε ό,τι αφορά την επεξεργασία των προσωπικών δεδομένων στον κόσμο των Μαζικών Δεδομένων*, 23 Ιανουαρίου 2017, σημείο 6.2.

179 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 11.

Ψευδωνυμοποίηση

Οι προσωπικές πληροφορίες περιέχουν χαρακτηριστικά, όπως το όνομα, την ημερομηνία γέννησης, το φύλο, τη διεύθυνση ή άλλα στοιχεία, τα οποία μπορούν να οδηγήσουν σε εξακρίβωση της ταυτότητας. Η διαδικασία της ψευδωνυμοποίησης δεδομένων προσωπικού χαρακτήρα σημαίνει ότι τα εν λόγω χαρακτηριστικά αντικαθίστανται από ψευδώνυμο.

Το **δίκαιο της ΕΕ** ορίζει την «ψευδωνυμοποίηση» ως «την επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα προσωπικού χαρακτήρα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι τα δεδομένα προσωπικού χαρακτήρα δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο»¹⁸⁰. Εν αντιθέσει προς τα ανωνυμοποιημένα δεδομένα, τα ψευδωνυμοποιημένα παραμένουν δεδομένα προσωπικού χαρακτήρα και, επομένως, υπόκεινται στη νομοθεσία για την προστασία των δεδομένων. Παρότι μπορεί να μειώνει τους κινδύνους ασφάλειας για τα υποκείμενα των δεδομένων, η ψευδωνυμοποίηση δεν εξαιρείται από το πεδίο εφαρμογής του ΓΚΠΔ.

Ο ΓΚΠΔ αναγνωρίζει διάφορες χρήσεις της ψευδωνυμοποίησης ως κατάλληλου τεχνικού μέτρου για την ενίσχυση της προστασίας των δεδομένων, και αναφέρεται ιδιαιτέρως για τον σχεδιασμό και την ασφάλεια της επεξεργασίας δεδομένων¹⁸¹. Η ψευδωνυμοποίηση αποτελεί επίσης κατάλληλη εγγύηση η οποία θα μπορούσε να χρησιμοποιηθεί για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς διαφορετικούς από εκείνους για τους οποίους αυτά συλλέχθηκαν αρχικά¹⁸².

Η ψευδωνυμοποίηση δεν αναφέρεται ρητώς στον νομικό ορισμό της Εκσυγχρονισμένης Σύμβασης 108 του **Συμβουλίου της Ευρώπης**. Ωστόσο, στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται ρητώς ότι «η χρήση ψευδωνύμου ή άλλου ψηφιακού αναγνωριστικού στοιχείου / ψηφιακής ταυτότητας δεν οδηγεί σε ανωνυμοποίηση των δεδομένων, καθώς το

¹⁸⁰ Ό.π., άρθρο 4 σημείο 5.

¹⁸¹ Ό.π., άρθρο 25 παράγραφος 1.

¹⁸² Ό.π., άρθρο 6 παράγραφος 4.

υποκείμενο των δεδομένων παραμένει ταυτοποιήσιμο ή εξατομικευμένο»¹⁸³. Ένας τρόπος ψευδωνυμοποίησης είναι η κρυπτογράφηση των δεδομένων. Άπαξ και τα δεδομένα ψευδωνυμοποιηθούν, ο σύνδεσμος με την ταυτότητα υφίσταται με τη μορφή ψευδωνύμου σε συνδυασμό με κλειδί αποκρυπτογράφησης. Ελλείψει τέτοιου κλειδιού, η εξακρίβωση της ταυτότητας των ψευδωνυμοποιημένων δεδομένων είναι δυσχερής. Ωστόσο, για όσους δικαιούνται να χρησιμοποιήσουν το κλειδί αποκρυπτογράφησης, η εκ νέου εξακρίβωση της ταυτότητας είναι ευχερώς εφικτή. Ιδιαίτερη προσοχή πρέπει να επιδεικνύεται όσον αφορά τη χρήση κλειδιών κρυπτογράφησης από μη εξουσιοδοτημένα πρόσωπα. Επομένως, «[τ]α ψευδώνυμα δεδομένα [...] πρέπει να θεωρούνται δεδομένα προσωπικού χαρακτήρα [...]» τα οποία καλύπτονται από την Εκσυγχρονισμένη Σύμβαση 108¹⁸⁴.

Επαλήθευση της ταυτότητας

Πρόκειται για τη διαδικασία με την οποία ένα πρόσωπο είναι σε θέση να αποδεικνύει ότι διαθέτει συγκεκριμένη ταυτότητα και/ή είναι εξουσιοδοτημένο να προβαίνει σε ορισμένες ενέργειες, όπως να εισέρχεται σε χώρο ασφαλείας ή να προβαίνει σε ανάληψη χρημάτων από τραπεζικό λογαριασμό. Η επαλήθευση της ταυτότητας μπορεί να πραγματοποιηθεί συγκρίνοντας βιομετρικά δεδομένα, όπως φωτογραφία ή δακτυλικά αποτυπώματα σε διαβατήριο, με τα δεδομένα του προσώπου που εμφανίζεται, για παράδειγμα, σε έλεγχο των υπηρεσιών μετανάστευσης¹⁸⁵. ή ζητώντας πληροφορίες οι οποίες θα πρέπει να είναι γνωστές μόνο στο πρόσωπο με ορισμένη ταυτότητα ή εξουσιοδότηση, όπως προσωπικό αναγνωριστικό αριθμό (PIN) ή κωδικό πρόσβασης ή ζητώντας την επίδειξη συγκεκριμένου διακριτικού το οποίο πρέπει να κατέχει αποκλειστικά και μόνο το πρόσωπο με ορισμένη ταυτότητα ή εξουσιοδότηση, όπως ειδική έξυπνη κάρτα ή κλειδί χρηματοκιβωτίου σε τράπεζα. Εκτός από τους κωδικούς πρόσβασης ή τις έξυπνες κάρτες, οι ηλεκτρονικές υπογραφές –ενίοτε σε συνδυασμό με PIN– είναι ένα μέσο το οποίο ενδείκνυται ιδιαίτερα για την εξακρίβωση και την επαλήθευση της ταυτότητας προσώπου στις ηλεκτρονικές επικοινωνίες.

¹⁸³ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 18.

¹⁸⁴ Ό.π.

¹⁸⁵ Ό.π., σημεία 56-57.

2.1.2. Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

Στο πλαίσιο του δικαίου της ΕΕ καθώς και του **δικαίου του Συμβουλίου της Ευρώπης**, υπάρχουν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα οι οποίες, εκ φύσεως, ενδέχεται να ενέχουν κίνδυνο για τα υποκείμενα των δεδομένων όταν υποβάλλονται σε επεξεργασία, και απαιτούν αυξημένη προστασία. Τα δεδομένα αυτά υπόκεινται στην αρχή της απαγόρευσης, και οι προϋποθέσεις υπό τις οποίες η επεξεργασία τους είναι νόμιμη είναι περιορισμένες.

Στο πλαίσιο της Εκσυγχρονισμένης Σύμβασης 108 (άρθρο 6) και του ΓΚΠΔ (άρθρο 9), οι ακόλουθες κατηγορίες θεωρούνται ευαίσθητα δεδομένα:

- δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή·
- δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν πολιτικά φρονήματα, θρησκευτικές ή άλλες πεποιθήσεις, συμπεριλαμβανομένων των φιλοσοφικών πεποιθήσεων·
- δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη συμμετοχή σε συνδικαλιστική οργάνωση·
- γενετικά δεδομένα και βιομετρικά δεδομένα τα οποία υποβάλλονται σε επεξεργασία με σκοπό την εξακρίβωση της ταυτότητας προσώπου·
- δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία, τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό.

Παράδειγμα: Η υπόθεση *Bodil Lindqvist*¹⁸⁶ αφορούσε τη μνεία διαφόρων προσώπων, με το όνομά τους ή άλλα μέσα, όπως τον αριθμό τηλεφώνου ή άλλες πληροφορίες σχετικά με τις ασχολίες κατά τον ελεύθερο χρόνο τους, σε ιστοσελίδα στο διαδίκτυο. Το ΔΕΕ έκρινε ότι «η αναφορά του γεγονότος ότι ένα πρόσωπο τραυματίστηκε στο πόδι και τελεί σε μερική αναρρωτική άδεια συνιστά δεδομένο προσωπικού χαρακτήρα σχετικό με την υγεία»¹⁸⁷.

¹⁸⁶ ΔΕΕ, C-101/01, *Ποινική δίκη κατά Bodil Lindqvist*, 6 Νοεμβρίου 2003, σκέψη 51.

¹⁸⁷ Πρώην οδηγία 95/46/ΕΚ, άρθρο 8 παράγραφος 1, πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 1.

Δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα

Η Εκσυγχρονισμένη Σύμβαση 108 περιλαμβάνει στον κατάλογο των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα δεδομένα τα οποία αφορούν αδικήματα, ποινικές δίκες και καταδίκες και σχετικά μέτρα ασφάλειας¹⁸⁸. Στο πλαίσιο του ΓΚΠΔ, τα δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας δεν αναφέρονται αυτά καθαυτά στον κατάλογο των ειδικών κατηγοριών δεδομένων, αλλά εξετάζονται σε χωριστό άρθρο. Το άρθρο 10 του ΓΚΠΔ προβλέπει ότι η επεξεργασία τέτοιων δεδομένων μπορεί να διενεργείται μόνο «υπό τον έλεγχο επίσημης αρχής ή εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων». Από την άλλη πλευρά, πλήρη μητρώα με πληροφορίες σχετικά με ποινικές καταδίκες μπορούν να τηρούνται μόνο υπό τον έλεγχο ειδικών επίσημων αρχών¹⁸⁹. Στην ΕΕ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της επιβολής του νόμου διέπεται από ειδική νομική πράξη, την οδηγία 2016/680/ΕΕ¹⁹⁰. Η οδηγία προβλέπει ειδικούς κανόνες για την προστασία δεδομένων, οι οποίοι είναι δεσμευτικοί για τις αρμόδιες αρχές όταν αυτές επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ειδικά για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων (βλ. [ενότητα 8.2.1](#)).

2.2. Επεξεργασία δεδομένων

Κύρια σημεία

- Η «επεξεργασία δεδομένων» αφορά κάθε πράξη που διενεργείται σε δεδομένα προσωπικού χαρακτήρα.

¹⁸⁸ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 6 παράγραφος 1.

¹⁸⁹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 10.

¹⁹⁰ Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (ΕΕ L 119 της 4.5.2016, σ. 89).

- Ο όρος «επεξεργασία» καλύπτει την αυτοματοποιημένη και τη μη αυτοματοποιημένη επεξεργασία.
- Βάσει του δικαίου της ΕΕ, η «επεξεργασία» αφορά επίσης τη χειροκίνητη επεξεργασία σε διαρθρωμένα συστήματα αρχειοθέτησης.
- Βάσει του δικαίου του Συμβουλίου της Ευρώπης, το εθνικό δίκαιο μπορεί να επεκτείνει την έννοια της «επεξεργασίας» ώστε να περιλαμβάνει τη χειροκίνητη επεξεργασία.

2.2.1. Η έννοια της επεξεργασίας δεδομένων

Η έννοια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα είναι περιεκτική **βάσει τόσο του δικαίου της ΕΕ, όσο και του δικαίου του Συμβουλίου της Ευρώπης:** ως «“επεξεργασία δεδομένων προσωπικού χαρακτήρα” [...] νοείται κάθε πράξη [...] όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή»¹⁹¹ δεδομένων προσωπικού χαρακτήρα. Η Εκσυγχρονισμένη Σύμβαση 108 προσθέτει στον ορισμό τη διατήρηση δεδομένων προσωπικού χαρακτήρα¹⁹².

Παράδειγμα: Στην υπόθεση *František Ryněš*¹⁹³, ο F. Ryněš κατέγραψε, μέσω του οικιακού συστήματος παρακολούθησης με κάμερες που είχε εγκαταστήσει για την προστασία της περιουσίας του, την εικόνα δύο προσώπων που έσπασαν κάποια παράθυρα του σπιτιού του. Το ΔΕΕ έκρινε ότι η επιτήρηση μέσω βίντεο η οποία περιλαμβάνει την καταγραφή και την αποθήκευση δεδομένων προσωπικού χαρακτήρα συνιστά αυτόματα επεξεργασία δεδομένων, η οποία εμπίπτει στο πεδίο εφαρμογής του δικαίου της ΕΕ για την προστασία δεδομένων.

¹⁹¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 2. Βλ. επίσης Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο β).

¹⁹² Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο β).

¹⁹³ ΔΕΕ, C-212/13, *František Ryněš κατά Úřad pro ochranu osobních údajů*, 11 Δεκεμβρίου 2014, σκέψη 25.

Παράδειγμα: Στην υπόθεση *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*¹⁹⁴, ο S. Manni ζήτησε να διαγραφούν από το μητρώο εταιρείας εκτίμησης κινδύνων τα δεδομένα προσωπικού χαρακτήρα που τον αφορούσαν, τα οποία τον συνέδεαν με την εκκαθάριση κτηματικής εταιρείας και είχαν, επομένως, αρνητικό αντίκτυπο στη φήμη του. Το ΔΕΕ έκρινε ότι «καταχωρίζοντας και διατηρώντας τις εν λόγω πληροφορίες στο μητρώο και ανακοινώνοντας τις πληροφορίες αυτές, ενδεχομένως, κατόπιν αιτήσεως, σε τρίτους, η αρχή που είναι επιφορτισμένη με την τήρηση του ως άνω μητρώου προβαίνει σε “επεξεργασία δεδομένων προσωπικού χαρακτήρα”, για την οποία η ίδια είναι ο “υπεύθυνος”».

Παράδειγμα: Εργοδότες συλλέγουν και επεξεργάζονται δεδομένα σχετικά με τους υπαλλήλους τους, συμπεριλαμβανομένων πληροφοριών σχετικών με τους μισθούς τους. Οι συμβάσεις απασχόλησης των υπαλλήλων παρέχουν τη νομική βάση για τη νόμιμη συλλογή και επεξεργασία των δεδομένων αυτών.

Οι εργοδότες θα πρέπει να διαβιβάσουν τα δεδομένα για τους μισθούς των υπαλλήλων τους στις φορολογικές αρχές. Αυτή η διαβίβαση δεδομένων αποτελεί επίσης «επεξεργασία» κατά την έννοια του όρου αυτού στην Εκσυγχρονισμένη Σύμβαση 108 και στον ΓΚΠΔ. Ωστόσο, η νομική βάση για την κοινοποίηση αυτή δεν είναι οι συμβάσεις απασχόλησης. Πρέπει να υπάρχει πρόσθετη νομική βάση για τις πράξεις επεξεργασίας οι οποίες έχουν ως αποτέλεσμα τη διαβίβαση δεδομένων σχετικών με τους μισθούς από τον εργοδότη στις φορολογικές αρχές. Η νομική αυτή βάση περιλαμβάνεται συνήθως στις διατάξεις της εθνικής φορολογικής νομοθεσίας. Χωρίς τέτοιες διατάξεις –και απουσία άλλης νομικής βάσης επεξεργασίας– αυτή η διαβίβαση δεδομένων προσωπικού χαρακτήρα συνιστά παράνομη επεξεργασία.

¹⁹⁴ ΔΕΕ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*, 9 Μαρτίου 2017, σκέψη 35.

2.2.2. Αυτοματοποιημένη επεξεργασία δεδομένων

Βάσει της Εκσυγχρονισμένης Σύμβασης 108 και του ΓΚΠΔ, η προστασία των δεδομένων εφαρμόζεται πλήρως στην αυτοματοποιημένη επεξεργασία δεδομένων.

Βάσει του **δικαίου της ΕΕ**, η αυτοματοποιημένη επεξεργασία δεδομένων αφορά την «εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα»¹⁹⁵. Παρόμοιος ορισμός περιλαμβάνεται στην Εκσυγχρονισμένη Σύμβαση 108¹⁹⁶. Πρακτικά, αυτό σημαίνει ότι κάθε αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα με τη βοήθεια, για παράδειγμα, προσωπικού υπολογιστή, κινητής συσκευής ή δρομολογητή εμπίπτει στους κανόνες περί προστασίας δεδομένων τόσο της ΕΕ, όσο και του Συμβουλίου της Ευρώπης.

Παράδειγμα: Η υπόθεση *Bodil Lindqvist*¹⁹⁷ αφορούσε την αναφορά διαφόρων προσώπων, με το όνομά τους ή άλλο στοιχείο, όπως τον αριθμό τηλεφώνου ή άλλες πληροφορίες σχετικά με τις ασχολίες κατά τον ελεύθερο χρόνο τους, σε ιστοσελίδα στο διαδίκτυο. Το ΔΕΕ έκρινε ότι «η εργασία που συνίσταται στην αναφορά, επί ιστοσελίδας του διαδικτύου, σε διάφορα πρόσωπα και στον προσδιορισμό τους είτε με το όνομά τους είτε με άλλα μέσα, για παράδειγμα με τον αριθμό τηλεφώνου τους ή με στοιχεία σχετικά με τις συνθήκες εργασίας τους και τις ασχολίες τους κατά τον ελεύθερο χρόνο, συνιστά “αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα”», κατά την έννοια του άρθρου 3 παράγραφος 1 της οδηγίας 95/46¹⁹⁸.

Παράδειγμα: Στην υπόθεση *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González*¹⁹⁹, ο M. Costeja González ζήτησε την αφαίρεση ή τροποποίηση συνδέσμου μεταξύ του ονόματός του στη μηχανή αναζήτησης Google και δύο σελίδων εφημερίδων που περιλάμβαναν ανακοίνωση πλειστηριασμού ακινήτου για την ανάκτηση κοινωνικο-ασφαλιστικών οφειλών. Το ΔΕΕ έκρινε ότι «ο φορέας εκμετάλλευσης μηχανής αναζήτησης, καθόσον ερευνά

195 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 1 και άρθρο 4 σημείο 2.

196 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχεία β) και γ). Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 21.

197 ΔΕΕ, C-101/01, *Ποινική δίκη κατά Bodil Lindqvist*, 6 Νοεμβρίου 2003, σκέψη 27.

198 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 1.

199 ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014.

με αυτοματοποιημένο, διαρκή και συστηματικό τρόπο το διαδίκτυο προς αναζήτηση πληροφοριών δημοσιευμένων σε αυτό, “συλλέγει” τέτοια δεδομένα τα οποία “ανακτά”, “καταχωρίζει” και “οργανώνει” εν συνεχεία στο πλαίσιο των προγραμμάτων ευρετηρίασης που διαθέτει, τα “αποθηκεύει” στους εξυπηρετητές του και, ενδεχομένως, τα “ανακοινώνει” και τα “θέτει στη διάθεση” των χρηστών της μηχανής υπό μορφή καταλόγων αποτελεσμάτων αναζήτησης»²⁰⁰. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι οι εν λόγω ενέργειες συνιστούν «επεξεργασία», «χωρίς να ασκεί επιρροή το ότι ο φορέας εκμετάλλευσης της μηχανής αναζήτησης προβαίνει στις ίδιες πράξεις και για άλλου είδους πληροφορίες και δεν κάνει διαφοροποίηση μεταξύ των πράξεων αυτών και των δεδομένων προσωπικού χαρακτήρα».

2.2.3. Μη αυτοματοποιημένη επεξεργασία δεδομένων

Παροχή προστασίας στα δεδομένα απαιτείται και στη χειροκίνητη επεξεργασία τους.

Η προστασία δεδομένων **βάσει του δικαίου της ΕΕ** δεν περιορίζεται σε καμία περίπτωση στην αυτοματοποιημένη επεξεργασία τους. Ως εκ τούτου, βάσει του δικαίου της ΕΕ, η προστασία δεδομένων εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα σε χειροκίνητο σύστημα αρχειοθέτησης, δηλαδή σε ειδικά διαρθρωμένο έντυπο αρχείο²⁰¹. Διαρθρωμένο σύστημα αρχειοθέτησης είναι αυτό το οποίο κατηγοριοποιεί ένα σύνολο δεδομένων προσωπικού χαρακτήρα, καθιστώντας τα προσβάσιμα βάσει ορισμένων κριτηρίων. Για παράδειγμα, εάν ένας εργοδότης διατηρεί έντυπο αρχείο με τίτλο «άδειες υπαλλήλων», το οποίο περιέχει όλα τα στοιχεία των αδειών που έλαβαν οι υπάλληλοι κατά το προηγούμενο έτος με αλφαβητική ταξινόμηση, το αρχείο αυτό θα συνιστά χειροκίνητο σύστημα αρχειοθέτησης, το οποίο υπόκειται στους κανόνες της ΕΕ περί προστασίας των δεδομένων. Ο λόγος γι' αυτή την επέκταση της προστασίας δεδομένων είναι ότι:

- τα έντυπα αρχεία μπορούν να διαρθρωθούν κατά τρόπο που καθιστά την εξεύρεση πληροφοριών γρήγορη και εύκολη.

²⁰⁰ Ό.π., σκέψη 28.

²⁰¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 1.

- η αποθήκευση δεδομένων προσωπικού χαρακτήρα σε διαρθρωμένα έντυπα αρχεία διευκολύνει την καταστρατήγηση των περιορισμών που προβλέπονται στον νόμο για την αυτοματοποιημένη επεξεργασία δεδομένων ²⁰².

Στο **δίκαιο του Συμβουλίου της Ευρώπης**, ο ορισμός της αυτόματης επεξεργασίας αναγνωρίζει ότι, μεταξύ αυτοματοποιημένων πράξεων, μπορεί να απαιτούνται ορισμένα στάδια χειροκίνητης χρήσης των δεδομένων προσωπικού χαρακτήρα ²⁰³. Το άρθρο 2 στοιχείο γ) της Εκσυγχρονισμένης Σύμβασης 108 προβλέπει ότι «[ό]ταν δεν χρησιμοποιείται αυτοματοποιημένη επεξεργασία, ως επεξεργασία δεδομένων νοείται πράξη ή σύνολο πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα εντός διαρθρωμένου συνόλου τέτοιων δεδομένων στο οποίο παρέχεται δυνατότητα πρόσβασης ή ανάκτησης βάσει συγκεκριμένων κριτηρίων».

2.3. Χρήστες δεδομένων προσωπικού χαρακτήρα

Κύρια σημεία

- Όποιος καθορίζει τον τρόπο και τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα άλλων προσώπων είναι «υπεύθυνος επεξεργασίας» βάσει του δικαίου προστασίας δεδομένων· εάν λαμβάνουν την απόφαση αυτή περισσότερα πρόσωπα από κοινού, μπορεί να είναι «από κοινού υπεύθυνοι επεξεργασίας».
- Ο «εκτελών την επεξεργασία» είναι φυσικό ή νομικό πρόσωπο το οποίο επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπευθύνου επεξεργασίας.
- Ο εκτελών την επεξεργασία καθίσταται υπεύθυνος επεξεργασίας εάν καθορίζει ο ίδιος τον τρόπο και τους σκοπούς της.
- Κάθε πρόσωπο στο οποίο κοινοποιούνται δεδομένα προσωπικού χαρακτήρα είναι «αποδέκτης».
- Ο «τρίτος» είναι φυσικό ή νομικό πρόσωπο, εκτός του υποκειμένου των δεδομένων, του υπευθύνου επεξεργασίας, του εκτελούντος την επεξεργασία και προσώπων εξουσιοδοτημένων να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

²⁰² Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 15.

²⁰³ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχεία β) και γ).

- Η συγκατάθεση ως νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι ελεύθερη, εν πλήρει επιγνώσει, συγκεκριμένη και αδι-αμφισβήτητη ένδειξη βούλησης με σαφή θετική ενέργεια με την οποία εκδηλώνεται η συμφωνία για την επεξεργασία.
- Για την επεξεργασία ειδικών κατηγοριών δεδομένων βάσει συγκατάθεσης απαιτείται ρητή συγκατάθεση.

2.3.1. Υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία

Η σημαντικότερη συνέπεια που απορρέει από την ιδιότητα του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι η νομική ευθύνη συμμόρφωσης προς τις αντίστοιχες υποχρεώσεις βάσει του δικαίου για την προστασία δεδομένων. Στον ιδιωτικό τομέα, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι συνήθως φυσικό ή νομικό πρόσωπο· στον δημόσιο τομέα, είναι συνήθως αρχή. Μεταξύ υπευθύνου επεξεργασίας δεδομένων και εκτελούντος την επεξεργασία υπάρχει σημαντική διαφορά: ο πρώτος είναι το φυσικό ή νομικό πρόσωπο που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, ενώ ο δεύτερος είναι το φυσικό ή νομικό πρόσωπο που επεξεργάζεται τα δεδομένα για λογαριασμό του υπευθύνου, ακολουθώντας αυστηρές εντολές. Καταρχήν, ο υπεύθυνος επεξεργασίας δεδομένων είναι αυτός που πρέπει να ασκεί έλεγχο στην επεξεργασία και έχει την ευθύνη αυτής, συμπεριλαμβανομένης της νομικής ευθύνης. Ωστόσο, με τη μεταρρύθμιση των κανόνων περί προστασίας δεδομένων, οι εκτελούντες την επεξεργασία υποχρεούνται πλέον να συμμορφώνονται με πολλές από τις απαιτήσεις που ισχύουν για τους υπευθύνους επεξεργασίας. Για παράδειγμα, βάσει του ΓΚΠΔ, οι εκτελούντες την επεξεργασία οφείλουν να τηρούν αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας ώστε να αποδεικνύουν τη συμμόρφωση προς τις υποχρεώσεις τους που απορρέουν από τον κανονισμό ²⁰⁴. Οι εκτελούντες την επεξεργασία υποχρεούνται επίσης να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να εγγυώνται την ασφάλεια της επεξεργασίας ²⁰⁵, να διορίζουν υπεύθυνο προστασίας δεδομένων σε ορισμένες περιπτώσεις ²⁰⁶ και να γνωστοποιούν τις παραβιάσεις δεδομένων στον υπεύθυνο επεξεργασίας ²⁰⁷.

²⁰⁴ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 30 παράγραφος 2.

²⁰⁵ Ό.π., άρθρο 32.

²⁰⁶ Ό.π., άρθρο 37.

²⁰⁷ Ό.π., άρθρο 33 παράγραφος 2.

Το κατά πόσον ένα πρόσωπο έχει την αρμοδιότητα να αποφασίζει και να καθορίζει τον σκοπό και τα μέσα της επεξεργασίας θα εξαρτάται από τα πραγματικά στοιχεία ή τις περιστάσεις της υπόθεσης. Σύμφωνα με τον ορισμό του υπευθύνου επεξεργασίας στον ΓΚΠΔ, μπορεί να είναι φυσικά πρόσωπα, νομικά πρόσωπα ή άλλοι φορείς. Ωστόσο, η Ομάδα εργασίας του άρθρου 29 τόνισε ότι, για να παρασχεθεί στα φυσικά πρόσωπα μια πιο σταθερή οντότητα για την άσκηση των δικαιωμάτων τους, «είναι προτιμότερο να θεωρείται υπεύθυνος της επεξεργασίας η εταιρεία ή ο φορέας παρά ένα συγκεκριμένο πρόσωπο εντός της εταιρείας ή του φορέα»²⁰⁸. Για παράδειγμα, ο υπεύθυνος επεξεργασίας για την κατάρτιση και τη διατήρηση καταλόγου διανομής όλων των ιατρών σε ορισμένη περιοχή είναι η εταιρεία που πωλεί υλικό υγειονομικής περίθαλψης στους ιατρούς και όχι ο διευθυντής πωλήσεων ο οποίος στην πραγματικότητα χρησιμοποιεί και διατηρεί τον κατάλογο.

Παράδειγμα: Όταν το τμήμα μάρκετινγκ της εταιρείας Sunshine προτίθεται να επεξεργαστεί δεδομένα για έρευνα αγοράς, υπεύθυνος της συγκεκριμένης επεξεργασίας θα είναι η εταιρεία Sunshine και όχι οι υπάλληλοι του τμήματος μάρκετινγκ. Το τμήμα μάρκετινγκ δεν μπορεί να είναι ο υπεύθυνος επεξεργασίας, καθώς δεν έχει αυτοτελή ταυτότητα.

Φυσικά πρόσωπα μπορεί να είναι υπεύθυνοι επεξεργασίας βάσει τόσο του δικαίου της ΕΕ, όσο και του δικαίου του Συμβουλίου της Ευρώπης. Ωστόσο, όταν επεξεργάζονται δεδομένα άλλων στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας, τα φυσικά πρόσωπα δεν εμπίπτουν στους κανόνες του ΓΚΠΔ και της Εκσυγχρονισμένης Σύμβασης 108 και δεν θεωρούνται υπεύθυνοι επεξεργασίας²⁰⁹. Άτομο το οποίο φυλάσσει την αλληλογραφία του, διατηρεί προσωπικό ημερολόγιο στο οποίο περιγράφει συμβάντα με φίλους και συναδέλφους και τηρεί τα ιατρικά αρχεία μελών της οικογένειάς του μπορεί να εξαιρείται από τους κανόνες περί προστασίας δεδομένων, αφού οι δραστηριότητες αυτές θα μπορούσαν να είναι αμιγώς προσωπικές ή απλώς οικιακές. Στον ΓΚΠΔ διευκρινίζεται περαιτέρω ότι στις προσωπικές ή οικιακές δραστηριότητες θα μπορούσαν επίσης να περιλαμβάνονται η κοινωνική δικτύωση και η επιγραμμική δραστηριότητα, όταν ασκούνται στο πλαίσιο αυτό²¹⁰. Αντιθέτως, οι κανόνες περί

208 Ομάδα εργασίας του άρθρου 29 (2010), *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010.

209 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 18 και άρθρο 2 παράγραφος 2 στοιχείο γ)- Εκσυγχρονισμένη Σύμβαση 108, άρθρο 3 παράγραφος 2.

210 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 18.

προστασίας δεδομένων εφαρμόζονται πλήρως όσον αφορά τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία οι οποίοι παρέχουν τα μέσα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για προσωπικές ή οικιακές δραστηριότητες (για παράδειγμα, πλατφόρμες κοινωνικής δικτύωσης) ²¹¹.

Η πρόσβαση των πολιτών στο διαδίκτυο και η δυνατότητα χρήσης πλατφορμών ηλεκτρονικού εμπορίου, κοινωνικών δικτύων και ιστολογίων για την ανταλλαγή προσωπικών πληροφοριών σχετικά με τους ίδιους και άλλα άτομα καθιστούν ολοένα και πιο δύσκολο τον διαχωρισμό μεταξύ προσωπικής και μη προσωπικής επεξεργασίας ²¹². Το κατά πόσον οι δραστηριότητες είναι αποκλειστικά προσωπικές ή οικιακές εξαρτάται από τις περιστάσεις ²¹³. Δραστηριότητες που έχουν επαγγελματικές ή εμπορικές πτυχές δεν μπορούν να εμπίπτουν στην εξαίρεση της οικιακής δραστηριότητας ²¹⁴. Επομένως, στην περίπτωση που η κλίμακα και η συχνότητα της επεξεργασίας δεδομένων υποδηλώνουν επαγγελματική δραστηριότητα ή δραστηριότητα πλήρους απασχόλησης, ένα φυσικό πρόσωπο μπορεί να θεωρηθεί υπεύθυνος επεξεργασίας. Επιπροσθέτως του επαγγελματικού ή εμπορικού χαρακτήρα της δραστηριότητας επεξεργασίας, ένας άλλος παράγοντας ο οποίος πρέπει να λαμβάνεται υπόψη είναι αν τα δεδομένα προσωπικού χαρακτήρα διατίθενται σε μεγάλο αριθμό προσώπων τα οποία βρίσκονται προδήλως εκτός της ιδιωτικής σφαίρας του φυσικού προσώπου. Κατά τη σχετική με την Οδηγία για την Προστασία Δεδομένων νομολογία, το δίκαιο για την προστασία δεδομένων θα εφαρμόζεται όταν ιδιώτης, κατά τη χρήση του διαδικτύου, δημοσιεύει δεδομένα που αφορούν τρίτους σε δημόσιο ιστότοπο. Το ΔΕΕ δεν έχει αποφανθεί ακόμη επί παρόμοιων πραγματικών περιστατικών βάσει του ΓΚΠΔ, ο οποίος παρέχει περισσότερη καθοδήγηση σχετικά με τα θέματα που θα μπορούσε να θεωρηθεί ότι δεν εμπίπτουν στο πεδίο εφαρμογής της νομοθεσίας για την προστασία δεδομένων βάσει της «εξαίρεσης λόγω οικιακής δραστηριότητας», όπως η χρήση των μέσων κοινωνικής δικτύωσης για προσωπικούς σκοπούς.

211 Ό.π., αιτιολογική σκέψη 18· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 29.

212 Βλ. τη δήλωση της Ομάδας εργασίας του άρθρου 29 για τις συζητήσεις σχετικά με τη δέσμη μέτρων μεταρρύθμισης για την προστασία δεδομένων (2013), *Annex 2: Proposals and Amendments regarding exemption for personal or household activities*, 27 Φεβρουαρίου 2013.

213 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 28.

214 Βλ. Γενικό Κανονισμό για την Προστασία Δεδομένων, αιτιολογική σκέψη 18, και Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 27.

Παράδειγμα: Η υπόθεση *Bodil Lindqvist*²¹⁵ αφορούσε την αναφορά διαφόρων προσώπων, με το όνομά τους ή άλλο στοιχείο, όπως τον αριθμό τηλεφώνου ή άλλες πληροφορίες σχετικά με τις ασχολίες κατά τον ελεύθερο χρόνο τους, σε ιστοσελίδα στο διαδίκτυο. Το ΔΕΕ υποστήριξε ότι «η εργασία που συνίσταται στην αναφορά, επί ιστοσελίδας του διαδικτύου, σε διάφορα πρόσωπα και στον προσδιορισμό τους είτε με το όνομά τους είτε με άλλα μέσα [...] συνιστά “αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα”», κατά την έννοια του άρθρου 3 παράγραφος 1 της Οδηγίας για την Προστασία Δεδομένων²¹⁶.

Τέτοια επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν συγκαταλέγεται στις αποκλειστικά προσωπικές ή οικιακές δραστηριότητες, οι οποίες δεν εμπίπτουν στο πεδίο εφαρμογής των κανόνων της ΕΕ περί προστασίας δεδομένων, καθώς η εξαίρεση αυτή «πρέπει [...] να ερμηνευθεί ως αφορώσα αποκλειστικά τις δραστηριότητες οι οποίες εντάσσονται στο πλαίσιο της ιδιωτικής ή οικογενειακής ζωής των ιδιωτών, πράγμα το οποίο προδήλως δεν ισχύει για την περίπτωση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα η οποία συνίσταται στη δημοσίευσή τους στο διαδίκτυο με συνέπεια να αποκτά πρόσβαση στα δεδομένα αυτά απροσδιόριστος αριθμός προσώπων»²¹⁷.

Σύμφωνα με το ΔΕΕ, οι οπτικές καταγραφές ιδιωτικά εγκατεστημένων καμερών ασφαλείας μπορούν επίσης να εμπίπτουν στη νομοθεσία της ΕΕ για την προστασία δεδομένων υπό ορισμένες περιστάσεις.

Παράδειγμα: Στην υπόθεση *František Ryneš*²¹⁸, ο F. Ryneš κατέγραψε, μέσω του οικιακού συστήματος παρακολούθησης με κάμερες που είχε εγκαταστήσει για την προστασία της περιουσίας του, την εικόνα δύο προσώπων που έσπασαν κάποια παράθυρα του σπιτιού του. Η καταγραφή παραδόθηκε στη συνέχεια στην αστυνομία και χρησιμοποιήθηκε κατά τη διάρκεια ποινικής διαδικασίας.

215 ΔΕΕ, C-101/01, *Ποινική δίκη κατά Bodil Lindqvist*, 6 Νοεμβρίου 2003.

216 Ό.π., σκέψη 27· πρώην οδηγία 95/46/ΕΚ, άρθρο 3 παράγραφος 1, πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 1.

217 ΔΕΕ, C-101/01, *Ποινική δίκη κατά Bodil Lindqvist*, 6 Νοεμβρίου 2003, σκέψη 47.

218 ΔΕΕ, C-212/13, *František Ryneš κατά Úřad pro ochranu osobních údajů*, 11 Δεκεμβρίου 2014, σκέψη 33.

Το ΔΕΕ έκρινε ότι «[σ]τον βαθμό που μια παρακολούθηση με κάμερα ασφαλείας [...] εκτείνεται, έστω και εν μέρει, στον δημόσιο χώρο και, ως εκ τούτου, εξέρχεται από την ιδιωτική σφαίρα αυτού που προβαίνει στην επεξεργασία των δεδομένων με το μέσο αυτό, δεν μπορεί να θεωρηθεί ως αποκλειστικώς “προσωπική ή οικιακή” δραστηριότητα [...]»²¹⁹.

Υπεύθυνος επεξεργασίας

Βάσει του δικαίου της ΕΕ, ο υπεύθυνος επεξεργασίας είναι πρόσωπο το οποίο «μόν[ο] ή από κοινού με άλλα, καθορίζ[ει] τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα»²²⁰. Ο υπεύθυνος επεξεργασίας καθορίζει με απόφασή του τους λόγους και τον τρόπο επεξεργασίας των δεδομένων.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, στην Εκσυγχρονισμένη Σύμβαση 108 ως «υπεύθυνος επεξεργασίας» νοείται «φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία, οργανισμός ή άλλος φορέας, ο οποίος, μόνος ή από κοινού με άλλους, έχει την εξουσία λήψης αποφάσεων σε σχέση με την επεξεργασία δεδομένων»²²¹. Αυτή η εξουσία λήψης αποφάσεων αφορά τους σκοπούς και τον τρόπο της επεξεργασίας, καθώς και τις κατηγορίες δεδομένων που θα υποβληθούν σε επεξεργασία και την πρόσβαση σε αυτά²²². Το κατά πόσον η εξουσία αυτή απορρέει από ορισμό βάσει νόμου ή από πραγματικές περιστάσεις πρέπει να αποφασίζεται κατά περίπτωση²²³.

Παράδειγμα: Η υπόθεση *Google Spain*²²⁴ ανέκυψε όταν ισπανός πολίτης ζήτησε να αφαιρεθεί από τη μηχανή αναζήτησης Google παλαιό άρθρο εφημερίδας το οποίο αναφερόταν στο οικονομικό ιστορικό του.

219 Πρώην οδηγία 95/46/ΕΚ, άρθρο 3 παράγραφος 2 δεύτερη περίπτωση, πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 2 στοιχείο γ).

220 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 7.

221 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο δ).

222 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 22.

223 Ό.π.

224 ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [τμήμα μειζονος συνθέσεως], 13 Μαΐου 2014.

Το ΔΕΕ κλήθηκε να διευκρινίσει αν η Google, ως φορέας εκμετάλλευσης μηχανής αναζήτησης, ήταν ο «υπεύθυνος επεξεργασίας» των δεδομένων, κατά την έννοια του άρθρου 2 στοιχείο δ) της Οδηγίας για την Προστασία Δεδομένων ²²⁵. Το ΔΕΕ έλαβε υπόψη ευρύ ορισμό της έννοιας του «υπευθύνου επεξεργασίας» προκειμένου να διασφαλιστεί «αποτελεσματική και πλήρης προστασία των υποκειμένων των [δεδομένων]» ²²⁶. Το ΔΕΕ αποφάνθηκε ότι ο φορέας εκμετάλλευσης μηχανής αναζήτησης καθόριζε τους σκοπούς και τον τρόπο της δραστηριότητας και ότι καθιστούσε προσβάσιμα τα δεδομένα που αναρτώνται σε ιστοσελίδες από εκδότες ιστοτόπων σε κάθε χρήστη του διαδικτύου ο οποίος πραγματοποιεί αναζήτηση με βάση το ονοματεπώνυμο του υποκειμένου των δεδομένων ²²⁷. Ως εκ τούτου, το ΔΕΕ έκρινε ότι η Google μπορεί να θεωρηθεί «υπεύθυνος επεξεργασίας» ²²⁸.

Όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι εγκατεστημένος εκτός ΕΕ, η εταιρεία αυτή πρέπει να διορίσει εγγράφως εκπρόσωπο στην ΕΕ ²²⁹. Στον ΓΚΠΔ επισημαίνεται ότι ο εκπρόσωπος πρέπει να είναι εγκατεστημένος «σε ένα από τα κράτη μέλη όπου βρίσκονται τα υποκείμενα των δεδομένων, των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σε σχέση με προσφορά αγαθών ή υπηρεσιών προς αυτά ή των οποίων η συμπεριφορά παρακολουθείται» ²³⁰. Εάν δεν έχει οριστεί εκπρόσωπος, και πάλι είναι δυνατή η άσκηση προσφυγής κατά του ίδιου του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία ²³¹.

Από κοινού υπεύθυνοι επεξεργασίας

Ο ΓΚΠΔ προβλέπει ότι, σε περίπτωση που δύο ή περισσότεροι υπεύθυνοι επεξεργασίας καθορίζουν από κοινού τους σκοπούς και τα μέσα της, αποτελούν από κοινού υπευθύνους επεξεργασίας. Αυτό σημαίνει ότι αποφασίζουν μαζί να

²²⁵ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 7· ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014, σκέψη 21.

²²⁶ ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014, σκέψη 34.

²²⁷ Ό.π., σκέψεις 35-40.

²²⁸ Ό.π., σκέψη 41.

²²⁹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 27 παράγραφος 1.

²³⁰ Ό.π., άρθρο 27 παράγραφος 3.

²³¹ Ό.π., άρθρο 27 παράγραφος 5.

επεξεργαστούν δεδομένα για έναν κοινό σκοπό²³². Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται ότι είναι δυνατή η ύπαρξη περισσότερων του ενός υπευθύνων επεξεργασίας ή από κοινού υπευθύνων επεξεργασίας και στο **πλαίσιο του Συμβουλίου της Ευρώπης**²³³.

Η Ομάδα εργασίας του άρθρου 29 επισημαίνει ότι η έννοια των από κοινού υπευθύνων επεξεργασίας μπορεί να προσλάβει διάφορες μορφές και η συμμετοχή των διαφόρων υπευθύνων επεξεργασίας στις δραστηριότητες ελέγχου ενδέχεται να μην είναι επιμερισμένη εξίσου²³⁴. Η ευελιξία αυτή καθιστά εφικτό να λαμβάνεται υπόψη η αυξανόμενη πολυπλοκότητα της τρέχουσας πραγματικότητας στον τομέα της επεξεργασίας δεδομένων²³⁵. Επομένως, οι από κοινού υπεύθυνοι επεξεργασίας πρέπει να καθορίζουν τις αντίστοιχες ευθύνες τους όσον αφορά τη συμμόρφωση προς τις υποχρεώσεις που απορρέουν από τον κανονισμό σε ειδική συμφωνία²³⁶.

Οι από κοινού υπεύθυνοι επεξεργασίας ευθύνονται, κατά συνέπεια, από κοινού για τη δραστηριότητα επεξεργασίας²³⁷. Στο πλαίσιο του **δικαίου της ΕΕ**, αυτό σημαίνει ότι κάθε υπεύθυνος επεξεργασίας ή εκτελών επεξεργασία μπορεί να θεωρηθεί πλήρως υπεύθυνος για τη συνολική ζημία που προκαλείται από την επεξεργασία των από κοινού υπευθύνων, προκειμένου να διασφαλιστεί αποτελεσματική αποζημίωση του υποκειμένου των δεδομένων²³⁸.

Παράδειγμα: Οι βάσεις δεδομένων τις οποίες διαχειρίζονται από κοινού περισσότερα πιστωτικά ιδρύματα και αφορούν τους υπερήμερους πελάτες τους αποτελούν σύνθετες παράδειγμα από κοινού υπευθύνων επεξεργασίας. Όταν ένα πρόσωπο υποβάλλει αίτηση πίστωσης σε τράπεζα η οποία είναι ένας εκ των από κοινού υπευθύνων επεξεργασίας, η τράπεζα συμβουλευεται τη βάση δεδομένων προκειμένου να λάβει ενημερωμένη απόφαση σχετικά με την πιστοληπτική ικανότητα του αιτούντος.

232 Ό.π., άρθρο 4 σημείο 7 και άρθρο 26.

233 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο δ). Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 22.

234 Ομάδα εργασίας του άρθρου 29 (2010), *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010, α. 19.

235 Ό.π.

236 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 79.

237 Ό.π., σκέψη 21.

238 Ό.π., άρθρο 82 παράγραφος 4.

Στις νομικές διατάξεις δεν αναφέρεται ρητώς αν καθέννας από τους από κοινού υπευθύνους επεξεργασίας πρέπει να έχει τον ίδιο κοινό σκοπό με τους άλλους ή αν αρκεί να αλληλεπικαλύπτονται οι σκοποί τους μόνο εν μέρει. Επί του παρόντος, δεν υπάρχει σχετική νομολογία σε ευρωπαϊκό επίπεδο. Στη Γνώμη του 2010 σχετικά με τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, η Ομάδα εργασίας του άρθρου 29 αναφέρει ότι οι από κοινού υπεύθυνοι επεξεργασίας μπορούν να μοιράζονται όλους τους σκοπούς και τον τρόπο επεξεργασίας ή μόνο μερικούς σκοπούς ή τρόπους ή μέρη αυτών ²³⁹. Ενώ στην πρώτη περίπτωση αυτό θα σημαίνει πολύ στενή σχέση μεταξύ των διαφορετικών παραγόντων, στη δεύτερη περίπτωση η σχέση θα είναι πιο χαλαρή.

Η Ομάδα εργασίας του άρθρου 29 τάσσεται υπέρ μιας ευρύτερης ερμηνείας της έννοιας των από κοινού υπευθύνων επεξεργασίας, με σκοπό να παρασχεθεί ένας βαθμός ευελιξίας ώστε να λαμβάνεται υπόψη η αυξανόμενη πολυπλοκότητα της τρέχουσας πραγματικότητας στον τομέα της επεξεργασίας δεδομένων ²⁴⁰. Η θέση της Ομάδας εργασίας αποτυπώθηκε σε υπόθεση που αφορούσε την Εταιρεία Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (Society for Worldwide Interbank Financial Telecommunication, SWIFT).

Παράδειγμα: Στην υπόθεση SWIFT, ευρωπαϊκά τραπεζικά ιδρύματα χρησιμοποιούσαν τη SWIFT, αρχικά ως εκτελούντα την επεξεργασία, για την πραγματοποίηση διαβιβάσεων δεδομένων στο πλαίσιο τραπεζικών συναλλαγών. Η SWIFT κοινοποίησε δεδομένα των εν λόγω τραπεζικών συναλλαγών, τα οποία ήταν αποθηκευμένα σε κέντρο υπολογιστικών υπηρεσιών στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ), στο Υπουργείο Οικονομικών των ΗΠΑ, χωρίς να έχει λάβει ρητή σχετική εντολή από τα ευρωπαϊκά τραπεζικά ιδρύματα που χρησιμοποιούσαν τις υπηρεσίες της. Κατά την αξιολόγηση της νομιμότητας της κατάστασης αυτής, η Ομάδα εργασίας του άρθρου 29 κατέληξε στο συμπέρασμα ότι τα ευρωπαϊκά τραπεζικά ιδρύματα που χρησιμοποιούσαν τις υπηρεσίες της SWIFT,

²³⁹ Ομάδα εργασίας του άρθρου 29 (2010), *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010, σ. 19.

²⁴⁰ Ό.π.

καθώς και η ίδια η SWIFT, έπρεπε να θεωρηθούν από κοινού υπεύθυνοι επεξεργασίας, υπεύθυνοι έναντι των ευρωπαϊών πελατών τους για την κοινοποίηση των δεδομένων τους στις αρχές των ΗΠΑ ²⁴¹.

Εκτελών την επεξεργασία

Βάσει του δικαίου της ΕΕ, ο εκτελών την επεξεργασία είναι το πρόσωπο το οποίο επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό υπευθύνου επεξεργασίας ²⁴². Οι δραστηριότητες που ανατίθενται στον εκτελούντα την επεξεργασία μπορεί να περιορίζονται σε πολύ συγκεκριμένο καθήκον ή πλαίσιο ή μπορεί να είναι αρκετά γενικές και συνολικές.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, η έννοια του εκτελούντος την επεξεργασία είναι ίδια με εκείνη στο πλαίσιο του δικαίου της ΕΕ ²⁴³.

Εξαιρουμένης της επεξεργασίας δεδομένων για λογαριασμό άλλων, οι εκτελούντες την επεξεργασία είναι οι ίδιοι υπεύθυνοι επεξεργασίας δεδομένων σε σχέση με την επεξεργασία που διενεργούν για δικούς τους σκοπούς, για παράδειγμα, για τη διαχείριση των υπαλλήλων, των πωλήσεων και των λογαριασμών τους.

Παράδειγμα: Η εταιρεία Eveready ειδικεύεται στην επεξεργασία δεδομένων για τη διαχείριση δεδομένων ανθρώπινου δυναμικού για λογαριασμό άλλων εταιρειών. Υπό την ιδιότητα αυτή, η Eveready είναι εκτελούσα την επεξεργασία. Ωστόσο, όταν η Eveready επεξεργάζεται τα δεδομένα των δικών της υπαλλήλων, είναι υπεύθυνος δραστηριοτήτων επεξεργασίας δεδομένων οι οποίες αποσκοπούν στην εκπλήρωση των υποχρεώσεων της ως εργοδότη.

²⁴¹ Ομάδα εργασίας του άρθρου 29 (2006), *Γνώμη 10/2006 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Παγκόσμια Εταιρεία Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT)*, WP 128, Βρυξέλλες, 22 Νοεμβρίου 2006.

²⁴² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 8.

²⁴³ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο στ).

Σχέση μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία

Όπως προαναφέρθηκε, ο υπεύθυνος επεξεργασίας ορίζεται ως το πρόσωπο που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας. Ο ΓΚΠΔ προβλέπει σαφώς ότι ο εκτελών την επεξεργασία μπορεί να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους ²⁴⁴. Η σύμβαση μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία είναι ουσιώδες στοιχείο της σχέσης τους και αποτελεί νομική απαίτηση ²⁴⁵.

Παράδειγμα: Ο διευθυντής της εταιρείας Sunshine αποφασίζει ότι η εταιρεία Cloudy –η οποία ειδικεύεται στην αποθήκευση δεδομένων στο υπολογιστικό νέφος– θα πρέπει να διαχειρίζεται τα δεδομένα των πελατών της Sunshine. Η Sunshine παραμένει ο υπεύθυνος επεξεργασίας και η Cloudy είναι μόνο η εκτελούσα την επεξεργασία, καθώς, βάσει της σύμβασης, η Cloudy μπορεί να χρησιμοποιεί τα δεδομένα των πελατών της Sunshine μόνο για τους σκοπούς που καθορίζει η Sunshine.

Εάν η εξουσία καθορισμού των μέσων επεξεργασίας ανατεθεί σε εκτελούντα την επεξεργασία, ο υπεύθυνος επεξεργασίας οφείλει, παρ' όλα αυτά, να είναι σε θέση να ασκεί κατάλληλου βαθμού έλεγχο στις αποφάσεις του εκτελούντος την επεξεργασία σχετικά με τα μέσα επεξεργασίας. Τη συνολική ευθύνη εξακολουθεί να έχει ο υπεύθυνος επεξεργασίας, ο οποίος πρέπει να ασκεί εποπτεία στους εκτελούντες την επεξεργασία ώστε να διασφαλίζει ότι οι αποφάσεις τους είναι σύμφωνες προς το δίκαιο για την προστασία δεδομένων και τις εντολές του.

Επιπλέον, εάν ο εκτελών την επεξεργασία δεν τηρήσει τις προϋποθέσεις επεξεργασίας δεδομένων που θέτει ο υπεύθυνος επεξεργασίας, ο εκτελών θα γίνει υπεύθυνος επεξεργασίας στο μέτρο που παρέβη τις εντολές του υπευθύνου επεξεργασίας. Κατά πάσα πιθανότητα η ενέργεια αυτή θα μετατρέψει τον εκτελούντα σε υπεύθυνο επεξεργασίας που ενεργεί παράνομα. Από την πλευρά του, ο αρχικός υπεύθυνος επεξεργασίας θα πρέπει να εξηγήσει τον τρόπο με τον οποίο ο εκτελών την επεξεργασία μπόρεσε να παραβεί την εντολή του ²⁴⁶. Στην

²⁴⁴ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 29.

²⁴⁵ Ό.π., άρθρο 28 παράγραφος 3.

²⁴⁶ Ό.π., άρθρο 82 παράγραφος 2.

πραγματικότητα, η Ομάδα εργασίας του άρθρου 29 τείνει σε τέτοιες περιπτώσεις να τεκμαίρει την ύπαρξη από κοινού υπευθύνων επεξεργασίας, δεδομένου ότι έτσι προστατεύονται με τον βέλτιστο τρόπο τα συμφέροντα των υποκειμένων των δεδομένων ²⁴⁷.

Ενδέχεται επίσης να υπάρχουν ζητήματα επιμερισμού ευθύνης εάν ο υπεύθυνος επεξεργασίας είναι μικρή επιχείρηση και ο εκτελών την επεξεργασία είναι μεγάλη εταιρεία, η οποία έχει τη δύναμη να υπαγορεύει τους όρους παροχής των υπηρεσιών της. Ωστόσο, σε τέτοιες περιστάσεις η Ομάδα εργασίας του άρθρου 29 υποστηρίζει ότι το επίπεδο της ευθύνης δεν πρέπει να μειώνεται λόγω της οικονομικής ανισορροπίας και ότι πρέπει να διατηρείται η ερμηνεία της έννοιας του υπευθύνου επεξεργασίας ²⁴⁸.

Για λόγους σαφήνειας και διαφάνειας, οι λεπτομέρειες της σχέσης υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία πρέπει να καταγράφονται σε γραπτή σύμβαση ²⁴⁹. Η σύμβαση πρέπει να μνημονεύει ιδίως το αντικείμενο, τη φύση, τον σκοπό και τη διάρκεια της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες υποκειμένων των δεδομένων. Θα πρέπει επίσης να καθορίζει τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία, όπως απαιτήσεις εμπιστευτικότητας και ασφάλειας. Η μη σύναψη τέτοιας σύμβασης συνιστά παράβαση της υποχρέωσης του υπευθύνου επεξεργασίας να παρέχει έγγραφη τεκμηρίωση αμοιβαίων αρμοδιοτήτων και μπορεί να επιφέρει κυρώσεις. Όταν προκαλείται ζημία επειδή ο εκτελών την επεξεργασία υπερέβη ή δεν τήρησε τις νόμιμες εντολές του υπευθύνου επεξεργασίας, εκτός από τον υπεύθυνο επεξεργασίας υπεύθυνος μπορεί να θεωρηθεί και ο εκτελών την επεξεργασία ²⁵⁰. Ο εκτελών την επεξεργασία οφείλει να τηρεί αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που πραγματοποιεί για λογαριασμό του υπευθύνου επεξεργασίας ²⁵¹. Τα αρχεία αυτά πρέπει να τίθενται στη διάθεση της εποπτικής αρχής

247 Ομάδα εργασίας του άρθρου 29 (2010), *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010, σ. 25. Ομάδα εργασίας του άρθρου 29 (2006), *Γνώμη 10/2006 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Εταιρεία Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT)*, WP 128, Βρυξέλλες, 22 Νοεμβρίου 2006.

248 Ομάδα εργασίας του άρθρου 29 (2010), *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010, σ. 26.

249 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 28 παράγραφοι 3 και 9.

250 Ό.π., άρθρο 82 παράγραφος 2.

251 Ό.π., άρθρο 30 παράγραφος 2.

κατόπιν αιτήματός της, καθώς τόσο ο υπεύθυνος επεξεργασίας όσο και ο εκτελών την επεξεργασία οφείλουν να συνεργάζονται με την εν λόγω αρχή κατά την εκτέλεση της αποστολής της²⁵². Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία έχουν επίσης τη δυνατότητα να τηρούν εγκεκριμένο κώδικα δεοντολογίας ή να συμμετέχουν σε μηχανισμό πιστοποίησης προκειμένου να αποδεικνύουν ότι συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ²⁵³.

Οι εκτελούντες την επεξεργασία ενδέχεται να θελήσουν να αναθέσουν ορισμένα καθήκοντα σε άλλους. Αυτό επιτρέπεται από τον νόμο, εφόσον καταρτιστούν κατάλληλοι συμβατικοί όροι μεταξύ του υπευθύνου της επεξεργασίας και του εκτελούντος την επεξεργασία, οι οποίοι θα προβλέπουν, μεταξύ άλλων, αν η εξουσιοδότηση του υπευθύνου επεξεργασίας θα είναι απαραίτητη σε κάθε μεμονωμένη περίπτωση ή αν θα αρκεί απλή ενημέρωση. Ο ΓΚΠΔ προβλέπει ότι ο αρχικός εκτελών την επεξεργασία παραμένει πλήρως υπόλογος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων προστασίας δεδομένων του άλλου εκτελούντος την επεξεργασία²⁵⁴.

Στο δίκαιο του Συμβουλίου της Ευρώπης εφαρμόζεται πλήρως η ερμηνεία των εννοιών του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία όπως εκτίθεται ανωτέρω²⁵⁵.

2.3.2. Αποδέκτες και τρίτοι

Η διαφορά μεταξύ των δύο αυτών κατηγοριών προσώπων ή οντοτήτων, οι οποίες καθιερώθηκαν με την Οδηγία για την Προστασία Δεδομένων, αφορά κυρίως τη σχέση τους με τον υπεύθυνο επεξεργασίας και, ως εκ τούτου, την εξουσιοδοτημένη πρόσβασή τους σε δεδομένα προσωπικού χαρακτήρα τα οποία κατέχει ο υπεύθυνος επεξεργασίας.

Ο «τρίτος» είναι πρόσωπο άλλο, πέραν του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία. Σύμφωνα με το άρθρο 4 σημείο 10 του ΓΚΠΔ, τρίτος είναι «οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο

252 Ό.π., άρθρο 30 παράγραφος 4 και άρθρο 31.

253 Ό.π., άρθρο 28 παράγραφος 5 και άρθρο 42 παράγραφος 4.

254 Ό.π., άρθρο 28 παράγραφος 4.

255 Βλ., για παράδειγμα, Εκσυγχρονισμένη Σύμβαση 108, άρθρο 2 στοιχείο β) και στ)· σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 1.

επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα». Αυτό σημαίνει ότι πρόσωπα που εργάζονται σε οργανισμό διαφορετικό από τον υπεύθυνο επεξεργασίας –ακόμη και αν αυτός ανήκει στον ίδιο όμιλο ή στην ίδια μητρική εταιρεία– θα είναι «τρίτοι» (ή θα ανήκουν σε «τρίτο»). Από την άλλη πλευρά, τα καταστήματα τράπεζας που επεξεργάζονται λογαριασμούς πελατών υπό την άμεση εποπτεία της κεντρικής διοίκησής τους δεν θα είναι «τρίτοι»²⁵⁶.

Ο όρος «αποδέκτης» είναι ευρύτερος από τον όρο «τρίτος». Κατά την έννοια του άρθρου 4 σημείο 9 του ΓΚΠΔ, ως αποδέκτης νοείται «το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι». Ο αποδέκτης μπορεί να είναι είτε πρόσωπο άλλο, πέραν του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία –οπότε θα είναι τρίτος– ή πρόσωπο εντός του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, όπως υπάλληλος ή άλλο τμήμα εντός της ίδιας εταιρείας ή αρχής.

Η διάκριση μεταξύ αποδεκτών και τρίτων έχει σημασία μόνο λόγω των προϋποθέσεων για τη νόμιμη κοινοποίηση δεδομένων. Οι υπάλληλοι υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία μπορούν να είναι αποδέκτες δεδομένων προσωπικού χαρακτήρα χωρίς καμία περαιτέρω νομική απαίτηση, εάν συμμετέχουν στις πράξεις επεξεργασίας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Αντιθέτως, τρίτος, ο οποίος αποτελεί αυτοτελή οντότητα σε σχέση με τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, δεν εξουσιοδοτείται να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα τα οποία επεξεργάζεται υπεύθυνος επεξεργασίας παρά μόνο για συγκεκριμένους νόμιμους λόγους σε συγκεκριμένη περίπτωση.

Παράδειγμα: Υπάλληλος υπευθύνου επεξεργασίας ο οποίος χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα στο πλαίσιο των καθηκόντων που του έχει αναθέσει ο εργοδότης του είναι αποδέκτης δεδομένων, αλλά όχι τρίτος, δεδομένου ότι χρησιμοποιεί τα δεδομένα εξ ονόματος και κατ' εντολή του υπευθύνου επεξεργασίας. Για παράδειγμα, εάν

²⁵⁶ Ομάδα εργασίας του άρθρου 29 (2010), *Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία»*, WP 169, Βρυξέλλες, 16 Φεβρουαρίου 2010, σ. 31.

ο εργοδότης κοινοποιήσει δεδομένα προσωπικού χαρακτήρα των υπαλλήλων του στο τμήμα ανθρώπινου δυναμικού ενόψει των επικείμενων αξιολογήσεων επιδόσεων, τα μέλη της ομάδας ανθρώπινου δυναμικού θα είναι αποδέκτες δεδομένων προσωπικού χαρακτήρα, καθώς τα δεδομένα τούς κοινοποιήθηκαν στο πλαίσιο της επεξεργασίας για τον υπεύθυνο επεξεργασίας.

Εάν, ωστόσο, ο οργανισμός παρέχει δεδομένα υπαλλήλων του σε εταιρεία κατάρτισης, η οποία θα τα χρησιμοποιήσει για την προετοιμασία εξατομικευμένου προγράμματος κατάρτισης για τους υπαλλήλους, η εν λόγω εταιρεία είναι τρίτος. Αυτό ισχύει διότι η εταιρεία παροχής υπηρεσιών κατάρτισης δεν διαθέτει ειδική νομιμοποίηση ή εξουσιοδότηση (η οποία στην περίπτωση του τμήματος ανθρώπινου δυναμικού απορρέει από τη σχέση απασχόλησης με τον υπεύθυνο επεξεργασίας) για να επεξεργαστεί τα εν λόγω δεδομένα προσωπικού χαρακτήρα. Με άλλα λόγια, η εταιρεία κατάρτισης δεν έλαβε τις πληροφορίες στο πλαίσιο της εργασίας της στον υπεύθυνο επεξεργασίας δεδομένων.

2.4. Συγκατάθεση

Κύρια σημεία

- Η συγκατάθεση ως νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι ελεύθερη, εν πλήρει επιγνώσει, συγκεκριμένη και αδιαμφισβήτητη ένδειξη βούλησης με σαφή θετική ενέργεια με την οποία εκδηλώνεται η συμφωνία για την επεξεργασία.
- Για την επεξεργασία ειδικών κατηγοριών δεδομένων απαιτείται ρητή συγκατάθεση.

Όπως θα δούμε αναλυτικά στο [κεφάλαιο 4](#), η συγκατάθεση είναι ένας από τους έξι νόμιμους λόγους επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Ως συγκατάθεση ορίζεται «κάθε ένδειξη βούλησης, ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη» ²⁵⁷.

²⁵⁷ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 11. Βλ. επίσης Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 2.

Για να θεωρείται έγκυρη η συγκατάθεση, στο **δίκαιο της ΕΕ** ορίζονται διάφορες προϋποθέσεις, με στόχο να διασφαλίζεται ότι τα υποκείμενα των δεδομένων είχαν πραγματικά την πρόθεση να εγκρίνουν συγκεκριμένη χρήση των δεδομένων που τα αφορούν:²⁵⁸

- Η συγκατάθεση πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη ένδειξη της συμφωνίας του υποκειμένου των δεδομένων για την επεξεργασία των δεδομένων που το αφορούν. Η πράξη αυτή μπορεί να είναι ενέργεια ή δήλωση.
- Το υποκείμενο των δεδομένων πρέπει να έχει το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή.
- Στο πλαίσιο γραπτής δήλωσης η οποία αφορά και άλλα θέματα, όπως «όρους παροχής υπηρεσίας», τα αιτήματα για συγκατάθεση πρέπει να υποβάλλονται με σαφή και απλή διατύπωση και σε κατανοητή και εύκολα προσβάσιμη μορφή, ώστε η συγκατάθεση να καθίσταται σαφώς διακριτή από άλλα θέματα· εάν ένα τμήμα της δήλωσης αυτής συνιστά παράβαση του ΓΚΠΔ, τότε δεν είναι δεσμευτικό.

Η συγκατάθεση θα είναι έγκυρη στο πλαίσιο του δικαίου για την προστασία δεδομένων μόνο εάν οι απαιτήσεις αυτές πληρούνται σωρευτικά. Ο υπεύθυνος επεξεργασίας οφείλει να αποδείξει ότι το υποκείμενο των δεδομένων συγκατέθηκε στην επεξεργασία των δεδομένων που το αφορούν²⁵⁹. Τα στοιχεία της έγκυρης συγκατάθεσης θα εξεταστούν περαιτέρω στην **ενότητα 4.1.1** σχετικά με τους νόμιμους λόγους επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Στη Σύμβαση 108 δεν περιλαμβάνεται ορισμός της συγκατάθεσης· η διατύπωση τέτοιου ορισμού επαφίεται στο εθνικό δίκαιο. Ωστόσο, **βάσει του δικαίου του Συμβουλίου της Ευρώπης**, τα στοιχεία της έγκυρης συγκατάθεσης αντιστοιχούν σε αυτά που αναλύθηκαν ανωτέρω²⁶⁰.

²⁵⁸ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 7.

²⁵⁹ Ό.π., άρθρο 7 παράγραφος 1.

²⁶⁰ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 2· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημεία 42-45.

Πρόσθετες απαιτήσεις για την εγκυρότητα της συγκατάθεσης βάσει του αστικού δικαίου, όπως δικαιοπρακτική ικανότητα, υπάρχουν βεβαίως και στο πλαίσιο της προστασίας δεδομένων, καθώς τέτοιες απαιτήσεις αποτελούν θεμελιώδη νομικά προαπαιτούμενα. Η μη έγκυρη συγκατάθεση προσώπων που δεν διαθέτουν δικαιοπρακτική ικανότητα θα έχει ως αποτέλεσμα την απουσία νομικής βάσης για την επεξεργασία δεδομένων που αφορούν τα εν λόγω πρόσωπα. Όσον αφορά τη δικαιοπρακτική ικανότητα ανηλίκων να συνάπτουν συμβάσεις, ο ΓΚΠΔ προβλέπει ότι οι κανόνες του περί του ελάχιστου ορίου ηλικίας για την εξασφάλιση έγκυρης συγκατάθεσης δεν επηρεάζουν το γενικό ενοχικό δίκαιο των κρατών μελών ²⁶¹.

Η συγκατάθεση πρέπει να παρέχεται σαφώς ώστε να μην υφίσταται αμφιβολία σχετικά με την πρόθεση του υποκειμένου των δεδομένων ²⁶². Η συγκατάθεση πρέπει να παρέχεται ρητώς όταν αφορά την επεξεργασία ευαίσθητων δεδομένων, και μπορεί να παρέχεται προφορικώς ή γραπτώς ²⁶³. Η συγκατάθεση μπορεί να παρέχεται με ηλεκτρονικά μέσα ²⁶⁴. Στο πλαίσιο τόσο του **δικαίου της ΕΕ** όσο και του **δικαίου του Συμβουλίου της Ευρώπης**, η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να παρέχεται με δήλωση ή με σαφή θετική ενέργεια ²⁶⁵. Επομένως, δεν μπορεί να συνάγεται από σιωπή, προσυμπληρωμένα τετραγωνίδια, συμπληρωμένα εκ των προτέρων έντυπα ή αδράνεια ²⁶⁶.

261 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 8 παράγραφος 3.

262 Ό.π., άρθρο 6 παράγραφος 1 στοιχείο α) και άρθρο 9 παράγραφος 2 στοιχείο α).

263 Ό.π., αιτιολογική σκέψη 32.

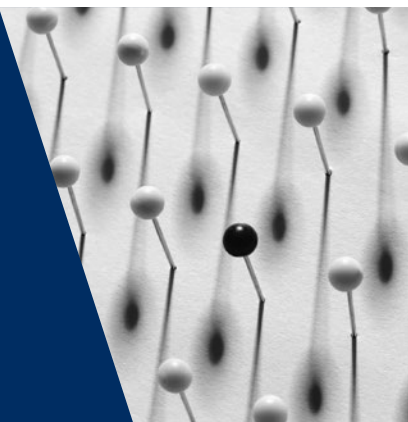
264 Ό.π.

265 Ό.π., άρθρο 4 σημείο 11· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 42.

266 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 32· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 42.

3

Βασικές αρχές του ευρωπαϊκού δικαίου για την προστασία δεδομένων



ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο α)	Η αρχή της νομιμότητας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 3
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο α)	Η αρχή της αντικειμενικότητας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο α) ΕΔΔΑ, Κ.Η. κ.λπ. κατά Σλοβακίας, προσφυγή αριθ. 32881/04, 2009
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο α) ΔΕΕ, C-201/14, <i>Smaranda Bara</i> κ.λπ. κατά <i>Casa Națională de Asigurări de Sănătate</i> κ.λπ., 2015	Η αρχή της διαφάνειας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο α) και άρθρο 8 ΕΔΔΑ, <i>Haralambie</i> κατά <i>Ρουμανίας</i> , προσφυγή αριθ. 21737/03, 2009
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο β)	Η αρχή του περιορισμού του σκοπού	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο β)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο γ) ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, <i>Digital Rights Ireland</i> και <i>Kärntner Landesregierung</i> κ.λπ. [Τμήμα μείζονος συνθέσεως], 2014	Η αρχή της ελαχιστοποίησης των δεδομένων	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο γ)

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο δ) <i>ΔΕΕ, C-553/07, College van burgemeester en wethouders van Rotterdam κατά E. E. Rijkeboer, 2009</i>	Η αρχή της ακρίβειας των δεδομένων	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο δ)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο ε) <i>ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, Digital Rights Ireland και Kärntner Landesregierung κ.λπ. [τμήμα μείζονος συνθέσεως], 2014</i>	Η αρχή του περιορισμού της περιόδου αποθήκευσης	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο ε) <i>ΕΔΔΑ, S. και Marper κατά Ηνωμένου Βασιλείου [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 2008</i>
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο στ) και άρθρο 32	Η αρχή της ασφάλειας των δεδομένων (ακεραιότητα και εμπιστευτικότητα)	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 2	Η αρχή της λογοδοσίας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10

Το άρθρο 5 του Γενικού Κανονισμού για την Προστασία Δεδομένων καθορίζει τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι αρχές αυτές αφορούν:

- τη νομιμότητα, την αντικειμενικότητα και τη διαφάνεια·
- τον περιορισμό του σκοπού·
- την ελαχιστοποίηση των δεδομένων·
- την ακρίβεια των δεδομένων·
- τον περιορισμό της περιόδου αποθήκευσης·
- την ακεραιότητα και την εμπιστευτικότητα.

Οι αρχές αυτές αποτελούν τη βάση για τις λεπτομερέστερες διατάξεις που περιέχονται στα επόμενα άρθρα του κανονισμού. Προβλέπονται επίσης στα άρθρα 5, 7, 8 και 10 της Εκσυγχρονισμένης Σύμβασης 108. Κάθε μεταγενέστερη νομοθεσία για την προστασία δεδομένων σε επίπεδο Συμβουλίου της Ευρώπης ή ΕΕ πρέπει να συμμορφώνεται προς τις αρχές αυτές, οι οποίες πρέπει να λαμβάνονται υπόψη κατά την ερμηνεία της εν λόγω νομοθεσίας. Βάσει του δικαίου της ΕΕ, περιορισμοί των αρχών που διέπουν την επεξεργασία επιτρέπονται μόνο στο μέτρο που αντιστοιχούν στα δικαιώματα και στις υποχρεώσεις που προβλέπονται στα άρθρα 12 έως 22 και πρέπει να σέβονται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών. Κάθε εξαίρεση από τις βασικές αυτές αρχές και κάθε περιορισμός αυτών πρέπει να προβλέπεται σε επίπεδο ΕΕ ή σε εθνικό επίπεδο ²⁶⁷. πρέπει να προβλέπεται από τον νόμο, να επιδιώκει θεμιτό σκοπό και να αποτελεί αναγκαίο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία ²⁶⁸. Οι τρεις προϋποθέσεις πρέπει να πληρούνται σωρευτικά.

3.1. Οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας της επεξεργασίας

Κύρια σημεία

- Οι αρχές της νομιμότητας, της αντικειμενικότητας και της διαφάνειας εφαρμόζονται σε κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Στο πλαίσιο του ΓΚΠΔ, η νομιμότητα απαιτεί να πληρούνται μία από τις ακόλουθες προϋποθέσεις:
 - συγκατάθεση του υποκειμένου των δεδομένων·
 - αναγκαιότητα για τη σύναψη σύμβασης·
 - έννομη υποχρέωση·
 - αναγκαιότητα για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου προσώπου·

²⁶⁷ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 11 παράγραφος 1· Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 23 παράγραφος 1.

²⁶⁸ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 23 παράγραφος 1.

- αναγκαιότητα για την εκπλήρωση καθήκοντος δημόσιου συμφέροντος
- αναγκαιότητα για τα έννομα συμφέροντα του υπευθύνου επεξεργασίας ή τρίτου, εκτός εάν υπερσχύουν έναντι αυτών τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται με θεμιτό τρόπο.
- Το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για τον κίνδυνο ώστε να διασφαλίζεται ότι η επεξεργασία δεν έχει απρόβλεπτες αρνητικές συνέπειες.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται με διαφανή τρόπο.
- Οι υπεύθυνοι επεξεργασίας πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων πριν από την επεξεργασία των δεδομένων τους, μεταξύ άλλων, για τον σκοπό της επεξεργασίας, καθώς και για την ταυτότητα και τη διεύθυνση του υπευθύνου επεξεργασίας.
- Οι πληροφορίες σχετικά με τις πράξεις επεξεργασίας πρέπει να παρέχονται με απλή και σαφή διατύπωση, ώστε τα υποκείμενα των δεδομένων να μπορούν να κατανοούν εύκολα τους κανόνες, τους κινδύνους, τις εγγυήσεις και τα δικαιώματα που σχετίζονται με αυτά.
- Τα υποκείμενα των δεδομένων έχουν δικαίωμα πρόσβασης στα δεδομένα που τα αφορούν όταν αυτά υποβάλλονται σε επεξεργασία.

3.1.1. Νομιμότητα της επεξεργασίας

Σύμφωνα με το **δίκαιο της ΕΕ και το δίκαιο του Συμβουλίου της Ευρώπης για την προστασία δεδομένων**, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται σύννομα ²⁶⁹. Η σύννομη επεξεργασία απαιτεί τη συγκατάθεση του υποκειμένου των δεδομένων ή άλλο νόμιμο λόγο ο οποίος προβλέπεται στη νομοθεσία για την προστασία δεδομένων ²⁷⁰. Στο άρθρο 6 παράγραφος 1 του ΓΚΠΔ προβλέπονται πέντε νόμιμοι λόγοι επεξεργασίας, επιπροσθέτως της συγκατάθεσης, δηλαδή περιπτώσεις όπου η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι αναγκαία για την εκτέλεση σύμβασης, για την

²⁶⁹ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 3· Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο α).

²⁷⁰ Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, άρθρο 8 παράγραφος 2· Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 40 και άρθρα 6-9· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 2· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 41.

εκπλήρωση καθήκοντος που εκτελείται κατά την άσκηση δημόσιας εξουσίας, για τη συμμόρφωση προς έννομη υποχρέωση, για τον σκοπό των έννομων συμφερόντων που επιδιώκουν ο υπεύθυνος επεξεργασίας ή τρίτοι ή για τη διαφύλαξη των ζωτικών συμφερόντων του υποκειμένου των δεδομένων. Οι λόγοι αυτοί θα εξεταστούν αναλυτικότερα στην [ενότητα 4.1](#).

3.1.2. Αντικειμενικότητα της επεξεργασίας

Επιπροσθέτως της νομιμότητας της επεξεργασίας, σύμφωνα με το δίκαιο της ΕΕ και το δίκαιο του Συμβουλίου της Ευρώπης για την προστασία δεδομένων, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται με αντικειμενικό τρόπο ²⁷¹. Η αρχή της αντικειμενικής επεξεργασίας διέπει πρωτίστως τη σχέση μεταξύ του υπευθύνου επεξεργασίας και του υποκειμένου των δεδομένων.

Οι υπεύθυνοι επεξεργασίας θα πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων και το ευρύ κοινό ότι θα επεξεργάζονται τα δεδομένα με σύννομο και διαφανή τρόπο και πρέπει να είναι σε θέση να αποδείξουν τη συμμόρφωση των πράξεων επεξεργασίας με τον ΓΚΠΔ. Οι πράξεις επεξεργασίας δεν πρέπει να διενεργούνται μυστικά, και τα υποκείμενα των δεδομένων θα πρέπει να έχουν επίγνωση των δυνητικών κινδύνων. Επιπλέον, στο μέτρο που είναι εφικτό, οι υπεύθυνοι επεξεργασίας πρέπει να ενεργούν κατά τρόπο που συμμορφώνεται άμεσα με τις επιθυμίες του υποκειμένου των δεδομένων, ιδίως όταν η συγκατάθεση αυτού αποτελεί τη νομική βάση για την επεξεργασία τους.

Παράδειγμα: Στην υπόθεση *Κ.Η. κ.λπ. κατά Σλοβακίας* ²⁷², οι προσφεύγουσες –Ρομά στην καταγωγή– είχαν νοσηλευτεί σε δύο νοσοκομεία στην ανατολική Σλοβακία κατά τη διάρκεια της εγκυμοσύνης και του τοκετού τους. Έπειτα από τον τοκετό, καμία από τις δύο δεν μπόρεσε να συλλάβει εκ νέου, παρά τις επανειλημμένες προσπάθειες. Τα εθνικά δικαστήρια διέταξαν τα νοσοκομεία να επιτρέψουν στις προσφεύγουσες και στους εκπροσώπους τους να συμβουλευτούν τα ιατρικά αρχεία τους και να λάβουν γραπτά αποσπάσματα αυτών, αλλά απέρριψαν το αίτημά τους να φωτοτυπήσουν τα έγγραφα, προβάλλοντας ως αιτιολογία την αποφυγή πιθανής κατάχρησής τους. Οι θετικές υποχρεώσεις των κρατών βάσει

271 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο α): Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο α).

272 ΕΔΔΑ, *Κ.Η. κ.λπ. κατά Σλοβακίας*, προσφυγή αριθ. 32881/04, 28 Απριλίου 2009.

του άρθρου 8 της ΕΣΔΑ περιλάμβαναν αναγκαστικά την υποχρέωση χορήγησης στο υποκείμενο των δεδομένων αντιγράφων των αρχείων δεδομένων που το αφορούν. Εναπέκειτο στο κράτος να καθορίσει τις ρυθμίσεις για τη χορήγηση των αντιγράφων αρχείων δεδομένων προσωπικού χαρακτήρα ή, κατά περίπτωση, να αποδείξει ότι συντρέχουν επιτακτικοί λόγοι για την απόρριψη τέτοιου αιτήματος. Στην περίπτωση των προσφευγουσών, τα εθνικά δικαστήρια αιτιολόγησαν την απαγόρευση που επιβλήθηκε στις προσφεύγουσες να λάβουν αντίγραφα των ιατρικών αρχείων κυρίως επικαλούμενα την ανάγκη προστασίας των σχετικών πληροφοριών από τυχόν κατάχρηση. Ωστόσο, το ΕΔΔΑ δεν διέκρινε με ποιον τρόπο οι προσφεύγουσες, στις οποίες είχε παρασχεθεί εν πάση περιπτώσει πρόσβαση στο σύνολο των ιατρικών αρχείων τους, μπορούσαν να κάνουν κατάχρηση πληροφοριών που αφορούσαν τις ίδιες. Επιπλέον, ο κίνδυνος τέτοιας κατάχρησης μπορούσε να είχε αποφευχθεί με άλλους τρόπους πέραν της άρνησης χορήγησης αντιγράφων των αρχείων στις προσφεύγουσες, όπως με τον περιορισμό του εύρους των προσώπων που δικαιούνταν πρόσβαση στα αρχεία. Το κράτος δεν κατόρθωσε να αποδείξει την ύπαρξη επαρκώς επιτακτικών λόγων για την άρνηση χορήγησης στις προσφεύγουσες αποτελεσματικής πρόσβασης σε πληροφορίες που αφορούσαν την υγεία τους. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι είχε σημειωθεί παράβαση του άρθρου 8.

Όσον αφορά τις υπηρεσίες διαδικτύου, τα χαρακτηριστικά των συστημάτων επεξεργασίας δεδομένων πρέπει να παρέχουν τη δυνατότητα στα υποκείμενα των δεδομένων να κατανοούν πραγματικά τι συμβαίνει με τα δεδομένα τους. Σε κάθε περίπτωση, η αρχή της αντικειμενικότητας βαίνει πέραν των υποχρεώσεων διαφάνειας και θα μπορούσε επίσης να συνδέεται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα με δεοντολογικό τρόπο.

Παράδειγμα: Το ερευνητικό τμήμα ενός πανεπιστημίου διεξάγει πείραμα αναλύοντας τις αλλαγές στη διάθεση 50 προσώπων. Τα πρόσωπα αυτά πρέπει να καταγράφουν σε ηλεκτρονικό αρχείο τις σκέψεις τους σε ωριαία βάση και σε δεδομένη χρονική στιγμή. Τα 50 πρόσωπα έδωσαν τη συγκατάθεσή τους για το συγκεκριμένο πείραμα και για τη συγκεκριμένη χρήση των δεδομένων από το πανεπιστήμιο. Το ερευνητικό τμήμα διαπιστώνει σύντομα ότι η καταχώριση σκέψεων ηλεκτρονικά μπορεί να είναι ιδιαίτερα χρήσιμη για μια άλλη εργασία η οποία επικεντρώνεται στην ψυχική υγεία, την οποία συντονίζει άλλη ομάδα. Παρότι το πανεπιστήμιο,

ως υπεύθυνος επεξεργασίας, θα μπορούσε να είχε χρησιμοποιήσει τα ίδια δεδομένα για τις εργασίες της άλλης ομάδας χωρίς περαιτέρω ενέργειες για τη διασφάλιση της νομιμότητας της επεξεργασίας, καθώς οι σκοποί είναι συμβατοί, ενημέρωσε τα πρόσωπα και ζήτησε εκ νέου τη συγκατάθεσή τους, εφαρμόζοντας τον δεοντολογικό κώδικά του στον τομέα της έρευνας και την αρχή της αντικειμενικότητας της επεξεργασίας.

3.1.3. Διαφάνεια της επεξεργασίας

Σύμφωνα με το **δίκαιο της ΕΕ και το δίκαιο του Συμβουλίου της Ευρώπης για την προστασία δεδομένων**, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται «με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων»²⁷³.

Η αρχή αυτή θεσπίζει την υποχρέωση του υπευθύνου επεξεργασίας να λαμβάνει κατάλληλα μέτρα ώστε να τηρεί ενήμερα τα υποκείμενα των δεδομένων –που μπορεί να είναι χρήστες ή πελάτες– σχετικά με τον τρόπο χρήσης των δεδομένων τους²⁷⁴. Η διαφάνεια μπορεί να αφορά τις πληροφορίες που παρέχονται στο φυσικό πρόσωπο προτού ξεκινήσει η επεξεργασία²⁷⁵, τις πληροφορίες στις οποίες τα υποκείμενα των δεδομένων πρέπει να έχουν άμεση πρόσβαση κατά τη διάρκεια της επεξεργασίας²⁷⁶, αλλά και τις πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων κατόπιν αιτήματός τους για πρόσβαση στα δεδομένα που τα αφορούν²⁷⁷.

Παράδειγμα: Στην υπόθεση *Haralambie κατά Ρουμανίας*²⁷⁸, ο οργανισμός μυστικών υπηρεσιών χορήγησε στον προσφεύγοντα πρόσβαση στις πληροφορίες που κατείχε σχετικά με αυτόν πέντε έτη μετά το αίτημά του. Το ΕΔΔΑ επανέλαβε ότι φυσικά πρόσωπα για τα οποία οι δημόσιες αρχές διατηρούσαν προσωπικούς φακέλους είχαν ζωτικό συμφέρον πρόσβασης σε αυτούς. Οι αρχές είχαν υποχρέωση να προβλέψουν αποτελεσματική

273 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο α)· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο α) και άρθρο 8.

274 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 12.

275 Ο.π., άρθρα 13 και 14.

276 Ομάδα εργασίας του άρθρου 29, *Γνώμη 2/2017 σχετικά με την επεξεργασία δεδομένων στην εργασία*, WP 249, σ. 23.

277 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 15.

278 ΕΔΔΑ, *Haralambie κατά Ρουμανίας*, προσφυγή αριθ. 21737/03, 27 Οκτωβρίου 2009.

διαδικασία για την παροχή πρόσβασης σε τέτοιες πληροφορίες. Το ΕΔΔΑ έκρινε ότι ούτε η ποσότητα των διαβιβασθέντων αρχείων ούτε οι αδυναμίες του συστήματος αρχειοθέτησης δικαιολογούσαν την πενταετή καθυστέρηση ικανοποίησης του αιτήματος του προσφεύγοντος για πρόσβαση στα αρχεία του. Οι αρχές δεν είχαν παράσχει στον προσφεύγοντα αποτελεσματική και προσιτή διαδικασία ώστε αυτός να μπορέσει να εξασφαλίσει πρόσβαση στα προσωπικά αρχεία του εντός εύλογου χρονικού διαστήματος. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι είχε σημειωθεί παράβαση του άρθρου 8 της ΕΣΔΑ.

Οι πράξεις επεξεργασίας πρέπει να εξηγούνται στα υποκείμενα των δεδομένων με εύκολα προσβάσιμο μέσο ώστε να διασφαλίζεται ότι κατανοούν τι θα συμβεί στα δεδομένα τους. Αυτό σημαίνει ότι το υποκείμενο των δεδομένων πρέπει να γνωρίζει τον συγκεκριμένο σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα κατά τον χρόνο συλλογής τους ²⁷⁹. Η διαφάνεια της επεξεργασίας επιβάλλει να χρησιμοποιείται σαφής και απλή γλώσσα ²⁸⁰. Οι ενδιαφερόμενοι πρέπει να έχουν επίγνωση των κινδύνων, των κανόνων, των εγγυήσεων και των δικαιωμάτων που αφορούν την επεξεργασία των δεδομένων που τους αφορούν ²⁸¹.

Το **δίκαιο του Συμβουλίου της Ευρώπης** προβλέπει επίσης ότι ορισμένες βασικές πληροφορίες πρέπει να παρέχονται υποχρεωτικά και με προδραστικό τρόπο από τον υπεύθυνο επεξεργασίας στα υποκείμενα των δεδομένων. Πληροφορίες σχετικά με το ονοματεπώνυμο και τη διεύθυνση του υπευθύνου επεξεργασίας (ή των από κοινού υπευθύνων επεξεργασίας), τη νομική βάση και τους σκοπούς της επεξεργασίας δεδομένων, τις κατηγορίες δεδομένων που υποβάλλονται σε επεξεργασία και τους αποδέκτες τους, καθώς και για τον τρόπο άσκησης των δικαιωμάτων, μπορούν να παρέχονται με κάθε κατάλληλο μέσο (μέσω ιστοτόπου, τεχνολογικών εργαλείων σε προσωπικές συσκευές κ.λπ.) υπό τον όρο οι πληροφορίες παρουσιάζονται αντικειμενικά και αποτελεσματικά στο υποκείμενο των δεδομένων. Οι πληροφορίες που παρουσιάζονται θα πρέπει να είναι εύκολα προσβάσιμες, ευανάγνωστες, κατανοητές και προσαρμοσμένες στα αντίστοιχα υποκείμενα των δεδομένων (για παράδειγμα, σε γλώσσα φιλική προς το παιδί όπου απαιτείται). Πρέπει να παρέχεται επίσης κάθε πρόσθετη πληροφορία η οποία είναι αναγκαία για να διασφαλίζεται η θεμιτή επεξεργασία των

279 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 39.

280 Ό.π.

281 Ό.π.

δεδομένων, ή η οποία είναι χρήσιμη για τον σκοπό αυτό, όπως η περίοδος διατήρησης, το σκεπτικό στο οποίο βασίζεται η επεξεργασία ή πληροφορίες σχετικά με διαβιβάσεις δεδομένων σε αποδέκτη που βρίσκεται σε άλλο συμβαλλόμενο ή μη συμβαλλόμενο μέρος (μεταξύ άλλων, αν το συγκεκριμένο μη συμβαλλόμενο μέρος παρέχει κατάλληλο επίπεδο προστασίας ή ποια είναι τα μέτρα που λαμβάνει ο υπεύθυνος επεξεργασίας για να διασφαλίσει κατάλληλο επίπεδο προστασίας δεδομένων)²⁸².

Δυνάμει του δικαιώματος πρόσβασης²⁸³, το υποκείμενο των δεδομένων δικαιούται να πληροφορηθεί, κατόπιν αιτήματός του, από τον υπεύθυνο επεξεργασίας αν τα δεδομένα του υποβάλλονται σε επεξεργασία και, εάν ναι, ποια από αυτά υποβάλλονται σε επεξεργασία²⁸⁴. Επιπλέον, δυνάμει του δικαιώματος ενημέρωσης²⁸⁵, τα πρόσωπα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία πρέπει να ενημερώνονται προδραστικά από τους υπευθύνους επεξεργασίας ή τους εκτελούντες την επεξεργασία σχετικά με τους σκοπούς, τη διάρκεια, τα μέσα της επεξεργασίας, μεταξύ άλλων, γενικά προτού ξεκινήσει η δραστηριότητα επεξεργασίας.

Παράδειγμα: Η υπόθεση *Smaranda Bara κ.λπ. κατά Prezidentele Casei Naționale de Asigurări de Sănătate, Casa Națională de Administrare Fiscală (ANAF)*²⁸⁶ αφορούσε τη διαβίβαση από την Εθνική Φορολογική Αρχή στο Εθνικό Ταμείο Ασφάλισης Υγείας στη Ρουμανία φορολογικών δεδομένων σχετικών με το εισόδημα ελεύθερων επαγγελματιών, βάσει των οποίων απαιτήθηκε η προκαταβολή εισφορών στο σύστημα ασφάλισης υγείας. Το ΔΕΕ κλήθηκε να αποφανθεί αν τα υποκείμενα των δεδομένων έπρεπε να είχαν ενημερωθεί σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας και τον σκοπό της διαβίβασης των δεδομένων πριν από την επεξεργασία τους από το Εθνικό Ταμείο Ασφάλισης Υγείας. Το ΔΕΕ έκρινε ότι, αν διοικητική αρχή κράτους μέλους διαβιβάζει δεδομένα προσωπικού χαρακτήρα σε άλλη διοικητική αρχή η οποία τα υποβάλλει σε περαιτέρω επεξεργασία, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται σχετικά με τη διαβίβαση ή την επεξεργασία.

282 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 68.

283 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 15.

284 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 και άρθρο 9 παράγραφος 1 στοιχείο β).

285 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 13 και 14.

286 ΔΕΕ, C-201/14, *Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ.*, 1 Οκτωβρίου 2015, σκέψεις 28-46.

Σε ορισμένες περιπτώσεις, επιτρέπονται παρεκκλίσεις από την υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων σχετικά με την επεξεργασία δεδομένων· αυτές θα εξεταστούν λεπτομερέστερα στην [ενότητα 6.1](#) που αναφέρεται στα δικαιώματα του υποκειμένου των δεδομένων.

3.2. Η αρχή του περιορισμού του σκοπού

Κύρια σημεία

- Ο σκοπός της επεξεργασίας δεδομένων πρέπει να καθορίζεται προτού ξεκινήσει η επεξεργασία.
- Δεν επιτρέπεται περαιτέρω επεξεργασία των δεδομένων κατά τρόπο ασύμβατο προς τον αρχικό σκοπό, παρότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει εξαιρέσεις από τον κανόνα αυτό για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς.
- Κατ' ουσίαν, η αρχή του περιορισμού του σκοπού σημαίνει ότι κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να πραγματοποιείται για συγκεκριμένο, καλά καθορισμένο σκοπό και μόνο για πρόσθετους, συγκεκριμένους σκοπούς οι οποίοι είναι συμβατοί προς τον αρχικό.

Η αρχή του περιορισμού του σκοπού συγκαταλέγεται στις θεμελιώδεις αρχές του ευρωπαϊκού δικαίου για την προστασία δεδομένων. Συνδέεται στενά με τη διαφάνεια, την προβλεψιμότητα και τον έλεγχο του χρήστη: εάν ο σκοπός της επεξεργασίας είναι επαρκώς συγκεκριμένος και σαφής, τα άτομα γνωρίζουν τι να περιμένουν και αυξάνονται η διαφάνεια και η ασφάλεια δικαίου. Ταυτόχρονα, η σαφής οριοθέτηση του σκοπού είναι σημαντική προϋπόθεση ώστε τα υποκείμενα των δεδομένων να μπορούν να ασκούν αποτελεσματικά τα δικαιώματά τους, όπως το δικαίωμα εναντίωσης στην επεξεργασία ²⁸⁷.

Σύμφωνα με την αρχή του περιορισμού του σκοπού, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να εκτελείται για συγκεκριμένο, καλά καθορισμένο σκοπό και μόνο για πρόσθετους σκοπούς οι οποίοι είναι συμβατοί προς τον αρχικό ²⁸⁸. Επομένως, η επεξεργασία δεδομένων προσωπικού

²⁸⁷ Ομάδα εργασίας του άρθρου 29 (2013), *Opinion 3/13 on purpose limitation*, WP 203, 2 Απριλίου 2013.

²⁸⁸ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο β).

χαρακτήρα για μη καθορισμένους και/ή μη περιορισμένους σκοπούς είναι παράνομη. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα χωρίς ορισμένο σκοπό, απλώς με το σκεπτικό ότι ενδέχεται να είναι χρήσιμα κάποια στιγμή στο μέλλον, επίσης δεν είναι σύλληψη. Η νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα εξαρτάται από τον σκοπό της επεξεργασίας, ο οποίος πρέπει να είναι ρητός, καθορισμένος και νόμιμος.

Κάθε νέος σκοπός επεξεργασίας δεδομένων ο οποίος είναι ασύμβατος με τον αρχικό πρέπει να έχει τη δική του νομική βάση και δεν μπορεί να δικαιολογείται από το γεγονός ότι τα δεδομένα αποκτήθηκαν αρχικά ή υποβλήθηκαν σε επεξεργασία για άλλο νόμιμο σκοπό. Από την άλλη πλευρά, η νόμιμη επεξεργασία περιορίζεται στον αρχικά καθορισμένο σκοπό, και για οποιονδήποτε νέο σκοπό απαιτείται νέα, χωριστή νομική βάση. Για παράδειγμα, η κοινοποίηση δεδομένων προσωπικού χαρακτήρα σε τρίτους για νέο σκοπό θα πρέπει να εξετάζεται προσεκτικά, καθώς μια τέτοια κοινοποίηση θα χρειάζεται πιθανώς πρόσθετη νομική βάση, διαφορετική από εκείνη στην οποία βασίστηκε η συλλογή των δεδομένων.

Παράδειγμα: Αεροπορική εταιρεία συλλέγει δεδομένα από τους επιβάτες της κατά την πραγματοποίηση κρατήσεων ώστε να εξασφαλίζει την ορθή εκτέλεση της πτήσης. Η αεροπορική εταιρεία θα χρειαστεί δεδομένα σχετικά με τους αριθμούς θέσεων των πελατών, ειδικούς φυσικούς περιορισμούς, όπως ανάγκη για αναπηρικά αμαξίδια, και ειδικές απαιτήσεις διατροφής, όπως γεύματα παρασκευασμένα κατά την εβραϊκή ή τη μουσουλμανική παράδοση. Εάν ζητηθεί από την αεροπορική εταιρεία να διαβιβάσει τα δεδομένα αυτά, τα οποία περιέχονται στις καταστάσεις με τα ονόματα επιβατών (PNR), στις υπηρεσίες μετανάστευσης στον αερολιμένα άφιξης, τα δεδομένα αυτά θα χρησιμοποιηθούν για σκοπούς μεταναστευτικού ελέγχου, οι οποίοι διαφέρουν από τον αρχικό σκοπό συλλογής τους. Επομένως, για τη διαβίβαση των δεδομένων αυτών σε υπηρεσία μετανάστευσης θα απαιτηθεί νέα και χωριστή νομική βάση.

Όταν εξετάζονται το πεδίο και τα όρια συγκεκριμένου σκοπού, η Εκσυγχρονισμένη Σύμβαση 108 και ο Γενικός Κανονισμός για την Προστασία Δεδομένων βασίζονται στην έννοια της συμβατότητας: η χρήση δεδομένων για συμβατούς σκοπούς επιτρέπεται λόγω της αρχικής νομικής βάσης. Ως εκ τούτου, η περαιτέρω επεξεργασία των δεδομένων δεν πρέπει να πραγματοποιείται κατά τρόπο μη αναμενόμενο ή ακατάλληλο ή κατά τρόπο στον οποίο ενδέχεται να

εναντιωθεί το υποκείμενο των δεδομένων ²⁸⁹. Για να αξιολογήσει αν η περαιτέρω επεξεργασία μπορεί να θεωρηθεί συμβατή, ο υπεύθυνος επεξεργασίας θα πρέπει να λάβει υπόψη (μεταξύ άλλων) τα εξής:

- «τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας
- το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους
- τη φύση των δεδομένων προσωπικού χαρακτήρα
- τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων και
- την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας» ²⁹⁰. Αυτό θα μπορούσε να πραγματοποιηθεί, για παράδειγμα, μέσω κρυπτογράφησης ή ψευδωνυμοποίησης.

Παράδειγμα: Η εταιρεία Sunshine αποκτά δεδομένα πελατών στο πλαίσιο της διαχείρισης των σχέσεων με τους πελάτες. Εν συνεχεία διαβιβάζει τα δεδομένα αυτά σε εταιρεία μάρκετινγκ, τη Moonlight, η οποία επιθυμεί να χρησιμοποιήσει τα δεδομένα για να υποστηρίξει τις εκστρατείες μάρκετινγκ τρίτων εταιρειών. Η διαβίβαση δεδομένων από τη Sunshine για σκοπούς μάρκετινγκ άλλων εταιρειών συνιστά μετέπειτα χρήση των δεδομένων για νέο σκοπό, ο οποίος είναι ασύμβατος με τη διαχείριση των σχέσεων με τους πελάτες, τον αρχικό σκοπό για τον οποίο η εταιρεία Sunshine συνέλεξε τα δεδομένα. Επομένως, η διαβίβαση των δεδομένων στην εταιρεία Moonlight απαιτεί χωριστή νομική βάση.

²⁸⁹ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 49.

²⁹⁰ Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 50 και άρθρο 6 παράγραφος 4· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 49.

Αντιθέτως, η χρήση από την εταιρεία Sunshine δεδομένων που προκύπτουν από τη διαχείριση των σχέσεων με τους πελάτες για τους δικούς της σκοπούς μάρκετινγκ, δηλαδή για την αποστολή σχετικών μηνυμάτων στους δικούς της πελάτες για τα δικά της προϊόντα, γίνεται γενικά δεκτή ως συμβατός σκοπός.

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων και την Εκσυγχρονισμένη Σύμβαση 108, η «περαιτέρω επεξεργασία για λόγους αρχι-θέτησης που άπτονται του δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς» θεωρείται εκ των προτέρων συμβατή με τον αρχικό σκοπό ²⁹¹. Ωστόσο, κατά την περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να υπάρχουν κατάλληλες εγγυήσεις, όπως ανωνυμοποίηση, κρυπτογράφηση ή ψευδωνυμοποίηση των δεδομένων ²⁹². Ο Γενικός Κανονισμός για την Προστασία Δεδομένων προσθέτει ότι «[ό]ταν το υποκείμενο των δεδομένων παρέσχε τη συναίνεσή του ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση, ειδικότερα, σημαντικών σκοπών στο πλαίσιο γενικού δημόσιου συμφέροντος, θα πρέπει να επιτρέπεται στον υπεύθυνο επεξεργασίας να προβαίνει στην περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη συμβατότητα των σκοπών» ²⁹³. Επομένως, όταν πραγματοποιείται περαιτέρω επεξεργασία, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται για τους σκοπούς, καθώς και για τα δικαιώματά του, όπως το δικαίωμα εναντίωσης ²⁹⁴.

Παράδειγμα: Η εταιρεία Sunshine συνέλεξε και αποθήκευσε δεδομένα για τους πελάτες της στο πλαίσιο της διαχείρισης των σχέσεων με αυτούς. Η περαιτέρω χρήση των δεδομένων αυτών από την εταιρεία Sunshine για στατιστική ανάλυση της αγοραστικής συμπεριφοράς των πελατών της επιτρέπεται, καθώς η κατάρτιση στατιστικών συνιστά συμβατό σκοπό. Δεν απαιτείται πρόσθετη νομική βάση, όπως η συγκατάθεση των υποκειμένων

291 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο β)-εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο β). Παράδειγμα τέτοιων εθνικών διατάξεων αποτελεί ο αυστριακός νόμος για την προστασία δεδομένων (*Datenschutzgesetz*), Ομοσπονδιακή Επίσημη Εφημερίδα I αριθ. 165/1999, σημείο 46.

292 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 4-Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο β)-Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 50.

293 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 50.

294 Ό.π.

των δεδομένων. Ωστόσο, για την περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα για στατιστικούς σκοπούς η Sunshine πρέπει να παρέχει κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Στα τεχνικά και οργανωτικά μέτρα τα οποία πρέπει να εφαρμόσει η Sunshine μπορεί να περιλαμβάνεται η ψευδωνυμοποίηση.

3.3. Η αρχή της ελαχιστοποίησης των δεδομένων

Κύρια σημεία

- Η επεξεργασία δεδομένων πρέπει να περιορίζεται στο αναγκαίο μέτρο για την εκπλήρωση νόμιμου σκοπού.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να πραγματοποιείται μόνο όταν ο σκοπός της επεξεργασίας δεν μπορεί να επιτευχθεί με άλλα μέσα.
- Η επεξεργασία δεδομένων δεν πρέπει να επεμβαίνει δυσανάλογα στα συμφέροντα, στα δικαιώματα και στις ελευθερίες που διακυβεύονται.

Σε επεξεργασία υποβάλλονται μόνο τα δεδομένα που είναι «κατάλληλα, συναφή και δεν είναι δυσανάλογα σε σχέση με τον σκοπό για τον οποίο συγκεντρώνονται και/ή υφίστανται περαιτέρω επεξεργασία»²⁹⁵. Οι κατηγορίες δεδομένων που επιλέγονται για επεξεργασία πρέπει να είναι αναγκαίες για την επίτευξη του δεδηλωμένου συνολικού σκοπού των πράξεων επεξεργασίας, και ο υπεύθυνος επεξεργασίας θα πρέπει να περιορίζει αυστηρά τη συλλογή δεδομένων σε τέτοιες πληροφορίες οι οποίες είναι άμεσα συναφείς με τον συγκεκριμένο σκοπό που επιδιώκεται με την επεξεργασία.

²⁹⁵ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο γ): Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο γ).

Παράδειγμα: Στην υπόθεση *Digital Rights Ireland*²⁹⁶, το ΔΕΕ εξέτασε το κύρος της οδηγίας για τη διατήρηση δεδομένων, η οποία είχε ως σκοπό την εναρμόνιση των εθνικών διατάξεων για τη διατήρηση δεδομένων προσωπικού χαρακτήρα που παράγονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δικτύων για ενδεχόμενη διαβίβαση σε αρμόδιες αρχές για την καταπολέμηση σοβαρών ποινικών αδικημάτων, όπως οργανωμένο έγκλημα και τρομοκρατία. Ανεξάρτητα από το γεγονός ότι ο στόχος αυτός θεωρήθηκε ότι ανταποκρίνεται πραγματικά σε σκοπό γενικού ενδιαφέροντος, η γενικευμένη διατύπωση με την οποία η οδηγία κάλυπτε «κάθε πρόσωπο και κάθε μέσο ηλεκτρονικής επικοινωνίας, καθώς και το σύνολο των δεδομένων κινήσεως άνευ ουδεμίας διαφοροποιήσεως, περιορισμού ή εξαιρέσεως σε σχέση προς τον σκοπό της καταπολεμήσεως των σοβαρών παραβάσεων», θεωρήθηκε προβληματική²⁹⁷.

Επιπλέον, με τη χρήση ειδικής τεχνολογίας ενίσχυσης της προστασίας της ιδιωτικής ζωής, είναι ενίοτε εφικτό να αποφευχθεί η χρήση δεδομένων προσωπικού χαρακτήρα ή να εφαρμοστούν μέτρα για τη μείωση της ικανότητας σύνδεσης δεδομένων με ένα συγκεκριμένο υποκείμενο δεδομένων (για παράδειγμα, μέσω ψευδωνυμοποίησης), με αποτέλεσμα να επιτυγχάνεται μια λύση που σέβεται την ιδιωτική ζωή, η οποία ενδείκνυται ιδιαίτερα σε πιο εκτεταμένα συστήματα επεξεργασίας.

Παράδειγμα: Δημοτικό συμβούλιο παρέχει έξυπνη κάρτα στους τακτικούς χρήστες του συστήματος δημόσιων μεταφορών της πόλης έναντι ορισμένου τέλους. Το ονοματεπώνυμο του χρήστη αναγράφεται επάνω στην κάρτα και είναι αποθηκευμένο σε ηλεκτρονική μορφή στον μικροεπεξεργαστή. Κάθε φορά που ο χρήστης παίρνει το λεωφορείο ή το τραμ, πρέπει να περνά την έξυπνη κάρτα μπροστά από τις συσκευές ανάγνωσης οι οποίες είναι εγκατεστημένες στα μέσα αυτά. Τα δεδομένα που διαβάζει η συσκευή διασταυρώνονται ηλεκτρονικά με βάση δεδομένων η οποία περιέχει τα ονοματεπώνυμα όλων των προσώπων που έχουν αγοράσει την κάρτα.

296 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [Τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

297 Ό.π., σκέψεις 44 και 57.

Το σύστημα αυτό δεν τηρεί την αρχή της ελαχιστοποίησης των δεδομένων με βέλτιστο τρόπο: ο έλεγχος του αν ένα πρόσωπο δικαιούται να χρησιμοποιεί τα μέσα μεταφοράς θα μπορούσε να πραγματοποιείται χωρίς σύγκριση των δεδομένων προσωπικού χαρακτήρα που περιέχονται στον μικροεπεξεργαστή της κάρτας με εκείνα που περιέχονται σε βάση δεδομένων. Θα αρκούσε, για παράδειγμα, μια ειδική ηλεκτρονική εικόνα, όπως γραμμικός κώδικας, στον μικροεπεξεργαστή της κάρτας ο οποίος, όταν ο χρήστης θα περνούσε την κάρτα μπροστά από τη διάταξη ανάγνωσης, θα επιβεβαίωνε αν η κάρτα είναι σε ισχύ ή όχι. Ένα τέτοιο σύστημα δεν θα κατέγραφε ποιος χρησιμοποίησε ένα συγκεκριμένο μέσο μεταφοράς και πότε. Αυτή θα ήταν η βέλτιστη λύση σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, καθώς η αρχή αυτή συνεπάγεται την υποχρέωση ελαχιστοποίησης της συλλογής δεδομένων.

Το άρθρο 5 παράγραφος 1 της Εκσυγχρονισμένης Σύμβασης 108 περιέχει απαίτηση αναλογικότητας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε σχέση με τον νόμιμο σκοπό που επιδιώκεται. Πρέπει να υφίσταται εύλογη ισορροπία μεταξύ όλων των διακυβευόμενων συμφερόντων σε όλα τα στάδια της επεξεργασίας. Αυτό σημαίνει ότι «[δ]εδομένα προσωπικού χαρακτήρα τα οποία είναι κατάλληλα και συναφή, αλλά συνεπάγονται δυσανάλογη επέμβαση στα θεμελιώδη δικαιώματα και τις ελευθερίες που διακυβεύονται θα πρέπει να θεωρούνται υπερβολικά»²⁹⁸.

3.4. Η αρχή της ακρίβειας των δεδομένων

Κύρια σημεία

- Ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει την αρχή της ακρίβειας των δεδομένων σε όλες τις πράξεις επεξεργασίας.
- Ανακριβή δεδομένα πρέπει να διαγράφονται ή να διορθώνονται χωρίς καθυστέρηση.
- Προκειμένου να διασφαλίζεται η ακρίβειά τους, τα δεδομένα μπορεί να χρειάζονται τακτικό έλεγχο και επικαιροποίηση.

²⁹⁸ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 52· Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο γ).

Υπεύθυνος επεξεργασίας ο οποίος κατέχει προσωπικές πληροφορίες δεν χρησιμοποιεί τις πληροφορίες αυτές αν δεν λάβει μέτρα που να διασφαλίζουν με εύλογη βεβαιότητα ότι τα δεδομένα είναι ακριβή και επικαιροποιημένα ²⁹⁹.

Η υποχρέωση διασφάλισης της ακρίβειας των δεδομένων πρέπει να εξετάζεται υπό το πλαίσιο του σκοπού της επεξεργασίας των δεδομένων.

Παράδειγμα: Στην υπόθεση *Rijkeboer* ³⁰⁰, το ΔΕΕ εξέτασε το αίτημα ολλανδού υπηκόου να λάβει πληροφορίες από τον δήμο του Άμστερνταμ σχετικά με την ταυτότητα των προσώπων στα οποία η τοπική αρχή είχε διαβιβάσει κατά τα δύο προηγούμενα έτη αρχεία που κατείχε και που τον αφορούσαν, καθώς και σχετικά με το περιεχόμενο των κοινοποιηθέντων δεδομένων. Το ΔΕΕ έκρινε ότι το «δικαίωμα στον σεβασμό της ιδιωτικής ζωής προϋποθέτει ότι θα διασφαλίζεται στον ενδιαφερόμενο ότι η επεξεργασία των δεδομένων του προσωπικού χαρακτήρα γίνεται κατά ορθό και νόμιμο τρόπο, δηλαδή ότι, ειδικότερα, τα προσωπικά δεδομένα που τον αφορούν είναι ακριβή και κοινοποιούνται σε αποδέκτες που έχουν προς τούτο δικαίωμα». Στη συνέχεια, το ΔΕΕ παρέπεμπε στο προοίμιο της Οδηγίας για την Προστασία Δεδομένων, στο οποίο επισημαίνεται ότι τα υποκείμενα των δεδομένων πρέπει να έχουν δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν προκειμένου να μπορούν να ελέγχουν αν είναι ακριβή ³⁰¹.

Ενδέχεται επίσης να υπάρχουν περιπτώσεις στις οποίες η επικαιροποίηση αποθηκευμένων δεδομένων απαγορεύεται εκ του νόμου, επειδή ο σκοπός της αποθήκευσης των δεδομένων είναι κυρίως να καταγραφούν ως ιστορικά «στιγμιότυπα».

Παράδειγμα: Ο ιατρικός φάκελος χειρουργικής επέμβασης δεν πρέπει να τροποποιείται, με άλλα λόγια να «επικαιροποιείται», ακόμη και αν αποδειχθεί αργότερα ότι πορίσματα που αναφέρονται στον φάκελο είναι εσφαλμένα. Σε τέτοιες περιπτώσεις, μπορούν να πραγματοποιηθούν

299 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο δ)· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο δ).

300 ΔΕΕ, C-553/07, *College van burgemeester en wethouders van Rotterdam κατά E. E. Rijkeboer*, 7 Μαΐου 2009.

301 Πρώην αιτιολογική σκέψη 41, προοίμιο της οδηγίας 95/46/ΕΚ.

μόνο προσθήκες στις παρατηρήσεις που υπάρχουν στον φάκελο, εφόσον επισημαίνονται σαφώς ως σημεία που προστέθηκαν σε μεταγενέστερο στάδιο.

Από την άλλη πλευρά, υπάρχουν καταστάσεις στις οποίες η επικαιροποίηση και ο τακτικός έλεγχος της ακρίβειας των δεδομένων αποτελεί απόλυτη αναγκαιότητα, λόγω της ζημίας που θα μπορούσε να προκληθεί στο υποκείμενο των δεδομένων εάν τα δεδομένα παρέμεναν ανακριβή.

Παράδειγμα: Όταν ένα πρόσωπο επιθυμεί να συνάψει σύμβαση δανείου με τραπεζικό ίδρυμα, η τράπεζα ελέγχει συνήθως την πιστοληπτική ικανότητα του δυνητικού πελάτη. Για τον σκοπό αυτό, υπάρχουν ειδικές βάσεις δεδομένων οι οποίες περιέχουν στοιχεία για το πιστωτικό ιστορικό φυσικών προσώπων. Εάν μια τέτοια βάση δεδομένων παρέχει ανακριβή ή παρωχημένα στοιχεία για ένα φυσικό πρόσωπο, το γεγονός αυτό μπορεί να έχει αρνητικές συνέπειες για το εν λόγω πρόσωπο. Επομένως, οι υπεύθυνοι επεξεργασίας τέτοιων βάσεων δεδομένων πρέπει να καταβάλλουν ιδιαίτερες προσπάθειες ώστε να τηρούν την αρχή της ακρίβειας των δεδομένων.

3.5. Η αρχή του περιορισμού της περιόδου αποθήκευσης

Κύρια σημεία

- Η αρχή του περιορισμού της περιόδου αποθήκευσης σημαίνει ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγράφονται ή να ανωνυμοποιούνται όταν δεν είναι πλέον αναγκαία για τους σκοπούς για τους οποίους συλλέχθηκαν.

Το άρθρο 5 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ και, ομοίως, το άρθρο 5 παράγραφος 4 στοιχείο ε) της Εκσυγχρονισμένης Σύμβασης 108 προβλέπουν ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να «διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα». Επομένως, τα δεδομένα πρέπει να διαγράφονται ή να

ανωνυμοποιούνται όταν οι σκοποί αυτοί έχουν εκπληρωθεί. Για τον σκοπό αυτό, «ο υπεύθυνος επεξεργασίας θα πρέπει να ορίζει προθεσμίες για τη διαγραφή τους ή για την περιοδική επανεξέτάσή τους» ώστε να διασφαλίζεται ότι τα δεδομένα δεν διατηρούνται περισσότερο από όσο είναι αναγκαίο ³⁰².

Στην υπόθεση *S. και Marper*, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι οι βασικές αρχές της συναφούς νομοθεσίας του Συμβουλίου της Ευρώπης και η εθνική νομοθεσία και πρακτική των λοιπών συμβαλλόμενων κρατών επιβάλλουν να είναι η διατήρηση των δεδομένων ανάλογη του σκοπού για τον οποίο έχουν συλλεχθεί και χρονικά περιορισμένη, ιδίως στον αστυνομικό τομέα ³⁰³.

Παράδειγμα: Στην υπόθεση *S. και Marper* ³⁰⁴, το ΕΔΔΑ αποφάνθηκε ότι η επ' αόριστον διατήρηση των δακτυλικών αποτυπωμάτων, κυτταρικών δειγμάτων και προφίλ DNA των δύο προσφευγόντων ήταν δυσανάλογη και μη αναγκαία σε μια δημοκρατική κοινωνία, δεδομένου ότι οι ποινικές διαδικασίες κατά αμφοτέρων των προσφευγόντων είχαν περατωθεί με αθώωση και παραίτηση, αντίστοιχα.

Ο χρονικός περιορισμός της αποθήκευσης δεδομένων προσωπικού χαρακτήρα εφαρμόζεται μόνο σε δεδομένα που διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων τους. Επομένως, νόμιμη αποθήκευση δεδομένων τα οποία δεν είναι πλέον αναγκαία θα μπορούσε να επιτευχθεί μέσω της ανωνυμοποίησής τους.

Η αρχειοθέτηση δεδομένων για λόγους δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς μπορεί να επιτρέπεται για μεγαλύτερα διαστήματα, εφόσον τα εν λόγω δεδομένα χρησιμοποιηθούν μόνο για τους ανωτέρω σκοπούς ³⁰⁵. Για τη συνεχή αποθήκευση και χρήση δεδομένων προσωπικού χαρακτήρα πρέπει να εφαρμόζονται κατάλληλα

302 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 39.

303 ΕΔΔΑ, *S. και Marper κατά Ηνωμένου Βασιλείου* [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008· βλ. επίσης, για παράδειγμα: ΕΔΔΑ, *M.M. κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 24029/07, 13 Νοεμβρίου 2012.

304 ΕΔΔΑ, *S. και Marper κατά Ηνωμένου Βασιλείου* [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008.

305 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο ε)· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο β) και άρθρο 11 παράγραφος 2.

τεχνικά και οργανωτικά μέτρα, ώστε να διασφαλίζονται τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων.

Στην Εκσυγχρονισμένη Σύμβαση 108 επιτρέπονται επίσης εξαιρέσεις από την αρχή του περιορισμού της περιόδου αποθήκευσης, υπό την προϋπόθεση ότι αυτές προβλέπονται από τον νόμο, σέβονται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και είναι αναγκαίες και ανάλογες για την επιδίωξη περιορισμένου αριθμού θεμιτών σκοπών ³⁰⁶. Σε αυτούς περιλαμβάνονται, μεταξύ άλλων, η προστασία της εθνικής ασφάλειας, η διερεύνηση και δίωξη ποινικών αδικημάτων, η εκτέλεση ποινικών κυρώσεων, η προστασία του υποκειμένου των δεδομένων και η προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών άλλων προσώπων.

Παράδειγμα: Στην υπόθεση *Digital Rights Ireland* ³⁰⁷, το ΔΕΕ έλεγξε το κύρος της οδηγίας για τη διατήρηση δεδομένων, η οποία είχε ως σκοπό την εναρμόνιση των εθνικών διατάξεων για τη διατήρηση δεδομένων προσωπικού χαρακτήρα που παράγονται ή υποβάλλονται σε επεξεργασία στο πλαίσιο διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δικτύων για την καταπολέμηση σοβαρών ποινικών αδικημάτων, όπως το οργανωμένο έγκλημα και η τρομοκρατία. Η οδηγία για τη διατήρηση δεδομένων επέβαλλε περίοδο διατήρησης των δεδομένων «τουλάχιστον έξι μηνών χωρίς να προβαίνει σε οποιαδήποτε διάκριση μεταξύ των κατηγοριών δεδομένων που προβλέπει το άρθρο 5 της εν λόγω αναλόγως της ενδεχόμενης χρησιμότητάς τους για τον επιδιωκόμενο σκοπό ή των θιγομένων προσώπων» ³⁰⁸. Το ΔΕΕ επισήμανε επίσης το πρόβλημα της απουσίας από την οδηγία για τη διατήρηση δεδομένων αντικειμενικών κριτηρίων, βάσει των οποίων πρέπει να καθορίζεται η ακριβής περίοδος διατήρησης των δεδομένων –η οποία μπορεί να κυμαίνεται από ελάχιστο διάστημα έξι μηνών ως μέγιστο διάστημα 24 μηνών– ώστε να διασφαλίζεται ότι η περίοδος διατήρησης θα περιορίζεται στον απολύτως αναγκαίο βαθμό ³⁰⁹.

306 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 11.1· Απιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημεία 91-98.

307 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [Τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

308 Ό.π., σκέψη 63.

309 Ό.π., σκέψη 64.

3.6. Η αρχή της ασφάλειας των δεδομένων

Κύρια σημεία

- Η ασφάλεια και η εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα είναι καθοριστικές για την αποφυγή αρνητικών συνεπειών για το υποκείμενο των δεδομένων.
- Τα μέτρα ασφάλειας μπορούν να είναι τεχνικής και/ή οργανωτικής φύσης.
- Η ψευδωνυμοποίηση είναι μια διαδικασία η οποία μπορεί να προστατεύσει τα δεδομένα προσωπικού χαρακτήρα.
- Η καταλληλότητα των μέτρων ασφάλειας πρέπει να καθορίζεται κατά περίπτωση και να επανεξετάζεται τακτικά.

Η αρχή της ασφάλειας των δεδομένων επιβάλλει να εφαρμόζονται κατάλληλα τεχνικά ή οργανωτικά μέτρα κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα για προστασία κατά τυχαίας, μη εξουσιοδοτημένης ή παράνομης πρόσβασης, χρήσης, τροποποίησης, κοινολόγησης, απώλειας, καταστροφής ή φθοράς³¹⁰. Σύμφωνα με τον ΓΚΠΔ, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία θα πρέπει να λαμβάνουν υπόψη «τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» όταν εφαρμόζουν τέτοια μέτρα³¹¹. Ανάλογα με τις ειδικές συνθήκες κάθε περίπτωσης, τα κατάλληλα τεχνικά και οργανωτικά μέτρα θα μπορούσαν να περιλαμβάνουν, για παράδειγμα, ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα και/ή τακτική δοκιμή και αξιολόγηση της αποτελεσματικότητας των μέτρων ώστε να διασφαλίζεται η ασφάλεια της επεξεργασίας δεδομένων³¹².

Όπως εξηγείται στην [ενότητα 2.1.1](#), ψευδωνυμοποίηση δεδομένων σημαίνει αντικατάσταση των χαρακτηριστικών στα δεδομένα προσωπικού χαρακτήρα – τα οποία καθιστούν εφικτή την ταυτοποίηση του υποκειμένου των δεδομένων – με ψευδώνυμο και τη διατήρηση των εν λόγω χαρακτηριστικών χωριστά, με τη

³¹⁰ Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 39 και άρθρο 5 παράγραφος 1 στοιχείο στ). Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7.

³¹¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 32 παράγραφος 1.

³¹² Ό.π.

χρήση τεχνικών ή οργανωτικών μέτρων. Η διαδικασία της ψευδωνυμοποίησης δεν πρέπει να συγχέεται με τη διαδικασία της ανωνυμοποίησης, στην οποία όλοι οι σύνδεσμοι που καθιστούν εφικτή την ταυτοποίηση του προσώπου έχουν διαρρηχθεί.

Παράδειγμα: Η πρόταση «Ο Charles Spencer, ο οποίος γεννήθηκε στις 3 Απριλίου 1967, είναι πατέρας τεσσάρων παιδιών, δύο αγοριών και δύο κοριτσιών» μπορεί, για παράδειγμα, να ψευδωνυμοποιηθεί ως εξής:

«Ο C.S. 1967 είναι πατέρας τεσσάρων παιδιών, δύο αγοριών και δύο κοριτσιών»· ή

«Ο 324 είναι πατέρας τεσσάρων παιδιών, δύο αγοριών και δύο κοριτσιών»· ή

«Ο YESz320I είναι πατέρας τεσσάρων παιδιών, δύο αγοριών και δύο κοριτσιών».

Οι χρήστες που έχουν πρόσβαση σε ψευδωνυμοποιημένα δεδομένα δεν έχουν συνήθως την ικανότητα να εξακριβώσουν την ταυτότητα του «Charles Spencer, ο οποίος γεννήθηκε στις 3 Απριλίου 1967» από τα στοιχεία «324» ή «YESz320I». Επομένως, τα δεδομένα αυτά είναι κατά κανόνα ασφαλέστερα έναντι ενδεχόμενης κατάχρησης.

Ωστόσο, τα δεδομένα στο πρώτο παράδειγμα είναι λιγότερο ασφαλή. Εάν η πρόταση «Ο C.S. 1967 είναι πατέρας τεσσάρων παιδιών, δύο αγοριών και δύο κοριτσιών» χρησιμοποιηθεί εντός του μικρού χωριού στο οποίο μένει ο Charles Spencer, τότε ο κ. Spencer μπορεί εύκολα να αναγνωριστεί. Η μέθοδος που χρησιμοποιείται για την ψευδωνυμοποίηση μπορεί να επηρεάσει την αποτελεσματικότητα της προστασίας δεδομένων.

Δεδομένα προσωπικού χαρακτήρα με κρυπτογραφημένα χαρακτηριστικά ή χαρακτηριστικά που τηρούνται χωριστά χρησιμοποιούνται σε πολλά πλαίσια ως τρόπος διαφύλαξης του απορρήτου της προσωπικής ταυτότητας. Η μέθοδος αυτή είναι ιδιαίτερα χρήσιμη όταν οι υπεύθυνοι επεξεργασίας πρέπει να διασφαλίσουν ότι πρόκειται για το ίδιο υποκείμενο δεδομένων, αλλά δεν χρειάζονται ή απαγορεύεται να γνωρίζουν την πραγματική ταυτότητα του υποκειμένου των δεδομένων. Αυτό συμβαίνει, για παράδειγμα, όταν ένας ερευνητής μελετά την εξέλιξη μιας νόσου σε ασθενείς, των οποίων η ταυτότητα είναι γνωστή μόνο

στο νοσοκομείο στο οποίο υποβάλλονται σε θεραπεία και από το οποίο ο ερευνητής αποκτά τα ψευδωνυμοποιημένα ιστορικά των περιπτώσεων. Επομένως, η ψευδωνυμοποίηση είναι ένα ισχυρό όπλο στο οπλοστάσιο της τεχνολογίας για την ενίσχυση της προστασίας της ιδιωτικής ζωής. Μπορεί να αποτελέσει σημαντικό στοιχείο κατά την εφαρμογή της προστασίας της ιδιωτικής ζωής ήδη από τον σχεδιασμό. Αυτό σημαίνει την ενσωμάτωση της προστασίας δεδομένων στο εσωτερικό των συστημάτων επεξεργασίας τους.

Το άρθρο 25 του ΓΚΠΔ, στο οποίο εξετάζεται η προστασία των δεδομένων ήδη από τον σχεδιασμό, αναφέρεται ρητά στην ψευδωνυμοποίηση ως παράδειγμα κατάλληλου τεχνικού και οργανωτικού μέτρου το οποίο θα πρέπει να εφαρμόζουν οι υπεύθυνοι επεξεργασίας για την τήρηση των αρχών της προστασίας δεδομένων και την ενσωμάτωση των απαραίτητων εγγυήσεων. Με τον τρόπο αυτό, οι υπεύθυνοι επεξεργασίας θα ανταποκρίνονται στις απαιτήσεις του κανονισμού και θα προστατεύουν τα δικαιώματα των υποκειμένων των δεδομένων όταν προβαίνουν σε επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν.

Η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης μπορεί να συμβάλει στην απόδειξη της συμμόρφωσης προς την απαίτηση της ασφάλειας της επεξεργασίας³¹³. Στη Γνώμη του σχετικά με τις συνέπειες, για την προστασία των δεδομένων, της επεξεργασίας των καταστάσεων με τα ονόματα επιβατών, το Συμβούλιο της Ευρώπης παρέχει και άλλα παραδείγματα κατάλληλων μέτρων ασφάλειας για την προστασία των δεδομένων προσωπικού χαρακτήρα σε συστήματα καταστάσεων επιβατών. Τέτοια μέτρα ασφάλειας είναι, για παράδειγμα, η τήρηση των δεδομένων σε ασφαλές φυσικό περιβάλλον, ο περιορισμός της πρόσβασης με αλληπάλληλες συνδέσεις και η προστασία της κοινοποίησης δεδομένων με ισχυρή κρυπτογράφηση³¹⁴.

Παράδειγμα: Οι ιστότοποι κοινωνικής δικτύωσης και οι φορείς παροχής ηλεκτρονικού ταχυδρομείου προσφέρουν στους χρήστες τη δυνατότητα να προσθέσουν ένα επιπλέον επίπεδο ασφάλειας δεδομένων στις υπηρεσίες που παρέχουν μέσω της καθιέρωσης της επαλήθευσης της ταυτότητας

313 Ό.π., άρθρο 32 παράγραφος 3.

314 Συμβούλιο της Ευρώπης, Επιτροπή της Σύμβασης 108, Γνώμη για τις επιπτώσεις της επεξεργασίας των ονομαστικών καταστάσεων επιβατών στην προστασία δεδομένων (*Opinion on the Data protection implications of the processing of Passenger Name Records*), T-PD(2016)18rev, 19 Αυγούστου 2016, σ. 9.

σε δύο επίπεδα. Επιπροσθέτως της καταχώρισης προσωπικού κωδικού, οι χρήστες πρέπει να εκτελούν δεύτερη διαδικασία σύνδεσης για να αποκτήσουν πρόσβαση στον προσωπικό λογαριασμό τους. Η δεύτερη αυτή διαδικασία μπορεί, για παράδειγμα, να συνίσταται στην καταχώριση κωδικού ασφάλειας ο οποίος αποστέλλεται στον αριθμό κινητού τηλεφώνου που συνδέεται με τον προσωπικό λογαριασμό. Με τον τρόπο αυτό, η επαλήθευση σε δύο στάδια παρέχει μεγαλύτερη προστασία των προσωπικών πληροφοριών κατά της μη εξουσιοδοτημένης πρόσβασης σε προσωπικούς λογαριασμούς μέσω δικτυοπαράβιασης.

Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 παρέχονται πρόσθετα παραδείγματα κατάλληλων εγγυήσεων, όπως η υποχρέωση επαγγελματικού απορρήτου ή η λήψη ειδικών μέτρων ασφάλειας, όπως η κρυπτογράφηση δεδομένων ³¹⁵. Όταν εφαρμόζει συγκεκριμένα μέτρα ασφάλειας, ο υπεύθυνος επεξεργασίας –ή, κατά περίπτωση, ο εκτελών την επεξεργασία– θα πρέπει να λαμβάνει υπόψη διάφορα στοιχεία, όπως τη φύση και τον όγκο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, τις δυνητικές αρνητικές συνέπειες για τα υποκείμενα των δεδομένων και την αναγκαιότητα περιορισμένης πρόσβασης στα δεδομένα ³¹⁶. Η εξέλιξη της τεχνολογίας όσον αφορά τις μεθόδους και τις τεχνικές ασφάλειας δεδομένων για την επεξεργασία δεδομένων πρέπει να λαμβάνεται υπόψη όταν εφαρμόζονται κατάλληλα μέτρα ασφάλειας. Το κόστος των μέτρων αυτών πρέπει να είναι ανάλογο της σοβαρότητας και της πιθανότητας εμφάνισης κινδύνων. Τα μέτρα ασφάλειας πρέπει να επανεξετάζονται τακτικά ώστε να μπορούν να επικαιροποιούνται, όπου απαιτείται ³¹⁷.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, τόσο η Εκσυγχρονισμένη Σύμβαση 108 όσο και ο ΓΚΠΔ επιβάλλουν στον υπεύθυνο επεξεργασίας να γνωστοποιεί αμελλητί στην αρμόδια εποπτική αρχή την παραβίαση και τους σχετικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων ³¹⁸. Παρόμοια υποχρέωση ανακοίνωσης στο υποκείμενο των δεδομένων υφίσταται όταν η παραβίαση των δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες του ³¹⁹. Για την ανακοίνωση τέτοιων παραβιάσεων στα υποκείμενα των δεδο-

³¹⁵ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 56.

³¹⁶ Ό.π., σκέψη 62.

³¹⁷ Ό.π., σκέψη 63.

³¹⁸ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 2· Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 33 παράγραφος 1.

³¹⁹ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 2· Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 34 παράγραφος 1.

μένων πρέπει να χρησιμοποιείται σαφής και απλή γλώσσα ³²⁰. Εάν ο εκτελών την επεξεργασία αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα, οφείλει να ενημερώσει αμελλητί τον υπεύθυνο επεξεργασίας ³²¹. Σε ορισμένες περιπτώσεις, ενδέχεται να ισχύουν εξαιρέσεις στην υποχρέωση γνωστοποίησης. Για παράδειγμα, ο υπεύθυνος επεξεργασίας δεν υποχρεούται να ενημερώσει την εποπτική αρχή όταν «η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» ³²². Επίσης, δεν είναι αναγκαία η ενημέρωση του υποκειμένου των δεδομένων όταν τα εφαρμοσθέντα μέτρα ασφάλειας καθιστούν αδύνατη την κατανόηση των δεδομένων από μη εξουσιοδοτημένα πρόσωπα ή όταν επακόλουθα μέτρα διασφαλίζουν ότι δεν είναι πλέον πιθανό να εμφανιστεί ο προαναφερόμενος υψηλός κίνδυνος ³²³. Εάν για την ανακοίνωση στα υποκείμενα των δεδομένων της παραβίασης των δεδομένων προσωπικού χαρακτήρα που τα αφορούν απαιτείται δυσανάλογη προσπάθεια εκ μέρους του υπευθύνου επεξεργασίας, μια δημόσια ανακοίνωση ή ένα παρόμοιο μέτρο μπορεί να διασφαλίσει ότι «τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο» ³²⁴.

3.7. Η αρχή της λογοδοσίας

Κύρια σημεία

- Η λογοδοσία επιβάλλει σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία να εφαρμόζουν, ενεργώς και αδιάλειπτα, μέτρα για την προώθηση και τη διασφάλιση της προστασίας των δεδομένων στις δραστηριότητες επεξεργασίας.
- Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία είναι υπεύθυνοι για τη συμμόρφωση των πράξεων επεξεργασίας προς το δίκαιο για την προστασία των δεδομένων και τις αντίστοιχες υποχρεώσεις τους.
- Οι υπεύθυνοι επεξεργασίας πρέπει να είναι σε θέση να αποδεικνύουν ανά πάσα στιγμή τη συμμόρφωση προς τις διατάξεις περί προστασίας των δεδομένων στα υποκείμενα των δεδομένων, στο ευρύ κοινό και στις εποπτικές αρχές. Οι εκτελούντες την επεξεργασία οφείλουν επίσης να συμμορφώνονται προς ορισμένες υποχρεώσεις οι οποίες συνδέονται αυστηρά με τη λογοδοσία (όπως τήρηση αρχείου πράξεων επεξεργασίας και διορισμός υπευθύνου προστασίας δεδομένων).

320 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 34 παράγραφος 2.

321 Ό.π., άρθρο 33 παράγραφος 1.

322 Ό.π.

323 Ό.π., άρθρο 34 παράγραφος 3 στοιχεία α) και β).

324 Ό.π., άρθρο 34 παράγραφος 3 στοιχείο γ).

Στον ΓΚΠΔ και στην Εκσυγχρονισμένη Σύμβαση 108 προβλέπεται ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση προς τις αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα και οι οποίες περιγράφονται στο παρόν κεφάλαιο ³²⁵. Για τον σκοπό αυτό, ο υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα ³²⁶. Παρότι η αρχή της λογοδοσίας που προβλέπεται στο άρθρο 5 παράγραφος 2 του ΓΚΠΔ απευθύνεται μόνο στους υπευθύνους επεξεργασίας, οι εκτελούντες την επεξεργασία αναμένεται επίσης να είναι υπόλογοι, δεδομένου ότι οφείλουν να συμμορφώνονται προς διάφορες υποχρεώσεις και συνδέονται στενά με την ευθύνη λογοδοσίας.

Στη νομοθεσία της ΕΕ και του Συμβουλίου της Ευρώπης για την προστασία των δεδομένων προβλέπεται επίσης ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να διασφαλίζει τη συμμόρφωση προς τις αρχές που διέπουν την προστασία των δεδομένων και εξετάζονται στις [ενότητες 3.1 έως 3.6](#) ³²⁷. Η Ομάδα εργασίας του άρθρου 29 επισημαίνει ότι «ο τύπος των διαδικασιών και των μηχανισμών θα διαφέρει ανάλογα με τους κινδύνους που ενέχει η επεξεργασία και με τη φύση των δεδομένων» ³²⁸.

Οι υπεύθυνοι επεξεργασίας μπορούν να διευκολύνουν τη συμμόρφωση προς την απαίτηση αυτή με διάφορους τρόπους, συμπεριλαμβανομένων των ακόλουθων:

- καταχώριση των δραστηριοτήτων επεξεργασίας και διάθεση αυτών στην εποπτική αρχή, κατόπιν αιτήματός της ³²⁹.
- σε ορισμένες περιπτώσεις, ορισμός υπευθύνου προστασίας δεδομένων, ο οποίος εμπλέκεται σε όλα τα θέματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα ³³⁰.

325 Ό.π., άρθρο 5 παράγραφος 2· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 1.

326 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 24.

327 Ό.π., άρθρο 5 παράγραφος 2· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 1.

328 Ομάδα εργασίας του άρθρου 29, *Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας*, WP 173, Βρυξέλλες, 13 Ιουλίου 2010, σκέψη 12.

329 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 30.

330 Ό.π., άρθρα 37-39.

- πραγματοποίηση εκτιμήσεων αντικτύπου σχετικά με την προστασία δεδομένων για τύπους επεξεργασίας οι οποίοι είναι πιθανό να συνεπάγονται υψηλό κίνδυνο για τα δικαιώματα και τις υποχρεώσεις φυσικών προσώπων ³³¹.
- διασφάλιση της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξορισμού ³³².
- εφαρμογή ρυθμίσεων και διαδικασιών για την άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων ³³³.
- τήρηση εγκεκριμένου κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης ³³⁴.

Παρότι η αρχή της λογοδοσίας που προβλέπεται στο άρθρο 5 παράγραφος 2 του ΓΚΠΔ δεν αφορά ειδικώς τους εκτελούντες την επεξεργασία, υπάρχουν διατάξεις οι οποίες συνδέονται με τη λογοδοσία και περιλαμβάνουν επίσης υποχρεώσεις γι' αυτούς, όπως η τήρηση αρχείου των δραστηριοτήτων επεξεργασίας και ο διορισμός υπευθύνου προστασίας δεδομένων για κάθε δραστηριότητα επεξεργασίας για την οποία απαιτείται ο εν λόγω υπεύθυνος ³³⁵. Οι εκτελούντες την επεξεργασία πρέπει να διασφαλίζουν επίσης την εφαρμογή όλων των αναγκαίων μέτρων που εγγυώνται την ασφάλεια των δεδομένων ³³⁶. Η νομικά δεσμευτική σύμβαση μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία πρέπει να προβλέπει ότι ο εκτελών την επεξεργασία θα συνδράμει τον υπεύθυνο επεξεργασίας σε ορισμένες απαιτήσεις συμμόρφωσης, π.χ. όταν διενεργεί εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων ή ενημερώνει τον υπεύθυνο της επεξεργασίας για τυχόν παραβίαση των δεδομένων προσωπικού χαρακτήρα την οποία έχει αντιληφθεί ³³⁷.

Το 2013 ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) εξέδωσε κατευθυντήριες γραμμές για την προστασία της ιδιωτικής ζωής, στις οποίες τονίζεται ότι οι υπεύθυνοι επεξεργασίας έχουν σημαντικό ρόλο στην πρακτική εφαρμογή της προστασίας των δεδομένων. Στις κατευθυντήριες γραμμές εμπεριέχεται

331 Ό.π., άρθρο 35· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 2.

332 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 25. Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 2 και 3.

333 Ό.π., άρθρο 12 και άρθρο 24.

334 Ό.π., άρθρο 40 και άρθρο 42.

335 Ό.π., άρθρο 5 παράγραφος 2 και άρθρα 30 και 37.

336 Ό.π., άρθρο 28 παράγραφος 3 στοιχείο γ).

337 Ό.π., άρθρο 28 παράγραφος 3 στοιχείο δ).

η αρχή της λογοδοσίας, σύμφωνα με την οποία «ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να είναι υπόλογος για τη συμμόρφωση προς μέτρα που υλοποιούν τις προαναφερθείσες [ουσιώδεις] αρχές»³³⁸.

Παράδειγμα: Νομοθετικό παράδειγμα στο οποίο δίνεται έμφαση στην αρχή της λογοδοσίας είναι η τροποποίηση³³⁹ το 2009 της οδηγίας 2002/58/EK για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Σύμφωνα με το άρθρο 4, όπως τροποποιήθηκε, η οδηγία επιβάλλει τη λήψη μέτρων που «διασφαλίζουν την εφαρμογή πολιτικής ασφάλειας σε σχέση με την επεξεργασία προσωπικών δεδομένων». Επομένως, όσον αφορά τις διατάξεις περί ασφάλειας της συγκεκριμένης οδηγίας, ο νομοθέτης έκρινε ότι ήταν αναγκαίο να προβλέψει ρητή απαίτηση θέσπισης και εφαρμογής πολιτικής ασφάλειας.

Σύμφωνα με τη γνώμη της Ομάδας εργασίας του άρθρου 29³⁴⁰, η λογοδοσία συνίσταται ουσιαστικά στην υποχρέωση του υπευθύνου επεξεργασίας:

- να θεσπίζει μέτρα τα οποία –υπό κανονικές συνθήκες– θα διασφαλίζουν την τήρηση των κανόνων προστασίας δεδομένων στο πλαίσιο των πράξεων επεξεργασίας και
- να διαθέτει τεκμηρίωση που να αποδεικνύει στα υποκείμενα των δεδομένων και στις εποπτικές αρχές τη λήψη μέτρων για την επίτευξη συμμόρφωσης προς τους κανόνες περί προστασίας δεδομένων.

Επομένως, η αρχή της λογοδοσίας επιβάλλει στους υπευθύνους επεξεργασίας να αποδεικνύουν ενεργά τη συμμόρφωση και όχι να αναμένουν απλώς από τα υποκείμενα των δεδομένων ή τις εποπτικές αρχές να επισημάνουν αδυναμίες.

338 ΟΟΣΑ (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, σημείο 14.

339 *Οδηγία 2009/136/EK* του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/EK για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/EK σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (ΕΕ L 337 της 18.12.2009, σ. 11).

340 Ομάδα εργασίας του άρθρου 29, *Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας*, WP 173, Βρυξέλλες, 13 Ιουλίου 2010.

4

Κανόνες του ευρωπαϊκού δικαίου για την προστασία δεδομένων

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Κανόνες περί νόμιμης επεξεργασίας δεδομένων		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο α) ΔΕΕ, C-543/09, <i>Deutsche Telekom AG κατά Bundesrepublik Deutschland</i> , 2011 ΔΕΕ, C-536/15, <i>Tele2 (Netherlands) BV κ.λπ. κατά Autoriteit Consument en Markt (ACM)</i> , 2017	Συγκατάθεση	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 3 παράγραφος 4 στοιχείο β) και άρθρο 3 παράγραφος 6 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 2
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο β)	(Προ)συμβατική σχέση	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 3 παράγραφος 4 στοιχείο β)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο γ)	Έννομες υποχρεώσεις του υπευθύνου επεξεργασίας	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 3 παράγραφος 4 στοιχείο α)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο δ)	Ζωτικά συμφέροντα του υποκειμένου των δεδομένων	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 3 παράγραφος 4 στοιχείο β)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο ε) ΔΕΕ, C-524/06, <i>Heinz Huber κατά Bundesrepublik Deutschland</i> [τμήμα μείζονος συνθέσεως], 2008	Δημόσιο συμφέρον και άσκηση δημόσιας εξουσίας	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 3 παράγραφος 4 στοιχείο β)

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο στ) <i>ΔΕΕ, C-13/16, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde κατά Rīgas pašvaldības SIA «Rīgas satiksme», 2017</i> <i>ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado, 2011</i>	Έννομα συμφέροντα τρίτων	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 3 παράγραφος 4 στοιχείο β) <i>ΕΔΔΑ, Υ κατά Τουρκίας, προσφυγή αριθ. 648/10, 2015</i>
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 4	Εξαίρεση από την αρχή του περιορισμού του σκοπού: περαιτέρω επεξεργασία για άλλους σκοπούς	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 στοιχείο β)
Κανόνες περί νόμιμης επεξεργασίας ευαίσθητων δεδομένων		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 1	Γενική απαγόρευση επεξεργασίας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 6
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2	Εξαιρέσεις από τη γενική απαγόρευση	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 6
Κανόνες περί ασφαλούς επεξεργασίας		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 32	Υποχρέωση διασφάλισης ασφαλούς επεξεργασίας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 1 <i>ΕΔΔΑ, Ι κατά Φινλανδίας, προσφυγή αριθ. 20511/03, 2008</i>
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 28 και άρθρο 32 παράγραφος 1 στοιχείο β)	Υποχρέωση εμπιστευτικότητας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 1
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 34 Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, άρθρο 4 παράγραφος 2	Γνωστοποιήσεις παραβιάσεων δεδομένων	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 2

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Κανόνες περί λογοδοσίας και προώθησης της συμμόρφωσης		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 12, 13 και 14	Διαφάνεια εν γένει	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 37, 38 και 39	Υπεύθυνοι προστασίας δεδομένων	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 1
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 30	Αρχεία των δραστηριοτήτων επεξεργασίας	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 35 και 36	Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 2
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 33 και 34	Γνωστοποιήσεις παραβιάσεων δεδομένων	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 2
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 40 και 41	Κώδικες δεοντολογίας	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 42 και 43	Πιστοποίηση	
Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 25 παράγραφος 1	Προστασία των δεδομένων ήδη από τον σχεδιασμό	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 2
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 25 παράγραφος 2	Προστασία δεδομένων εξ ορισμού	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 3

Οι αρχές έχουν κατ' ανάγκη γενικό χαρακτήρα. Η εφαρμογή τους σε συγκεκριμένες καταστάσεις συνοδεύεται από έναν βαθμό διακριτικής ευχέρειας όσον αφορά την ερμηνεία και την επιλογή μέσων. Βάσει του **δικαίου του Συμβουλίου της Ευρώπης**, εναπόκειται στους συμβαλλομένους στην Εκσυγχρονισμένη Σύμβαση 108 να διευκρινίσουν αυτή τη διακριτική ευχέρεια όσον αφορά την ερμηνεία στο εθνικό τους δίκαιο. Η κατάσταση στο **δίκαιο της ΕΕ** είναι διαφορετική: για την καθιέρωση της προστασίας δεδομένων στην εσωτερική αγορά, κρίθηκε αναγκαίο να θεσπιστούν πιο λεπτομερείς κανόνες σε επίπεδο ΕΕ για την εναρμόνιση του επιπέδου προστασίας των δεδομένων των εθνικών νομοθεσιών των κρατών μελών. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων θεσπίζει, βάσει των αρχών που προβλέπονται στο άρθρο 5, ένα επίπεδο λεπτομερών κανόνων, οι

οποίοι είναι άμεσα εφαρμοστέοι στην εθνική έννομη τάξη. Επομένως, οι παρατηρήσεις που ακολουθούν σχετικά με τους λεπτομερείς κανόνες περί προστασίας των δεδομένων σε ευρωπαϊκό επίπεδο αφορούν κυρίως το δίκαιο της ΕΕ.

4.1. Κανόνες περί νόμιμης επεξεργασίας

Κύρια σημεία

- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να είναι νόμιμη εάν πληροί ένα από τα ακόλουθα κριτήρια:
 - η επεξεργασία γίνεται με τη συγκατάθεση του υποκειμένου των δεδομένων·
 - η επεξεργασία δεδομένων προσωπικού χαρακτήρα απαιτείται βάσει συμβατικής σχέσης·
 - η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας·
 - η επεξεργασία δεδομένων προσωπικού χαρακτήρα απαιτείται λόγω ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου·
 - η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον·
 - η επεξεργασία υπαγορεύεται από τα έννομα συμφέροντα των υπευθύνων επεξεργασίας ή τρίτων, εκτός εάν υπερισχύει έναντι των συμφερόντων αυτών το συμφέρον ή τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων.
- Η νόμιμη επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα διέπεται από ειδικό, αυστηρότερο καθεστώς.

4.1.1. Νόμιμοι λόγοι επεξεργασίας δεδομένων

Το κεφάλαιο II του Γενικού Κανονισμού για την Προστασία Δεδομένων, με τίτλο «Αρχές», προβλέπει ότι κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνεται, πρώτον, προς τις αρχές που σχετίζονται με την ποιότητα των δεδομένων και προβλέπονται στο άρθρο 5 του ΓΚΠΔ. Σύμφωνα με μία από τις αρχές αυτές, τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να «υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο». Δεύτερον, προκειμένου να είναι η επεξεργασία σύννομη, πρέπει να βασίζεται σε έναν από τους νόμιμους λόγους που καθιστούν θεμιτή την επεξεργασία δεδομένων,

οι οποίοι απαριθμούνται στο άρθρο 6³⁴¹ για τα μη ευαίσθητα δεδομένα προσωπικού χαρακτήρα και στο άρθρο 9 για τις ειδικές κατηγορίες δεδομένων (ή ευαίσθητα δεδομένα). Ομοίως, στο κεφάλαιο II της Εκσυγχρονισμένης Σύμβασης 108, στο οποίο καθορίζονται οι «βασικές αρχές για την προστασία των δεδομένων προσωπικού χαρακτήρα», προβλέπεται ότι, προκειμένου να είναι σύννομη, η επεξεργασία δεδομένων πρέπει να είναι «ανάλογη σε σχέση με τον επιδιωκόμενο θεμιτό σκοπό».

Ανεξάρτητα από τον νόμιμο λόγο επεξεργασίας δεδομένων στον οποίο βασίζεται ο υπεύθυνος επεξεργασίας για την επεξεργασία δεδομένων, θα πρέπει επίσης να εφαρμόζει τις εγγυήσεις που προβλέπονται στο γενικό νομικό καθεστώς για την προστασία δεδομένων.

Συγκατάθεση

Στο δίκαιο του Συμβουλίου της Ευρώπης, η συγκατάθεση αναφέρεται στο άρθρο 5 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108. Αναφέρεται επίσης στη νομολογία του ΕΔΔΑ και σε διάφορες συστάσεις του Συμβουλίου της Ευρώπης³⁴². **Στο δίκαιο της ΕΕ**, η συγκατάθεση, ως βάση για τη σύννομη επεξεργασία δεδομένων, προβλέπεται σαφώς στο άρθρο 6 του ΓΚΠΔ και μνημονεύεται επίσης ρητώς στο άρθρο 8 του Χάρτη. Τα χαρακτηριστικά της έγκυρης συγκατάθεσης επεξηγούνται στον ορισμό της συγκατάθεσης στο άρθρο 4, ενώ οι προϋποθέσεις εξασφάλισης έγκυρης συγκατάθεσης αναλύονται στο άρθρο 7, και οι ειδικοί κανόνες για τη συγκατάθεση παιδιού σε σχέση με τις υπηρεσίες της κοινωνίας των πληροφοριών προβλέπονται στο άρθρο 8 του ΓΚΠΔ.

Όπως επεξηγείται στην [ενότητα 2.4](#), η συγκατάθεση πρέπει να είναι ελεύθερη, εν πλήρει επιγνώσει, συγκεκριμένη και αδιαμφισβήτητη. Η συγκατάθεση πρέπει να είναι δήλωση ή σαφής θετική ενέργεια με την οποία δηλώνεται συμφωνία

341 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-465/00, C-138/01 και C-139/01, *Rechnungshof κατά Österreichischer Rundfunk κ.λπ.* και *Christa Neukomm και Joseph Lauerermann κατά Österreichischer Rundfunk*, 20 Μαΐου 2003, σκέψη 65· ΔΕΕ, C-524/06, *Heinz Huber κατά Bundesrepublik Deutschland* [τμήμα μειζονος συνθέσεως], 16 Δεκεμβρίου 2008, σκέψη 48· ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado*, 24 Νοεμβρίου 2011, σκέψη 26.

342 Βλ., για παράδειγμα, Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2010), Σύσταση CM/Rec (2010)13 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την προστασία των φυσικών προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της κατάρτισης προφίλ (σύσταση σχετικά με την κατάρτιση προφίλ), 23 Νοεμβρίου 2010, άρθρο 3 παράγραφος 4 στοιχείο β).

στην επεξεργασία, το δε πρόσωπο δικαιούται να ανακαλέσει ανά πάσα στιγμή τη συγκατάθεσή του. Οι υπεύθυνοι επεξεργασίας οφείλουν να τηρούν επαληθεύσιμο αρχείο της συγκατάθεσης.

Ελεύθερη συγκατάθεση

Στο πλαίσιο της Εκσυγχρονισμένης Σύμβασης 108 του **Συμβουλίου της Ευρώπης**, η συγκατάθεση του υποκειμένου των δεδομένων πρέπει «να δηλώνει την ελεύθερη έκφραση εκούσιας επιλογής»³⁴³. Ελεύθερη συγκατάθεση υπάρχει μόνο «εάν το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι σε θέση να έχει πραγματική επιλογή και δεν υπάρχει κίνδυνος εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν δώσει τη συγκατάθεσή του»³⁴⁴. Συναφώς, το **δίκαιο της ΕΕ** προβλέπει ότι η συγκατάθεση δεν θεωρείται ότι δόθηκε ελεύθερα «αν το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί»³⁴⁵. Στον ΓΚΠΔ τονίζεται ότι «[κ]ατά την εκτίμηση κατά πόσο η συγκατάθεση δίνεται ελεύθερα, λαμβάνεται ιδιαίτερως υπόψη κατά πόσο, μεταξύ άλλων, για την εκτέλεση σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, τίθεται ως προϋπόθεση η συγκατάθεση στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που δεν είναι αναγκαία για την εκτέλεση της εν λόγω σύμβασης»³⁴⁶. Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται ότι «[δ]εν επιτρέπεται να ασκείται, άμεση ή έμμεση, αδικαιολόγητη επιρροή ή πίεση (η οποία μπορεί να είναι οικονομικού ή άλλου χαρακτήρα) στο υποκείμενο των δεδομένων, και η συγκατάθεση δεν θα πρέπει να θεωρείται ότι παρέχεται ελεύθερα όταν το υποκείμενο των δεδομένων δεν έχει πραγματική επιλογή ή δεν είναι σε θέση να αρνηθεί ή να ανακαλέσει τη συγκατάθεση χωρίς να ζημιωθεί»³⁴⁷.

Παράδειγμα: Κάποιοι δήμοι στο κράτος Α αποφάσισαν να καθιερώσουν κάρτες διαμονής με ενσωματωμένο μικροεπεξεργαστή. Η απόκτηση των ηλεκτρονικών αυτών καρτών δεν είναι υποχρεωτική για τους κατοίκους. Ωστόσο, οι κάτοικοι οι οποίοι δεν διαθέτουν την κάρτα δεν έχουν πρόσβαση

343 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 42.

344 Βλ. επίσης Ομάδα εργασίας του άρθρου 29 (2011), *Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης*, WP 187, 13 Ιουλίου 2011, σ. 12.

345 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 42.

346 Ό.π., άρθρο 7 παράγραφος 4.

347 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 42.

σε διάφορες σημαντικές διοικητικές υπηρεσίες, όπως είναι η δυνατότητα να καταβάλλουν τους δημοτικούς φόρους μέσω του διαδικτύου, να υποβάλλουν καταγγελίες ηλεκτρονικά επωφελούμενοι από υποχρέωση της αρχής να απαντήσει εντός προθεσμίας τριών ημερών, ή ακόμη και η δυνατότητα να αποφεύγουν τις ουρές αναμονής, να προμηθεύονται μειωμένα εισιτήρια για παραστάσεις στο δημοτικό συναυλιακό κέντρο και να χρησιμοποιούν τις συσκευές σάρωσης στην είσοδο.

Στο παράδειγμα αυτό, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τους δήμους δεν μπορεί να βασιστεί στη συγκατάθεση. Δεδομένου ότι ασκείται τουλάχιστον έμμεση πίεση στους κατοίκους για να αποκτήσουν την ηλεκτρονική κάρτα και να συμφωνήσουν στην επεξεργασία, η συγκατάθεση δεν παρέχεται ελεύθερα. Επομένως, η ανάπτυξη του συστήματος ηλεκτρονικών καρτών των δήμων πρέπει να βασιστεί σε άλλο νόμιμο λόγο που δικαιολογεί την επεξεργασία. Για παράδειγμα, οι δήμοι θα μπορούσαν να ισχυριστούν ότι η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον, λόγος ο οποίος αποτελεί νόμιμη βάση για την επεξεργασία δυνάμει του άρθρου 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ ³⁴⁸.

Η ελεύθερη συγκατάθεση θα μπορούσε επίσης να αμφισβητηθεί σε περιπτώσεις εξάρτησης, όταν υπάρχει σημαντική οικονομική ή άλλη ανισορροπία μεταξύ του υπευθύνου επεξεργασίας που εξασφαλίζει τη συγκατάθεση και του υποκειμένου των δεδομένων που παρέχει τη συγκατάθεση ³⁴⁹. Χαρακτηριστικό παράδειγμα τέτοιων ανισορροπιών και εξάρτησης είναι η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον εργοδότη στο πλαίσιο σχέσης απασχόλησης. Σύμφωνα με την Ομάδα εργασίας του άρθρου 29, «[ο]ι εργαζόμενοι δεν είναι σχεδόν ποτέ σε θέση να παράσχουν ελεύθερα, να αρνηθούν ή να ανακαλέσουν τη συγκατάθεση, δεδομένης της εξάρτησης που προκύπτει από τη σχέση εργοδότη/εργαζομένου. Λαμβανομένης υπόψη της ανισορροπίας ισχύος, οι

348 Ομάδα εργασίας του άρθρου 29 (2011), *Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης*, WP 187, 13 Ιουλίου 2011, σ. 16. Άλλες περιπτώσεις στις οποίες η επεξεργασία δεδομένων δεν μπορεί να βασιστεί σε συγκατάθεση, αλλά απαιτείται διαφορετική νομική βάση προκειμένου να καταστεί η επεξεργασία σύμφωνη αναφέρονται στις σ. 14 και 17 της γνώμης.

349 Βλ. επίσης Ομάδα εργασίας του άρθρου 29 (2001), *Γνωμοδότηση 8/2001 για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο εργασιακό πλαίσιο*, WP 48, Βρυξέλλες, 13 Σεπτεμβρίου 2001· Ομάδα εργασίας του άρθρου 29 (2005), *Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995*, WP 114, Βρυξέλλες, 25 Νοεμβρίου 2005· Ομάδα εργασίας του άρθρου 29 (2017), *Opinion 2/2017 on data processing at work*, WP 249, Βρυξέλλες, 8 Ιουνίου 2017.

εργαζόμενοι μπορούν να παρέχουν ελεύθερη συγκατάθεση μόνο σε εξαιρετικές περιπτώσεις, όταν η αποδοχή ή η απόρριψη πρότασης δεν συνδέεται με καμία συνέπεια»³⁵⁰.

Παράδειγμα: Μεγάλη εταιρεία σχεδιάζει να δημιουργήσει κατάλογο με τα ονόματα όλων των υπαλλήλων, τα καθήκοντά τους στην επιχείρηση και την επαγγελματική τους διεύθυνση, με μοναδικό σκοπό τη βελτίωση της επικοινωνίας εντός της επιχείρησης. Ο προϊστάμενος του τμήματος προσωπικού προτείνει να προστεθεί στον κατάλογο η φωτογραφία κάθε υπαλλήλου, ώστε να καθίσταται ευκολότερη η αναγνώριση συναδέλφων σε συσκέψεις. Οι εκπρόσωποι των εργαζομένων ζητούν αυτό να γίνεται μόνο εάν ο κάθε υπάλληλος παράσχει τη συγκατάθεσή του.

Σε μια τέτοια περίπτωση, η συγκατάθεση του υπαλλήλου θα πρέπει να αναγνωριστεί ως η νομική βάση για την επεξεργασία των φωτογραφιών στον κατάλογο, επειδή πιστεύεται ότι ο υπάλληλος δεν θα υποστεί καμία συνέπεια είτε συμφωνήσει είτε αρνηθεί να δημοσιευθεί η φωτογραφία του.

Παράδειγμα: Η εταιρεία Α σχεδιάζει συνάντηση μεταξύ τριών υπαλλήλων της και των διευθυντών της εταιρείας Β, προκειμένου να συζητήσουν ενδεχόμενη μελλοντική συνεργασία στο πλαίσιο ενός έργου. Η συνάντηση θα πραγματοποιηθεί στους χώρους της εταιρείας Β, η οποία ζητεί από την Α να της αποστείλει μέσω ηλεκτρονικού ταχυδρομείου τα ονόματα, τα βιογραφικά σημειώματα και φωτογραφίες των συμμετεχόντων στη συνάντηση. Η εταιρεία Β ισχυρίζεται ότι χρειάζεται τα ονόματα και τις φωτογραφίες των συμμετεχόντων ώστε το προσωπικό ασφάλειας στην είσοδο του κτιρίου να μπορέσει να επιβεβαιώσει ότι είναι τα εν λόγω πρόσωπα, ενώ με τα βιογραφικά σημειώματα θα μπορέσουν οι διευθυντές να προετοιμαστούν καλύτερα για τη συνάντηση. Στην περίπτωση αυτή, η διαβίβαση από την εταιρεία Α των δεδομένων προσωπικού χαρακτήρα των υπαλλήλων της δεν μπορεί να βασιστεί στη συγκατάθεση. Η συγκατάθεση δεν θα μπορούσε να θεωρηθεί «ελεύθερη», καθώς οι υπάλληλοι ενδέχεται να υποστούν αρνητικές συνέπειες εάν απορρίψουν την πρόταση (για παράδειγμα, ενδέχεται να αντικατασταθούν από άλλο

350 Ομάδα εργασίας του άρθρου 29, Γνώμη 2/2017 σχετικά με την επεξεργασία δεδομένων στο χώρο εργασίας (*Opinion 2/2017 on data processing at work*), WP 249, Βρυξέλλες, 8 Ιουνίου 2017.

συνάδελφο όχι μόνο στη συνάντηση, αλλά και στη συνεργασία με την εταιρεία Β και στη συμμετοχή στο έργο εν γένει). Επομένως, η επεξεργασία πρέπει να βασιστεί σε άλλο νόμιμο λόγο.

Ωστόσο, αυτό δεν σημαίνει ότι η συγκατάθεση δεν μπορεί ποτέ να είναι έγκυρη σε περιπτώσεις στις οποίες η άρνησή της θα έχει κάποιες αρνητικές συνέπειες. Για παράδειγμα, εάν η άρνηση συγκατάθεσης στην απόκτηση κάρτας πελάτη υπεραγοράς έχει ως αποτέλεσμα μόνο την απώλεια μικρής έκπτωσης επί της τιμής ορισμένων προϊόντων, η συγκατάθεση θα μπορούσε να είναι έγκυρη νομική βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα των πελατών εκείνων που συγκατατέθηκαν στην απόκτηση τέτοιας κάρτας. Δεν υπάρχει εξάρτηση μεταξύ εταιρείας και πελάτη, και οι συνέπειες της μη συγκατάθεσης δεν είναι αρκετά σοβαρές ώστε να εμποδίζουν την ελεύθερη επιλογή του υποκειμένου των δεδομένων (εφόσον η μείωση της τιμής είναι αρκετά μικρή ώστε να μην επηρεάζει την ελεύθερη επιλογή του).

Ωστόσο, όταν τα προϊόντα ή οι υπηρεσίες μπορούν να αποκτηθούν μόνον εάν ορισμένα δεδομένα προσωπικού χαρακτήρα κοινοποιηθούν στον υπεύθυνο επεξεργασίας ή περαιτέρω σε τρίτους, η συγκατάθεση του υποκειμένου των δεδομένων στην κοινοποίηση των δεδομένων που το αφορούν και τα οποία δεν είναι αναγκαία για τη σύμβαση δεν μπορεί να θεωρηθεί ελεύθερη απόφαση και, επομένως, δεν είναι έγκυρη βάσει του δικαίου για την προστασία δεδομένων ³⁵¹. Ο ΓΚΠΔ απαγορεύει, μάλλον αυστηρά, τη σύνδεση της συγκατάθεσης με την παροχή προϊόντων και υπηρεσιών ³⁵².

Παράδειγμα: Η συμφωνία επιβατών για τη διαβίβαση από αεροπορική εταιρεία των ονομαστικών καταστάσεων επιβατών (δηλαδή, στοιχείων σχετικά με την ταυτότητα, τις διατροφικές συνήθειες ή τα προβλήματα υγείας τους) στις υπηρεσίες μετανάστευσης συγκεκριμένης ξένης χώρας δεν μπορεί να θεωρηθεί έγκυρη συγκατάθεση βάσει του δικαίου για την προστασία δεδομένων, καθώς ο επιβάτης που ταξιδεύει δεν έχει άλλη επιλογή εφόσον επιθυμεί να επισκεφθεί τη συγκεκριμένη χώρα. Για τη σύννομη διαβίβαση των δεδομένων αυτών απαιτείται άλλη νομική βάση, πέραν της συγκατάθεσης, και πιθανότατα ειδικός νόμος.

³⁵¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 7 παράγραφος 4.

³⁵² Ό.π.

Συγκατάθεση εν πλήρει επιγνώσει

Το υποκείμενο των δεδομένων πρέπει να διαθέτει επαρκείς πληροφορίες προτού προβεί στην επιλογή του. Στην εν πλήρει επιγνώσει συγκατάθεση θα παρέχεται συνήθως ακριβής και ευνόητη περιγραφή του θέματος για το οποίο ζητείται συγκατάθεση. Όπως εξηγεί η Ομάδα εργασίας του άρθρου 29, η συγκατάθεση πρέπει να βασίζεται σε εκτίμηση και κατανόηση των πραγματικών περιστατικών και των συνεπειών της πράξης του υποκειμένου των δεδομένων με την οποία συγκατατίθεται στην επεξεργασία. Ως εκ τούτου, «[τ]ο ενδιαφερόμενο άτομο πρέπει να λάβει, με σαφή και κατανοητό τρόπο, κατάλληλη και πλήρη ενημέρωση για όλα τα σχετικά θέματα [...] όπως οι κατηγορίες των σχετικών δεδομένων, οι σκοποί της επεξεργασίας, οι αποδέκτες ή κατηγορίες αποδεκτών των δεδομένων και τα δικαιώματα του προσώπου στο οποίο αναφέρονται τα δεδομένα»³⁵³. Προκειμένου η συγκατάθεση να είναι εν πλήρει επιγνώσει, τα φυσικά πρόσωπα πρέπει να έχουν επίσης επίγνωση των συνεπειών της μη συγκατάθεσης στην επεξεργασία.

Λαμβανομένης υπόψη της σημασίας της εν πλήρει επιγνώσει συγκατάθεσης, ο ΓΚΠΔ και η Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 επιδίωξαν να αποσαφηνίσουν την έννοια αυτή. Σύμφωνα με τις αιτιολογικές σκέψεις του ΓΚΠΔ, εν πλήρει επιγνώσει συγκατάθεση σημαίνει ότι «το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει τουλάχιστον την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα προσωπικού χαρακτήρα» τα οποία υποβάλλονται σε επεξεργασία³⁵⁴.

Στην εξαιρετική περίπτωση που η συγκατάθεση χρησιμοποιείται ως παρέκκλιση, για να διασφαλιστεί νόμιμος λόγος διεθνούς διαβίβασης δεδομένων, τότε ο υπεύθυνος επεξεργασίας οφείλει να ενημερώνει το υποκείμενο των δεδομένων για τους πιθανούς κινδύνους που εγκυμονούν τέτοιες διαβιβάσεις, λόγω της απουσίας απόφασης επάρκειας και κατάλληλων εγγυήσεων, προκειμένου η συγκατάθεση αυτή να μπορεί να θεωρηθεί έγκυρη³⁵⁵.

Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 προσδιορίζεται ότι πρέπει να παρέχονται πληροφορίες σχετικά με τις συνέπειες της απόφασης του

353 Ομάδα εργασίας του άρθρου 29 (2007), *Εγγραφο εργασίας σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία στο πλαίσιο των ηλεκτρονικών μητρώων υγείας (HMY)*, WP 131, Βρυξέλλες, 15 Φεβρουαρίου 2007.

354 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 42.

355 Ό.π., άρθρο 49 παράγραφος 1 στοιχείο α).

υποκειμένου των δεδομένων, και ειδικότερα «τι συνεπάγεται η συγκατάθεση και σε ποιο βαθμό παρέχεται»³⁵⁶.

Η ποιότητα των πληροφοριών είναι σημαντική. Ποιότητα των πληροφοριών σημαίνει ότι η γλώσσα των πληροφοριών θα πρέπει να είναι προσαρμοσμένη στους προβλεπόμενους αποδέκτες. Οι πληροφορίες πρέπει να παρέχονται χωρίς τη χρήση ιδιωμάτων, με σαφή και απλή διατύπωση, την οποία ο μέσος χρήστης θα πρέπει να είναι σε θέση να κατανοήσει³⁵⁷. Οι πληροφορίες πρέπει επίσης να είναι εύκολα διαθέσιμες στο υποκείμενο των δεδομένων και μπορούν να παρέχονται προφορικά ή γραπτά. Η προσβασιμότητα και η προβολή των πληροφοριών είναι σημαντικά στοιχεία: οι πληροφορίες πρέπει να είναι σαφώς ορατές και εμφανείς. Σε διαδικτυακό περιβάλλον, τα ενημερωτικά σημειώματα πολλών επιπέδων μπορούν να αποτελέσουν μια καλή λύση, καθώς παρέχουν τη δυνατότητα στα υποκείμενα των δεδομένων να επιλέξουν αν θέλουν να έχουν πρόσβαση σε συνοπτική ή εκτενέστερη εκδοχή των πληροφοριών.

Συγκεκριμένη συγκατάθεση

Προκειμένου να είναι η συγκατάθεση έγκυρη, πρέπει επίσης να αφορά συγκεκριμένα τον σκοπό της επεξεργασίας, ο οποίος πρέπει να περιγράφεται σαφώς και με αδιαμφισβήτητο τρόπο. Αυτό συμβαδίζει με την ποιότητα των πληροφοριών που παρέχονται σχετικά με τον σκοπό της συγκατάθεσης. Στο πλαίσιο αυτό, σημασία θα έχουν οι εύλογες προσδοκίες του μέσου υποκειμένου των δεδομένων. Η συγκατάθεση του υποκειμένου των δεδομένων πρέπει να ζητηθεί εκ νέου εάν πρόκειται να προστεθούν ή να τροποποιηθούν πράξεις επεξεργασίας, κατά τρόπο που δεν θα μπορούσε να είχε προβλεφθεί εύλογα όταν είχε παρασχεθεί η αρχική συγκατάθεση, οι οποίες έχουν επομένως ως αποτέλεσμα να μεταβάλλεται ο σκοπός της συγκατάθεσης. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς³⁵⁸.

356 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 42.

357 Ομάδα εργασίας του άρθρου 29 (2011), *Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης*, WP 187, 13 Ιουλίου 2011, σ. 19.

358 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 32.

Παραδείγματα: Στην υπόθεση *Deutsche Telekom AG* ³⁵⁹, το ΔΕΕ εξέτασε αν φορέας παροχής τηλεπικοινωνιών που όφειλε να διαβιβάσει δεδομένα προσωπικού χαρακτήρα συνδρομητών, τα οποία επρόκειτο να δημοσιευθούν σε καταλόγους, χρειαζόταν νέα συγκατάθεση από τα υποκείμενα των δεδομένων ³⁶⁰, καθώς οι αποδέκτες των δεδομένων δεν κατονομάζονταν αρχικά όταν παρασχέθηκε η συγκατάθεση.

Το ΔΕΕ αποφάνθηκε ότι, βάσει του άρθρου 12 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, η παροχή εκ νέου συγκατάθεσης δεν ήταν αναγκαία για τη διαβίβαση των δεδομένων. Εφόσον τα υποκείμενα των δεδομένων είχαν τη δυνατότητα να συγκατατεθούν μόνο στον σκοπό της επεξεργασίας –ο οποίος ήταν η δημοσίευση των δεδομένων που τα αφορούσαν–, δεν μπορούσαν να επιλέξουν μεταξύ διαφορετικών καταλόγων στους οποίους θα ήταν δυνατόν να δημοσιευθούν τα εν λόγω δεδομένα.

Όπως επισήμανε το ΔΕΕ, «από την ερμηνεία του άρθρου 12 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες βάσει του πλαισίου και του συστήματος στα οποία εντάσσεται η διάταξη αυτή προκύπτει ότι η διαλαμβανόμενη στην παράγραφο 2 του άρθρου αυτού συγκατάθεση αφορά τον σκοπό της δημοσίευσης των δεδομένων προσωπικού χαρακτήρα σε δημόσιο κατάλογο και όχι ειδικά την ταυτότητα του εκδότη του καταλόγου αυτού» ³⁶¹. Επιπροσθέτως, «επιζήμια για συνδρομητή μπορεί να αποβεί [μάλλον] η δημοσίευση των δεδομένων προσωπικού χαρακτήρα σε κατάλογο με ειδικό σκοπό» ³⁶² και όχι η ταυτότητα του εκδότη.

Η υπόθεση *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV κατά Autoriteit Consument en Markt (ACM)* ³⁶³ αφορούσε το αίτημα βελγικής εταιρείας παροχής υπηρεσιών πληροφοριών καταλόγου και καταλόγου

359 ΔΕΕ, C-543/09, *Deutsche Telekom AG κατά Bundesrepublik Deutschland*, 5 Μαΐου 2011. Βλ. ιδίως σκέψεις 53 και 54.

360 Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (ΕΕ L 201 της 31.7.2002, σ. 37) (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

361 ΔΕΕ, C-543/09, *Deutsche Telekom AG κατά Bundesrepublik Deutschland*, 5 Μαΐου 2011, σκέψη 61.

362 Ό.π., σκέψη 62.

363 ΔΕΕ, C-536/15, *Tele2 (Netherlands) BV κ.λπ. κατά Autoriteit Consument en Markt (ACM)*, 15 Μαρτίου 2017.

συνδρομητών προς εταιρείες που χορηγούν αριθμούς τηλεφώνου στις Κάτω Χώρες να της παράσχουν πρόσβαση σε δεδομένα σχετικά με τους συνδρομητές τους. Η βελγική εταιρεία επικαλέστηκε υποχρέωση βάσει της οδηγίας για τις καθολικές υπηρεσίες ³⁶⁴. Η υποχρέωση αυτή επιβάλλει στις εταιρείες που χορηγούν αριθμούς τηλεφώνου να καθιστούν διαθέσιμους τους αριθμούς στις εταιρείες παροχής υπηρεσιών πληροφοριών καταλόγου που τους ζητούν, εάν οι συνδρομητές έχουν συγκατατεθεί στη δημοσίευση των αριθμών τους. Οι ολλανδικές εταιρείες απέρριψαν το αίτημα, με την αιτιολογία ότι δεν υποχρεούνταν να παράσχουν τα επίμαχα δεδομένα σε επιχείρηση εγκατεστημένη σε άλλο κράτος μέλος. Υποστήριξαν ότι οι χρήστες έδωσαν τη συγκατάθεσή τους για τη δημοσίευση των αριθμών τους θεωρώντας ότι αυτοί θα δημοσιεύονταν σε ολλανδικό κατάλογο. Το ΔΕΕ αποφάνθηκε ότι η οδηγία για τις καθολικές υπηρεσίες αφορά όλα τα αιτήματα επιχειρήσεων παροχής υπηρεσιών πληροφοριών καταλόγου, ανεξάρτητα από το κράτος μέλος στο οποίο αυτές είναι εγκατεστημένες. Το ΔΕΕ αποφάνθηκε επίσης ότι η διαβίβαση των ίδιων δεδομένων σε άλλη επιχείρηση με σκοπό τη δημοσίευση δημόσιου καταλόγου χωρίς να εξασφαλιστεί εκ νέου η συγκατάθεση των συνδρομητών δεν θίγει την ουσία του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα ³⁶⁵. Επομένως, η επιχείρηση που χορηγεί αριθμούς τηλεφώνου δεν απαιτείται να διατυπώνει το αίτημα παροχής συγκατάθεσης που απευθύνει στους συνδρομητές της κατά τρόπον ώστε αυτοί να παρέχουν τη συγκατάθεσή τους χωριστά για κάθε κράτος μέλος προς το οποίο ενδέχεται να διαβιβαστούν τα στοιχεία που τους αφορούν ³⁶⁶.

Αδιαμφισβήτητη συγκατάθεση

Κάθε συγκατάθεση πρέπει να παρέχεται με αδιαμφισβήτητο τρόπο ³⁶⁷. Αυτό σημαίνει ότι δεν θα πρέπει να υφίσταται εύλογη αμφιβολία για τη βούληση του υποκειμένου των δεδομένων να δηλώσει τη συμφωνία του στην επεξεργασία

364 Οδηγία 2002/22/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 7ης Μαρτίου 2002, για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών (οδηγία καθολικής υπηρεσίας) (ΕΕ 2002 L 108, σ. 51), όπως τροποποιήθηκε με την οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 (οδηγία για τις καθολικές υπηρεσίες) (ΕΕ 2009 L 337, σ. 11).

365 ΔΕΕ, C-536/15, *Tele2 (Netherlands) BV κ.λπ. κατά Autoriteit Consument en Markt (ACM)*, 15 Μαρτίου 2017, σκέψη 36.

366 Ό.π., σκέψεις 40-41.

367 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 11.

των δεδομένων που το αφορούν. Για παράδειγμα, η αδράνεια του υποκειμένου των δεδομένων δεν υποδηλώνει αδιαμφισβήτητη συγκατάθεση.

Πρόκειται για την περίπτωση στην οποία ο υπεύθυνος επεξεργασίας εξασφαλίζει τη συγκατάθεση με δηλώσεις, στο πλαίσιο των πολιτικών του για την προστασία της ιδιωτικής ζωής, του τύπου «χρησιμοποιώντας την υπηρεσία μας, συγκατατίθεστε στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που σας αφορούν». Στην περίπτωση αυτή, ο υπεύθυνος επεξεργασίας θα πρέπει να διασφαλίζει τη συγκατάθεση των χρηστών στις πολιτικές αυτές με μη αυτόματο τρόπο και ατομικά.

Εάν η συγκατάθεση παρέχεται εγγράφως στο πλαίσιο σύμβασης, η συγκατάθεση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να εξατομικεύεται και, εν πάση περιπτώσει, «θα πρέπει να παρέχονται εγγυήσεις που να διασφαλίζουν ότι το υποκείμενο των δεδομένων γνωρίζει αυτό το γεγονός και σε ποιο βαθμό έχει συγκατατεθεί»³⁶⁸.

Απαιτήσεις για τη συγκατάθεση παιδιών

Ο ΓΚΠΔ προβλέπει ειδική προστασία για τα παιδιά στο πλαίσιο της παροχής υπηρεσιών της κοινωνίας των πληροφοριών, επειδή «τα παιδιά μπορεί να έχουν μικρότερη επίγνωση των σχετικών κινδύνων, συνεπειών και εγγυήσεων και των δικαιωμάτων τους σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα»³⁶⁹. Επομένως, βάσει του **δικαίου της ΕΕ**, όταν πάροχοι υπηρεσιών της κοινωνίας των πληροφοριών επεξεργάζονται δεδομένα προσωπικού χαρακτήρα παιδιών ηλικίας κάτω των 16 ετών βάσει συγκατάθεσης, η επεξεργασία θα είναι σύννομη «μόνο εάν και στον βαθμό που η εν λόγω συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού»³⁷⁰. Τα κράτη μέλη μπορούν να προβλέπουν κατώτερο όριο ηλικίας στο εθνικό δίκαιο, όχι όμως κατώτερο των 13 ετών³⁷¹. Η συγκατάθεση του προσώπου που έχει τη γονική μέριμνα δεν είναι απαραίτητη «σε συνάρτηση με υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε ένα παιδί»³⁷². Κάθε ενημέ-

368 Ό.π., αιτιολογική σκέψη 42.

369 Ό.π., αιτιολογική σκέψη 38.

370 Ό.π. άρθρο 8 παράγραφος 1 πρώτο εδάφιο. Η έννοια των υπηρεσιών της κοινωνίας των πληροφοριών ορίζεται στο άρθρο 4 σημείο 25 του Γενικού Κανονισμού για την Προστασία Δεδομένων.

371 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 8 παράγραφος 1 δεύτερη περίπτωση.

372 Ό.π., αιτιολογική σκέψη 38.

ρωση και ανακοίνωση, εάν η επεξεργασία απευθύνεται σε παιδί, θα πρέπει να διατυπώνεται σε σαφή και απλή γλώσσα την οποία το παιδί να μπορεί να κατανοεί εύκολα ³⁷³.

Δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή

Ο ΓΚΠΔ προβλέπει γενικό δικαίωμα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή ³⁷⁴. Το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για το δικαίωμα αυτό προτού δώσει τη συγκατάθεσή του και μπορεί να ασκήσει το δικαίωμα αυτό κατά τη διακριτική του ευχέρεια. Δεν θα πρέπει να προβλέπεται απαίτηση αιτιολόγησης της ανάκλησης, και δεν θα πρέπει να υφίσταται κίνδυνος αρνητικών συνεπειών πέραν της παύσης τυχόν οφελών που ενδέχεται να απορρέουν από την προηγούμενης συμφωνηθείσα χρήση των δεδομένων. Η ανάκληση της συγκατάθεσης θα πρέπει να είναι εξίσου εύκολη με την παροχή της ³⁷⁵. Δεν νοείται ελεύθερη συγκατάθεση εάν το υποκείμενο των δεδομένων δεν είναι σε θέση να ανακαλέσει τη συγκατάθεσή του χωρίς να ζημιωθεί ή εάν η ανάκληση δεν είναι εξίσου εύκολη με την παροχή της συγκατάθεσης ³⁷⁶.

Παράδειγμα: Πελάτης συμφωνεί να λαμβάνει διαφημιστική αλληλογραφία σε διεύθυνση την οποία παρέχει σε υπεύθυνο επεξεργασίας δεδομένων. Εάν ο πελάτης ανακαλέσει τη συγκατάθεσή του, ο υπεύθυνος επεξεργασίας οφείλει να σταματήσει αμέσως να αποστέλλει διαφημιστική αλληλογραφία. Δεν θα πρέπει να υπάρξουν συνέπειες υπό μορφή ποινής, όπως η επιβολή τέλους. Ωστόσο, η ανάκληση αφορά το μέλλον και δεν έχει αναδρομική ισχύ. Για το διάστημα κατά το οποίο τα δεδομένα προσωπικού χαρακτήρα του πελάτη υποβλήθηκαν σε σύμφωνη επεξεργασία –με τη συγκατάθεση του πελάτη– δεν υφίσταται παράβαση της νομοθεσίας. Η ανάκληση εμποδίζει κάθε περαιτέρω επεξεργασία των δεδομένων αυτών, εκτός εάν η επεξεργασία είναι σύμφωνη με το δικαίωμα διαγραφής ³⁷⁷.

373 Ό.π., αιτιολογική σκέψη 58. Βλ. επίσης Εκσυγχρονισμένη Σύμβαση 108, άρθρο 15 στοιχείο ε) δεύτερη περίπτωση. Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημεία 68 και 125.

374 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 7 παράγραφος 3· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 45.

375 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 7 παράγραφος 3.

376 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 42· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 42.

377 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 17 παράγραφος 1 στοιχείο β).

Αναγκαιότητα για την εκτέλεση σύμβασης

Βάσει του δικαίου της ΕΕ, το άρθρο 6 παράγραφος 1 στοιχείο β) του ΓΚΠΔ προβλέπει ακόμη μία βάση σύννομης επεξεργασίας, και συγκεκριμένα την περίπτωση όπου αυτή είναι «απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος». Η διάταξη αυτή καλύπτει και τις προσυμβατικές σχέσεις. Για παράδειγμα, σε περιπτώσεις στις οποίες ένα μέρος προτίθεται να συνάψει σύμβαση, αλλά δεν το έχει πράξει ακόμη, ενδεχομένως επειδή χρειάζεται να διενεργηθούν ορισμένοι ακόμη έλεγχοι. Εάν ένα μέρος χρειάζεται να επεξεργαστεί δεδομένα για τον σκοπό αυτό, η επεξεργασία αυτή είναι σύννομη εφόσον είναι απαραίτητη «για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης»³⁷⁸.

Η έννοια της επεξεργασίας δεδομένων ως «θεμιτής βάσης προβλεπόμενης από τον νόμο» στο άρθρο 5 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108 περιλαμβάνει επίσης «την επεξεργασία δεδομένων για την εκτέλεση σύμβασης (ή για προσυμβατικά μέτρα, κατόπιν αιτήματος του υποκειμένου των δεδομένων) στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος»³⁷⁹.

Έννομες υποχρεώσεις του υπευθύνου επεξεργασίας

Το **δίκαιο της ΕΕ** προβλέπει ακόμη έναν λόγο που καθιστά σύννομη την επεξεργασία δεδομένων, και συγκεκριμένα την περίπτωση που αυτή «είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας» [άρθρο 6 παράγραφος 1 στοιχείο γ) του ΓΚΠΔ]. Η διάταξη αυτή αφορά υπευθύνους επεξεργασίας που δραστηριοποιούνται τόσο στον ιδιωτικό, όσο και στον δημόσιο τομέα· οι έννομες υποχρεώσεις υπευθύνων επεξεργασίας δεδομένων στον δημόσιο τομέα μπορούν επίσης να εμπίπτουν στο πεδίο εφαρμογής του άρθρου 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ. Υπάρχουν πολλά παραδείγματα περιπτώσεων στις οποίες ο νόμος υποχρεώνει τους υπευθύνους επεξεργασίας του ιδιωτικού τομέα να επεξεργάζονται δεδομένα σχετικά με συγκεκριμένα υποκείμενα δεδομένων. Για παράδειγμα, οι εργοδότες πρέπει να επεξεργάζονται δεδομένα των υπαλλήλων τους για λόγους κοινωνικής ασφάλισης και για

378 Ό.π., άρθρο 6 παράγραφος 1 στοιχείο β).

379 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 46· Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2010), Σύσταση CM/Rec (2010)13 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την προστασία των φυσικών προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της κατάρτισης προφίλ (σύσταση σχετικά με την κατάρτιση προφίλ), 23 Νοεμβρίου 2010, άρθρο 3 παράγραφος 4 στοιχείο β).

φορολογικούς σκοπούς, και οι επιχειρήσεις πρέπει να επεξεργάζονται δεδομένα των πελατών τους για φορολογικούς σκοπούς.

Η έννομη υποχρέωση μπορεί να προκύπτει από το δίκαιο της Ένωσης ή κράτους μέλους, το οποίο θα μπορούσε να αποτελεί τη βάση για μία ή περισσότερες πράξεις επεξεργασίας. Το δίκαιο θα πρέπει να προσδιορίζει τον σκοπό της επεξεργασίας, να θεσπίζει προδιαγραφές για τον καθορισμό του υπευθύνου επεξεργασίας, του είδους των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, των εκάστοτε υποκειμένων των δεδομένων, των οντοτήτων στις οποίες μπορούν να κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, των περιορισμών σκοπού, της περιόδου αποθήκευσης και άλλων μέτρων για την εξασφάλιση σύννομης και θεμιτής επεξεργασίας³⁸⁰. Κάθε νόμος ο οποίος αποτελεί τη βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνεται τόσο προς τα άρθρα 7 και 8 του Χάρτη, όσο και προς το άρθρο 8 της ΕΣΔΑ.

Οι έννομες υποχρεώσεις του υπευθύνου επεξεργασίας αποτελούν επίσης βάση για τη σύννομη επεξεργασία δεδομένων **στο πλαίσιο του δικαίου του Συμβουλίου της Ευρώπης**³⁸¹. Όπως ήδη επισημάνθηκε, οι έννομες υποχρεώσεις του υπευθύνου επεξεργασίας του ιδιωτικού τομέα είναι απλώς μία συγκεκριμένη περίπτωση έννομων συμφερόντων άλλων προσώπων, όπως προβλέπεται στο άρθρο 8 παράγραφος 2 της ΕΣΔΑ. Επομένως, το παράδειγμα των εργοδοτών που επεξεργάζονται δεδομένα σχετικά με τους υπαλλήλους τους είναι επίσης συναφές στο πλαίσιο του δικαίου του Συμβουλίου της Ευρώπης.

Ζωτικά συμφέροντα του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου

Στο πλαίσιο του δικαίου της ΕΕ, το άρθρο 6 παράγραφος 1 στοιχείο δ) του ΓΚΠΔ προβλέπει ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι σύννομη εάν «είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου». Ο νόμιμος αυτός λόγος μπορεί να προβληθεί για την επεξεργασία δεδομένων προσωπικού χαρακτήρα βάσει των

380 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 45.

381 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2010), Σύσταση CM/Rec (2010)13 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την προστασία των φυσικών προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της κατάρτισης προφίλ (σύσταση σχετικά με την κατάρτιση προφίλ), 23 Νοεμβρίου 2010, άρθρο 3 παράγραφος 4 στοιχείο α).

ζωτικών συμφερόντων άλλου φυσικού προσώπου μόνο «εάν είναι πρόδηλο ότι η επεξεργασία δεν μπορεί να έχει άλλη νομική βάση»³⁸². Ενίοτε ένα είδος επεξεργασίας ενδέχεται να βασιζέται σε λόγους τόσο δημόσιου συμφέροντος, όσο και ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου. Αυτό συμβαίνει, για παράδειγμα, όταν παρακολουθούνται επιδημίες και η εξέλιξή τους ή όταν υπάρχει επείγουσα ανθρωπιστική ανάγκη.

Στο δίκαιο του Συμβουλίου της Ευρώπης, τα ζωτικά συμφέροντα του υποκειμένου των δεδομένων δεν αναφέρονται στο άρθρο 8 της ΕΣΔΑ. Ωστόσο, τα ζωτικά συμφέροντα του υποκειμένου των δεδομένων θεωρείται ότι υπονοούνται στην έννοια της «νόμιμης βάσης» του άρθρου 5 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108, η οποία αναφέρεται στη νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα³⁸³.

Δημόσιο συμφέρον και άσκηση δημόσιας εξουσίας

Λαμβανομένων υπόψη των πολλών ενδεχόμενων τρόπων οργάνωσης των δημόσιων υποθέσεων, το άρθρο 6 παράγραφος 1 στοιχείο ε) του ΓΚΠΔ ορίζει ότι τα δεδομένα προσωπικού χαρακτήρα μπορούν να υποβάλλονται νομίμως σε επεξεργασία εάν αυτή «είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας»³⁸⁴.

Παράδειγμα: Στην υπόθεση *Huber κατά Bundesrepublik Deutschland*³⁸⁵, ο H. Huber, αυστριακός υπήκοος κάτοικος Γερμανίας, ζήτησε από την Ομοσπονδιακή Υπηρεσία Μετανάστευσης και Προσφύγων τη διαγραφή των δεδομένων του που είχαν καταχωριστεί στο Κεντρικό Μητρώο Αλλοδαπών (εφεξής AZR). Το μητρώο αυτό, το οποίο περιέχει δεδομένα προσωπικού χαρακτήρα σχετικά με μη γερμανούς υπηκόους της ΕΕ οι οποίοι διαμένουν στη Γερμανία για περισσότερο από τρεις μήνες, χρησιμοποιείται για στατιστικούς σκοπούς και από τις διωκτικές και δικαστικές αρχές κατά τη διερεύνηση και τη δίωξη εγκληματικών ενεργειών ή δραστηριοτήτων που συνιστούν απειλή για τη δημόσια

382 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 46.

383 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 46.

384 Βλ. Γενικό Κανονισμό για την Προστασία Δεδομένων, αιτιολογική σκέψη 45.

385 ΔΕΕ, C-524/06, *Heinz Huber κατά Bundesrepublik Deutschland* [τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008.

ασφάλεια. Το αιτούν δικαστήριο ζήτησε από το ΔΕΕ να διευκρινίσει αν η επεξεργασία δεδομένων προσωπικού χαρακτήρα από μητρώο όπως το Κεντρικό Μητρώο Αλλοδαπών –στο οποίο έχουν επίσης πρόσβαση άλλες δημόσιες αρχές– συνάδει με το δίκαιο της ΕΕ, δεδομένου ότι δεν υφίσταται αντίστοιχο μητρώο για τους Γερμανούς υπηκόους.

Το ΔΕΕ αποφάνθηκε ότι, βάσει του άρθρου 7 στοιχείο ε) της οδηγίας 95/46³⁸⁶, η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να είναι θεμιτή εάν είναι απαραίτητη για την εκπλήρωση έργου δημόσιου συμφέροντος ή επιπίπτοντος στην άσκηση δημόσιας εξουσίας.

Σύμφωνα με το ΔΕΕ, «λαμβάνομένου υπόψη του σκοπού που συνίσταται στην εξασφάλιση ενός επιπέδου προστασίας ισοδύναμου σε όλα τα κράτη μέλη, η έννοια της αναγκαιότητας όπως απορρέει από το άρθρο 7, στοιχείο ε', της οδηγίας 95/46³⁸⁷ [...] δεν μπορεί να έχει περιεχόμενο που μεταβάλλεται αναλόγως του κράτους μέλους. Επομένως, πρόκειται για αυτοτελή έννοια του κοινοτικού δικαίου η οποία πρέπει να ερμηνευθεί κατά τρόπο που να ανταποκρίνεται πλήρως στον σκοπό της οδηγίας αυτής όπως αυτός ορίζεται στο άρθρο της 1, παράγραφος 1»³⁸⁸.

Το ΔΕΕ επισήμανε ότι το δικαίωμα διαμονής των πολιτών της Ένωσης στο έδαφος κράτους μέλους του οποίου δεν είναι υπήκοοι δεν είναι απεριόριστο, αλλά ασκείται υπό τους περιορισμούς και υπό τις προϋποθέσεις που προβλέπονται από τη Συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας, καθώς και από τις διατάξεις που θεσπίζονται για την εφαρμογή της. Επομένως, ακόμη και αν είναι καταρχήν νόμιμη η χρήση μητρώου όπως το AZR για τον σκοπό της υποστήριξης των αρχών που είναι επιφορτισμένες με την εφαρμογή της ρύθμισης για το δικαίωμα διαμονής, ένα τέτοιο μητρώο δεν μπορεί να περιέχει άλλες πληροφορίες από αυτές που είναι αναγκαίες για τον σκοπό αυτό. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι ένα τέτοιο σύστημα επεξεργασίας δεδομένων προσωπικού χαρακτήρα συνάδει με το δίκαιο της ΕΕ μόνο εάν περιέχει αποκλειστικά τα δεδομένα που είναι αναγκαία για την εφαρμογή της εν λόγω ρύθμισης και εάν ο συγκεντρωτικός χαρακτήρας του παρέχει

386 Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7 στοιχείο ε), πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο ε).

387 Ό.π.

388 ΔΕΕ, C-524/06, *Heinz Huber κατά Bundesrepublik Deutschland* [τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008, σκέψη 52.

τη δυνατότητα αποτελεσματικότερης εφαρμογής της ρύθμισης αυτής. Το εθνικό δικαστήριο πρέπει να εξακριβώσει αν οι προϋποθέσεις αυτές πληρούνται στη συγκεκριμένη υπόθεση. Σε διαφορετική περίπτωση, η αποθήκευση και η επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μητρώο όπως το AZR για στατιστικούς σκοπούς δεν μπορούν, σε καμία βάση, να θεωρηθούν αναγκαίες κατά την έννοια του άρθρου 7 στοιχείο ε) ³⁸⁹ της οδηγίας 95/46 ³⁹⁰.

Τέλος, όσον αφορά το ερώτημα της χρήσης των δεδομένων που περιέχονται στο μητρώο για σκοπούς καταπολέμησης της εγκληματικότητας, το ΔΕΕ αποφάνθηκε ότι ο σκοπός αυτός «αφορά οπωσδήποτε τη δίωξη διαπραχθέντων εγκλημάτων, ανεξαρτήτως της ιθαγένειας των δραστών». Το επίμαχο μητρώο δεν περιέχει δεδομένα προσωπικού χαρακτήρα που αφορούν υπηκόους του οικείου κράτους μέλους, και αυτή η διαφορετική μεταχείριση συνιστά διάκριση η οποία απαγορεύεται από το άρθρο 18 της ΣΛΕΕ. Ως εκ τούτου, το ΔΕΕ αποφάνθηκε ότι η διάταξη αυτή «απαγορεύει τη δημιουργία από ένα κράτος μέλος ειδικού συστήματος επεξεργασίας δεδομένων προσωπικού χαρακτήρα των πολιτών της Ένωσης που δεν είναι υπήκοοι του κράτους μέλους αυτού με σκοπό την καταπολέμηση της εγκληματικότητας» ³⁹¹.

Η χρήση δεδομένων προσωπικού χαρακτήρα από αρχές που δραστηριοποιούνται στη δημόσια σφαίρα διέπεται επίσης από το άρθρο 8 της **ΕΣΔΑ** και κατά περίπτωση από το άρθρο 5 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108 ³⁹².

Έννομα συμφέροντα που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος

Βάσει του **δικαίου της ΕΕ**, έννομα συμφέροντα δεν έχει μόνο το υποκείμενο των δεδομένων. Σύμφωνα με το άρθρο 6 παράγραφος 1 στοιχείο στ) του ΓΚΠΔ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να είναι σύμφωνη εάν «είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει

³⁸⁹ Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7 στοιχείο ε), πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο ε).

³⁹⁰ ΔΕΕ, C-524/06, *Heinz Huber κατά Bundesrepublik Deutschland* [τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008, σκέψεις 54, 58-59 και 66-68.

³⁹¹ Ό.π., σκέψεις 78 και 81.

³⁹² Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημεία 46-47.

ο υπεύθυνος επεξεργασίας ή τρίτος [εκτός δημόσιων αρχών κατά την άσκηση των καθηκόντων τους], εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα [...]»³⁹³.

Η ύπαρξη έννομου συμφέροντος πρέπει να αξιολογείται προσεκτικά σε κάθε συγκεκριμένη περίπτωση³⁹⁴. Εάν προσδιοριστούν τα έννομα συμφέροντα του υπευθύνου επεξεργασίας, αυτά πρέπει στη συνέχεια να σταθμιστούν με τα συμφέροντα ή τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων³⁹⁵. Οι εύλογες προσδοκίες του υποκειμένου των δεδομένων πρέπει να λαμβάνονται υπόψη στο πλαίσιο μιας τέτοιας αξιολόγησης για τη διαπίστωση του αν τα συμφέροντα του υπευθύνου επεξεργασίας υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων του υποκειμένου των δεδομένων³⁹⁶. Εάν τα δικαιώματα του υποκειμένου των δεδομένων υπερισχύουν των έννομων συμφερόντων του υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας μπορεί να λάβει μέτρα και να εφαρμόσει εγγυήσεις ώστε να διασφαλίσει την ελαχιστοποίηση του αντίκτυπου στα δικαιώματα του υποκειμένου των δεδομένων (όπως ψευδωνυμοποίηση των δεδομένων) και να αντιστρέψει την «ισορροπία» για να μπορέσει να επικαλεστεί νομίμως την έγκυρη αυτή βάση για την επεξεργασία. Στη Γνώμη της σχετικά με την έννοια των έννομων συμφερόντων του υπευθύνου επεξεργασίας, η Ομάδα εργασίας του άρθρου 29 τόνισε τον κρίσιμο ρόλο της λογοδοσίας και της διαφάνειας, και του δικαιώματος του υποκειμένου των δεδομένων να εναντιωθεί στην επεξεργασία των δεδομένων που το αφορούν ή στην πρόσβαση σε αυτά, στην τροποποίηση, στη διαγραφή ή στη διαβίβαση αυτών, κατά τη στάθμιση των έννομων συμφερόντων του υπευθύνου επεξεργασίας και των συμφερόντων των θεμελιωδών δικαιωμάτων του υποκειμένου των δεδομένων³⁹⁷.

Στις αιτιολογικές σκέψεις του ΓΚΠΔ παρέχονται ορισμένα παραδείγματα σχετικά με το τι συνιστά έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας.

393 Σε σύγκριση με την οδηγία 95/46, ο Γενικός Κανονισμός για την Προστασία Δεδομένων παρέχει περισσότερα παραδείγματα περιπτώσεων που θεωρείται ότι συνιστούν έννομο συμφέρον.

394 Γενικός Κανονισμός για την Προστασία Δεδομένων, προοίμιο, αιτιολογική σκέψη 47.

395 Ομάδα εργασίας του άρθρου 29 (2014), *Γνώμη 06/2014 σχετικά με την έννοια των εννόμων συμφερόντων του υπευθύνου επεξεργασίας, σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ*, WP 217, 4 Απριλίου 2014.

396 Ό.π.

397 Ό.π.

Για παράδειγμα, η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων όταν πραγματοποιείται για την άμεση εμπορική προώθηση ή όταν η εν λόγω επεξεργασία είναι «αυστηρά αναγκαία για τους σκοπούς πρόληψης της απάτης»³⁹⁸.

Στη νομολογία του, το ΔΕΕ ανέλυσε το κριτήριο για τον καθορισμό του τι συνιστά έννομο συμφέρον.

Παράδειγμα: Η υπόθεση *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*³⁹⁹ αφορούσε ζημία που προκλήθηκε σε τρόλεϊ της εταιρείας μεταφορών της Ρίγας από επιβάτη ο οποίος ξαφνικά άνοιξε την πόρτα ενός ταξί. Η Rīgas satiksme επιθυμούσε να ασκήσει αγωγή αποζημίωσης κατά του επιβάτη. Ωστόσο, η αστυνομία δεν ήταν διατεθειμένη να δώσει παρά μόνο το ονοματεπώνυμο του επιβάτη και αρνήθηκε να παράσχει τον αριθμό ταυτότητας και τη διεύθυνσή του, με το επιχείρημα ότι η γνωστοποίηση αυτή θα ήταν παράνομη βάσει του εθνικού δικαίου για την προστασία δεδομένων.

Το λετονικό αιτούν δικαστήριο ζήτησε από το ΔΕΕ να εκδώσει προδικαστική απόφαση και να διευκρινίσει αν η νομοθεσία της ΕΕ για την προστασία δεδομένων επιβάλλει υποχρέωση κοινοποίησης όλων των δεδομένων προσωπικού χαρακτήρα που είναι αναγκαία για την άσκηση αγωγής κατά προσώπου που εικάζεται ότι ευθύνεται για διοικητική παράβαση⁴⁰⁰.

Το ΔΕΕ διευκρίνισε ότι το δίκαιο της ΕΕ για την προστασία δεδομένων περιλαμβάνει τη δυνατότητα –όχι την υποχρέωση– γνωστοποίησης δεδομένων σε τρίτο για τους σκοπούς των έννομων συμφερόντων που επιδιώκει το πρόσωπο αυτό⁴⁰¹. Το ΔΕΕ καθόρισε τρεις προϋποθέσεις οι οποίες πρέπει να πληρούνται σωρευτικώς προκειμένου να είναι σύννομη η επεξεργασία δεδομένων επί τη βάση των «έννομων συμφερόντων»⁴⁰². Πρώτον, ο τρίτος στον οποίο κοινοποιούνται τα δεδομένα πρέπει να επιδιώκει έννομο συμφέρον. Στην προκειμένη περίπτωση, αυτό σημαίνει

398 Γενικός Κανονισμός για την Προστασία Δεδομένων, προοίμιο, αιτιολογική σκέψη 47.

399 ΔΕΕ, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde κατά Rīgas pašvaldības SIA «Rīgas satiksme»*, 4 Μαΐου 2017.

400 Ό.π., σκέψη 23.

401 Ό.π., σκέψη 26.

402 Ό.π., σκέψεις 28-34.

ότι το αίτημα παροχής προσωπικών πληροφοριών για την άσκηση αγωγής κατά προσώπου που προκάλεσε υλική ζημία συνιστά έννομο συμφέρον τρίτου. Δεύτερον, η επεξεργασία των δεδομένων προσωπικού χαρακτήρα πρέπει να είναι αναγκαία για τους σκοπούς των επιδιωκόμενων έννομων συμφερόντων. Στην προκειμένη περίπτωση, η απόκτηση προσωπικών πληροφοριών, όπως η διεύθυνση και/ή ο αριθμός ταυτότητας, είναι απολύτως απαραίτητη για την εξακρίβωση της ταυτότητας του εν λόγω προσώπου. Τρίτον, τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων δεν πρέπει να υπερισχύουν των εννόμων συμφερόντων του υπευθύνου επεξεργασίας ή του τρίτου. Η στάθμιση των συμφερόντων πρέπει να πραγματοποιείται κατά περίπτωση, λαμβανομένων υπόψη στοιχείων όπως η σοβαρότητα της παραβίασης των δικαιωμάτων του υποκειμένου των δεδομένων ή ακόμη η ηλικία του υποκειμένου των δεδομένων, σε ορισμένες περιπτώσεις. Ωστόσο, στη συγκεκριμένη περίπτωση το ΔΕΕ δεν θεώρησε την άρνηση κοινοποίησης δικαιολογημένη απλώς και μόνο επειδή το υποκείμενο των δεδομένων ήταν ανήλικος.

Στην υπόθεση *ASNEF και FECEMD*, το ΔΕΕ αποφάνθηκε ρητώς επί της επεξεργασίας δεδομένων βάσει του νόμιμου λόγου των «έννομων συμφερόντων», ο οποίος προβλεπόταν τότε στο άρθρο 7 στοιχείο στ) της Οδηγίας για την Προστασία Δεδομένων ⁴⁰³.

Παράδειγμα: Στην υπόθεση *ASNEF και FECEMD* ⁴⁰⁴, το ΔΕΕ διευκρίνισε ότι το εθνικό δίκαιο δεν μπορεί να θεσπίζει επιπλέον προϋποθέσεις, για τη σύννομη επεξεργασία των δεδομένων, σε εκείνες που προβλέπονται στο άρθρο 7 στοιχείο στ) της οδηγίας ⁴⁰⁵. Επρόκειτο για περίπτωση στην οποία το ισπανικό δίκαιο για την προστασία δεδομένων περιείχε διάταξη βάσει της οποίας ιδιώτες τρίτοι μπορούσαν να προβάλουν έννομο συμφέρον στην επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνον εάν οι πληροφορίες είχαν ήδη περιληφθεί σε πηγές προσβάσιμες στο κοινό.

403 Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7 στοιχείο στ), πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο στ).

404 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado*, 24 Νοεμβρίου 2011.

405 Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7 στοιχείο στ), πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο στ).

Το ΔΕΕ επισήμανε κατ' αρχάς ότι σκοπός της οδηγίας 95/46 ⁴⁰⁶ είναι να καταστήσει ισοδύναμο σε όλα τα κράτη μέλη το επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Εξάλλου, η προσέγγιση των εφαρμοστέων στον τομέα αυτό εθνικών νομοθεσιών δεν πρέπει να οδηγήσει στην εξασθένηση της προστασίας που εξασφαλίζουν. Πρέπει, αντιθέτως, να έχει ως σκοπό την κατοχύρωση υψηλού επιπέδου προστασίας στην ΕΕ ⁴⁰⁷. Ως εκ τούτου, το ΔΕΕ αποφάνθηκε ότι «από τον σκοπό που συνίσταται στη διασφάλιση ισοδυνάμου επιπέδου προστασίας σε όλα τα κράτη μέλη προκύπτει ότι το άρθρο 7 της οδηγίας 95/46 ⁴⁰⁸ προβλέπει εξαντλητικό και περιοριστικό κατάλογο των περιπτώσεων κατά τις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να θεωρηθεί σύμφωνη». Επιπλέον, «τα κράτη μέλη δεν μπορούν ούτε να προσθέτουν νέες αρχές σχετικά με τη νομιμοποίηση επεξεργασιών δεδομένων προσωπικού χαρακτήρα στο άρθρο 7 της οδηγίας 95/46 ⁴⁰⁹ ούτε να προβλέπουν πρόσθετες απαιτήσεις που τροποποιούν το περιεχόμενο μιας εκ των έξι αρχών που προβλέπει» το άρθρο 7 ⁴¹⁰. Το ΔΕΕ έκανε δεκτό ότι, όσον αφορά τη στάθμιση που είναι απαραίτητη δυνάμει του άρθρου 7 στοιχείο στ) της οδηγίας 95/46/ΕΚ, είναι δυνατόν να ληφθεί υπόψη το γεγονός ότι η σοβαρότητα της προσβολής των θεμελιωδών δικαιωμάτων του προσώπου το οποίο αφορά η εν λόγω επεξεργασία μπορεί να ποικίλλει ανάλογα με το εάν τα επίδικα δεδομένα περιλαμβάνονται ήδη ή όχι σε προσβάσιμες στο κοινό πηγές.

Ωστόσο, το άρθρο 7 στοιχείο στ) της οδηγίας «απαγορεύει σε κράτος μέλος να αποκλείει κατηγορηματικώς και γενικώς τη δυνατότητα επεξεργασίας ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, χωρίς να επιτρέπει στάθμιση των οικείων αντιτιθεμένων δικαιωμάτων και συμφερόντων στο πλαίσιο συγκεκριμένης περιπτώσεως».

406 Πρώην Οδηγία για την Προστασία Δεδομένων, πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων.

407 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado*, 24 Νοεμβρίου 2011, σκέψη 28. Βλ. Οδηγία για την Προστασία Δεδομένων, αιτιολογικές σκέψεις 8 και 10.

408 Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7, πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο στ).

409 Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7, πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6.

410 Ό.π.

Λαμβανομένων υπόψη των περιστάσεων αυτών, το ΔΕΕ κατέληξε στο συμπέρασμα ότι το άρθρο 7 στοιχείο στ) της οδηγίας 95/46⁴¹¹ πρέπει να θεωρηθεί ότι «απαγορεύει εθνική νομοθεσία η οποία, ελλείψει της συγκαταθέσεως του ενδιαφερομένου προσώπου και για να επιτραπεί η επεξεργασία των δεδομένων προσωπικού χαρακτήρα η οποία είναι απαραίτητη για την επίτευξη του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος της επεξεργασίας αυτής ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα αυτά, απαιτεί, εκτός του σεβασμού των θεμελιωδών δικαιωμάτων και ελευθεριών του τελευταίου, τα εν λόγω δεδομένα να περιλαμβάνονται σε προσβάσιμες στο κοινό πηγές, αποκλείοντας έτσι κατηγορηματικώς και γενικώς οποιαδήποτε επεξεργασία δεδομένων που δεν περιλαμβάνονται σε αυτές τις πηγές»⁴¹².

Οσάκις τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία βάσει «νόμιμων λόγων», το φυσικό πρόσωπο έχει το δικαίωμα να εναντιωθεί ανά πάσα στιγμή στην επεξεργασία για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, σύμφωνα με το άρθρο 21 παράγραφος 1 του ΓΚΠΔ. Ο υπεύθυνος επεξεργασίας οφείλει να παύσει την επεξεργασία, εκτός εάν μπορεί να αποδείξει ότι συντρέχουν επιτακτικοί νόμιμοι λόγοι για τη συνέχισή της.

Όσον αφορά το **δίκαιο του Συμβουλίου της Ευρώπης**, παρόμοιες διατυπώσεις περιέχονται στην Εκσυγχρονισμένη Σύμβαση 108⁴¹³ και στις συστάσεις του Συμβουλίου της Ευρώπης. Στη σύσταση σχετικά με την κατάρτιση προφίλ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς κατάρτισης προφίλ αναγνωρίζεται ως νόμιμη εάν είναι αναγκαία για την προστασία των έννομων συμφερόντων άλλων, «εκτός εάν των συμφερόντων αυτών υπερισχύουν τα θεμελιώδη δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων»⁴¹⁴. Επιπλέον, η «προστασία των δικαιωμάτων και ελευθεριών άλλων» μνημονεύεται

411 Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7 στοιχείο στ), πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 1 στοιχείο στ).

412 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* και *Federación de Comercio Electrónico y Marketing Directo (FECEMD)* κατά *Administración del Estado*, 24 Νοεμβρίου 2011, σκέψεις 40, 44 και 48-49.

413 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 46.

414 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2010), *Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23 Νοεμβρίου 2010, άρθρο 3 παράγραφος 4 στοιχείο β) (σύσταση σχετικά με την κατάρτιση προφίλ).

στο άρθρο 8 παράγραφος 2 της ΕΣΔΑ ως ένας από τους νόμιμους λόγους περιορισμού του δικαιώματος στην προστασία δεδομένων.

Παράδειγμα: Στην υπόθεση *Υ κατά Τουρκίας*⁴¹⁵, ο προσφεύγων ήταν οροθετικός. Καθώς δεν είχε τις αισθήσεις του κατά την άφιξή του στο νοσοκομείο, το πλήρωμα του ασθενοφόρου ενημέρωσε το προσωπικό του νοσοκομείου ότι ήταν οροθετικός. Ο προσφεύγων υποστήριξε ενώπιον του ΕΔΔΑ ότι η κοινοποίηση της πληροφορίας αυτής συνιστούσε παραβίαση του δικαιώματος στον σεβασμό της ιδιωτικής του ζωής. Ωστόσο, λαμβανομένης υπόψη της αναγκαιότητας προστασίας της ασφάλειας του προσωπικού του νοσοκομείου, η γνωστοποίηση της πληροφορίας αυτής δεν θεωρήθηκε ότι συνιστά παραβίαση των δικαιωμάτων του.

4.1.2. Επεξεργασία ειδικών κατηγοριών δεδομένων (ευαίσθητα δεδομένα)

Στο **δίκαιο του Συμβουλίου της Ευρώπης** προβλέπεται ότι εναπόκειται στο εθνικό δίκαιο η θέσπιση κατάλληλων μέσων προστασίας για τη χρήση ευαίσθητων δεδομένων, εφόσον πληρούνται οι προϋποθέσεις του άρθρου 6 της Εκσυγχρονισμένης Σύμβασης 108, δηλαδή εάν οι κατάλληλες διασφαλίσεις οι οποίες συμπληρώνουν τις άλλες διατάξεις της Σύμβασης έχουν κατοχυρωθεί από τον νόμο. Στο **δίκαιο της ΕΕ**, το άρθρο 9 του ΓΚΠΔ προβλέπει λεπτομερές καθεστώς για την επεξεργασία ειδικών κατηγοριών δεδομένων (καλούμενα επίσης «ευαίσθητα δεδομένα») τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις και συμμετοχή σε συνδικαλιστική οργάνωση, για την επεξεργασία γενετικών και βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, καθώς και δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προανατολισμό. Η επεξεργασία ευαίσθητων δεδομένων καταρχήν απαγορεύεται⁴¹⁶.

Προβλέπεται, ωστόσο, εξαντλητικός κατάλογος εξαιρέσεων από την απαγόρευση αυτή, ο οποίος παρατίθεται στο άρθρο 9 παράγραφος 2 του ΓΚΠΔ και παρέχει νόμιμους λόγους για την επεξεργασία ευαίσθητων δεδομένων. Στις εξαιρέσεις αυτές περιλαμβάνονται περιπτώσεις στις οποίες:

⁴¹⁵ ΕΔΔΑ, *Υ κατά Τουρκίας*, προσφυγή αριθ. 648/10, 17 Φεβρουαρίου 2015.

⁴¹⁶ Πρώην Οδηγία για την Προστασία Δεδομένων, άρθρο 7 στοιχείο στ), πλέον Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 1.

- το υποκείμενο των δεδομένων συγκατατίθεται ρητώς στην επεξεργασία·
- η επεξεργασία πραγματοποιείται από μη κερδοσκοπικό φορέα με πολιτικούς, φιλοσοφικούς, θρησκευτικούς ή συνδικαλιστικούς σκοπούς, στο πλαίσιο των νόμιμων δραστηριοτήτων του, και αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του για τους σκοπούς αυτούς·
- η επεξεργασία αφορά δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων·
- η επεξεργασία είναι απαραίτητη:
 - για την εκπλήρωση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στο πλαίσιο της απασχόλησης, της κοινωνικής ασφάλισης και της κοινωνικής προστασίας·
 - για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου (όταν το υποκείμενο των δεδομένων δεν μπορεί να συγκατατεθεί)·
 - για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα·
 - για σκοπούς προληπτικής ή επαγγελματικής ιατρικής: «εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας»·
 - για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς·
 - για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, ή
 - για λόγους ουσιαστικού δημόσιου συμφέροντος·

Επομένως, για την επεξεργασία ειδικών κατηγοριών δεδομένων η ύπαρξη συμβατικής σχέσης με το υποκείμενο των δεδομένων δεν θεωρείται νομική βάση για τη σύννομη επεξεργασία ευαίσθητων δεδομένων, με εξαίρεση την περίπτωση σύμβασης με επαγγελματία του τομέα της υγείας με την επιφύλαξη της υποχρέωσης τήρησης επαγγελματικού απορρήτου ⁴¹⁷.

Ρητή συγκατάθεση του υποκειμένου των δεδομένων

Βάσει του **δικαίου της ΕΕ**, ο πρώτος λόγος στον οποίο μπορεί να βασιστεί η σύννομη επεξεργασία οποιωνδήποτε δεδομένων, ανεξάρτητα από το αν είναι ευαίσθητα ή μη, είναι η συγκατάθεση του υποκειμένου των δεδομένων. Στην περίπτωση ευαίσθητων δεδομένων, η συγκατάθεση αυτή πρέπει να παρέχεται ρητώς. Ωστόσο, το δίκαιο της ΕΕ ή των κρατών μελών μπορεί να προβλέπει ότι το υποκείμενο των δεδομένων δεν μπορεί να άρει την απαγόρευση της επεξεργασίας ειδικών κατηγοριών δεδομένων ⁴¹⁸. Αυτό θα μπορούσε να συμβεί, για παράδειγμα, όταν η επεξεργασία συνεπάγεται ασυνήθιστους κινδύνους για το υποκείμενο των δεδομένων.

Εργατικό δίκαιο ή δίκαιο κοινωνικής ασφάλισης και κοινωνικής προστασίας

Βάσει του **δικαίου της ΕΕ**, η απαγόρευση του άρθρου 9 παράγραφος 1 μπορεί να αρθεί αν η επεξεργασία είναι απαραίτητη για την εκπλήρωση υποχρεώσεων ή την άσκηση δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δικαιωμάτων στον τομέα της απασχόλησης ή της κοινωνικής ασφάλισης. Ωστόσο, η επεξεργασία πρέπει να επιτρέπεται από το δίκαιο της ΕΕ ή κράτους μέλους ή από συλλογική συμφωνία κατά το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων ⁴¹⁹. Τα αρχεία απασχόλησης που τηρεί ένας οργανισμός ενδέχεται να περιέχουν ευαίσθητα προσωπικά δεδομένα υπό ορισμένες προϋποθέσεις που προσδιορίζονται στον ΓΚΠΔ και στη σχετική εθνική νομοθεσία. Παραδείγματα ευαίσθητων δεδομένων μπορεί να είναι η συμμετοχή σε συνδικαλιστική οργάνωση ή πληροφορίες σχετικά με την υγεία.

417 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2 στοιχεία η) και θ).

418 Ό.π., άρθρο 9 παράγραφος 2 στοιχείο α).

419 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2 στοιχείο β).

Ζωτικά συμφέροντα του υποκειμένου των δεδομένων ή άλλου προσώπου

Βάσει του **δικαίου της ΕΕ**, όπως και στην περίπτωση των μη ευαίσθητων δεδομένων, τα ευαίσθητα δεδομένα μπορούν να υποβληθούν σε επεξεργασία για την εξυπηρέτηση των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου ⁴²⁰. Όταν η επεξεργασία βασίζεται στα ζωτικά συμφέροντα άλλου προσώπου, ο νόμιμος αυτός λόγος μπορεί να προβληθεί μόνο «εάν είναι πρόδηλο ότι η επεξεργασία δεν μπορεί να έχει άλλη νομική βάση» ⁴²¹. Σε ορισμένες περιπτώσεις, η επεξεργασία δεδομένων προσωπικού χαρακτήρα ενδέχεται να προστατεύει τόσο ατομικά, όσο και δημόσια συμφέροντα, για παράδειγμα, όταν η επεξεργασία είναι απαραίτητη για ανθρωπιστικούς σκοπούς ⁴²².

Προκειμένου να είναι η επεξεργασία ευαίσθητων δεδομένων σύμφωνη στη βάση αυτή, θα πρέπει να είναι αδύνατον να ζητηθεί η συγκατάθεση του υποκειμένου των δεδομένων επειδή, για παράδειγμα, το υποκείμενο των δεδομένων δεν είχε τις αισθήσεις του ή απουσίαζε και η επικοινωνία μαζί του δεν ήταν εφικτή. Με άλλα λόγια, το πρόσωπο δεν είχε τη σωματική ή τη νομική ικανότητα να παράσχει συγκατάθεση.

Φιλανθρωπικοί ή μη κερδοσκοπικοί φορείς

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται επίσης στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο. Ωστόσο, η προστασία πρέπει να αφορά αποκλειστικά τα μέλη ή πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του ⁴²³. Τα ευαίσθητα δεδομένα δεν μπορούν να κοινοποιηθούν εκτός των φορέων αυτών χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων.

⁴²⁰ Ό.π., άρθρο 9 παράγραφος 2 στοιχείο γ).

⁴²¹ Ό.π., αιτιολογική σκέψη 46.

⁴²² Ό.π.

⁴²³ Ό.π., άρθρο 9 παράγραφος 2 στοιχείο δ).

Δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων

Το άρθρο 9 παράγραφος 2 στοιχείο ε) του ΓΚΠΔ προβλέπει ότι η επεξεργασία δεν απαγορεύεται εάν αφορά δεδομένα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων. Παρότι η έννοια της φράσης «προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων» δεν ορίζεται στον κανονισμό, δεδομένου ότι αποτελεί εξαίρεση στην απαγόρευση επεξεργασίας ευαίσθητων δεδομένων, πρέπει να ερμηνεύεται αυστηρά και υπό την έννοια ότι το υποκείμενο των δεδομένων πρέπει να έχει εκούσια δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν. Επομένως, όταν η τηλεόραση μεταδίδει βίντεο προερχόμενο από κάμερα βιντεοεπιτήρησης στο οποίο φαίνεται, μεταξύ άλλων, ο τραυματισμός πυροσβέστη κατά την προσπάθεια εκκένωσης κτιρίου, δεν μπορεί να θεωρηθεί ότι ο πυροσβέστης δημοσιοποίησε προδήλως τα δεδομένα. Από την άλλη πλευρά, εάν ο πυροσβέστης αποφασίσει να περιγράψει το συμβάν και να δημοσιεύσει το βίντεο και φωτογραφίες σε δημόσια ιστοσελίδα, τότε πρόκειται για εκούσια, θετική ενέργεια δημοσιοποίησης των δεδομένων προσωπικού χαρακτήρα που τον αφορούν. Αξίζει να σημειωθεί ότι η δημοσιοποίηση δεδομένων δεν συνιστά συγκατάθεση, αλλά αποτελεί ένα άλλο είδος άδειας για την επεξεργασία ειδικών κατηγοριών δεδομένων.

Το γεγονός ότι το υποκείμενο των δεδομένων είχε δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία δεν απαλλάσσει τους υπευθύνους επεξεργασίας από τις υποχρεώσεις τους βάσει του δικαίου για την προστασία δεδομένων. Για παράδειγμα, η αρχή του περιορισμού του σκοπού εξακολουθεί να εφαρμόζεται στα δεδομένα προσωπικού χαρακτήρα, έστω και αν έχουν δημοσιοποιηθεί ⁴²⁴.

Νομικές αξιώσεις

Η επεξεργασία ειδικών κατηγοριών δεδομένων η οποία «είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων», είτε σε δικαστική διαδικασία είτε σε διοικητική ή εξωδικαστική διαδικασία ⁴²⁵, επιτρέπεται επίσης βάσει του ΓΚΠΔ ⁴²⁶. Στην περίπτωση αυτή, η επεξεργασία πρέπει να σχετίζεται με συγκεκρι-

424 Ομάδα εργασίας του άρθρου 29 (2013), *Opinion 3/13 on purpose limitation*, WP 203, Βρυξέλλες, 2 Απριλίου 2013, σ. 14.

425 Γενικός Κανονισμός για την Προστασία Δεδομένων, προοίμιο, αιτιολογική σκέψη 52.

426 Ό.π., άρθρο 9 παράγραφος 2 στοιχείο στ).

μένη νομική αξίωση, και την άσκηση αυτής ή την άμυνα κατά αυτής αντίστοιχα, και μπορεί να ζητηθεί από οποιονδήποτε από τους διαδίκους.

Όταν ενεργούν υπό τη δικαιοδοτική τους ιδιότητα, τα δικαστήρια μπορούν να επεξεργάζονται ειδικές κατηγορίες δεδομένων στο πλαίσιο της επίλυσης νομικής διαφοράς ⁴²⁷. Παραδείγματα τέτοιων ειδικών κατηγοριών δεδομένων, στο πλαίσιο αυτό, μπορούν να περιλαμβάνουν γενετικά δεδομένα για τη διαπίστωση της σχέσης γονέα-τέκνου ή κατάσταση της υγείας, όταν μέρος των αποδεικτικών στοιχείων αφορά λεπτομέρειες τραύματος που υπέστη το θύμα αξιόποινης πράξης.

Λόγοι ουσιαστικού δημόσιου συμφέροντος

Σύμφωνα με το άρθρο 9 παράγραφος 2 στοιχείο ζ) του ΓΚΠΔ, τα κράτη μέλη μπορούν να προβλέπουν περαιτέρω περιστάσεις στις οποίες μπορεί να επιτρέπεται η επεξεργασία ευαίσθητων δεδομένων, εφόσον:

- η επεξεργασία των δεδομένων είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος
- η επεξεργασία προβλέπεται από το ευρωπαϊκό ή το εθνικό δίκαιο·
- το ευρωπαϊκό ή το εθνικό δίκαιο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται το δικαίωμα στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων ⁴²⁸.

Χαρακτηριστικό παράδειγμα αποτελούν τα ηλεκτρονικά συστήματα ιατρικών φακέλων. Τα συστήματα αυτά καθιστούν εφικτή την παροχή δεδομένων που αφορούν την υγεία, τα οποία συλλέγονται από παρόχους υγειονομικής περίθαλψης στο πλαίσιο της θεραπείας ασθενούς, σε άλλους παρόχους υγειονομικής περίθαλψης του ίδιου ασθενούς σε ευρεία κλίμακα, συνήθως σε εθνικό επίπεδο.

Η Ομάδα εργασίας του άρθρου 29 κατέληξε στο συμπέρασμα ότι δεν ήταν δυνατή η δημιουργία τέτοιων συστημάτων βάσει των ισχυόντων νομικών

⁴²⁷ Ό.π.

⁴²⁸ Ό.π., άρθρο 9 παράγραφος 2 στοιχείο ζ).

κανόνων για την επεξεργασία δεδομένων των ασθενών ⁴²⁹. Ωστόσο, ηλεκτρονικά συστήματα ιατρικών φακέλων μπορούν να υπάρχουν εάν βασίζονται σε «λόγους ουσιαστικού δημόσιου συμφέροντος» ⁴³⁰. Για τη θέσπισή της, θα απαιτούνταν ρητή νομική βάση, η οποία θα περιλάμβανε τις αναγκαίες εγγυήσεις για την ασφαλή λειτουργία του συστήματος ⁴³¹.

Άλλοι λόγοι επεξεργασίας ευαίσθητων δεδομένων

Ο ΓΚΠΔ προβλέπει ότι η επεξεργασία ευαίσθητων δεδομένων επιτρέπεται όταν είναι απαραίτητη για ⁴³²:

- σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας
- λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυννοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή κράτους μέλους. Η ρύθμιση πρέπει να προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων του υποκειμένου των δεδομένων
- σκοπούς αρχειοθέτησης, επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς βάσει του δικαίου της Ένωσης ή κράτους μέλους. Η ρύθμιση πρέπει να είναι ανάλογη προς τον επιδιωκόμενο στόχο, να σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και να προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

429 Ομάδα εργασίας του άρθρου 29 (2007), Έγγραφο εργασίας σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία στο πλαίσιο των ηλεκτρονικών μητρώων υγείας (ΗΜΥ), WP 131, Βρυξέλλες, 15 Φεβρουαρίου 2007. Βλ. επίσης Γενικό Κανονισμό για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 3.

430 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2 στοιχείο ζ).

431 Ομάδα εργασίας του άρθρου 29 (2007), Έγγραφο εργασίας σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία στο πλαίσιο των ηλεκτρονικών μητρώων υγείας (ΗΜΥ), WP 131, Βρυξέλλες, 15 Φεβρουαρίου 2007.

432 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2 στοιχεία η), θ) και ι).

Πρόσθετες προϋποθέσεις βάσει του εθνικού δικαίου

Ο ΓΚΠΔ επιτρέπει επίσης στα κράτη μέλη να θεσπίζουν ή να διατηρούν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία⁴³³.

4.2. Κανόνες περί ασφάλειας της επεξεργασίας

Κύρια σημεία

- Οι κανόνες για την ασφάλεια της επεξεργασίας υποχρεώνουν τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποφυγή μη εξουσιοδοτημένης επέμβασης στις πράξεις επεξεργασίας δεδομένων.
- Το αναγκαίο επίπεδο ασφάλειας των δεδομένων καθορίζεται από:
 - τα χαρακτηριστικά ασφάλειας τα οποία είναι διαθέσιμα στην αγορά για κάθε συγκεκριμένο τύπο επεξεργασίας
 - το κόστος
 - τους κινδύνους που ενέχει η επεξεργασία των δεδομένων για τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
- Η διασφάλιση του απορρήτου των δεδομένων προσωπικού χαρακτήρα απορρέει από τη γενική αρχή που αναγνωρίζεται στον Γενικό Κανονισμό για την Προστασία Δεδομένων.

Βάσει τόσο του δικαίου της ΕΕ όσο και του δικαίου του Συμβουλίου της Ευρώπης, οι υπεύθυνοι επεξεργασίας υπέχουν γενική υποχρέωση διαφάνειας και λογοδοσίας όταν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα και, ιδίως, για παραβιάσεις δεδομένων, όταν σημειώνονται τέτοιες παραβιάσεις. Σε περίπτωση παραβιάσεων δεδομένων προσωπικού χαρακτήρα, οι υπεύθυνοι επεξεργασίας οφείλουν να ενημερώνουν τις εποπτικές αρχές, εκτός εάν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Τα υποκείμενα των δεδομένων θα πρέπει επίσης να

⁴³³ Ό.π., άρθρο 9 παράγραφος 2 στοιχείο η) και άρθρο 9 παράγραφος 4.

ενημερώνονται σχετικά με παραβίαση δεδομένων προσωπικού χαρακτήρα όταν αυτή ενδέχεται να θέσει σε μεγάλο κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

4.2.1. Στοιχεία ασφάλειας δεδομένων

Σύμφωνα με τις σχετικές διατάξεις του **δικαίου της ΕΕ**:

«Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων [...]»⁴³⁴.

Τα μέτρα αυτά περιλαμβάνουν, μεταξύ άλλων, τα εξής:

- ψευδωνυμοποίηση και κρυπτογράφηση δεδομένων προσωπικού χαρακτήρα ⁴³⁵.
- διασφάλιση του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας ⁴³⁶.
- αποκατάσταση της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση απώλειας δεδομένων ⁴³⁷.
- διαδικασία για τη δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των μέτρων για τη διασφάλιση της επεξεργασίας ⁴³⁸.

434 Ό.π., άρθρο 32 παράγραφος 1.

435 Ό.π., άρθρο 32 παράγραφος 1 στοιχείο α).

436 Ό.π., άρθρο 32 παράγραφος 1 στοιχείο β).

437 Ό.π., άρθρο 32 παράγραφος 1 στοιχείο γ).

438 Ό.π., άρθρο 32 παράγραφος 1 στοιχείο δ).

Παρόμοια διάταξη προβλέπεται στο **δίκαιο του Συμβουλίου της Ευρώπης**:

«Κάθε συμβαλλόμενος μεριμνά ώστε ο υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκτελών την επεξεργασία να λαμβάνει κατάλληλα μέτρα ασφάλειας κατά κινδύνων όπως η τυχαία ή μη εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και η καταστροφή, η απώλεια, η χρήση, η τροποποίηση ή η κοινολόγηση των δεδομένων αυτών»⁴³⁹.

Βάσει του **δικαίου της ΕΕ και του δικαίου του Συμβουλίου της Ευρώπης**, σε περίπτωση παραβίασης δεδομένων η οποία ενδέχεται να έχει αντίκτυπο στα δικαιώματα και στις ελευθερίες φυσικών προσώπων, ο υπεύθυνος επεξεργασίας υποχρεούται να ενημερώσει την εποπτική αρχή για την παραβίαση (βλ. [ενότητα 4.2.3](#)).

Σε αρκετές περιπτώσεις ισχύουν επίσης βιομηχανικά, εθνικά και διεθνή πρότυπα τα οποία έχουν αναπτυχθεί για την ασφαλή επεξεργασία των δεδομένων. Για παράδειγμα, η European Privacy Seal (σφραγίδα σεβασμού των προσωπικών δεδομένων, EuroPriSe) είναι ένα έργο της ΕΕ στον τομέα των διευρωπαϊκών δικτύων στις τηλεπικοινωνίες (Trans-European Telecommunications Networks), το οποίο διερευνά τις δυνατότητες πιστοποίησης προϊόντων, ιδίως λογισμικού, για τη διευκόλυνση της συμμόρφωσης με το ευρωπαϊκό δίκαιο για την προστασία δεδομένων. Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) συστάθηκε για τη βελτίωση της ικανότητας της ΕΕ, των κρατών μελών της ΕΕ και της επιχειρηματικής κοινότητας να προλαμβάνουν, να αντιμετωπίζουν και να αποκρίνονται σε προβλήματα ασφάλειας δικτύων και πληροφοριών⁴⁴⁰. Ο ENISA δημοσιεύει τακτικά αναλύσεις για τις τρέχουσες απειλές ασφάλειας, καθώς και συμβουλές για τους τρόπους αντιμετώπισής τους⁴⁴¹.

Η ασφάλεια των δεδομένων δεν επιτυγχάνεται μόνο με την ύπαρξη του κατάλληλου εξοπλισμού –υλισμικού και λογισμικού. Απαιτεί επίσης κατάλληλους εσωτερικούς κανόνες οργάνωσης. Οι εσωτερικοί αυτοί κανόνες θα αφορούν, στη βέλτιστη εκδοχή τους, τα ακόλουθα ζητήματα:

⁴³⁹ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 1.

⁴⁴⁰ Κανονισμός (ΕΕ) αριθ. 526/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013, σχετικά με τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) και την κατάργηση του κανονισμού (ΕΚ) αριθ. 460/2004 (ΕΕ L 165 της 18.6.2013, σ. 41).

⁴⁴¹ Για παράδειγμα, ENISA (2016), *Cyber Security and Resilience of smart cars. Good practices and recommendations*: ENISA (2016), *Security of Mobile Payments and Digital Wallets*.

- τακτική παροχή πληροφοριών σε όλους τους υπαλλήλους σχετικά με τους κανόνες περί ασφάλειας δεδομένων και τις υποχρεώσεις τους βάσει του δικαίου για την προστασία δεδομένων, ιδίως όσον αφορά τις υποχρεώσεις εμπιστευτικότητας
- σαφή κατανομή αρμοδιοτήτων και σαφή περιγραφή καθηκόντων σε θέματα επεξεργασίας δεδομένων, ιδίως όσον αφορά αποφάσεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα και διαβίβασης δεδομένων σε τρίτους ή σε υποκείμενα των δεδομένων
- χρήση δεδομένων προσωπικού χαρακτήρα μόνο σύμφωνα με τις εντολές του αρμόδιου προσώπου ή σύμφωνα με τους γενικούς κανόνες
- προστασία της πρόσβασης σε χώρους και σε υλισμικό και λογισμικό του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, συμπεριλαμβανομένων ελέγχων σχετικά με την εξουσιοδότηση πρόσβασης
- διασφάλιση της χορήγησης εξουσιοδοτήσεων πρόσβασης σε δεδομένα προσωπικού χαρακτήρα από το αρμόδιο πρόσωπο και απαίτηση κατάλληλης τεκμηρίωσης
- αυτοματοποιημένα πρωτόκολλα σχετικά με την ηλεκτρονική πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και τακτικοί έλεγχοι των εν λόγω πρωτοκόλλων από την εσωτερική υπηρεσία εποπτείας (ως εκ τούτου, όλες οι δραστηριότητες επεξεργασίας δεδομένων πρέπει να καταγράφονται)
- προσεκτική τεκμηρίωση άλλων μορφών κοινοποίησης, εκτός της αυτοματοποιημένης πρόσβασης σε δεδομένα, ώστε να αποδεικνύεται ότι δεν έχει σημειωθεί παράνομη διαβίβαση δεδομένων.

Η παροχή κατάλληλης κατάρτισης και εκπαίδευσης στα μέλη του προσωπικού σε θέματα ασφάλειας δεδομένων είναι επίσης σημαντικό στοιχείο των αποτελεσματικών προφυλάξεων ασφάλειας. Πρέπει επίσης να εφαρμόζονται ελεγκτικές διαδικασίες ώστε τα κατάλληλα μέτρα να μην υπάρχουν μόνο στη θεωρία, αλλά να εφαρμόζονται και να λειτουργούν στην πράξη (όπως εσωτερικοί ή εξωτερικοί έλεγχοι).

Στα μέτρα για τη βελτίωση του επιπέδου ασφάλειας που εξασφαλίζει ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία περιλαμβάνονται μέσα

όπως υπεύθυνοι προστασίας δεδομένων προσωπικού χαρακτήρα, εκπαίδευση των υπαλλήλων σε θέματα ασφάλειας, τακτικοί έλεγχοι, δοκιμές διείσδυσης και σφραγίδες ποιότητας.

Παράδειγμα: Στην υπόθεση *Ι κατά Φινλανδίας*⁴⁴², η προσφεύγουσα δεν ήταν σε θέση να αποδείξει ότι άλλοι υπάλληλοι του νοσοκομείου στο οποίο εργαζόταν είχαν αποκτήσει παράνομα πρόσβαση στον δικό της ιατρικό φάκελο. Επομένως, τα εθνικά δικαστήρια απέρριψαν την προσφυγή της περί παραβίασης του δικαιώματός της στην προστασία δεδομένων. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι υπήρξε παράβαση του άρθρου 8 της ΕΣΔΑ, επειδή το σύστημα καταχώρισης των ιατρικών φακέλων του νοσοκομείου «δεν έδινε τη δυνατότητα να διαπιστωθεί αναδρομικά η χρήση των φακέλων των ασθενών, δεδομένου ότι εμφάνιζε μόνο τις πέντε πιο πρόσφατες ιατρικές επισκέψεις, τα δε στοιχεία αυτά διαγράφονταν μόλις ο φάκελος επέστρεφε στο αρχείο». Καθοριστικός παράγοντας για το ΕΔΔΑ υπήρξε το γεγονός ότι το σύστημα αρχειοθέτησης που εφαρμοζόταν στο νοσοκομείο αντέβαινε σαφώς στις νομικές απαιτήσεις του εθνικού δικαίου, στοιχείο στο οποίο τα εθνικά δικαστήρια δεν είχαν δώσει τη δέουσα βαρύτητα.

Η ΕΕ έχει εκδώσει την οδηγία για την ασφάλεια των συστημάτων δικτύου και πληροφοριών⁴⁴³, η οποία είναι η πρώτη νομική πράξη σε επίπεδο ΕΕ για την ασφάλεια στον κυβερνοχώρο. Σκοπός της οδηγίας είναι, αφενός, η βελτίωση της ασφάλειας στον κυβερνοχώρο σε εθνικό επίπεδο και, αφετέρου, η αύξηση του επιπέδου συνεργασίας εντός της ΕΕ. Η οδηγία επιβάλλει επίσης υποχρεώσεις σε φορείς εκμετάλλευσης βασικών υπηρεσιών (συμπεριλαμβανομένων φορέων εκμετάλλευσης στους τομείς της ενέργειας, της υγείας, των τραπεζών, των μεταφορών, των ψηφιακών υποδομών κ.λπ.) και παρόχους ψηφιακών υπηρεσιών για τη διαχείριση των κινδύνων, τη διαφύλαξη της ασφάλειας των οικείων συστημάτων δικτύου και πληροφοριών και την αναφορά συμβάντων που αφορούν την ασφάλεια.

442 ΕΔΔΑ, *Ι κατά Φινλανδίας*, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008.

443 Οδηγία (ΕΕ) 2016/1148 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 6ης Ιουλίου 2016, σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση (ΕΕ L 194 της 19.7.2016, σ. 1).

Προοπτικές

Τον Σεπτέμβριο του 2017 η Ευρωπαϊκή Επιτροπή πρότεινε σχέδιο κανονισμού με σκοπό τη μεταρρύθμιση της εντολής του ENISA, προκειμένου να ληφθούν υπόψη οι νέες αρμοδιότητες και τα νέα καθήκοντα του Οργανισμού βάσει της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Σκοπός του προτεινόμενου κανονισμού είναι η διεύρυνση των καθηκόντων του ENISA και η ενίσχυση του ρόλου του ως «σημείου αναφοράς στο οικοσύστημα της ΕΕ για την ασφάλεια στον κυβερνοχώρο»⁴⁴⁴. Ο προτεινόμενος κανονισμός δεν θα πρέπει να θίγει τις αρχές του ΓΚΠΔ και, αποσαφηνίζοντας τα αναγκαία στοιχεία που συνθέτουν τα ευρωπαϊκά συστήματα πιστοποίησης της ασφάλειας στον κυβερνοχώρο, και επιπλέον θα πρέπει να ενισχύει την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Παράλληλα, τον Σεπτέμβριο του 2017 η Ευρωπαϊκή Επιτροπή πρότεινε σχέδιο εκτελεστικού κανονισμού για τον προσδιορισμό των στοιχείων που λαμβάνουν υπόψη οι πάροχοι ψηφιακών υπηρεσιών ώστε να διαφυλάσσουν την ασφάλεια των οικείων συστημάτων δικτύου και πληροφοριών, όπως προβλέπεται στο άρθρο 16 παράγραφος 8 της οδηγίας για την ασφάλεια των συστημάτων δικτύου και πληροφοριών. Κατά τον χρόνο σύνταξης του παρόντος εγχειριδίου, οι συζητήσεις σχετικά με τις δύο αυτές προτάσεις βρίσκονταν σε εξέλιξη.

4.2.2. Εμπιστευτικότητα

Στο δίκαιο της ΕΕ, ο ΓΚΠΔ αναγνωρίζει την εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο γενικής αρχής⁴⁴⁵. Οι πάροχοι διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών πρέπει να διασφαλίζουν την εμπιστευτικότητα. Υποχρεούνται επίσης να διαφυλάσσουν την ασφάλεια των υπηρεσιών τους⁴⁴⁶.

444 Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τον ENISA, τον «οργανισμό της ΕΕ για την ασφάλεια στον κυβερνοχώρο» και την κατάργηση του κανονισμού (ΕΕ) αριθ. 526/2013, καθώς και σχετικά με την πιστοποίηση της ασφάλειας στον κυβερνοχώρο στον τομέα της τεχνολογίας πληροφοριών και επικοινωνιών («πράξη για την ασφάλεια στον κυβερνοχώρο»), COM(2017) 477 της 13ης Σεπτεμβρίου 2017, σ. 6.

445 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 5 παράγραφος 1 στοιχείο στ).

446 Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, άρθρο 5 παράγραφος 1.

Παράδειγμα: Υπάλληλος ασφαλιστικής εταιρείας δέχεται τηλεφωνική κλήση στον χώρο εργασίας της από πρόσωπο που ισχυρίζεται ότι είναι πελάτης και ζητεί πληροφορίες σχετικά με το ασφαλιστήριο συμβόλαιό του.

Η υποχρέωση τήρησης του απορρήτου των δεδομένων του πελάτη επιβάλλει στην υπάλληλο να εφαρμόσει τουλάχιστον κάποια ελάχιστα μέτρα ασφάλειας προτού κοινοποιήσει δεδομένα προσωπικού χαρακτήρα. Αυτό μπορεί να το κάνει, για παράδειγμα, προτείνοντας στον πελάτη να τον καλέσει σε αριθμό τηλεφώνου ο οποίος είναι καταχωρισμένος στον φάκελό του.

Σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο στ), τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»).

Δυνάμει του άρθρου 32 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία οφείλουν να εφαρμόζουν τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται υψηλό επίπεδο ασφάλειας. Τα μέτρα αυτά περιλαμβάνουν, μεταξύ άλλων, την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα, τη δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας της επεξεργασίας σε συνεχή βάση, την αξιολόγηση και τη δοκιμή της αποτελεσματικότητας των μέτρων και τη δυνατότητα αποκατάστασης της επεξεργασίας σε περίπτωση φυσικού ή τεχνικού συμβάντος. Επιπλέον, η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης μπορεί να χρησιμοποιηθεί ως στοιχείο για να αποδειχθεί η συμμόρφωση προς την αρχή της ακεραιότητας και της εμπιστευτικότητας. Εξάλλου, σύμφωνα με το άρθρο 28 του ΓΚΠΔ, η σύμβαση που συνδέει τον υπεύθυνο επεξεργασίας με τον εκτελούντα την επεξεργασία πρέπει να προβλέπει ότι ο εκτελών την επεξεργασία θα διασφαλίσει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα εκ του νόμου υποχρέωση τήρησης εμπιστευτικότητας.

Η υποχρέωση εμπιστευτικότητας δεν εκτείνεται σε καταστάσεις στις οποίες τα δεδομένα περιέρχονται σε γνώση προσώπου υπό την ιδιότητά του ως ιδιώτη και όχι ως υπαλλήλου του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Στην περίπτωση αυτή, τα άρθρα 32 και 28 του ΓΚΠΔ δεν εφαρμόζονται, καθώς η χρήση δεδομένων προσωπικού χαρακτήρα από ιδιώτες εξαιρείται πλήρως από το πεδίο εφαρμογής του κανονισμού όταν η εν λόγω χρήση εμπίπτει εντός των ορίων της λεγόμενης εξαίρεσης λόγω οικιακής δραστηριότητας ⁴⁴⁷. Η εξαίρεση λόγω οικιακής δραστηριότητας αφορά τη χρήση δεδομένων προσωπικού χαρακτήρα «από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας» ⁴⁴⁸. Ωστόσο, μετά την απόφαση του ΔΕΕ στην υπόθεση *Bodil Lindqvist* ⁴⁴⁹, η εξαίρεση αυτή πρέπει να ερμηνεύεται συσταλτικά, ιδίως όσον αφορά την κοινοποίηση δεδομένων. Ειδικότερα, η εξαίρεση λόγω οικιακής δραστηριότητας δεν θα εκτείνεται στη δημοσιοποίηση δεδομένων προσωπικού χαρακτήρα σε απεριόριστο αριθμό αποδεκτών στο διαδίκτυο ούτε στην επεξεργασία δεδομένων που έχει επαγγελματικές ή εμπορικές πτυχές (για περισσότερες πληροφορίες σχετικά με την υπόθεση, βλ. [ενότητες 2.1.2, 2.2.2 και 2.3.1](#)).

Η «εμπιστευτικότητα των επικοινωνιών» είναι μια άλλη πτυχή της εμπιστευτικότητας, η οποία ρυθμίζεται από *lex specialis*. Οι ειδικοί κανόνες για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών βάσει της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες επιβάλλουν στα κράτη μέλη να απαγορεύουν την ακρόαση, την υποκλοπή, την αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών μεταδεδομένων από πρόσωπα πλην των χρηστών ή χωρίς τη συγκατάθεση των χρηστών ⁴⁵⁰. Το εθνικό δίκαιο μπορεί να επιτρέπει εξαιρέσεις από την αρχή αυτή μόνο για λόγους εθνικής ασφάλειας, άμυνας, πρόληψης ή ανίχνευσης εγκλημάτων, και μόνο εάν τα μέτρα αυτά είναι αναγκαία και ανάλογα προς τους επιδιωκόμενους σκοπούς ⁴⁵¹. Οι ίδιοι κανόνες θα ισχύουν στο πλαίσιο του μελλοντικού κανονισμού για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, αλλά το πεδίο εφαρμογής της νομικής πράξης για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θα επεκταθεί πέραν των διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ώστε να καλύπτει επίσης τις επικοινωνίες που πραγματοποιούνται μέσω υπηρεσιών που παρέχονται

447 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 2 παράγραφος 2 στοιχείο γ).

448 Ό.π.

449 ΔΕΕ, C-101/01, *Ποινική δίκη κατά Bodil Lindqvist*, 6 Νοεμβρίου 2003.

450 Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, άρθρο 5 παράγραφος 1.

451 Ό.π., άρθρο 15 παράγραφος 1.

επιπροσθέτως από τον προμηθευτή, δηλαδή υπηρεσίες ΟΤΤ (όπως κινητές εφαρμογές).

Στο δίκαιο του Συμβουλίου της Ευρώπης, η υποχρέωση εμπιστευτικότητας εντάσσεται στην έννοια της ασφάλειας δεδομένων του άρθρου 7 παράγραφος 1 της Εκσυγχρονισμένης Σύμβασης 108, το οποίο αφορά την ασφάλεια των δεδομένων.

Για τους εκτελούντες την επεξεργασία, εμπιστευτικότητα σημαίνει ότι δεν μπορούν να κοινοποιούν τα δεδομένα σε τρίτους ή άλλους αποδέκτες χωρίς εξουσιοδότηση. Για τους υπαλλήλους του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, η εμπιστευτικότητα επιβάλλει να χρησιμοποιούν τα δεδομένα προσωπικού χαρακτήρα μόνο σύμφωνα με τις εντολές των αρμόδιων προϊσταμένων τους.

Η υποχρέωση εμπιστευτικότητας πρέπει να περιλαμβάνεται σε κάθε σύμβαση που συνάπτεται μεταξύ των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία για λογαριασμό τους. Επιπλέον, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία θα πρέπει να λαμβάνουν ειδικά μέτρα για να θεσπίζουν νομική υποχρέωση τήρησης της εμπιστευτικότητας για τους υπαλλήλους τους, το οποίο επιτυγχάνεται συνήθως με την ενσωμάτωση ρητρών εμπιστευτικότητας στη σύμβαση απασχόλησης του υπαλλήλου.

Η αθέτηση της επαγγελματικής υποχρέωσης τήρησης εμπιστευτικότητας είναι αξιόποινη πράξη σε πολλά κράτη μέλη της ΕΕ και συμβαλλόμενα μέρη της Σύμβασης 108.

4.2.3. Γνωστοποιήσεις παραβίασης δεδομένων προσωπικού χαρακτήρα

Η παραβίαση δεδομένων προσωπικού χαρακτήρα αφορά παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση δεδομένων προσωπικού χαρακτήρα ή πρόσβαση σε αυτά κατά την επεξεργασία ⁴⁵². Παρότι νέες τεχνολογίες, όπως η κρυπτογράφηση, παρέχουν πλέον περισσότερες δυνατότητες για την εγγύηση της ασφάλειας της επεξεργα-

⁴⁵² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 4 σημείο 12· βλ. επίσης Ομάδα εργασίας του άρθρου 29 (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3 Οκτωβρίου 2017, σ. 8.

σίας, οι παραβιάσεις των δεδομένων παραμένουν σύνθετες φαινόμενο. Τα αίτια των παραβιάσεων μπορούν να ποικίλλουν, από τυχαία σφάλματα των προσώπων που εργάζονται σε έναν οργανισμό έως εξωτερικές απειλές, όπως χάκερ ή εγκληματικές οργανώσεις που δραστηριοποιούνται στον κυβερνοχώρο.

Οι παραβιάσεις των δεδομένων μπορεί να είναι ιδιαίτερα επιζήμιες σε ό,τι αφορά τα δικαιώματα στην ιδιωτική ζωή και στην προστασία των δεδομένων των φυσικών προσώπων, τα οποία λόγω της παραβίασης χάνουν τον έλεγχο των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Οι παραβιάσεις ενδέχεται να οδηγήσουν σε υποκλοπή ταυτότητας ή απάτη, οικονομική απώλεια ή υλική ζημία, απώλεια της εμπιστευτικότητας δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο και ζημία στη φήμη του υποκειμένου των δεδομένων. Στις κατευθυντήριες γραμμές σχετικά με τη γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα βάσει του κανονισμού 2016/679, η Ομάδα εργασίας του άρθρου 29 εξηγεί ότι οι παραβιάσεις μπορεί να έχουν τριών ειδών επιπτώσεις στα δεδομένα προσωπικού χαρακτήρα: κοινοποίηση, απώλεια και/ή μεταβολή⁴⁵³. Επιπροσθέτως της υποχρέωσης λήψης μέτρων ώστε να επιτευχθεί η ασφάλεια της επεξεργασίας, όπως αναλύεται στην **ενότητα 4.2**, είναι εξίσου σημαντικό να διασφαλίζεται ότι, όταν σημειώνονται παραβιάσεις, οι υπεύθυνοι επεξεργασίας τις αντιμετωπίζουν κατάλληλα και έγκαιρα.

Οι εποπτικές αρχές και τα φυσικά πρόσωπα συχνά δεν γνωρίζουν ότι έχει σημειωθεί παραβίαση δεδομένων, με αποτέλεσμα τα φυσικά πρόσωπα να μη λαμβάνουν μέτρα για να προστατευθούν από τις αρνητικές συνέπειές της. Για την κατοχύρωση των δικαιωμάτων των φυσικών προσώπων και τον περιορισμό των επιπτώσεων των παραβιάσεων των δεδομένων, **η ΕΕ και το Συμβούλιο της Ευρώπης** επιβάλλουν, σε ορισμένες περιπτώσεις, στους υπευθύνους επεξεργασίας υποχρέωση γνωστοποίησης.

Στο πλαίσιο της Εκσυγχρονισμένης Σύμβασης 108 του **Συμβουλίου της Ευρώπης**, τα συμβαλλόμενα μέρη οφείλουν, τουλάχιστον, να υποχρεώνουν τους υπευθύνους επεξεργασίας να γνωστοποιούν στην αρμόδια εποπτική αρχή παραβιάσεις δεδομένων οι οποίες ενδέχεται να συνιστούν σοβαρή επέμβαση στα δικαιώματα των υποκειμένων των δεδομένων. Η γνωστοποίηση αυτή θα πρέπει να πραγματοποιείται «αμελλητί»⁴⁵⁴.

453 Ομάδα εργασίας του άρθρου 29 (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3 Οκτωβρίου 2017, σ. 6.

454 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 7 παράγραφος 2· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημεία 64-66.

Το **δίκαιο της ΕΕ** θεσπίζει λεπτομερές καθεστώς το οποίο ρυθμίζει τον χρόνο και το περιεχόμενο των γνωστοποιήσεων ⁴⁵⁵. Σύμφωνα με αυτό, οι υπεύθυνοι επεξεργασίας οφείλουν να γνωστοποιούν ορισμένες παραβιάσεις δεδομένων στις εποπτικές αρχές αμελλητί και, εάν είναι εφικτό, εντός 72 ωρών από τη στιγμή που έλαβαν γνώση της παραβίασης. Εάν δεν πραγματοποιηθεί εντός 72 ωρών, η γνωστοποίηση πρέπει να συνοδεύεται από αιτιολόγηση για την καθυστέρηση. Οι υπεύθυνοι επεξεργασίας απαλλάσσονται από την απαίτηση γνωστοποίησης μόνο όταν είναι σε θέση να αποδείξουν ότι η παραβίαση των δεδομένων δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των ενδιφερόμενων φυσικών προσώπων.

Στον κανονισμό προσδιορίζονται οι ελάχιστες πληροφορίες οι οποίες πρέπει να περιλαμβάνονται στη γνωστοποίηση ώστε να μπορεί η εποπτική αρχή να λάβει τα αναγκαία μέτρα ⁴⁵⁶. Στη γνωστοποίηση πρέπει να περιλαμβάνονται, τουλάχιστον, περιγραφή της φύσης της παραβίασης των δεδομένων και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων δεδομένων, καθώς και περιγραφή των ενδεχόμενων συνεπειών της παραβίασης και των μέτρων που εφαρμόζει ο υπεύθυνος επεξεργασίας για την αντιμετώπιση και την άμβλυνση των συνεπειών της. Επιπλέον, θα πρέπει να παρέχονται το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας ώστε η εποπτική αρχή να μπορεί να εξασφαλίσει περισσότερες πληροφορίες, εφόσον απαιτηθεί.

Εάν η παραβίαση δεδομένων ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, οι υπεύθυνοι επεξεργασίας οφείλουν να ενημερώσουν αμελλητί τα εν λόγω φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) για την παραβίαση ⁴⁵⁷. Οι πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων, συμπεριλαμβανομένης της περιγραφής της παραβίασης δεδομένων, πρέπει να συντάσσονται σε απλή και σαφή γλώσσα και να περιλαμβάνουν πληροφορίες παρόμοιες με εκείνες που απαιτούνται για τις γνωστοποιήσεις στις εποπτικές αρχές. Σε ορισμένες περιπτώσεις, οι υπεύθυνοι επεξεργασίας ενδέχεται να απαλλάσσονται από την υποχρέωση γνωστοποίησης τέτοιων παραβιάσεων στα υποκείμενα των δεδομένων. Εξαιρέσεις ισχύουν όταν ο υπεύθυνος επεξεργασίας έχει υιοθετήσει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά είχαν εφαρμοστεί στα επηρεαζόμενα

455 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 33 και 34.

456 Ό.π., άρθρο 33 παράγραφος 3.

457 Ό.π., άρθρο 34.

από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση. Η λήψη μέτρων από τον υπεύθυνο επεξεργασίας μετά την παραβίαση, προκειμένου να διασφαλιστεί ότι δεν είναι πλέον πιθανό να προκύψει βλάβη για τα δικαιώματα των υποκειμένων των δεδομένων, μπορεί επίσης να απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωση γνωστοποίησης στα υποκείμενα των δεδομένων. Τέλος, εάν η γνωστοποίηση συνεπάγεται υπέρμετρη προσπάθεια εκ μέρους του υπευθύνου επεξεργασίας, τα υποκείμενα των δεδομένων μπορούν να ενημερωθούν για την παραβίαση με άλλα μέσα, όπως δημόσια ανακοίνωση ή άλλα παρόμοια μέτρα ⁴⁵⁸.

Η υποχρέωση γνωστοποίησης παραβιάσεων δεδομένων στις εποπτικές αρχές και στα υποκείμενα των δεδομένων αφορά τους υπευθύνους επεξεργασίας. Ωστόσο, παραβιάσεις των δεδομένων μπορεί να σημειωθούν ανεξάρτητα από το αν η επεξεργασία πραγματοποιείται από υπεύθυνο επεξεργασίας ή από εκτελούντα την επεξεργασία. Για τον λόγο αυτό, είναι σημαντικό να διασφαλίζεται ότι και οι εκτελούντες την επεξεργασία υποχρεούνται να αναφέρουν τις παραβιάσεις δεδομένων. Στην περίπτωση αυτή, οφείλουν να γνωστοποιήσουν αμελλητί τις παραβιάσεις των δεδομένων στον υπεύθυνο επεξεργασίας ⁴⁵⁹. Στη συνέχεια, ο υπεύθυνος επεξεργασίας φέρει την ευθύνη της ενημέρωσης των εποπτικών αρχών και των επηρεαζόμενων υποκειμένων των δεδομένων, σύμφωνα με τους προαναφερθέντες κανόνες και εντός του προαναφερθέντος χρονικού πλαισίου.

4.3. Κανόνες περί λογοδοσίας και προώθησης της συμμόρφωσης

Κύρια σημεία

- Προκειμένου να διασφαλίζεται η λογοδοσία στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία οφείλουν να τηρούν αρχεία των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνοι και να τα παρέχουν στις εποπτικές αρχές, κατόπιν αιτήματός τους.

458 Ό.π., άρθρο 34 παράγραφος 3 στοιχείο γ).

459 Ό.π., άρθρο 33 παράγραφος 2.

- Ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει διάφορα μέσα για την προώθηση της συμμόρφωσης:
 - τον διορισμό υπευθύνων προστασίας δεδομένων σε ορισμένες περιπτώσεις
 - τη διενέργεια εκτίμησης αντικτύπου πριν από την έναρξη των δραστηριοτήτων επεξεργασίας οι οποίες ενδέχεται να προκαλέσουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων·
 - προηγούμενη διαβούλευση με την αρμόδια εποπτική αρχή, εάν από την εκτίμηση αντικτύπου προκύπτει ότι η επεξεργασία συνεπάγεται κινδύνους οι οποίοι δεν μπορούν να μετριαστούν·
 - κώδικες δεοντολογίας για υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία για τον προσδιορισμό της εφαρμογής του κανονισμού σε διάφορους τομείς επεξεργασίας
 - μηχανισμούς πιστοποίησης, σφραγίδες και σήματα.
- Το δίκαιο του Συμβουλίου της Ευρώπης προτείνει παρόμοια μέσα για την προώθηση της συμμόρφωσης στην Εκσυγχρονισμένη Σύμβαση 108.

Η αρχή της λογοδοσίας είναι ιδιαίτερα σημαντική για τη διασφάλιση της επιβολής των κανόνων περί προστασίας δεδομένων στην Ευρώπη. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση προς τους κανόνες περί προστασίας δεδομένων. Η λογοδοσία δεν θα πρέπει να ενεργοποιείται μόνο μετά την παράβαση. Αντιθέτως, οι υπεύθυνοι επεξεργασίας έχουν την υποχρέωση να εφαρμόζουν προληπτικά κατάλληλες πολιτικές διαχείρισης δεδομένων σε όλα τα στάδια της επεξεργασίας. Το ευρωπαϊκό δίκαιο για την προστασία των δεδομένων επιβάλλει στους υπευθύνους επεξεργασίας να εφαρμόζουν τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζουν, και να είναι σε θέση να αποδείξουν, ότι η επεξεργασία πραγματοποιείται σύννομα. Στα μέτρα αυτά συγκαταλέγονται ο διορισμός υπευθύνων προστασίας δεδομένων, η τήρηση αρχείων και τεκμηρίωσης που σχετίζονται με την επεξεργασία και η διενέργεια εκτιμήσεων αντικτύπου στην προστασία της ιδιωτικής ζωής.

4.3.1. Υπεύθυνοι προστασίας δεδομένων

Οι υπεύθυνοι προστασίας δεδομένων (ΥΠΔ) είναι πρόσωπα τα οποία παρέχουν συμβουλές σχετικά με τη συμμόρφωση προς τους κανόνες περί προστασίας δεδομένων σε οργανισμούς που πραγματοποιούν επεξεργασία δεδομένων. Αποτελούν «ακρογωνιαίο λίθο λογοδοσίας», καθώς διευκολύνουν τη συμμόρφωση,

ενώ ενεργούν επίσης ως ενδιάμεσοι μεταξύ των εποπτικών αρχών, των υποκειμένων των δεδομένων και του οργανισμού που τους διόρισε.

Στο δίκαιο του Συμβουλίου της Ευρώπης, το άρθρο 10 παράγραφος 1 της Εκσυγχρονισμένης Σύμβασης 108 προβλέπει γενική υποχρέωση λογοδοσίας των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία. Σύμφωνα με αυτή, επιβάλλεται στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία να λαμβάνουν κάθε κατάλληλο μέτρο προκειμένου να συμμορφώνονται προς τους κανόνες περί προστασίας δεδομένων που προβλέπονται στη Σύμβαση, και να είναι σε θέση να αποδείξουν ότι η επεξεργασία που πραγματοποιείται υπό τον έλεγχό τους συμμορφώνεται προς τις διατάξεις της Σύμβασης. Παρότι η Σύμβαση δεν προσδιορίζει τα συγκεκριμένα μέτρα τα οποία θα πρέπει να θεσπίσουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία, στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται ότι ο διορισμός ΥΠΔ είναι ένα ενδεχόμενο μέτρο που συμβάλλει στην απόδειξη της συμμόρφωσης. Στους ΥΠΔ θα πρέπει να παρέχονται όλα τα αναγκαία μέσα για την εκπλήρωση της εντολής τους ⁴⁶⁰.

Εν αντιθέσει προς ό,τι ισχύει στο δίκαιο του Συμβουλίου της Ευρώπης, **στο δίκαιο της ΕΕ**, ο διορισμός ΥΠΔ δεν εναπόκειται πάντοτε στη διακριτική ευχέρεια των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία, αλλά είναι υποχρεωτικός σε ορισμένες περιπτώσεις. Ο ΓΚΠΔ αναγνωρίζει ότι ο ΥΠΔ διαδραματίζει καίριο ρόλο στο νέο σύστημα διακυβέρνησης και προβλέπει λεπτομερείς διατάξεις σχετικά με τον διορισμό, τη θέση, τις υποχρεώσεις και τα καθήκοντα του υπευθύνου ⁴⁶¹.

Ο ΓΚΠΔ καθιστά υποχρεωτικό τον διορισμό ΥΠΔ σε τρεις συγκεκριμένες περιπτώσεις: όταν η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα· όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή όταν οι βασικές δραστηριότητες συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα ⁴⁶². Αν και όροι όπως «συστηματική παρακολούθηση σε μεγάλη κλίμακα» και «βασικές δραστηριότητες» δεν

⁴⁶⁰ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 87.

⁴⁶¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 37 έως 39.

⁴⁶² Ό.π., άρθρο 37 παράγραφος 1.

ορίζονται στον κανονισμό, η Ομάδα εργασίας του άρθρου 29 εξέδωσε κατευθυντήριες γραμμές σχετικά με τον τρόπο ερμηνείας τους ⁴⁶³.

Παράδειγμα: Οι εταιρείες μέσων κοινωνικής δικτύωσης και οι μηχανές αναζήτησης πιθανότατα θεωρούνται υπεύθυνοι επεξεργασίας των οποίων οι πράξεις επεξεργασίας απαιτούν την τακτική και συστηματική παρακολούθηση υποκειμένων δεδομένων σε μεγάλη κλίμακα. Το επιχειρηματικό μοντέλο τέτοιων εταιρειών βασίζεται στην επεξεργασία μεγάλων ποσοτήτων δεδομένων προσωπικού χαρακτήρα· οι εταιρείες αυτές αποκομίζουν σημαντικά έσοδα προσφέροντας στοχευμένες διαφημιστικές υπηρεσίες και παρέχοντας τη δυνατότητα σε άλλες εταιρείες να διαφημίζονται στους ιστότοπούς τους. Η στοχευμένη διαφήμιση βασίζεται σε δημογραφικά στοιχεία και στο ιστορικό αγорών ή στην προηγούμενη αγοραστική συμπεριφορά των καταναλωτών. Επομένως, απαιτεί τη συστηματική παρακολούθηση των συνηθειών και της συμπεριφοράς των υποκειμένων των δεδομένων στο διαδίκτυο.

Παράδειγμα: Ένα νοσοκομείο και μια ασφαλιστική εταιρεία υγειονομικής περίθαλψης αποτελούν χαρακτηριστικά παραδείγματα υπευθύνων επεξεργασίας των οποίων οι δραστηριότητες συνίστανται σε μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Τα δεδομένα που αποκαλύπτουν πληροφορίες σχετικά με την υγεία φυσικού προσώπου συνιστούν ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα βάσει τόσο του δικαίου του Συμβουλίου της Ευρώπης, όσο και του δικαίου της ΕΕ και, επομένως, χρήζουν αυξημένης προστασίας. Το δίκαιο της ΕΕ αναγνωρίζει επίσης ως ειδικές κατηγορίες τα γενετικά και τα βιομετρικά δεδομένα. Στο μέτρο που νοσοκομειακά ιδρύματα και ασφαλιστικές εταιρείες επεξεργάζονται τέτοια δεδομένα σε μεγάλη κλίμακα, υποχρεούνται βάσει του ΓΚΠΔ να διορίζουν ΥΠΔ.

Επιπλέον, το άρθρο 37 παράγραφος 4 του ΓΚΠΔ προβλέπει ότι, σε περιπτώσεις άλλες πλην των τριών υποχρεωτικών περιπτώσεων του άρθρου 37 παράγραφος 1, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων

⁴⁶³ Ομάδα εργασίας του άρθρου 29 (2017), *Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων*, WP 243 rev.01, όπως αναθεωρήθηκαν τελευταία και εκδόθηκαν στις 5 Απριλίου 2017.

την επεξεργασία μπορούν να ορίζουν ΥΠΔ ή, όπου απαιτείται από το δίκαιο της Ένωσης ή του κράτους μέλους, θα ορίζουν υποχρεωτικά ΥΠΔ.

Όλοι οι υπόλοιποι οργανισμοί δεν υποχρεούνται από τον νόμο να διορίζουν ΥΠΔ. Ωστόσο, ο ΓΚΠΔ προβλέπει ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία μπορούν να επιλέξουν να διορίσουν οικειοθελώς ΥΠΔ, ενώ προβλέπει επίσης τη δυνατότητα των κρατών μελών να καταστήσουν τον ορισμό αυτό υποχρεωτικό για περισσότερα είδη οργανισμών από τα προβλεπόμενα στον κανονισμό ⁴⁶⁴.

Όταν ο υπεύθυνος επεξεργασίας διορίσει ΥΠΔ, πρέπει να διασφαλίσει ότι ο εν λόγω υπεύθυνος προστασίας δεδομένων θα «συμμετέχει δεόντως και εγκαίρως σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα» εντός του οργανισμού ⁴⁶⁵. Για παράδειγμα, ο ΥΠΔ θα πρέπει να συμμετέχει στην παροχή συμβουλών σχετικά με τη διενέργεια εκτιμήσεων αντικτύπου για την προστασία δεδομένων καθώς και στη δημιουργία και στην τήρηση αρχείων των δραστηριοτήτων επεξεργασίας στον οργανισμό. Για να μπορούν οι ΥΠΔ να εκτελούν αποτελεσματικά τα καθήκοντά τους, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία οφείλουν να τους παρέχουν τους αναγκαίους πόρους, συμπεριλαμβανομένων οικονομικών πόρων, υποδομών και εξοπλισμού. Άλλες απαιτήσεις περιλαμβάνουν την παροχή στους ΥΠΔ επαρκούς χρόνου για την εκτέλεση των καθηκόντων τους καθώς και συνεχούς κατάρτισης ώστε να μπορούν να αναπτύσσουν την εμπειρογνωμοσύνη τους και να είναι ενήμεροι για όλες τις εξελίξεις στο δίκαιο της προστασίας δεδομένων ⁴⁶⁶.

Ο ΓΚΠΔ θεσπίζει ορισμένες βασικές εγγυήσεις ώστε να διασφαλίζεται ότι οι ΥΠΔ θα ενεργούν ανεξάρτητα. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία πρέπει να φροντίζουν ώστε, κατά την άσκηση των καθηκόντων τους που σχετίζονται με την προστασία δεδομένων, οι ΥΠΔ να μη λαμβάνουν εντολές από την εταιρεία, συμπεριλαμβανομένων προσώπων που ανήκουν στο ανώτατο διοικητικό επίπεδο. Επιπλέον, δεν πρέπει να απολύονται ούτε να υφίστανται κυρώσεις με οποιονδήποτε τρόπο επειδή επιτέλεσαν τα καθήκοντά τους ⁴⁶⁷. Για παράδειγμα, ΥΠΔ συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον

464 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 37 παράγραφοι 3 και 4.

465 Ό.π., άρθρο 38 παράγραφος 1.

466 Ομάδα εργασίας του άρθρου 29 (2017), *Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων*, WP 243 γεν.01, όπως αναθεωρήθηκαν τελευταία και εκδόθηκαν στις 5 Απριλίου 2017, σημείο 3.1.

467 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 38 παράγραφοι 2 και 3.

εκτελούντα την επεξεργασία να διενεργήσει εκτίμηση αντικτύπου στην προστασία των δεδομένων επειδή θεωρεί ότι είναι πιθανό η επεξεργασία να έχει ως αποτέλεσμα υψηλό κίνδυνο για τα υποκείμενα των δεδομένων. Η εταιρεία διαφωνεί με τη συμβουλή του ΥΠΔ, δεν θεωρεί ότι είναι βάσιμη και, ως εκ τούτου, αποφασίζει να μη διενεργήσει εκτίμηση αντικτύπου. Η εταιρεία μπορεί να αγνοήσει τη συμβουλή, αλλά δεν μπορεί να απολύσει τον ΥΠΔ ούτε να του επιβάλει κυρώσεις για τη συμβουλή του.

Τέλος, τα καθήκοντα και οι υποχρεώσεις του ΥΠΔ περιγράφονται λεπτομερώς στο άρθρο 39 του ΓΚΠΔ. Σε αυτά περιλαμβάνονται οι απαιτήσεις να ενημερώνει και να συμβουλεύει τις εταιρείες και τους υπαλλήλους που πραγματοποιούν την επεξεργασία για τις υποχρεώσεις τους βάσει της νομοθεσίας και να παρακολουθεί τη συμμόρφωση προς τους ενωσιακούς και εθνικούς κανόνες περί προστασίας δεδομένων, διενεργώντας ελέγχους και παρέχοντας κατάρτιση στο προσωπικό που συμμετέχει σε πράξεις επεξεργασίας. Ο ΥΠΔ πρέπει να συνεργάζεται επίσης με την εποπτική αρχή και να ενεργεί ως σημείο επικοινωνίας με αυτήν σε θέματα σχετικά με την επεξεργασία δεδομένων, όπως, για παράδειγμα, η παράβιαση δεδομένων.

Όσον αφορά τα δεδομένα προσωπικού χαρακτήρα που χειρίζονται όργανα και οργανισμοί της ΕΕ, ο κανονισμός 45/2001 προβλέπει ότι κάθε όργανο και οργανισμός της Ένωσης πρέπει να διορίσει ΥΠΔ. Καθήκον του ΥΠΔ είναι να διασφαλίζει ότι οι διατάξεις του κανονισμού εφαρμόζονται ορθά εντός των οργάνων και των οργανισμών της ΕΕ καθώς και ότι τα υποκείμενα των δεδομένων και οι υπεύθυνοι επεξεργασίας ενημερώνονται για τα δικαιώματα και τις υποχρεώσεις τους ⁴⁶⁸. Ο ΥΠΔ είναι επίσης υποχρεωμένος να απαντά σε αιτήματα του ΕΕΠΔ και να συνεργάζεται μαζί του, όταν απαιτείται. Όπως και ο ΓΚΠΔ, ο κανονισμός 45/2001 περιέχει διατάξεις σχετικά με την ανεξαρτησία του ΥΠΔ κατά την εκτέλεση των καθηκόντων του και προβλέπει την υποχρέωση παροχής στον ΥΠΔ του αναγκαίου προσωπικού και των αναγκαίων πόρων ⁴⁶⁹. Τα όργανα και οι οργανισμοί της ΕΕ (ή υπηρεσίες των οργανισμών αυτών) οφείλουν να ενημερώνουν τον ΥΠΔ πριν από τη διενέργεια οποιασδήποτε πράξης επεξεργασίας και να τηρούν αρχείο όλων των πράξεων επεξεργασίας που γνωστοποιούν ⁴⁷⁰.

468 Βλ. άρθρο 24 παράγραφος 1 του κανονισμού (ΕΚ) αριθ. 45/2001 για τον πλήρη κατάλογο των καθηκόντων του υπευθύνου προστασίας δεδομένων.

469 Κανονισμός (ΕΚ) αριθ. 45/2001, άρθρο 24 παράγραφοι 6 και 7.

470 Ό.π., άρθρα 25 και 26.

4.3.2. Αρχεία των δραστηριοτήτων επεξεργασίας

Για να είναι σε θέση να αποδεικνύουν τη συμμόρφωση και να καθίστανται υπόλογες, οι εταιρείες υποχρεούνται συχνά εκ του νόμου να τεκμηριώνουν και να τηρούν αρχεία για τις δραστηριότητές τους. Χαρακτηριστικά παραδείγματα είναι το φορολογικό δίκαιο και ο λογιστικός έλεγχος που επιβάλλουν σε όλες τις εταιρείες να τηρούν εκτενή τεκμηρίωση και αρχεία. Η θέσπιση παρόμοιων απαιτήσεων σε άλλους τομείς του δικαίου, ιδίως στο δίκαιο προστασίας δεδομένων, είναι επίσης απαραίτητη, καθώς η τήρηση αρχείων αποτελεί σημαντικό μέσο για τη διευκόλυνση της συμμόρφωσης προς τους κανόνες περί προστασίας δεδομένων. Επομένως, το **δίκαιο της ΕΕ** προβλέπει ότι οι υπεύθυνοι επεξεργασίας, ή οι εκπρόσωποί τους, πρέπει να τηρούν αρχείο των δραστηριοτήτων επεξεργασίας που εκτελούνται υπ' ευθύνη τους ⁴⁷¹. Σκοπός της υποχρέωσης αυτής είναι να διασφαλιστεί ότι, εάν απαιτηθεί, οι εποπτικές αρχές θα διαθέτουν την αναγκαία τεκμηρίωση ώστε να μπορούν να επιβεβαιώσουν τη νομιμότητα της επεξεργασίας.

Οι πληροφορίες που πρέπει να τεκμηριώνονται περιλαμβάνουν τα εξής:

- το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπευθύνου επεξεργασίας, του εκπροσώπου του υπευθύνου επεξεργασίας και του υπευθύνου προστασίας δεδομένων·
- τους σκοπούς της επεξεργασίας·
- περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα που αφορά η επεξεργασία·
- πληροφορίες για τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα·
- πληροφορίες για το αν πρόκειται να διενεργηθούν ή διενεργήθηκαν διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό·
- όπου είναι δυνατό, τις προβλεπόμενες προθεσμίες διαγραφής των διαφόρων κατηγοριών δεδομένων προσωπικού χαρακτήρα, καθώς και επισκόπηση των τεχνικών μέτρων που έχουν ληφθεί ώστε να διασφαλίζεται η ασφάλεια της επεξεργασίας ⁴⁷².

⁴⁷¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 30.

⁴⁷² Ό.π., άρθρο 30 παράγραφος 1.

Η υποχρέωση τήρησης αρχείων των δραστηριοτήτων επεξεργασίας, βάσει του ΓΚΠΔ, αφορά όχι μόνο τους υπευθύνους επεξεργασίας αλλά και τους εκτελούντες την επεξεργασία. Αυτή είναι μια σημαντική εξέλιξη, δεδομένου ότι, πριν από την έκδοση του κανονισμού, η σύμβαση μεταξύ του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία κάλυπτε κυρίως τις υποχρεώσεις του εκτελούντος την επεξεργασία. Η υποχρέωση των εκτελούντων την επεξεργασία να τηρούν αρχεία προβλέπεται πλέον απευθείας από τον νόμο.

Ο ΓΚΠΔ προβλέπει μία εξαίρεση από την υποχρέωση αυτή. Η απαίτηση τήρησης αρχείων δεν εφαρμόζεται σε επιχείρηση ή οργανισμό (υπεύθυνο προστασίας ή εκτελούντα την επεξεργασία) που απασχολεί λιγότερα από 250 άτομα. Ωστόσο, η εξαίρεση εξαρτάται από ορισμένες προϋποθέσεις: ο οργανισμός δεν πρέπει να διενεργεί επεξεργασία η οποία ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων, η επεξεργασία πρέπει να είναι μόνο περιστασιακή και δεν πρέπει να περιλαμβάνει ειδικές κατηγορίες δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

Η τήρηση αρχείων δραστηριοτήτων επεξεργασίας θα πρέπει να παρέχει στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία τη δυνατότητα να αποδεικνύουν τη συμμόρφωση προς τον κανονισμό. Θα πρέπει επίσης να παρέχει τη δυνατότητα στις εποπτικές αρχές να παρακολουθούν τη νομιμότητα της επεξεργασίας. Όταν η εποπτική αρχή ζητεί πρόσβαση στα αρχεία αυτά, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία υποχρεούνται να συνεργάζονται και να τα θέτουν στη διάθεσή της.

4.3.3. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων και προηγούμενη διαβούλευση

Οι πράξεις επεξεργασίας ενέχουν ορισμένους εγγενείς κινδύνους για τα δικαιώματα των φυσικών προσώπων. Τα δεδομένα προσωπικού χαρακτήρα ενδέχεται να χαθούν, να κοινοποιηθούν σε μη εξουσιοδοτημένα πρόσωπα ή να υποβληθούν σε παράνομη επεξεργασία. Όπως είναι φυσικό, οι κίνδυνοι διαφέρουν ανάλογα με τη φύση και την έκταση της επεξεργασίας. Πράξεις μεγάλης κλίμακας που αφορούν την επεξεργασία ευαίσθητων δεδομένων, για παράδειγμα, ενέχουν πολύ υψηλότερο βαθμό κινδύνου για τα υποκείμενα των δεδομένων σε σχέση με τους κινδύνους που ενδεχομένως εγκυμονούνται όταν μια

μικρή εταιρεία επεξεργάζεται τις διευθύνσεις και τους προσωπικούς αριθμούς τηλεφώνου των υπαλλήλων της.

Καθώς νέες τεχνολογίες κάνουν την εμφάνισή τους και η επεξεργασία καθίσταται ολοένα και πιο πολύπλοκη, οι υπεύθυνοι επεξεργασίας πρέπει να αντιμετωπίζουν τους κινδύνους αυτούς ξεετάζοντας τον ενδεχόμενο αντίκτυπο της σκοπούμενης επεξεργασίας προτού ξεκινήσουν την επεξεργασία. Έτσι παρέχεται η δυνατότητα στους οργανισμούς να προσδιορίζουν, να αντιμετωπίζουν και να μετράζουν τους κινδύνους εκ των προτέρων, περιορίζοντας σημαντικά το ενδεχόμενο αρνητικού αντικτύπου στα φυσικά πρόσωπα ως αποτέλεσμα της επεξεργασίας.

Εκτιμήσεις αντικτύπου σχετικά με την προστασία δεδομένων προβλέπονται **τόσο στο δίκαιο του Συμβουλίου της Ευρώπης, όσο και στο δίκαιο της ΕΕ**. Στο νομικό πλαίσιο του Συμβουλίου της Ευρώπης, το άρθρο 10 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108 επιβάλλει στα συμβαλλόμενα μέρη να διασφαλίζουν ότι οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία «ξεετάζουν τον ενδεχόμενο αντίκτυπο σκοπούμενης επεξεργασίας δεδομένων στα δικαιώματα και στις θεμελιώδεις ελευθερίες των υποκειμένων των δεδομένων πριν από την έναρξη τέτοιας επεξεργασίας» και, μετά την εκτίμηση, σχεδιάζουν την επεξεργασία κατά τρόπο ώστε να αποφεύγονται ή να ελαχιστοποιούνται οι κίνδυνοι που σχετίζονται με την επεξεργασία.

Το δίκαιο της ΕΕ επιβάλλει παρόμοια, αναλυτικότερη υποχρέωση στους υπευθύνους επεξεργασίας που εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ. Το άρθρο 35 ορίζει ότι πρέπει να διενεργείται εκτίμηση αντικτύπου όταν η επεξεργασία ενδέχεται να εγκυμονεί υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Ο κανονισμός δεν ορίζει τον τρόπο με τον οποίο πρέπει να εκτιμάται η πιθανότητα επέλευσης του κινδύνου, αλλά αναφέρει αντιθέτως τους ενδεχόμενους κινδύνους ⁴⁷³. Περιέχει κατάλογο πράξεων επεξεργασίας οι οποίες θεωρούνται υψηλού κινδύνου και για τις οποίες είναι ιδιαίτερως αναγκαία η διενέργεια προηγούμενης εκτίμησης αντικτύπου, συγκεκριμένα σε περιπτώσεις στις οποίες:

- δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για τη λήψη αποφάσεων που αφορούν φυσικά πρόσωπα, κατόπιν οποιασδήποτε

473 Γενικός Κανονισμός για την Προστασία Δεδομένων, προοίμιο, αιτιολογική σκέψη 75.

συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών που αφορούν τα φυσικά πρόσωπα (κατάρτιση προφίλ).

- ευαίσθητα δεδομένα ή δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία σε μεγάλη κλίμακα·
- η επεξεργασία αφορά μεγάλης κλίμακας, συστηματική παρακολούθηση δημοσίως προσβάσιμων χώρων.

Οι εποπτικές αρχές πρέπει να καταρτίζουν και να δημοσιοποιούν κατάλογο με τα είδη των πράξεων επεξεργασίας που πρέπει να υπόκεινται σε εκτιμήσεις αντικτύπου. Μπορούν επίσης να καταρτίζουν κατάλογο πράξεων επεξεργασίας οι οποίες εξαιρούνται από την υποχρέωση αυτή ⁴⁷⁴.

Όταν απαιτείται εκτίμηση αντικτύπου, ο υπεύθυνος επεξεργασίας πρέπει να αξιολογεί την αναγκαιότητα και την αναλογικότητα της επεξεργασίας καθώς και τους ενδεχόμενους κινδύνους για τα δικαιώματα των φυσικών προσώπων. Η εκτίμηση αντικτύπου πρέπει να περιέχει επίσης τα σχεδιαζόμενα μέτρα ασφάλειας για την αντιμετώπιση των κινδύνων που προσδιορίζονται σε αυτήν. Για την κατάρτιση των καταλόγων, οι εποπτικές αρχές των κρατών μελών υποχρεούνται να συνεργάζονται μεταξύ τους και με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Με τον τρόπο αυτό θα διασφαλιστεί μια συνεκτική προσέγγιση σε ολόκληρη την ΕΕ για τις πράξεις εκείνες που απαιτούν εκτίμηση αντικτύπου, και οι υπεύθυνοι επεξεργασίας θα υπόκεινται σε παρόμοιες απαιτήσεις ανεξάρτητα από τον τόπο στον οποίο βρίσκονται.

Εάν, από την εκτίμηση αντικτύπου, προκύπτει ότι η επεξεργασία θα προκαλέσει υψηλό κίνδυνο για τα δικαιώματα των φυσικών προσώπων και ότι δεν θεσπίστηκαν μέτρα για τον μετριασμό του κινδύνου, ο υπεύθυνος επεξεργασίας πρέπει να ζητήσει τη γνώμη της αρμόδιας εποπτικής αρχής προτού ξεκινήσει την πράξη επεξεργασίας ⁴⁷⁵.

474 Ό.π., άρθρο 35 παράγραφοι 4 και 5.

475 Ό.π., άρθρο 36 παράγραφος 1 Ομάδα εργασίας του άρθρου 29 (2017), *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ)* και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, WP 248 rev.01, Βρυξέλλες, 4 Οκτωβρίου 2017.

Η Ομάδα εργασίας του άρθρου 29 εξέδωσε κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων και τον καθορισμό του κατά πόσον η επεξεργασία ενδέχεται να δημιουργήσει υψηλό κίνδυνο ⁴⁷⁶. Ανέπτυξε εννέα κριτήρια τα οποία συμβάλλουν στον καθορισμό του αν απαιτείται η διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σε συγκεκριμένη περίπτωση ⁴⁷⁷: 1) αξιολόγηση ή βαθμολόγηση· 2) λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο· 3) συστηματική παρακολούθηση· 4) ευαίσθητα δεδομένα· 5) δεδομένα μεγάλης κλίμακας επεξεργασίας· 6) αντιστοίχιση ή συνδυασμός συνόλων δεδομένων· 7) δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων· 8) καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων· 9) η επεξεργασία η οποία αυτή καθαυτήν «εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση». Η Ομάδα εργασίας του άρθρου 29 θέσπισε τον εμπειρικό κανόνα ότι οι πράξεις επεξεργασίας που πληρούν λιγότερα από δύο κριτήρια συνεπάγονται χαμηλότερα επίπεδα κινδύνου και δεν απαιτούν τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, ενώ εκείνες που πληρούν δύο ή περισσότερα κριτήρια απαιτούν τη διενέργεια τέτοιας εκτίμησης. Στις περιπτώσεις στις οποίες δεν είναι σαφές αν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων, η Ομάδα εργασίας του άρθρου 29 συνιστά τη διενέργεια τέτοιας εκτίμησης, επειδή είναι «χρήσιμο εργαλείο για τους υπεύθυνους επεξεργασίας προκειμένου να συμμορφώνονται με τη νομοθεσία για την προστασία των δεδομένων» ⁴⁷⁸. Όταν εισάγεται νέα τεχνολογία επεξεργασίας δεδομένων, είναι σημαντικό να διενεργείται εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ⁴⁷⁹.

4.3.4. Κώδικες δεοντολογίας

Οι κώδικες δεοντολογίας καταρτίζονται ώστε να χρησιμοποιηθούν σε αρκετούς βιομηχανικούς τομείς και στόχος τους είναι η περιγραφή και η αποσαφήνιση της εφαρμογής του ΓΚΠΔ στους συγκεκριμένους τομείς. Σε ό,τι αφορά τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία δεδομένων

476 Ομάδα εργασίας του άρθρου 29 (2017), *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679*, WP 248 rev.01, Βρυξέλλες, 4 Οκτωβρίου 2017.

477 Ό.π., σ. 9-11.

478 Ό.π., σ. 9.

479 Ό.π.

προσωπικού χαρακτήρα, η κατάρτιση τέτοιων κωδίκων μπορεί να βελτιώσει σημαντικά τη συμμόρφωση και την εφαρμογή των κανόνων της ΕΕ περί προστασίας δεδομένων. Η εμπειρογνωμοσύνη των μελών του τομέα θα διευκολύνει την εξεύρεση λύσεων οι οποίες είναι πρακτικές και, επομένως, είναι πιθανόν να εφαρμοστούν. Αναγνωρίζοντας τη σημασία τέτοιων κωδίκων για την αποτελεσματική εφαρμογή του δικαίου για την προστασία δεδομένων, ο ΓΚΠΔ καλεί τα κράτη μέλη, τις εποπτικές αρχές, την Επιτροπή και το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων να προωθήσουν την κατάρτιση κωδίκων δεοντολογίας οι οποίοι πρόκειται να συμβάλουν στην ορθή εφαρμογή του κανονισμού σε ολόκληρη την ΕΕ ⁴⁸⁰. Οι κώδικες μπορούν να αποσαφηνίζουν την εφαρμογή του κανονισμού σε συγκεκριμένους τομείς, σε θέματα όπως η συλλογή δεδομένων προσωπικού χαρακτήρα, οι πληροφορίες που πρέπει να παρέχονται στα υποκείμενα των δεδομένων και στο ευρύ κοινό και η άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων.

Προκειμένου να διασφαλίζεται η συμμόρφωση των κωδίκων δεοντολογίας προς τους κανόνες που θεσπίζει ο ΓΚΠΔ, οι κώδικες πρέπει να υποβάλλονται στην αρμόδια εποπτική αρχή πριν από την έκδοσή τους. Στη συνέχεια, η εποπτική αρχή γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου κώδικα προς τον κανονισμό και, εάν κρίνει ότι ο κώδικας παρέχει κατάλληλες εγγυήσεις, τον εγκρίνει ⁴⁸¹. Οι εποπτικές αρχές πρέπει να δημοσιεύουν τους εγκεκριμένους κώδικες δεοντολογίας καθώς και τα κριτήρια στα οποία βασίστηκε η έγκρισή τους. Όταν σχέδιο κώδικα αφορά δραστηριότητες επεξεργασίας σε περισσότερα κράτη μέλη, προτού εγκρίνει το σχέδιο κώδικα, ή την τροποποίηση ή επέκταση του κώδικα, η αρμόδια εποπτική αρχή υποβάλλει τον κώδικα στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, το οποίο γνωμοδοτεί σχετικά με τη συμμόρφωση του κώδικα προς τον ΓΚΠΔ. Η Επιτροπή μπορεί, μέσω εκτελεστικών πράξεων, να αποφασίζει οι εγκεκριμένοι κώδικες δεοντολογίας που της υποβάλλονται να έχουν γενική ισχύ εντός της Ένωσης.

Η τήρηση κώδικα δεοντολογίας συνεπάγεται σημαντικά πλεονεκτήματα τόσο για τα υποκείμενα των δεδομένων, όσο και για τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία. Οι κώδικες αυτοί παρέχουν λεπτομερή καθοδήγηση, η οποία προσαρμόζει τις νομικές απαιτήσεις σε συγκεκριμένους τομείς και προάγει τη διαφάνεια των δραστηριοτήτων επεξεργασίας. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία μπορούν επίσης να

480 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 40 παράγραφος 1.

481 Ό.π., άρθρο 40 παράγραφος 5.

χρησιμοποιούν τους κώδικες ως απτή απόδειξη της συμμόρφωσής τους προς το δίκαιο της ΕΕ καθώς και ως τρόπο βελτίωσης της δημόσιας εικόνας τους ως οργανισμών που δίνουν προτεραιότητα και είναι προσηλωμένοι στην προστασία δεδομένων στο πλαίσιο της λειτουργίας τους. Εγκεκριμένοι κώδικες δεοντολογίας, σε συνδυασμό με δεσμευτικές και εκτελεστές υποχρεώσεις, μπορούν να χρησιμοποιηθούν ως κατάλληλες εγγυήσεις για τη διαβίβαση δεδομένων σε τρίτες χώρες. Προκειμένου να διασφαλίζεται ότι οι οργανισμοί που τηρούν τους κώδικες δεοντολογίας όντως συμμορφώνονται με αυτούς, είναι δυνατόν να διοριστεί ειδικός φορέας (διαπιστευμένος από την αρμόδια εποπτική αρχή) για την παρακολούθηση και τη διασφάλιση της συμμόρφωσης. Για την αποτελεσματική εκτέλεση της αποστολής του, ο φορέας πρέπει να είναι ανεξάρτητος, να διαθέτει αποδεδειγμένη εμπειρογνωμοσύνη στα θέματα που ρυθμίζονται από τον κώδικα δεοντολογίας και να διαθέτει διαφανείς διαδικασίες και δομές ώστε να είναι σε θέση να χειρίζεται καταγγελίες σχετικά με παραβάσεις του κώδικα⁴⁸².

Στο πλαίσιο του **δικαίου του Συμβουλίου της Ευρώπης**, η Εκσυγχρονισμένη Σύμβαση 108 προβλέπει ότι το επίπεδο προστασίας δεδομένων που εγγυάται η εθνική νομοθεσία μπορεί να ενισχυθεί αποτελεσματικά με οικειοθελή μέτρα ρύθμισης, όπως κώδικες ορθής πρακτικής ή επαγγελματικής δεοντολογίας. Ωστόσο, αυτά είναι απλώς οικειοθελή μέτρα στο πλαίσιο της Εκσυγχρονισμένης Σύμβασης 108: δεν μπορεί να αντληθεί εξ αυτών καμία έννομη υποχρέωση εφαρμογής των εν λόγω μέτρων στην πράξη, παρότι κάτι τέτοιο συνιστάται, και τα εν λόγω μέτρα δεν επαρκούν αφ' εαυτών για να διασφαλιστεί πλήρης συμμόρφωση προς τη Σύμβαση⁴⁸³.

4.3.5. Πιστοποίηση

Πέραν των κωδίκων δεοντολογίας, άλλα μέσα με τα οποία οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία μπορούν να αποδείξουν τη συμμόρφωση προς τον ΓΚΠΔ είναι οι μηχανισμοί πιστοποίησης και οι σφραγίδες και τα σήματα προστασίας δεδομένων. Για τον σκοπό αυτό, ο κανονισμός προβλέπει εθελοντικό σύστημα πιστοποίησης βάσει του οποίου ορισμένοι φορείς ή εποπτικές αρχές μπορούν να εκδίδουν πιστοποιήσεις. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία οι οποίοι επιλέγουν να προσχωρήσουν σε μηχανισμό πιστοποίησης μπορούν να εξασφαλίσουν μεγαλύτερη προβολή και αξιοπιστία, καθώς οι πιστοποιήσεις, οι σφραγίδες και τα σήματα παρέχουν τη

482 Ό.π., άρθρο 41 παράγραφοι 1 και 2.

483 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 33.

δυνατότητα στα υποκείμενα των δεδομένων να αξιολογούν ταχέως το επίπεδο προστασίας που παρέχει ένας οργανισμός όσον αφορά την επεξεργασία δεδομένων. Υπενθυμίζεται, ωστόσο, ότι το γεγονός ότι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διαθέτει τέτοια πιστοποίηση δεν μειώνει τα καθήκοντα και τις υποχρεώσεις του όσον αφορά τη συμμόρφωση προς όλες τις απαιτήσεις του κανονισμού.

4.4. Προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

Προστασία των δεδομένων ήδη από τον σχεδιασμό

Το **δίκαιο της ΕΕ** επιβάλλει στους υπευθύνους επεξεργασίας να θεσπίζουν μέτρα για την αποτελεσματική εφαρμογή αρχών προστασίας των δεδομένων και για την ενσωμάτωση των απαραίτητων εγγυήσεων, ώστε να πληρούνται οι απαιτήσεις του κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων ⁴⁸⁴. Τα μέτρα αυτά θα πρέπει να εφαρμόζονται τόσο κατά την επεξεργασία, όσο και κατά τον καθορισμό των μέσων επεξεργασίας. Κατά την εφαρμογή των μέτρων αυτών, ο υπεύθυνος επεξεργασίας πρέπει να λαμβάνει υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα καθώς και τους κινδύνους και τη σοβαρότητα αυτών για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων ⁴⁸⁵.

Το **δίκαιο του Συμβουλίου της Ευρώπης** υποχρεώνει τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να αξιολογούν τον ενδεχόμενο αντίκτυπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στα δικαιώματα και στις ελευθερίες των υποκειμένων των δεδομένων πριν από την έναρξη της επεξεργασίας. Επιπλέον, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία υποχρεούνται να σχεδιάζουν την επεξεργασία δεδομένων κατά τρόπο ώστε να αποφεύγεται ή να ελαχιστοποιείται ο κίνδυνος επεμβάσεων στα εν λόγω δικαιώματα και στις εν λόγω ελευθερίες και να εφαρμόζουν τεχνικά

484 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 25 παράγραφος 1.

485 Βλ. Ομάδα εργασίας του άρθρου 29 (2017), *Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679, WP 248 rev.01, 4 Οκτωβρίου 2017. Βλ. επίσης ENISA (2015), Privacy and Data Protection by Design – from policy to engineering, 12 Ιανουαρίου 2015.*

και οργανωτικά μέτρα τα οποία λαμβάνουν υπόψη τις συνέπειες του δικαιώματος στην προστασία των προσωπικών δεδομένων σε όλα τα στάδια κατά την επεξεργασία προσωπικών δεδομένων ⁴⁸⁶.

Προστασία δεδομένων εξ ορισμού

Το **δίκαιο της ΕΕ** επιβάλλει στον υπεύθυνο επεξεργασίας να εφαρμόζει κατάλληλα μέτρα ώστε να διασφαλίζεται, εξ ορισμού, ότι θα υποβληθούν σε επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα τα οποία είναι απαραίτητα για τον εκάστοτε σκοπό. Η υποχρέωση αυτή ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους ⁴⁸⁷. Ένα τέτοιο μέτρο πρέπει να διασφαλίζει, για παράδειγμα, ότι δεν έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα των υποκειμένων των δεδομένων όλοι οι υπάλληλοι του υπευθύνου επεξεργασίας. Ο ΕΕΠΔ παρέχει περαιτέρω καθοδήγηση στο *Necessity Toolkit* ⁴⁸⁸.

Το **δίκαιο του Συμβουλίου της Ευρώπης** υποχρεώνει τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία να εφαρμόζουν τεχνικά και οργανωτικά μέτρα ώστε να λαμβάνονται υπόψη οι συνέπειες του δικαιώματος στην προστασία των δεδομένων και να εφαρμόζουν τεχνικά και οργανωτικά μέτρα τα οποία λαμβάνουν υπόψη τις συνέπειες του δικαιώματος στην προστασία των προσωπικών δεδομένων σε όλα τα στάδια κατά την επεξεργασία προσωπικών δεδομένων ⁴⁸⁹.

Το 2016 ο ENISA δημοσίευσε έκθεση σχετικά με τα διαθέσιμα εργαλεία και τις υπηρεσίες για την προστασία της ιδιωτικής ζωής ⁴⁹⁰. Μεταξύ άλλων παρατηρήσεων, η αξιολόγηση αυτή παρέχει κατάλογο κριτηρίων και παραμέτρων που αποτελούν δείκτες καλών ή ανεπαρκών πρακτικών για την προστασία της ιδιωτικής ζωής. Παρότι ορισμένα κριτήρια σχετίζονται άμεσα με τις διατάξεις του ΓΚΠΔ

486 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 2 και 3· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 89.

487 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 25 παράγραφος 2.

488 Ευρωπαϊός Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ), (2017), *Necessity Toolkit*, Βρυξέλλες, 11 Απριλίου 2017.

489 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 10 παράγραφος 3· Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 89.

490 ENISA, *PETs controls matrix: A systematic approach for assessing online and mobile privacy tools*, 20 Δεκεμβρίου 2016.

–όπως η χρήση ψευδωνυμοποίησης και οι εγκεκριμένοι μηχανισμοί πιστοποίησης-, άλλα αποτελούν καινοτόμες πρωτοβουλίες για τη διασφάλιση της προστασίας της ιδιωτικής ζωής ήδη από τον σχεδιασμό και εξ ορισμού. Για παράδειγμα, το κριτήριο της χρησιμότητας, παρότι δεν σχετίζεται άμεσα με την ιδιωτική ζωή, ενδέχεται να βελτιώνει την προστασία της, καθώς μπορεί να καταστήσει εφικτή την ευρύτερη υιοθέτηση εργαλείου ή υπηρεσίας για την προστασία της ιδιωτικής ζωής. Πράγματι, τα εργαλεία για την προστασία της ιδιωτικής ζωής των οποίων η πρακτική εφαρμογή είναι δύσκολη μπορεί να έχουν πολύ χαμηλά επίπεδα υιοθέτησης από το ευρύ κοινό, ακόμη και αν παρέχουν πολύ ισχυρές εγγυήσεις προστασίας της ιδιωτικής ζωής. Επιπλέον, το κριτήριο της ωριμότητας και της σταθερότητας του εργαλείου για την προστασία της ιδιωτικής ζωής –υπό την έννοια του τρόπου με τον οποίο το εργαλείο εξελίσσεται με την πάροδο του χρόνου και ανταποκρίνεται σε υφιστάμενες ή νέες προκλήσεις σχετικές με την προστασία της ιδιωτικής ζωής- είναι καθοριστικής σημασίας. Άλλες τεχνολογίες που εξασφαλίζουν καλύτερη προστασία της ιδιωτικής ζωής, για παράδειγμα, στο πλαίσιο ασφαλών επικοινωνιών, περιλαμβάνουν την κρυπτογράφηση από την πηγή έως τον προορισμό (επικοινωνία στην οποία τα μόνα πρόσωπα τα οποία μπορούν να διαβάσουν τα μηνύματα είναι τα πρόσωπα που επικοινωνούν)- κρυπτογράφηση πελάτη-εξυπηρετητή (κρυπτογράφηση του διαύλου επικοινωνίας μεταξύ πελάτη και εξυπηρετητή)- εξακρίβωση ταυτότητας (επαλήθευση των ταυτοτήτων των μερών που επικοινωνούν)- και ανώνυμη επικοινωνία (κανένας τρίτος δεν μπορεί να εξακριβώσει την ταυτότητα των μερών που επικοινωνούν).

5

Ανεξάρτητη εποπτεία

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Ο Χάρτης, άρθρο 8 παράγραφος 3 Συνθήκη για τη λειτουργία της ΕΕ, άρθρο 16 παράγραφος 2 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 51 έως 59 ΔΕΕ, C-518/07, <i>Ευρωπαϊκή Επιτροπή κατά Ομοσπονδιακής Δημοκρατίας της Γερμανίας</i> [τμήμα μείζονος συνθέσεως], 2010 ΔΕΕ, C-614/10, <i>Ευρωπαϊκή Επιτροπή κατά Δημοκρατίας της Αυστρίας</i> [τμήμα μείζονος συνθέσεως], 2012 ΔΕΕ, C-288/12, <i>Ευρωπαϊκή Επιτροπή κατά Ουγγαρίας</i> [τμήμα μείζονος συνθέσεως], 2014 ΔΕΕ, C-362/14, <i>Maximillian Schrems κατά Data Protection Commissioner</i> [τμήμα μείζονος συνθέσεως], 2015	Εποπτικές αρχές	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 15
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 60 έως 67	Συνεργασία μεταξύ εποπτικών αρχών	Εκσυγχρονισμένη Σύμβαση 108, άρθρα 16-21
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 68 έως 76	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων	

Κύρια σημεία

- Η ανεξάρτητη εποπτεία είναι ουσιώδες στοιχείο του ευρωπαϊκού δικαίου για την προστασία δεδομένων και κατοχυρώνεται στο άρθρο 8 παράγραφος 3 του Χάρτη.
- Για τη διασφάλιση αποτελεσματικής προστασίας των δεδομένων, πρέπει να ιδρύονται ανεξάρτητες εποπτικές αρχές, βάσει του εθνικού δικαίου.
- Οι εποπτικές αρχές πρέπει να ενεργούν με πλήρη ανεξαρτησία, η οποία πρέπει να διασφαλίζεται στην ιδρυτική νομοθετική πράξη και να αντικατοπτρίζεται στην ειδική οργανωτική δομή τους.
- Οι εποπτικές αρχές έχουν ειδικές εξουσίες και συγκεκριμένα καθήκοντα. Σε αυτές περιλαμβάνονται, μεταξύ άλλων:
 - η παρακολούθηση και η προώθηση της επεξεργασίας δεδομένων σε εθνικό επίπεδο·
 - η παροχή συμβουλών σε υποκείμενα δεδομένων και υπευθύνους επεξεργασίας καθώς και στην κυβέρνηση και στο ευρύ κοινό·
 - η εξέταση καταγγελιών και η παροχή συνδρομής στα υποκείμενα των δεδομένων σε σχέση με εικαζόμενες παραβιάσεις των δικαιωμάτων προστασίας δεδομένων·
 - η εποπτεία υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία.
- Οι εποπτικές αρχές έχουν επίσης εξουσία παρέμβασης, εφόσον είναι αναγκαίο, μέσω:
 - προειδοποίησης, επίπληξης ή ακόμη και επιβολής προστίμων σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία·
 - διαταγής διόρθωσης, κλειδώματος ή διαγραφής δεδομένων·
 - επιβολής απαγόρευσης επεξεργασίας ή διοικητικού προστίμου·
 - παραπομπής υποθέσεων στο δικαστήριο.
- Καθώς η επεξεργασία δεδομένων προσωπικού χαρακτήρα αφορά συχνά υπευθύνους επεξεργασίας, εκτελούντες την επεξεργασία και υποκείμενα δεδομένων που βρίσκονται σε διαφορετικά κράτη, οι εποπτικές αρχές υποχρεούνται να συνεργάζονται μεταξύ τους σε διασυνοριακά ζητήματα ώστε να διασφαλίζεται η αποτελεσματική προστασία των φυσικών προσώπων στην Ευρώπη.

- Στην ΕΕ, ο Γενικός Κανονισμός για την Προστασία Δεδομένων θεσπίζει «μηχανισμό μίας στάσης» για υποθέσεις διασυνοριακής επεξεργασίας. Ορισμένες εταιρείες ασκούν δραστηριότητες διασυνοριακής επεξεργασίας λόγω του ότι επεξεργάζονται δεδομένα προσωπικού χαρακτήρα μέσω διαφόρων εγκαταστάσεων σε περισσότερα του ενός κράτη μέλη ή μέσω μίας μόνης εγκατάστασης στην Ένωση, αλλά η οποία επηρεάζει ουσιαστικά υποκείμενα των δεδομένων σε περισσότερα του ενός κράτη μέλη. Στο πλαίσιο του μηχανισμού, οι εταιρείες αυτές θα χρειάζεται να επικοινωνούν μόνο με μία εθνική εποπτική Αρχή Προστασίας Δεδομένων.
- Ο μηχανισμός συνεργασίας και συνεκτικότητας θα καταστήσει εφικτή τη συντονισμένη προσέγγιση όλων των εποπτικών αρχών που εμπλέκονται στην υπόθεση. Η επικεφαλής εποπτική αρχή –της κύριας ή της μόνης εγκατάστασης– θα διαβουλεύεται με τις άλλες ενδιαφερόμενες εποπτικές αρχές και θα υποβάλλει σε αυτές το σχέδιο απόφασής της.
- Όπως ισχύει και με την τρέχουσα Ομάδα εργασίας του άρθρου 29, η εποπτική αρχή κάθε κράτους μέλους και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ) θα είναι μέλη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων.
- Τα καθήκοντα του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων περιλαμβάνουν, για παράδειγμα, την παρακολούθηση της ορθής εφαρμογής του κανονισμού, την παροχή συμβουλών στην Επιτροπή σε σχετικά θέματα και την έκδοση γνώμων, κατευθυντήριων γραμμών ή βέλτιστων πρακτικών σε διάφορα θέματα.
- Η κύρια διαφορά είναι ότι το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δεν θα εκδίδει μόνο γνώμες, όπως συνέβαινε στο πλαίσιο της οδηγίας 95/46/ΕΚ. Θα εκδίδει επίσης δεσμευτικές αποφάσεις σχετικά με περιπτώσεις στις οποίες εποπτική αρχή προβάλλει σχετική και αιτιολογημένη ένσταση σε υποθέσεις του «μηχανισμού μίας στάσης»· όταν υπάρχει διαφωνία σχετικά με το ποια εποπτική αρχή είναι η επικεφαλής και, τέλος, όταν η αρμόδια εποπτική αρχή δεν ζητεί ή δεν εφαρμόζει τη γνώμη του ΕΣΠΔ. Σκοπός είναι να διασφαλίζεται η συνεκτική εφαρμογή του κανονισμού σε όλα τα κράτη μέλη.

Η ανεξάρτητη εποπτεία είναι ουσιαστικό στοιχείο του ευρωπαϊκού δικαίου για την προστασία δεδομένων. Τόσο στο δίκαιο της ΕΕ, όσο και στο δίκαιο του Συμβουλίου της Ευρώπης η ύπαρξη ανεξάρτητων εποπτικών αρχών θεωρείται απαραίτητη για την αποτελεσματική προστασία των δικαιωμάτων και των ελευθεριών των φυσικών προσώπων σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Καθώς η επεξεργασία δεδομένων είναι πλέον πανταχού παρούσα και ολοένα και πιο δυσνόητη για τα φυσικά πρόσωπα, οι εποπτικές αυτές αρχές είναι οι θεματοφύλακες της ψηφιακής εποχής. Στην ΕΕ, η ύπαρξη ανεξάρτητων εποπτικών αρχών θεωρείται ένα από τα πιο ουσιαστικά στοιχεία του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα, το οποίο κατοχυρώνεται στο πρωτογενές δίκαιο της ΕΕ. Το άρθρο 8 παράγραφος 3 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ και το άρθρο 16

παράγραφος 2 της ΣΛΕΕ αναγνωρίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα ως θεμελιώδες δικαίωμα και βεβαιώνουν ότι η συμμόρφωση προς τους κανόνες περί προστασίας δεδομένων πρέπει να υπόκειται στον έλεγχο ανεξάρτητης αρχής.

Η σημασία της ανεξάρτητης εποπτείας για το δίκαιο της προστασίας δεδομένων έχει αναγνωριστεί και στη νομολογία.

Παράδειγμα: Στην υπόθεση *Schrems*⁴⁹¹, το ΔΕΕ εξέτασε αν η διαβίβαση δεδομένων προσωπικού χαρακτήρα στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ), βάσει της πρώτης συμφωνίας ασφαλούς λιμένα μεταξύ ΕΕ και ΗΠΑ, ήταν σύμφωνη με το δίκαιο της ΕΕ για την προστασία δεδομένων, λαμβανομένων υπόψη των αποκαλύψεων του Edward Snowden σχετικά με τη διενέργεια μαζικής παρακολούθησης από τη National Security Agency των ΗΠΑ. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ στηριζόταν σε απόφαση που εξέδωσε η Ευρωπαϊκή Επιτροπή το 2000, δυνάμει της οποίας επιτρεπόταν η διαβίβαση δεδομένων προσωπικού χαρακτήρα από την ΕΕ σε οργανισμούς στις ΗΠΑ οι οποίοι αυτοπιστοποιούνται στο πλαίσιο του συστήματος ασφαλούς λιμένα, με τον όρο ότι το σύστημα διασφαλίζει κατάλληλο επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα. Όταν της ζητήθηκε να διερευνήσει την καταγγελία του προσφεύγοντος όσον αφορά τη νομιμότητα των διαβιβάσεων δεδομένων μετά τις αποκαλύψεις Snowden, η ιρλανδική εποπτική αρχή απέρριψε την καταγγελία με την αιτιολογία ότι η ύπαρξη της απόφασης της Επιτροπής σχετικά με την επάρκεια του καθεστώτος προστασίας δεδομένων των ΗΠΑ που αντικατοπτρίζονταν στις αρχές ασφαλούς λιμένα («απόφαση ασφαλούς λιμένα») δεν της επέτρεπε να διερευνήσει περαιτέρω την καταγγελία.

Ωστόσο, το ΔΕΕ αποφάνθηκε ότι η ύπαρξη απόφασης της Επιτροπής που επιτρέπει τις διαβιβάσεις δεδομένων σε τρίτες χώρες οι οποίες διασφαλίζουν κατάλληλα επίπεδα προστασίας δεν εξαλείφει ούτε περιορίζει τις εξουσίες των εθνικών εποπτικών αρχών. Το ΔΕΕ επισήμανε ότι οι εξουσίες των εν λόγω αρχών να παρακολουθούν και να διασφαλίζουν τη συμμόρφωση προς τους κανόνες της ΕΕ περί προστασίας δεδομένων απορρέουν από το πρωτογενές δίκαιο της ΕΕ, ιδίως το άρθρο 8

491 ΔΕΕ, C-362/14, *Maximillian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015.

παράγραφος 3 του Χάρτη και το άρθρο 16 παράγραφος 2 της ΣΛΕΕ. «Η σύσταση ανεξάρτητων αρχών ελέγχου [...] συνιστά έτσι [...] ουσιώδες στοιχείο του σεβασμού της προστασίας των ατόμων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα»⁴⁹².

Ως εκ τούτου, το ΔΕΕ αποφάνθηκε ότι, έστω και αν η διαβίβαση δεδομένων προσωπικού χαρακτήρα αποτέλεσε αντικείμενο απόφασης επάρκειας της Επιτροπής, όταν υποβάλλεται καταγγελία σε εθνική εποπτική αρχή, η αρχή οφείλει να την εξετάσει με τη δέουσα επιμέλεια. Η εποπτική αρχή μπορεί να απορρίψει την καταγγελία εάν κρίνει ότι είναι αβάσιμη. Το ΔΕΕ επισήμανε ότι, σε μια τέτοια περίπτωση, το δικαίωμα αποτελεσματικής δικαστικής προστασίας επιβάλλει να μπορούν τα φυσικά πρόσωπα να προσβάλουν την απόφαση αυτή ενώπιον των εθνικών δικαστηρίων, τα οποία μπορούν να παραπέμψουν την υπόθεση στο ΔΕΕ για έκδοση προδικαστικής απόφασης σχετικά με το κύρος της απόφασης της Επιτροπής. Εάν η εποπτική αρχή κρίνει την καταγγελία βάσιμη, πρέπει να έχει την εξουσία να παρίσταται ενώπιον δικαστηρίου και να προσφύγει ενώπιον των εθνικών δικαστηρίων. Τα εθνικά δικαστήρια μπορούν να παραπέμψουν την υπόθεση στο ΔΕΕ, καθώς είναι το μόνο όργανο που διαθέτει την εξουσία να αποφανθεί επί του κύρους απόφασης επάρκειας της Επιτροπής⁴⁹³.

Στη συνέχεια, το ΔΕΕ εξέτασε το κύρος της απόφασης ασφαλούς λιμένα για να διαπιστώσει αν το σύστημα διαβιβάσεων ήταν σύμφωνο προς τους κανόνες της ΕΕ περί προστασίας δεδομένων. Το ΔΕΕ διαπίστωσε ότι το άρθρο 3 της απόφασης ασφαλούς λιμένα περιόριζε τις δυνατότητες των εθνικών εποπτικών αρχών (οι οποίες αναγνωρίζονται από την Οδηγία για την Προστασία Δεδομένων) να λαμβάνουν μέτρα για την αποφυγή διαβιβάσεων δεδομένων σε περίπτωση ανεπαρκούς επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ. Λαμβανομένης υπόψη της σημασίας των ανεξάρτητων εποπτικών αρχών για τη διασφάλιση συμμόρφωσης προς το δίκαιο για την προστασία δεδομένων, το ΔΕΕ αποφάνθηκε ότι, βάσει της Οδηγίας για την Προστασία Δεδομένων και σε συνδυασμό με τον Χάρτη, η Επιτροπή δεν είχε την αρμοδιότητα να περιορίσει τις εξουσίες των ανεξάρτητων εποπτικών αρχών κατ' αυτόν

492 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015, σκέψη 41.

493 Ό.π., σκέψεις 53-66.

τον τρόπο. Ο περιορισμός των εξουσιών των εποπτικών αρχών ήταν ένας από τους λόγους για τους οποίους το ΔΕΕ κήρυξε ανίσχυρη την απόφαση ασφαλούς λιμένα.

Επομένως, το ευρωπαϊκό δίκαιο απαιτεί την ανεξάρτητη εποπτεία ως σημαντικό μηχανισμό για τη διασφάλιση αποτελεσματικής προστασίας δεδομένων. Οι ανεξάρτητες εποπτικές αρχές είναι τα πρώτα σημεία επικοινωνίας για τα υποκείμενα των δεδομένων σε περίπτωση παραβιάσεων της ιδιωτικής ζωής ⁴⁹⁴. Βάσει του δικαίου της ΕΕ και του δικαίου του Συμβουλίου της Ευρώπης, η ίδρυση εποπτικών αρχών είναι υποχρεωτική. Και τα δύο νομικά πλαίσια περιγράφουν τα καθήκοντα και τις εξουσίες των αρχών αυτών με τρόπο παρόμοιο με τον προβλεπόμενο στον ΓΚΠΔ. Επομένως, καταρχήν, οι εποπτικές αρχές θα πρέπει να λειτουργούν με τον ίδιο τρόπο βάσει του δικαίου της ΕΕ και του δικαίου του Συμβουλίου της Ευρώπης ⁴⁹⁵.

5.1. Ανεξαρτησία

Το **δίκαιο της ΕΕ** και το **δίκαιο του Συμβουλίου της Ευρώπης** απαιτούν από κάθε εποπτική αρχή να ενεργεί με πλήρη ανεξαρτησία κατά την εκτέλεση των καθηκόντων της και κατά την άσκηση των εξουσιών της ⁴⁹⁶. Η ανεξαρτησία της εποπτικής αρχής και των μελών της, καθώς και του προσωπικού της, από άμεσες ή έμμεσες εξωτερικές επιρροές είναι θεμελιώδους σημασίας προκειμένου να διασφαλίζεται πλήρης αντικειμενικότητα όταν λαμβάνονται αποφάσεις σε θέματα προστασίας των δεδομένων. Δεν αρκεί η νομοθεσία στην οποία βασίζεται η ίδρυση του εποπτικού φορέα να περιέχει διατάξεις που εγγυώνται συγκεκριμένα την ανεξαρτησία του, αλλά πρέπει και η οργανωτική δομή της αρχής να αποδεικνύει την ανεξαρτησία της. Το 2010 το ΔΕΕ εξέτασε –για πρώτη φορά– τον βαθμό στον οποίο οι εποπτικές αρχές προστασίας δεδομένων απαιτείται να είναι ανεξάρτητες ⁴⁹⁷. Στα επιλεγμένα παραδείγματα αποτυπώνεται ο ορισμός της έννοιας της «πλήρους ανεξαρτησίας» από το ΔΕΕ.

494 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο δ).

495 Ό.π., άρθρο 51· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 15.

496 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 52 παράγραφος 1· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 15 παράγραφος 5.

497 FRA (2010), *Fundamental rights: challenges and achievements in 2010*, Annual report 2010, σ. 59, FRA (2010), *Data protection in the European Union: the role of National Data Protection Authorities*, Μάιος 2010.

Παράδειγμα: Στην υπόθεση *Ευρωπαϊκή Επιτροπή κατά Ομοσπονδιακής Δημοκρατίας της Γερμανίας*⁴⁹⁸, η Ευρωπαϊκή Επιτροπή ζήτησε από το ΔΕΕ να αναγνωρίσει ότι η Γερμανία είχε μεταφέρει εσφαλμένα στην εθνική έννομη τάξη την απαίτηση περί «πλήρους ανεξαρτησίας» της αρμόδιας για τη διασφάλιση της προστασίας των δεδομένων εποπτικής αρχής και ότι, επομένως, είχε παραβεί τις υποχρεώσεις της που απορρέουν από το άρθρο 28 παράγραφος 1 της Οδηγίας για την Προστασία των Δεδομένων. Σύμφωνα με την άποψη της Επιτροπής, το γεγονός ότι η Γερμανία είχε θέσει υπό κρατική επίβλεψη τις εποπτικές αρχές που παρακολουθούν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στα διάφορα ομόσπονδα κρατίδια (Länder), προκειμένου να διασφαλίζεται συμμόρφωση με το δίκαιο για την προστασία δεδομένων, συνιστούσε παράβαση της απαίτησης ανεξαρτησίας.

Το ΔΕΕ επισήμανε ότι η φράση «με πλήρη ανεξαρτησία» πρέπει να ερμηνεύεται βάσει του καθεαυτού γράμματος της διάταξης αυτής καθώς και των σκοπών και της οικονομίας της νομοθεσίας της ΕΕ για την προστασία δεδομένων⁴⁹⁹. Το ΔΕΕ τόνισε ότι οι εποπτικές αρχές είναι οι «θεματοφύλακες» των δικαιωμάτων που σχετίζονται με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Επομένως, η ίδρυσή τους στα κράτη μέλη θεωρείται «ουσιώδες στοιχείο του σεβασμού της προστασίας των ατόμων από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα»⁵⁰⁰. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι «κατά την άσκηση των καθηκόντων τους, οι αρχές ελέγχου πρέπει να ενεργούν αντικειμενικά και αμερόληπτα. Προς τούτο, δεν πρέπει να υπόκεινται σε καμία εξωτερική επιρροή, δηλαδή ούτε στην επιρροή των ελεγχομένων οργανισμών ούτε στην άμεση ή έμμεση επιρροή του κράτους ή των Länder»⁵⁰¹.

Το ΔΕΕ αποφάνθηκε επίσης ότι η φράση «πλήρης ανεξαρτησία» θα πρέπει να ερμηνευτεί λαμβανομένης υπόψη της ανεξαρτησίας του ΕΕΠΔ, όπως ορίζεται στον κανονισμό για την προστασία δεδομένων στα όργανα της ΕΕ. Στον εν λόγω κανονισμό, η έννοια της ανεξαρτησίας επιβάλλει στον ΕΕΠΔ να μη ζητεί ούτε να δέχεται εντολές από οποιονδήποτε.

498 ΔΕΕ, C-518/07, *Ευρωπαϊκή Επιτροπή κατά Ομοσπονδιακής Δημοκρατίας της Γερμανίας* [τμήμα μείζονος συνθέσεως], 9 Μαρτίου 2010, σκέψη 27.

499 Ό.π., σκέψεις 17 και 29.

500 Ό.π., σκέψη 23.

501 Ό.π., σκέψη 25.

Ως εκ τούτου, το ΔΕΕ αποφάνθηκε ότι –λόγω της επίβλεψης δημόσιων αρχών– οι εποπτικές αρχές στη Γερμανία δεν ήταν πλήρως ανεξάρτητες κατά την έννοια του δικαίου της ΕΕ για την προστασία δεδομένων.

Παράδειγμα: Στην υπόθεση *Ευρωπαϊκή Επιτροπή κατά Δημοκρατίας της Αυστρίας*⁵⁰², το ΔΕΕ επισήμανε παρόμοια προβλήματα με την ανεξαρτησία ορισμένων μελών και προσωπικού της αυστριακής αρχής προστασίας δεδομένων (επιτροπή προστασίας δεδομένων, DSK). Το ΔΕΕ κατέληξε στο συμπέρασμα ότι το γεγονός πως η Ομοσπονδιακή Καγκελαρία παρείχε στην εποπτική αρχή το προσωπικό της υπονόμει την απαίτηση ανεξαρτησίας που προβλέπεται στο δίκαιο της ΕΕ για την προστασία δεδομένων. Το ΔΕΕ αποφάνθηκε επίσης ότι η απαίτηση να ενημερώνεται συνεχώς η Καγκελαρία για το έργο της εποπτικής αρχής αναιρούσε την πλήρη ανεξαρτησία της εποπτικής αρχής.

Παράδειγμα: Στην υπόθεση *Ευρωπαϊκή Επιτροπή κατά Ουγγαρίας*⁵⁰³, παρόμοιες εθνικές πρακτικές που επηρέαζαν την ανεξαρτησία του προσωπικού απαγορεύτηκαν. Το ΔΕΕ επισήμανε ότι «η απαίτηση [...] περί διασφάλισης της ασκήσεως από κάθε αρχή ελέγχου των καθηκόντων που της έχουν ανατεθεί με πλήρη ανεξαρτησία συνεπάγεται για το οικείο κράτος μέλος την υποχρέωση σεβασμού της διάρκειας της θητείας τέτοιων αρχής μέχρι την αρχικώς προβλεπόμενη λήξη της». Το ΔΕΕ έκρινε επίσης ότι «[η] Ουγγαρία, θέτοντας πρόωρα τέρμα στη θητεία της αρχής ελέγχου της προστασίας των δεδομένων προσωπικού χαρακτήρα, παρέβη τις υποχρεώσεις που υπέχει από την οδηγία 95/46/ΕΚ [...]».

Η έννοια και τα κριτήρια της «πλήρους ανεξαρτησίας» προβλέπονται πλέον ρητά στον ΓΚΠΔ, ο οποίος ενσωματώνει τις αρχές που θεσπίστηκαν μέσω των ανωτέρω αποφάσεων του ΔΕΕ. Δυνάμει του κανονισμού, η πλήρης ανεξαρτησία των εποπτικών αρχών κατά την εκτέλεση των καθηκόντων τους και την άσκηση των εξουσιών τους συνεπάγεται τα εξής⁵⁰⁴:

502 ΔΕΕ, C-614/10, *Ευρωπαϊκή Επιτροπή κατά Δημοκρατίας της Αυστρίας* [τμήμα μείζονος συνθέσεως], 16 Οκτωβρίου 2012, σκέψεις 59 και 63.

503 ΔΕΕ, C-288/12, *Ευρωπαϊκή Επιτροπή κατά Ουγγαρίας* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014, σκέψεις 50 και 67.

504 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 52.

- τα μέλη κάθε εποπτικής αρχής δεν πρέπει να υφίστανται εξωτερικές επιρροές –άμεσες ή έμμεσες– και δεν πρέπει να ζητούν ούτε να λαμβάνουν οδηγίες από κανέναν·
- τα μέλη κάθε εποπτικής αρχής πρέπει να απέχουν από κάθε πράξη ασυμβίβαστη προς τα καθήκοντά τους, για την αποφυγή συγκρούσεων συμφερόντων·
- τα κράτη μέλη πρέπει να παρέχουν σε κάθε εποπτική αρχή τους απαραίτητους ανθρώπινους, τεχνικούς και οικονομικούς πόρους και τις υποδομές για την αποτελεσματική εκτέλεση των καθηκόντων της·
- τα κράτη μέλη πρέπει να διασφαλίζουν ότι κάθε εποπτική αρχή επιλέγει δικούς της υπαλλήλους·
- ο οικονομικός έλεγχος στον οποίο υπόκειται κάθε εποπτική αρχή βάσει του εθνικού δικαίου δεν πρέπει να επηρεάζει την ανεξαρτησία της. Οι εποπτικές αρχές πρέπει να διαθέτουν χωριστούς και δημόσιους ετήσιους προϋπολογισμούς, οι οποίοι καθιστούν εφικτή την ορθή λειτουργία τους.

Η ανεξαρτησία των εποπτικών αρχών θεωρείται επίσης ουσιώδης απαίτηση βάσει του δικαίου του Συμβουλίου της Ευρώπης. Η Εκσυγχρονισμένη Σύμβαση 108 υποχρεώνει τις εποπτικές αρχές να «ενεργούν με πλήρη ανεξαρτησία και αμεροληψία κατά την εκτέλεση των καθηκόντων και την άσκηση των εξουσιών τους», χωρίς να ζητούν ούτε να δέχονται οδηγίες⁵⁰⁵. Με τον τρόπο αυτό, η Σύμβαση αναγνωρίζει ότι οι αρχές αυτές μπορούν να προστατεύουν αποτελεσματικά τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που σχετίζονται με την επεξεργασία δεδομένων μόνο εφόσον ασκούν τα καθήκοντά τους με πλήρη ανεξαρτησία. Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 προβλέπονται ορισμένα στοιχεία τα οποία συμβάλλουν στη διαφύλαξη της ανεξαρτησίας αυτής. Τέτοια στοιχεία είναι η δυνατότητα των εποπτικών αρχών να προσλαμβάνουν δικούς τους υπαλλήλους και να λαμβάνουν αποφάσεις χωρίς να υπόκεινται σε εξωτερικές παρεμβάσεις, καθώς και παράγοντες που σχετίζονται με τη διάρκεια της άσκησης των καθηκόντων τους και με τις περιπτώσεις στις οποίες μπορεί να παύσουν να ασκούν τα καθήκοντά τους⁵⁰⁶.

505 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 15 παράγραφος 5.

506 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108.

5.2. Αρμοδιότητα και εξουσίες

Στο δίκαιο της ΕΕ, ο ΓΚΠΔ περιγράφει τις αρμοδιότητες και την οργανωτική δομή των εποπτικών αρχών και ορίζει ότι αυτές πρέπει να είναι αρμόδιες και να διαθέτουν εξουσία άσκησης των καθηκόντων που προβλέπονται από τον κανονισμό.

Η εποπτική αρχή είναι το κύριο όργανο, στο εθνικό δίκαιο, το οποίο διασφαλίζει τη συμμόρφωση προς τη νομοθεσία της ΕΕ για την προστασία δεδομένων. Οι εποπτικές αρχές διαθέτουν ολοκληρωμένο κατάλογο καθηκόντων και εξουσιών, πέραν της παρακολούθησης, ο οποίος περιλαμβάνει προδραστικές και προληπτικές δραστηριότητες εποπτείας. Για την εκτέλεση των καθηκόντων αυτών, οι εποπτικές αρχές πρέπει να διαθέτουν κατάλληλες εξουσίες έρευνας, διορθωτικές εξουσίες και συμβουλευτικές εξουσίες, οι οποίες απαριθμούνται στα άρθρα 57 και 58 του ΓΚΠΔ, όπως ⁵⁰⁷:

- να παρέχουν συμβουλές σε υπευθύνους επεξεργασίας και υποκείμενα των δεδομένων σε κάθε θέμα σχετικό με την προστασία δεδομένων·
- να εγκρίνουν τυποποιημένες συμβατικές ρήτρες, δεσμευτικούς εταιρικούς κανόνες ή διοικητικές ρυθμίσεις·
- να ερευνούν πράξεις επεξεργασίας και να επεμβαίνουν ανάλογα·
- να απαιτούν την υποβολή κάθε πληροφορίας που έχει σημασία για την εποπτεία των δραστηριοτήτων του υπευθύνου επεξεργασίας·
- να απευθύνουν προειδοποιήσεις ή επιπλήξεις σε υπευθύνους επεξεργασίας και να διατάσσουν την αποστολή στα υποκείμενα των δεδομένων γνωστοποιήσεων για την παραβίαση δεδομένων προσωπικού χαρακτήρα·
- να διατάσσουν τη διόρθωση, το κλείδωμα, τη διαγραφή ή την καταστροφή δεδομένων·
- να επιβάλλουν προσωρινή ή οριστική απαγόρευση της επεξεργασίας ή διοικητικά πρόστιμα·
- να παραπέμπουν υπόθεση στο δικαστήριο.

⁵⁰⁷ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 57 και 58. Βλ. επίσης Σύμβαση 108, πρόσθετο πρωτόκολλο, άρθρο 1.

Για την άσκηση των καθηκόντων της, η εποπτική αρχή πρέπει να έχει πρόσβαση σε όλα τα δεδομένα προσωπικού χαρακτήρα και τις πληροφορίες που απαιτούνται για την έρευνα, καθώς και σε όλους τους χώρους στους οποίους ο υπεύθυνος επεξεργασίας τηρεί σχετικές πληροφορίες. Σύμφωνα με το ΔΕΕ, οι εξουσίες της εποπτικής αρχής θα πρέπει να ερμηνεύονται ευρέως ώστε να διασφαλίζεται πλήρης αποτελεσματικότητα της προστασίας των δεδομένων για τα υποκείμενα των δεδομένων στην ΕΕ.

Παράδειγμα: Στην υπόθεση *Schrems*, το ΔΕΕ εξέτασε αν η διαβίβαση δεδομένων προσωπικού χαρακτήρα στις Ηνωμένες Πολιτείες της Αμερικής (ΗΠΑ), βάσει της πρώτης συμφωνίας ασφαλούς λιμένα μεταξύ ΕΕ και ΗΠΑ, ήταν σύμφωνη με το δίκαιο της ΕΕ για την προστασία δεδομένων, λαμβανομένων υπόψη των αποκαλύψεων του Edward Snowden. Κατά τη συλλογιστική του ΔΕΕ, οι εθνικές εποπτικές αρχές –ενεργώντας υπό την ιδιότητα του ανεξάρτητου παρατηρητή της επεξεργασίας δεδομένων από υπευθύνους επεξεργασίας– μπορούν να εμποδίζουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, παρά την ύπαρξη απόφασης επάρκειας, εάν υπάρχουν εύλογες αποδείξεις ότι η τρίτη χώρα δεν εγγυάται πλέον κατάλληλη προστασία⁵⁰⁸.

Κάθε εποπτική αρχή είναι αρμόδια να ασκεί εξουσίες έρευνας και παρέμβασης στην επικράτειά της. Ωστόσο, καθώς οι δραστηριότητες υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία έχουν συχνά διασυνοριακό χαρακτήρα και η επεξεργασία δεδομένων επηρεάζει υποκείμενα των δεδομένων που βρίσκονται σε περισσότερα κράτη μέλη, τίθεται το ζήτημα του καταμερισμού των αρμοδιοτήτων μεταξύ των διαφόρων εποπτικών αρχών. Το ΔΕΕ είχε την ευκαιρία να εξετάσει το ζήτημα αυτό στην υπόθεση *Weltimmo*.

Παράδειγμα: Στην υπόθεση *Weltimmo*⁵⁰⁹, το ΔΕΕ εξέτασε την αρμοδιότητα εθνικών εποπτικών αρχών να χειρίζονται υποθέσεις που αφορούν οργανισμούς μη εγκατεστημένους στη δικαιοδοσία τους. Η *Weltimmo* ήταν εταιρεία καταχωρισμένη στη Σλοβακία, η οποία διαχειριζόταν ιστοσελίδα μεσιτείας ακινήτων με αγγελίες για ακίνητα που βρίσκονταν

508 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015, σκέψεις 26-36 και 40-41.

509 ΔΕΕ, C-230/14, *Weltimmo s. r. o. κατά Nemzeti Adatvédelmi és Információs szabadság Hatóság*, 1 Οκτωβρίου 2015.

στην Ουγγαρία. Δημοσιεύοντας αγγελίες κατέθεσαν καταγγελία στην ουγγρική εποπτική αρχή προστασίας των δεδομένων για παράβαση του ουγγρικού δικαίου για την προστασία δεδομένων, και η αρχή επέβαλε πρόστιμο στη Weltimmo. Η εταιρεία προσέφυγε κατά του προστίμου ενώπιον των εθνικών δικαστηρίων και η υπόθεση παραπέμφθηκε στο ΔΕΕ, προκειμένου αυτό να εξακριβώσει αν η οδηγία της ΕΕ για την προστασία των δεδομένων επέτρεπε στις εποπτικές αρχές κράτους μέλους να εφαρμόσουν το οικείο εθνικό δίκαιο για την προστασία δεδομένων σε εταιρεία καταχωρισμένη σε άλλο κράτος μέλος.

Σύμφωνα με το ΔΕΕ, το άρθρο 4 παράγραφος 1 στοιχείο α) της Οδηγίας για την Προστασία των Δεδομένων επιτρέπει την εφαρμογή της νομοθεσίας για την προστασία δεδομένων κράτους μέλους διαφορετικού από εκείνο στο οποίο είναι καταχωρισμένος ο υπεύθυνος επεξεργασίας «υπό την προϋπόθεση ωστόσο ότι αυτός ασκεί, μέσω μόνιμης εγκαταστάσεως στο έδαφος του κράτους μέλους αυτού, πραγματική και ουσιαστικού χαρακτήρα δραστηριότητα, έστω και περιορισμένη, στο πλαίσιο της οποίας πραγματοποιείται η επεξεργασία αυτή». Το ΔΕΕ επισήμανε ότι, βάσει των πληροφοριών που είχε στη διάθεσή του, η Weltimmo ασκούσε πραγματική και ουσιαστικού χαρακτήρα δραστηριότητα στην Ουγγαρία, καθώς η εταιρεία είχε εκπρόσωπο στην Ουγγαρία ο οποίος ήταν καταχωρισμένος στο σλοβακικό μητρώο εταιρειών με διεύθυνση στην Ουγγαρία, καθώς και τραπεζικό λογαριασμό και γραμματοθυρίδα στην Ουγγαρία, και ασκούσε επίσης δραστηριότητες στην Ουγγαρία στην ουγγρική γλώσσα. Οι πληροφορίες αυτές υποδείκνυαν την ύπαρξη εγκατάστασης και καθιστούσαν τη δραστηριότητα της Weltimmo υποκείμενη στην ουγγρική νομοθεσία για την προστασία δεδομένων και στη δικαιοδοσία της ουγγρικής εποπτικής αρχής. Ωστόσο, το ΔΕΕ διευκρίνισε ότι εναπόκειται στο εθνικό δικαστήριο να εξακριβώσει τις πληροφορίες και να αποφασίσει αν, όντως, η Weltimmo διέθετε εγκατάσταση στην Ουγγαρία.

Εάν το αιτούν δικαστήριο διαπίστωνε ότι η Weltimmo διέθετε εγκατάσταση στην Ουγγαρία, η ουγγρική εποπτική αρχή θα είχε εξουσία επιβολής προστίμου. Ωστόσο, εάν το εθνικό δικαστήριο έκρινε το αντίθετο, δηλαδή ότι η Weltimmo δεν διαθέτει εγκατάσταση στην Ουγγαρία, το εφαρμοστέο δίκαιο θα ήταν, κατά συνέπεια, αυτό του κράτους μέλους ή των κρατών μελών στα οποία η εταιρεία είναι καταχωρισμένη. Στην περίπτωση αυτή, δεδομένου ότι οι εξουσίες των εποπτικών αρχών πρέπει να ασκούνται με σεβασμό της εδαφικής κυριαρχίας των άλλων κρατών μελών, η ουγγρική

αρχή δεν θα μπορούσε να επιβάλει κυρώσεις. Καθώς η Οδηγία για την Προστασία Δεδομένων περιλάμβανε υποχρέωση συνεργασίας των εποπτικών αρχών, η συγγρική αρχή θα μπορούσε, ωστόσο, να ζητήσει από τη σλοβακική ομόλογό της να εξετάσει την υπόθεση, να τεκμηριώσει παράβαση της σλοβακικής νομοθεσίας και να επιβάλει τις κυρώσεις που προβλέπονται από τη σλοβακική νομοθεσία.

Με την έκδοση του ΓΚΠΔ θεσπίστηκαν λεπτομερείς κανόνες σχετικά με την αρμοδιότητα των εποπτικών αρχών σε διασυνοριακές υποθέσεις. Ο κανονισμός θεσπίζει «μηχανισμό μίας στάσης» και προβλέπει διατάξεις που επιβάλλουν τη συνεργασία μεταξύ διαφορετικών εποπτικών αρχών. Για την αποτελεσματική συνεργασία σε διασυνοριακές υποθέσεις, ο ΓΚΠΔ απαιτεί τον καθορισμό επικεφαλής εποπτικής αρχής, η οποία είναι η εποπτική αρχή της κύριας ή της μόνης εγκατάστασης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία⁵¹⁰. Η επικεφαλής εποπτική αρχή είναι αρμόδια για διασυνοριακές υποθέσεις, είναι ο μοναδικός συνομιλητής του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και συντονίζει τη συνεργασία με άλλες εποπτικές αρχές για την επίτευξη συναίνεσης. Η συνεργασία περιλαμβάνει ανταλλαγή πληροφοριών, αμοιβαία παροχή συνδρομής για την παρακολούθηση και τη διερεύνηση, καθώς και λήψη δεσμευτικών αποφάσεων⁵¹¹.

Στο δίκαιο του Συμβουλίου της Ευρώπης, οι αρμοδιότητες και οι εξουσίες των εποπτικών αρχών προβλέπονται στο άρθρο 15 της Εκσυγχρονισμένης Σύμβασης 108. Οι εξουσίες αυτές αντιστοιχούν σε εκείνες που αναγνωρίζονται στις εποπτικές αρχές στο δίκαιο της ΕΕ, συμπεριλαμβανομένων εξουσιών έρευνας και παρέμβασης, έκδοσης αποφάσεων και επιβολής διοικητικών κυρώσεων σχετικά με παραβάσεις των διατάξεων της Σύμβασης, και εξουσιών να μετέχουν σε νομικές διαδικασίες. Οι ανεξάρτητες εποπτικές αρχές έχουν επίσης την αρμοδιότητα να χειρίζονται αιτήματα και καταγγελίες που υποβάλλονται από τα υποκείμενα των δεδομένων, να ευαισθητοποιούν το κοινό σχετικά με το δίκαιο για την προστασία δεδομένων και να παρέχουν συμβουλές σε εθνικούς υπευθύνους λήψης αποφάσεων σχετικά με κάθε νομοθετικό ή διοικητικό μέτρο το οποίο προβλέπει την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

⁵¹⁰ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 56 παράγραφος 1.

⁵¹¹ Ό.π., άρθρο 60.

5.3. Συνεργασία

Ο ΓΚΠΔ θεσπίζει γενικό πλαίσιο για τη συνεργασία μεταξύ εποπτικών αρχών και προβλέπει ειδικότερους κανόνες σχετικά με τη συνεργασία εποπτικών αρχών σε διασυνοριακές δραστηριότητες επεξεργασίας δεδομένων.

Βάσει του ΓΚΠΔ, οι εποπτικές αρχές παρέχουν αμοιβαία συνδρομή και ανταλλάσσουν σχετικές πληροφορίες για την υλοποίηση και την εφαρμογή του κανονισμού με συνεκτικό τρόπο ⁵¹². Μεταξύ άλλων, η εποπτική αρχή στην οποία υποβάλλεται αίτημα πραγματοποιεί διαβουλεύσεις, ελέγχους και έρευνες. Οι εποπτικές αρχές μπορούν να πραγματοποιούν κοινές επιχειρήσεις, μεταξύ άλλων και κοινές έρευνες, και να θεσπίζουν κοινά μέτρα επιβολής με τη συνεργασία υπαλλήλων από όλες τις εποπτικές αρχές ⁵¹³.

Στην ΕΕ, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία δραστηριοποιούνται ολοένα και περισσότερο σε διακρατικό επίπεδο. Αυτό επιβάλλει τη στενή συνεργασία μεταξύ των αρμόδιων εποπτικών αρχών των κρατών μελών, προκειμένου να διασφαλίζεται η συμμόρφωση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα προς τις απαιτήσεις του ΓΚΠΔ. Στο πλαίσιο του «μηχανισμού μίας στάσης» του κανονισμού, εάν υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία διαθέτει εγκαταστάσεις σε περισσότερα κράτη μέλη, ή εάν διαθέτει μία εγκατάσταση, αλλά οι πράξεις επεξεργασίας επηρεάζουν ουσιαστικά υποκείμενα δεδομένων σε περισσότερα του ενός κράτη μέλη, η εποπτική αρχή της κύριας (ή μόνης) εγκατάστασης είναι η επικεφαλής αρχή για τις διασυνοριακές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Οι επικεφαλής αρχές έχουν την εξουσία να λάβουν μέτρα επιβολής κατά του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Στόχος του «μηχανισμού μίας στάσης» είναι η βελτίωση της εναρμόνισης και της ομοιόμορφης εφαρμογής του δικαίου της ΕΕ για την προστασία δεδομένων στα διάφορα κράτη μέλη. Είναι επίσης επωφελής για τις επιχειρήσεις, καθώς μπορούν με τον τρόπο αυτό να επικοινωνούν μόνο με την επικεφαλής αρχή και όχι με πολλές εποπτικές αρχές. Αυτό αυξάνει την ασφάλεια δικαίου για τις επιχειρήσεις και, στην πράξη, θα έχει επίσης ως αποτέλεσμα οι αποφάσεις να λαμβάνονται ταχύτερα και να μη βρίσκονται οι επιχειρήσεις αντιμέτωπες με διαφορετικές εποπτικές αρχές οι οποίες εγείρουν αντικρουόμενες απαιτήσεις.

512 Ό.π., άρθρο 61 παράγραφοι 1 έως 3 και άρθρο 62 παράγραφος 1.

513 Ό.π., άρθρο 62 παράγραφος 1.

Ο προσδιορισμός της επικεφαλής αρχής προϋποθέτει τον καθορισμό του τόπου κύριας εγκατάστασης μιας επιχείρησης στην ΕΕ. Ο όρος «κύρια εγκατάσταση» ορίζεται στον ΓΚΠΔ. Επιπλέον, η Ομάδα εργασίας του άρθρου 29 εξέδωσε κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, οι οποίες περιλαμβάνουν τα κριτήρια για τον προσδιορισμό της κύριας εγκατάστασης ⁵¹⁴.

Προκειμένου να διασφαλίζεται υψηλό επίπεδο προστασίας των δεδομένων σε ολόκληρη την ΕΕ, η επικεφαλής εποπτική αρχή δεν ενεργεί μόνη. Πρέπει να συνεργάζεται με τις άλλες ενδιαφερόμενες εποπτικές αρχές για τη λήψη αποφάσεων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία, σε μια προσπάθεια επίτευξης συναίνεσης και διασφάλισης συνεκτικότητας. Η συνεργασία μεταξύ των αρμόδιων εποπτικών αρχών περιλαμβάνει ανταλλαγή πληροφοριών, αμοιβαία συνδρομή και διενέργεια κοινών ερευνών και δραστηριοτήτων παρακολούθησης ⁵¹⁵. Όταν παρέχουν αμοιβαία συνδρομή, οι εποπτικές αρχές πρέπει να χειρίζονται με ακρίβεια τα αιτήματα πληροφοριών που υποβάλλουν άλλες εποπτικές αρχές και να λαμβάνουν μέτρα ελέγχου, όπως, για παράδειγμα, προηγούμενες εγκρίσεις και διαβουλεύσεις με τον υπεύθυνο επεξεργασίας σχετικά με τις δραστηριότητες επεξεργασίας του, ελέγχους ή έρευνες. Η αμοιβαία συνδρομή σε εποπτικές αρχές άλλων κρατών πρέπει να παρέχεται κατόπιν αιτήματος αμελητή και το αργότερο έναν μήνα μετά την παραλαβή του αιτήματος ⁵¹⁶.

Όταν ο υπεύθυνος επεξεργασίας διαθέτει εγκαταστάσεις σε περισσότερα κράτη μέλη, οι εποπτικές αρχές μπορούν να διεξάγουν κοινές επιχειρήσεις, μεταξύ άλλων έρευνες και μέτρα επιβολής, στις οποίες συμμετέχουν μέλη του προσωπικού των εποπτικών αρχών των άλλων κρατών μελών ⁵¹⁷.

Η συνεργασία μεταξύ διαφόρων εποπτικών αρχών είναι σημαντική απαίτηση και στο πλαίσιο του δικαίου του Συμβουλίου της Ευρώπης. Η Εκσυγχρονισμένη Σύμβαση 108 προβλέπει ότι οι εποπτικές αρχές πρέπει να συνεργάζονται μεταξύ τους στον βαθμό που είναι αναγκαίος για την εκτέλεση των καθηκόντων τους ⁵¹⁸.

514 Ομάδα εργασίας του άρθρου 29 (2016), *Κατευθυντήριες γραμμές για τον προσδιορισμό της επικεφαλής εποπτικής αρχής των υπευθύνων επεξεργασίας ή των εκτελούντων την επεξεργασία*, WP 244, Βρυξέλλες, 13 Δεκεμβρίου 2016, όπως αναθεωρήθηκε στις 5 Απριλίου 2017.

515 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 60 παράγραφοι 1 έως 3.

516 Ό.π., άρθρο 61 παράγραφοι 1 και 2.

517 Ό.π., άρθρο 62 παράγραφος 1.

518 Εκσυγχρονισμένη Σύμβαση 108, άρθρα 16 και 17.

Η συνεργασία αυτή θα πρέπει να περιλαμβάνει, για παράδειγμα, ανταλλαγή κάθε σχετικής και χρήσιμης πληροφορίας καθώς και συντονισμό ερευνών και ανάληψη κοινών δράσεων ⁵¹⁹.

5.4. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Η σημασία των ανεξάρτητων εποπτικών αρχών και οι κύριες αρμοδιότητες που τους ανατίθενται στο πλαίσιο του ευρωπαϊκού δικαίου για την προστασία δεδομένων περιγράφηκαν σε προηγούμενο τμήμα του παρόντος κεφαλαίου. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) είναι ένας ακόμη σημαντικός παράγοντας για τη διασφάλιση της αποτελεσματικής και συνεκτικής εφαρμογής των κανόνων περί προστασίας δεδομένων σε ολόκληρη την ΕΕ.

Ο ΓΚΠΔ σύστησε το ΕΣΠΔ ως όργανο της ΕΕ με νομική προσωπικότητα ⁵²⁰. Είναι ο διάδοχος της Ομάδας εργασίας του άρθρου 29 ⁵²¹, η οποία είχε συσταθεί δυνάμει της Οδηγία για την Προστασία Δεδομένων με σκοπό να συμβουλευεί την Επιτροπή σχετικά με μέτρα της ΕΕ που επηρεάζουν τα δικαιώματα των φυσικών προσώπων ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ιδιωτική ζωή, να προάγει την ομοιόμορφη εφαρμογή της οδηγίας και να παρέχει γνώμες εμπειρογνώμονα στην Επιτροπή σε θέματα σχετικά με την προστασία δεδομένων. Η Ομάδα εργασίας του άρθρου 29 απαρτιζόταν από εκπροσώπους των εποπτικών αρχών των κρατών μελών της ΕΕ, καθώς και εκπροσώπους της Επιτροπής και του ΕΕΠΔ.

Όπως και η Ομάδα εργασίας του άρθρου 29, το ΕΣΠΔ απαρτίζεται από τους προϊσταμένους των εποπτικών αρχών των κρατών μελών και τον ΕΕΠΔ ή τους εκπροσώπους τους ⁵²². Ο ΕΕΠΔ έχει τα ίδια δικαιώματα ψήφου με τους προϊσταμένους των εποπτικών αρχών των κρατών μελών, με εξαίρεση υποθέσεις που

519 Ό.π., άρθρο 17.

520 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 68.

521 Βάσει της οδηγίας 95/46/ΕΚ, η Ομάδα εργασίας του άρθρου 29 έπρεπε να παρέχει συμβουλές στην Επιτροπή σχετικά με κάθε μέτρο της ΕΕ που επηρεάζει τα δικαιώματα των φυσικών προσώπων ως προς την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την ιδιωτική ζωή, να προάγει την ομοιόμορφη εφαρμογή της οδηγίας και να παρέχει γνώμες εμπειρογνώμονα στην Επιτροπή σε θέματα σχετικά με την προστασία δεδομένων. Η Ομάδα εργασίας του άρθρου 29 απαρτιζόταν από εκπροσώπους των εποπτικών αρχών των κρατών μελών της ΕΕ, καθώς και εκπροσώπους της Επιτροπής και του ΕΕΠΔ.

522 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 68 παράγραφος 3.

σχετίζονται με επίλυση διαφορών, στις οποίες μπορεί να ψηφίζει μόνο σε σχέση με αποφάσεις που αφορούν τις αρχές και τους κανόνες που ισχύουν στα θεσμικά όργανα της Ένωσης και οι οποίοι αντιστοιχούν κατ' ουσίαν προς εκείνους του ΓΚΠΔ. Η Επιτροπή δικαιούται να συμμετέχει στις δραστηριότητες και στις συνεδριάσεις του ΕΣΠΔ, αλλά δεν έχει δικαίωμα ψήφου ⁵²³. Το ΕΣΠΔ εκλέγει τον πρόεδρό του (ο οποίος το εκπροσωπεί) και δύο αναπληρωτές προέδρους από τα μέλη του με απλή πλειοψηφία για πενταετή θητεία. Επιπλέον, το ΕΣΠΔ έχει στη διάθεσή του γραμματεία, την οποία παρέχει ο ΕΕΠΔ, ώστε το ΕΣΠΔ να διαθέτει αναλυτική, διοικητική και υλικοτεχνική στήριξη ⁵²⁴.

Τα καθήκοντα του ΕΣΠΔ περιγράφονται αναλυτικά στα άρθρα 64, 65 και 70 του ΓΚΠΔ και περιλαμβάνουν ολοκληρωμένες υποχρεώσεις που μπορούν να υποδιαιρεθούν σε τρεις κύριες δραστηριότητες:

- **Συνεκτικότητα:** Το ΕΣΠΔ μπορεί να εκδίδει νομικά δεσμευτικές αποφάσεις σε τρεις περιπτώσεις: όταν εποπτική αρχή προβάλλει σχετική και αιτιολογημένη ένσταση σε υποθέσεις του «μηχανισμού μίας στάσης»· όταν υπάρχει διαφωνία σχετικά με την επικεφαλής εποπτική αρχή· και, τέλος, όταν η αρμόδια εποπτική αρχή δεν ζητεί ή δεν εφαρμόζει τη γνώμη του ΕΣΠΔ ⁵²⁵. Κύρια ευθύνη του ΕΣΠΔ είναι να διασφαλίζει τη συνεκτική εφαρμογή του ΓΚΠΔ σε ολόκληρη την ΕΕ, και διαδραματίζει καθοριστικό ρόλο στον μηχανισμό συνεκτικότητας, ο οποίος περιγράφεται στην [ενότητα 5.5](#).
- **Διαβούλευση:** Τα καθήκοντα του ΕΣΠΔ περιλαμβάνουν την παροχή συμβουλών στην Επιτροπή σχετικά με κάθε θέμα το οποίο αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ένωση, όπως τροποποιήσεις του ΓΚΠΔ, αναθεωρήσεις της νομοθεσίας της ΕΕ που αφορούν επεξεργασία δεδομένων και ενδέχεται να έλθουν σε σύγκρουση με τους κανόνες της ΕΕ περί προστασίας δεδομένων ή έκδοση αποφάσεων επάρκειας από την Επιτροπή, οι οποίες επιτρέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό.
- **Καθοδήγηση:** Το ΕΣΠΔ εκδίδει επίσης κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για να προωθήσει τη συνεκτική εφαρμογή του κανονισμού και προάγει τη συνεργασία και την ανταλλαγή γνώσεων μεταξύ

⁵²³ Ό.π., άρθρο 68 παράγραφοι 4 και 5.

⁵²⁴ Ό.π., άρθρα 73 και 75.

⁵²⁵ Ό.π., άρθρο 65.

εποπτικών αρχών. Επιπλέον, πρέπει να παροτρύνει τις ενώσεις υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία να καταρτίζουν κώδικες δεοντολογίας και να θεσπίζουν μηχανισμούς πιστοποίησης και σφραγίδες προστασίας δεδομένων.

Οι αποφάσεις του ΕΣΠΔ μπορούν να προσβληθούν ενώπιον του ΔΕΕ.

5.5. Ο μηχανισμός συνεκτικότητας του ΓΚΠΔ

Ο ΓΚΠΔ θεσπίζει μηχανισμό συνεκτικότητας για τη διασφάλιση της συνεκτικής εφαρμογής του κανονισμού σε όλα τα κράτη μέλη, στο πλαίσιο του οποίου οι εποπτικές αρχές συνεργάζονται μεταξύ τους και, κατά περίπτωση, με την Επιτροπή. Ο μηχανισμός συνεκτικότητας χρησιμοποιείται σε δύο περιπτώσεις. Η πρώτη αφορά γνώμες του ΕΣΠΔ σε περιπτώσεις στις οποίες η αρμόδια εποπτική αρχή προτίθεται να θεσπίσει μέτρα, όπως κατάλογο πράξεων επεξεργασίας που απαιτούν εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων, ή να καθορίσει τυποποιημένες συμβατικές ρήτρες. Η δεύτερη περίπτωση αφορά δεσμευτικές αποφάσεις του ΕΣΠΔ για τις εποπτικές αρχές σε υποθέσεις «μηχανισμού μίας στάσης», στις οποίες η εποπτική αρχή δεν εφαρμόζει ή δεν ζητεί τη γνώμη του ΕΣΠΔ.

6

Δικαιώματα των υποκειμένων των δεδομένων και επιβολή τους

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Δικαίωμα ενημέρωσης		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 12 ΔΕΕ, C-473/12, <i>Institut professionnel des agents immobiliers (IPI) κατά Englebert</i> κ.λπ., 2013 ΔΕΕ, C-201/14, <i>Smaranda Bara</i> κ.λπ. κατά <i>Casa Națională de Asigurări de Sănătate</i> κ.λπ., 2015	Διαφάνεια πληροφοριών	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφοι 1 και 2 και άρθρο 14 παράγραφοι 1 και 2	Περιεχόμενο πληροφοριών	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 παράγραφος 1
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 1 και άρθρο 14 παράγραφος 3	Χρόνος παροχής πληροφοριών	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο β).
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 12 παράγραφοι 1, 5 και 7	Τρόπος παροχής πληροφοριών	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο β).
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο δ) και άρθρο 14 παράγραφος 2 στοιχείο ε), άρθρα 77, 78 και 79	Δικαίωμα υποβολής καταγγελίας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο στ)

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Δικαίωμα πρόσβασης		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 15 παράγραφος 1 ΔΕΕ, C-553/07, <i>College van burgemeester en wethouders van Rotterdam</i> κατά <i>E. E. Rijkeboer</i>, 2009 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, <i>YS</i> κατά <i>Minister voor Immigratie, Integratie en Asiel</i> και <i>Minister voor Immigratie, Integratie en Asiel</i> κατά <i>M</i> και <i>S</i>, 2014 ΔΕΕ, C-434/16, <i>Peter Nowak</i> κατά <i>Data Protection Commissioner</i>, 2017	Δικαίωμα πρόσβασης του φυσικού προσώπου στα δεδομένα που το αφορούν	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο β) ΕΔΔΑ, <i>Leander</i> κατά <i>Σουηδίας</i>, προσφυγή αριθ. 9248/81, 1987
Δικαίωμα διόρθωσης		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 16	Διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο ε) ΕΔΔΑ, <i>Cemalettin Canli</i> κατά <i>Τουρκίας</i>, προσφυγή αριθ. 22427/04, 2008 ΕΔΔΑ, <i>Giubotaru</i> κατά <i>Μολδαβίας</i>, προσφυγή αριθ. 27138/04, 2010
Δικαίωμα διαγραφής		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 17 παράγραφος 1	Η διαγραφή δεδομένων προσωπικού χαρακτήρα	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο ε) ΕΔΔΑ, <i>Segerstedt-Wiberg</i> κ.λπ. κατά <i>Σουηδίας</i>, προσφυγή αριθ. 62332/00, 2006
ΔΕΕ, C-131/12, <i>Google Spain SL, Google Inc.</i> κατά <i>Agencia Española de Protección de Datos (AEPD)</i>, <i>Mario Costeja González</i> [τμήμα μείζονος συνθέσεως], 2014 ΔΕΕ, C-398/15, <i>Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce</i> κατά <i>Salvatore Manni</i>, 2017	Το δικαίωμα στη λήθη	

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Δικαίωμα περιορισμού της επεξεργασίας		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 18 παράγραφος 1	Δικαίωμα περιορισμού της χρήσης των δεδομένων προσωπικού χαρακτήρα	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 19	Υποχρέωση γνωστοποίησης	
Δικαίωμα στη φορητότητα των δεδομένων		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 20	Δικαίωμα στη φορητότητα των δεδομένων	
Δικαίωμα εναντίωσης		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 21 παράγραφος 1 <i>ΔΕΕ, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni, 2017</i>	Δικαίωμα εναντίωσης για λόγους που σχετίζονται με την ιδιαίτερη κατάσταση του υποκειμένου των δεδομένων	Σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 5 παράγραφος 3 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο δ)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 21 παράγραφος 2	Δικαίωμα εναντίωσης στη χρήση δεδομένων για σκοπούς εμπορικής προώθησης	Σύσταση σχετικά με την άμεση εμπορική προώθηση, άρθρο 4 παράγραφος 1
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 21 παράγραφος 5	Δικαίωμα εναντίωσης με αυτοματοποιημένα μέσα	
Δικαιώματα τα οποία σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 22	Δικαιώματα τα οποία σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο α)
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 21	Δικαιώματα εναντίωσης στην αυτοματοποιημένη λήψη αποφάσεων	

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο στ)	Δικαιώματα σε λογική εξήγηση	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο γ)
Προσφυγές, ευθύνη, κυρώσεις και αποζημίωση		
Ο Χάρτης, άρθρο 47 ΔΕΕ, C-362/14, <i>Maximillian Schrems κατά Data Protection Commissioner</i> [τμήμα μείζονος συνθέσεως], 2015 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 77 έως 84	Για παραβάσεις του εθνικού δικαίου για την προστασία δεδομένων	ΕΣΔΑ, άρθρο 13 (μόνο για τα κράτη μέλη του Συμβουλίου της Ευρώπης) Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο στ), άρθρα 12, 15, 16-21 ΕΔΔΑ, <i>Κ.Υ. κατά Φινλανδίας</i> , προσφυγή αριθ. 2872/02, 2008 ΕΔΔΑ, <i>Biriuk κατά Λιθουανίας</i> , προσφυγή αριθ. 23373/03, 2008
Κανονισμός για την προστασία δεδομένων στα όργανα της ΕΕ, άρθρα 34 και 49 ΔΕΕ, C-28/08 P, <i>Ευρωπαϊκή Επιτροπή κατά The Bavarian Lager Co. Ltd</i> [τμήμα μείζονος συνθέσεως], 2010	Για παραβάσεις του δικαίου της ΕΕ από όργανα και οργανισμούς της ΕΕ	

Η αποτελεσματικότητα των κανόνων δικαίου εν γένει, και των δικαιωμάτων των υποκειμένων των δεδομένων ειδικότερα, εξαρτάται σε σημαντικό βαθμό από την ύπαρξη κατάλληλων μηχανισμών επιβολής τους. Στην ψηφιακή εποχή, η επεξεργασία δεδομένων είναι πανταχού παρούσα και γίνεται ολοένα και πιο δυσνόητη για τα φυσικά πρόσωπα. Για τον μετριασμό των ανισορροπιών ισχύος μεταξύ υποκειμένων των δεδομένων και υπευθύνων επεξεργασίας, τα φυσικά πρόσωπα έχουν ορισμένα δικαιώματα ώστε να ασκούν μεγαλύτερο έλεγχο στην επεξεργασία των προσωπικών πληροφοριών τους. Το δικαίωμα πρόσβασης του φυσικού προσώπου στα δεδομένα που το αφορούν και το δικαίωμα διόρθωσης αυτών κατοχυρώνονται στο άρθρο 8 παράγραφος 2 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, έγγραφο το οποίο συνιστά πρωτογενές δίκαιο της ΕΕ και έχει θεμελιώδη αξία στην έννομη τάξη της ΕΕ. Στο παράγωγο δίκαιο της ΕΕ –ειδικότερα στον Γενικό Κανονισμό για την Προστασία Δεδομένων– θεσπίζεται συνεκτικό νομικό πλαίσιο, το οποίο ενισχύει τα υποκείμενα των δεδομένων παρέχοντάς τους δικαιώματα έναντι των υπευθύνων επεξεργασίας. Επιπροσθέτως

των δικαιωμάτων πρόσβασης και διόρθωσης, ο ΓΚΠΔ αναγνωρίζει σειρά άλλων δικαιωμάτων, όπως το δικαίωμα διαγραφής («δικαίωμα στη λήθη»), το δικαίωμα εναντίωσης στην επεξεργασία δεδομένων ή περιορισμού αυτής, καθώς και δικαιώματα που σχετίζονται με την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ. Παρόμοιες εγγυήσεις οι οποίες παρέχουν στα υποκείμενα των δεδομένων τη δυνατότητα να ασκούν αποτελεσματικό έλεγχο επί των δεδομένων που τα αφορούν περιέχονται επίσης στην Εκσυγχρονισμένη Σύμβαση 108. Στο άρθρο 9 απαριθμούνται τα δικαιώματα τα οποία θα πρέπει να μπορούν να ασκούν τα φυσικά πρόσωπα σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Τα συμβαλλόμενα μέρη πρέπει να διασφαλίζουν ότι τα δικαιώματα αυτά παρέχονται σε κάθε υποκείμενο δεδομένων στη δικαιοδοσία τους και ότι συνοδεύονται από αποτελεσματικά νομικά και πρακτικά μέσα ώστε τα υποκείμενα των δεδομένων να μπορούν να τα ασκούν.

Πέραν της παροχής δικαιωμάτων στα φυσικά πρόσωπα, είναι εξίσου σημαντικό να θεσπίζονται μηχανισμοί οι οποίοι να παρέχουν στα υποκείμενα των δεδομένων τη δυνατότητα να προσφεύγουν κατά της παραβίασης των δικαιωμάτων τους, να αποδίδουν ευθύνη στους υπευθύνους επεξεργασίας και να αξιώνουν αποζημίωση. Το δικαίωμα πραγματικής προσφυγής, όπως κατοχυρώνεται στην ΕΣΔΑ και στον Χάρτη, απαιτεί να διατίθενται σε κάθε πρόσωπο το δικαίωμα δικαστικής προσφυγής.

6.1. Τα δικαιώματα των υποκειμένων των δεδομένων

Κύρια σημεία

- Με την επιφύλαξη περιορισμένων εξαιρέσεων, κάθε υποκείμενο δεδομένων δικαιούται να ενημερώνεται σχετικά με οποιαδήποτε επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν από τον εκάστοτε υπεύθυνο επεξεργασίας.
- Τα υποκείμενα των δεδομένων έχουν δικαίωμα:
 - πρόσβασης στα δεδομένα τους και εξασφάλισης ορισμένων πληροφοριών σχετικά με την επεξεργασία·
 - διόρθωσης των δεδομένων τους από τον υπεύθυνο επεξεργασίας, εάν τα δεδομένα είναι ανακριβή·

- διαγραφής των δεδομένων τους από τον υπεύθυνο επεξεργασίας, κατά περίπτωση, εάν ο υπεύθυνος επεξεργασίας επεξεργάζεται τα δεδομένα που τα αφορούν κατά παράβαση του νόμου·
- προσωρινού περιορισμού της επεξεργασίας·
- μεταφοράς των δεδομένων που τα αφορούν σε άλλον υπεύθυνο επεξεργασίας, υπό ορισμένες προϋποθέσεις.
- Επιπλέον, τα υποκείμενα των δεδομένων έχουν το δικαίωμα να εναντιωθούν στην επεξεργασία:
 - για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή τους·
 - λόγω χρήσης των δεδομένων που τα αφορούν για άμεση εμπορική προώθηση.
- Τα υποκείμενα των δεδομένων έχουν δικαίωμα να μην υπόκεινται σε αποφάσεις που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ, οι οποίες παράγουν έννομα αποτελέσματα ή τα επηρεάζουν σημαντικά. Τα υποκείμενα των δεδομένων έχουν επίσης δικαίωμα:
 - εξασφάλισης ανθρώπινης παρέμβασης από τον υπεύθυνο επεξεργασίας·
 - έκφρασης άποψης και αμφισβήτησης της απόφασης που βασίζεται σε αυτοματοποιημένη επεξεργασία.

6.1.1. Δικαίωμα ενημέρωσης

Σύμφωνα με το **δίκαιο του Συμβουλίου της Ευρώπης** και το **δίκαιο της ΕΕ**, οι υπεύθυνοι πράξεων επεξεργασίας υποχρεούνται να ενημερώνουν το υποκείμενο των δεδομένων κατά τη συλλογή των δεδομένων προσωπικού χαρακτήρα που τα αφορούν σχετικά με τη σκοπούμενη επεξεργασία τους. Η υποχρέωση αυτή δεν εξαρτάται από αίτημα του υποκειμένου των δεδομένων, αλλά αντιθέτως ο υπεύθυνος επεξεργασίας πρέπει να συμμορφώνεται προς αυτήν προδραστικά, ανεξάρτητα από το αν το υποκείμενο των δεδομένων θα εκφράσει ενδιαφέρον για την ενημέρωση.

Στο δίκαιο του Συμβουλίου της Ευρώπης, βάσει του άρθρου 8 της Εκσυγχρονισμένης Σύμβασης 108, τα συμβαλλόμενα μέρη πρέπει να προβλέπουν ότι οι υπεύθυνοι επεξεργασίας θα ενημερώνουν τα υποκείμενα των δεδομένων σχετικά με την ταυτότητα και τη συνήθη διαμονή τους, τη νομική βάση και τον σκοπό της επεξεργασίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, τους αποδέκτες των δεδομένων προσωπικού

χαρακτήρα που τα αφορούν (εφόσον υπάρχουν) και τον τρόπο με τον οποίο μπορούν να ασκήσουν τα προβλεπόμενα στο άρθρο 9 δικαιώματά τους, στα οποία περιλαμβάνονται τα δικαιώματα πρόσβασης, διόρθωσης και προσφυγής. Κάθε άλλη πρόσθετη πληροφορία η οποία θεωρείται αναγκαία για τη διασφάλιση αντικειμενικής και διαφανούς επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει επίσης να γνωστοποιείται στα υποκείμενα των δεδομένων. Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 διευκρινίζεται ότι οι πληροφορίες που παρουσιάζονται στα υποκείμενα των δεδομένων «θα πρέπει να είναι προσβάσιμες, ευανάγνωστες, κατανοητές και προσαρμοσμένες στα οικεία υποκείμενα των δεδομένων»⁵²⁶.

Βάσει του δικαίου της ΕΕ, η αρχή της διαφάνειας απαιτεί κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα να είναι γενικά διαφανής για τα φυσικά πρόσωπα. Τα φυσικά πρόσωπα έχουν το δικαίωμα να γνωρίζουν ποια δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται ή υποβάλλονται άλλως σε επεξεργασία, και με ποιον τρόπο, καθώς και να ενημερώνονται για τους κινδύνους, τις εγγυήσεις και τα δικαιώματά τους σε σχέση με την επεξεργασία⁵²⁷. Πράγματι, το άρθρο 12 του ΓΚΠΔ καθορίζει ευρεία και συνολική υποχρέωση των υπευθύνων επεξεργασίας να παρέχουν διαφανείς πληροφορίες και/ή να ανακοινώνουν στα υποκείμενα των δεδομένων τον τρόπο με τον οποίο μπορούν να ασκήσουν τα δικαιώματά τους⁵²⁸. Οι πληροφορίες πρέπει να είναι συνοπτικές, διαφανείς, κατανοητές και εύκολα προσβάσιμες, και να παρέχονται με σαφή και απλή διατύπωση. Πρέπει να παρέχονται εγγράφως, μεταξύ άλλων ηλεκτρονικώς, εφόσον ενδείκνυται, ενώ μπορούν να παρέχονται ακόμη και προφορικώς, κατόπιν αιτήματος του υποκειμένου των δεδομένων, εφόσον η ταυτότητα του υποκειμένου των δεδομένων αποδεικνύεται αδιαμφισβήτητη. Οι πληροφορίες παρέχονται χωρίς υπερβολική καθυστέρηση ή υπερβολικά έξοδα⁵²⁹.

Στα άρθρα 13 και 14 του ΓΚΠΔ εξετάζεται το δικαίωμα ενημέρωσης των υποκειμένων των δεδομένων σε περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα συλλέγονται απευθείας από αυτά και σε περιπτώσεις στις οποίες δεν συλλέγονται από αυτά, αντίστοιχα.

526 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 68.

527 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 39.

528 Ο.π., άρθρα 13 και 14· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 παράγραφος 1 στοιχείο β).

529 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 12 παράγραφος 5· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο β).

Η έκταση του δικαιώματος ενημέρωσης και οι περιορισμοί του στο πλαίσιο του δικαίου της ΕΕ έχουν αποσαφηνιστεί στη νομολογία του ΔΕΕ.

Παράδειγμα: Στην υπόθεση *Institut professionnel des agents immobiliers (IPI) κατά Englebert* ⁵³⁰, το ΔΕΕ κλήθηκε να ερμηνεύσει το άρθρο 13 παράγραφος 1 της οδηγίας 95/46. Το άρθρο αυτό παρέχει στα κράτη μέλη τη δυνατότητα να επιλέξουν αν θα θεσπίσουν νομοθετικά μέτρα για να περιορίσουν την εμβέλεια του δικαιώματος ενημέρωσης του υποκειμένου των δεδομένων όταν αυτό είναι αναγκαίο για την προστασία, μεταξύ άλλων, των δικαιωμάτων και των ελευθεριών τρίτων και για την πρόληψη και τη διερεύνηση παραβάσεων του ποινικού νόμου ή της δεοντολογίας των νομοθετικά κατοχυρωμένων επαγγελματιών. Το IPI είναι επαγγελματική οργάνωση κτηματομεσιτών στο Βέλγιο, αρμόδια για τη διασφάλιση της συμμόρφωσης προς την ορθή πρακτική του επαγγέλματος του κτηματομεσίτη. Ζήτησε από εθνικό δικαστήριο να αναγνωρίσει ότι οι εναγόμενοι είχαν παραβεί επαγγελματικούς κανόνες και να τους διατάξει να παύσουν διάφορες κτηματομεσιτικές δραστηριότητες. Η αγωγή βασίστηκε σε αποδεικτικά στοιχεία τα οποία είχαν συλλέξει ιδιωτικοί ντετέκτιβ, τους οποίους είχε χρησιμοποιήσει το IPI.

Το εθνικό δικαστήριο είχε αμφιβολίες για την αξία των αποδεικτικών στοιχείων των ντετέκτιβ, καθώς υπήρχε το ενδεχόμενο να είχαν αποκτηθεί χωρίς να τηρηθούν οι απαιτήσεις περί προστασίας των δεδομένων της βελγικής νομοθεσίας, και ιδίως η υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν πριν από τη συλλογή των σχετικών πληροφοριών. Το ΔΕΕ επισήμανε ότι, σύμφωνα με το άρθρο 13 παράγραφος 1, τα κράτη μέλη «μπορούν», αλλά δεν υποχρεούνται να προβλέπουν στην εθνική νομοθεσία τους εξαιρέσεις από την υποχρέωση ενημέρωσης των υποκειμένων των δεδομένων για την επεξεργασία των δεδομένων τους. Καθώς το άρθρο 13 παράγραφος 1 προβλέπει την πρόληψη, τη διερεύνηση, τη διαπίστωση και τη δίωξη παραβάσεων του ποινικού νόμου ή της δεοντολογίας ως λόγους για τους οποίους τα κράτη μέλη μπορούν να περιορίζουν τα δικαιώματα των φυσικών προσώπων, η δραστηριότητα οργάνωσης όπως το IPI και των

530 ΔΕΕ, C-473/12, *Institut professionnel des agents immobiliers (IPI) κατά Geoffrey Englebert* κ.λπ., 7 Νοεμβρίου 2013.

ιδιωτικών ντετέκτιβ που ενήργησαν για λογαριασμό της θα μπορούσε να βασιστεί στη διάταξη αυτή. Ωστόσο, εάν το κράτος μέλος δεν προβλέπει τέτοια εξαίρεση, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται.

Παράδειγμα: Στην υπόθεση *Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ.*⁵³¹, το ΔΕΕ κλήθηκε να διευκρινίσει αν σύμφωνα με το δίκαιο της ΕΕ απαγορεύεται η διαβίβαση δεδομένων προσωπικού χαρακτήρα από εθνική διοικητική αρχή σε άλλη διοικητική αρχή για μεταγενέστερη επεξεργασία, χωρίς ενημέρωση των υποκειμένων των δεδομένων σχετικά με την εν λόγω διαβίβαση και επεξεργασία. Στην εν λόγω υπόθεση, η εθνική φορολογική αρχή δεν ενημέρωσε τους προσφεύγοντες, πριν από τη διαβίβαση, ότι επρόκειτο να διαβιβάσει τα δεδομένα που τους αφορούσαν στο εθνικό ταμείο κοινωνικών ασφαλίσεων.

Το ΔΕΕ έκρινε ότι η απαίτηση του δικαίου της ΕΕ περί ενημέρωσης των υποκειμένων των δεδομένων σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν «έχει ακόμη μεγαλύτερη σημασία καθώς από αυτήν εξαρτάται η άσκηση από τα πρόσωπα αυτά του δικαιώματός τους να έχουν πρόσβαση στα υπό επεξεργασία δεδομένα [...] και του δικαιώματός τους να αντιτάσσονται στην επεξεργασία των εν λόγω δεδομένων». Η αρχή της θεμιτής επεξεργασίας απαιτεί να ενημερώνονται τα υποκείμενα των δεδομένων για τη διαβίβαση των δεδομένων που τα αφορούν σε άλλο δημόσιο φορέα για περαιτέρω επεξεργασία από τον εν λόγω φορέα. Σύμφωνα με το άρθρο 13 παράγραφος 1 της οδηγίας 95/46, τα κράτη μέλη μπορούν να περιορίζουν το δικαίωμα ενημέρωσης, εάν αυτό είναι αναγκαίο για τη διαφύλαξη σημαντικού οικονομικού συμφέροντος του κράτους, συμπεριλαμβανομένων φορολογικών θεμάτων. Ωστόσο, οι περιορισμοί αυτοί πρέπει να επιβάλλονται με νομοθετικά μέτρα. Δεδομένου ότι ο καθορισμός των δεδομένων που επρόκειτο να διαβιβαστούν και οι λεπτομερείς ρυθμίσεις για τη διαβίβαση δεν προβλέπονταν σε νομοθετικό μέτρο, αλλά μόνο σε πρωτόκολλο μεταξύ των δύο δημόσιων αρχών, δεν πληρούνταν οι προϋποθέσεις παρέκκλισης βάσει του δικαίου της ΕΕ. Οι προσφεύγοντες θα έπρεπε να

531 ΔΕΕ, C-201/14, *Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ.*, 1 Οκτωβρίου 2015.

έχουν ενημερωθεί εκ των προτέρων για τη διαβίβαση των δεδομένων τους στο Εθνικό Ταμείο Κοινωνικών Ασφαλίσεων και για τη μεταγενέστερη επεξεργασία των δεδομένων αυτών από τον εν λόγω φορέα.

Περιεχόμενο των πληροφοριών

Βάσει του άρθρου 8 παράγραφος 1 της Εκσυγχρονισμένης Σύμβασης 108, ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία η οποία διασφαλίζει θεμιτή και διαφανή επεξεργασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων:

- της ταυτότητας και της συνήθους διαμονής ή εγκατάστασης του υπευθύνου επεξεργασίας
- της νομικής βάσης και των στόχων της σκοπούμενης επεξεργασίας
- των κατηγοριών δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία
- των αποδεκτών ή κατηγοριών αποδεκτών των δεδομένων προσωπικού χαρακτήρα, ενδεχομένως
- των τρόπων με τους οποίους τα υποκείμενα των δεδομένων μπορούν να ασκήσουν τα δικαιώματά τους.

Βάσει του ΓΚΠΔ, όταν τα δεδομένα προσωπικού χαρακτήρα λαμβάνονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας υποχρεούται να παρέχει σε αυτό τις ακόλουθες πληροφορίες κατά την απόκτηση των δεδομένων ⁵³²:

- την ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του υπευθύνου προστασίας δεδομένων
- τον σκοπό και τη νομική βάση της επεξεργασίας, δηλαδή σύμβαση ή έννομη υποχρέωση

⁵³² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 1.

- το έννομο συμφέρον που επιδιώκει ο υπεύθυνος επεξεργασίας, εάν αυτό αποτελεί τη βάση για την επεξεργασία·
- τους ενδεχόμενους αποδέκτες ή κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα·
- αν τα δεδομένα θα διαβιβαστούν σε τρίτη χώρα ή διεθνή οργανισμό και αν η διαβίβαση αυτή βασίζεται σε απόφαση επάρκειας ή στηρίζεται σε κατάλληλες εγγυήσεις·
- το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα και, εάν δεν είναι εφικτό να καθοριστεί το διάστημα αυτό, τα κριτήρια που χρησιμοποιούνται για τον καθορισμό του χρονικού διαστήματος αποθήκευσης·
- τα δικαιώματα του υποκειμένου των δεδομένων όσον αφορά την επεξεργασία, όπως δικαιώματα πρόσβασης, διόρθωσης, διαγραφής και περιορισμού της επεξεργασίας ή εναντίωσης σε αυτήν·
- αν η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική ή συμβατική υποχρέωση, αν το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν καθώς και τις συνέπειες σε περίπτωση μη παροχής τους·
- την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ·
- το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή·
- την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσης.

Σε περιπτώσεις αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, τα υποκείμενα των δεδομένων πρέπει να λαμβάνουν σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται στην κατάρτιση προφίλ, τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για τα υποκείμενα των δεδομένων.

Στις περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα δεν λαμβάνονται απευθείας από το υποκείμενο των δεδομένων, ο υπεύθυνος

επεξεργασίας πρέπει να ενημερώνει το φυσικό πρόσωπο για την προέλευση των δεδομένων προσωπικού χαρακτήρα. Εν πάση περιπτώσει, ο υπεύθυνος επεξεργασίας οφείλει, μεταξύ άλλων, να ενημερώνει τα υποκείμενα των δεδομένων σχετικά με την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ ⁵³³. Τέλος, εάν ο υπεύθυνος επεξεργασίας προτίθεται να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα για σκοπό διαφορετικό από εκείνον που δηλώθηκε αρχικά στο υποκείμενο των δεδομένων, οι αρχές του περιορισμού του σκοπού και της διαφάνειας απαιτούν να ενημερώσει το υποκείμενο των δεδομένων σχετικά με τον νέο αυτό σκοπό. Οι υπεύθυνοι επεξεργασίας πρέπει να παρέχουν πληροφορίες πριν από κάθε περαιτέρω επεξεργασία. Με άλλα λόγια, στις περιπτώσεις στις οποίες το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του για την επεξεργασία, ο υπεύθυνος επεξεργασίας πρέπει να λάβει εκ νέου τη συγκατάθεσή του εάν ο σκοπός της επεξεργασίας των δεδομένων αλλάξει ή εάν προστεθούν περαιτέρω σκοποί.

Χρόνος παροχής πληροφοριών

Ο ΓΚΠΔ προβλέπει δύο διαφορετικά ενδεχόμενα και δύο χρονικά σημεία κατά τα οποία ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να παρέχει πληροφορίες στο υποκείμενο των δεδομένων:

- Όταν τα δεδομένα προσωπικού χαρακτήρα λαμβάνονται απευθείας από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας πρέπει να του παρέχει όλες τις σχετικές πληροφορίες και να το ενημερώνει για τα δικαιώματά του βάσει του ΓΚΠΔ κατά τον χρόνο λήψης των δεδομένων ⁵³⁴.

Εάν ο υπεύθυνος επεξεργασίας έχει την πρόθεση να επεξεργαστεί περαιτέρω τα δεδομένα για διαφορετικό σκοπό, παρέχει όλες τις σχετικές πληροφορίες προτού πραγματοποιηθεί η επεξεργασία.

- Όταν τα δεδομένα προσωπικού χαρακτήρα δεν λαμβάνονται απευθείας από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας υποχρεούται να του παράσχει τις πληροφορίες σχετικά με την επεξεργασία «εντός εύλογης

⁵³³ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 και άρθρο 14 παράγραφος 2 (στοιχείο στ).

⁵³⁴ Ό.π., άρθρο 13 παράγραφοι 1 και 2, εισαγωγική φράση στην οποία ο Γενικός Κανονισμός για την Προστασία Δεδομένων αναφέρεται στην υποχρέωση ενημέρωσης «κατά τη λήψη των δεδομένων προσωπικού χαρακτήρα».

προθεσμίας από τη συλλογή των δεδομένων προσωπικού χαρακτήρα, αλλά το αργότερο εντός ενός μηνός» ή προτού αυτά κοινοποιηθούν σε τρίτο ⁵³⁵.

Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται ότι, εάν η ενημέρωση του υποκειμένου των δεδομένων δεν είναι εφικτή κατά την έναρξη της επεξεργασίας, αυτή μπορεί να πραγματοποιηθεί σε μεταγενέστερο στάδιο, π.χ. όταν ο υπεύθυνος επεξεργασίας επικοινωνήσει με το υποκείμενο των δεδομένων για οποιονδήποτε λόγο ⁵³⁶.

Διάφοροι τρόποι παροχής πληροφοριών

Βάσει τόσο του δικαίου του Συμβουλίου της Ευρώπης όσο και του δικαίου της ΕΕ, οι πληροφορίες που πρέπει να παρέχει ο υπεύθυνος επεξεργασίας στα υποκείμενα των δεδομένων πρέπει να είναι σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή. Πρέπει να παρέχονται εγγράφως ή με άλλα μέσα, συμπεριλαμβανομένων ηλεκτρονικών μέσων, κάνοντας χρήση απλής, σαφούς και εύκολα κατανοητής γλώσσας. Κατά την παροχή πληροφοριών, ο υπεύθυνος επεξεργασίας μπορεί να χρησιμοποιεί τυποποιημένα εικονίδια για την παροχή των πληροφοριών με ευδιάκριτο και κατανοητό τρόπο ⁵³⁷. Για παράδειγμα, εικονίδιο που αναπαριστά λουκέτο μπορεί να χρησιμοποιηθεί για να υποδηλώσει ότι τα δεδομένα συλλέγονται με ασφάλεια και/ή κρυπτογραφούνται. Τα υποκείμενα των δεδομένων μπορούν να ζητήσουν να τους παρασχεθούν οι πληροφορίες προφορικά. Οι πληροφορίες πρέπει να παρέχονται δωρεάν, εκτός εάν τα αιτήματα του υποκειμένου των δεδομένων είναι προδήλως αβάσιμα ή υπερβολικά (δηλαδή, επαναλαμβανόμενα) ⁵³⁸. Η εύκολη πρόσβαση στις παρεχόμενες πληροφορίες είναι καθοριστικής σημασίας για την ικανότητα του υποκειμένου των δεδομένων να ασκήσει τα δικαιώματά του τα οποία προβλέπονται στο δίκαιο της ΕΕ για την προστασία δεδομένων.

Η αρχή της θεμιτής επεξεργασίας επιβάλλει να είναι οι πληροφορίες εύκολα κατανοητές από τα υποκείμενα των δεδομένων. Η γλώσσα που χρησιμοποιείται

535 Ό.π., άρθρο 13 παράγραφος 3 και άρθρο 14 παράγραφος 3· βλ. επίσης την αναφορά σε εύλογο χρονικό διάστημα και χωρίς υπερβολική καθυστέρηση στην Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 παράγραφος 1 στοιχείο β).

536 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 70.

537 Η Ευρωπαϊκή Επιτροπή θα αναλύσει περαιτέρω τις πληροφορίες που θα παρουσιάζονται με εικονίδια και τις διαδικασίες για την παροχή τυποποιημένων εικονιδίων μέσω κατ' εξουσιοδότηση πράξεων· βλ. Γενικό Κανονισμό για την Προστασία Δεδομένων, άρθρο 12 παράγραφος 8.

538 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 12 παράγραφοι 1, 5 και 7, και Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο β).

πρέπει να είναι κατάλληλη για τους αποδέκτες. Το ύψος και το είδος της γλώσσας θα πρέπει να διαφέρει ανάλογα με το αν το κοινό στο οποίο απευθύνεται είναι, για παράδειγμα, ενήλικος ή παιδί, το ευρύ κοινό ή εμπειρογνώμονας του ακαδημαϊκού χώρου. Το ζήτημα της εξεύρεσης της κατάλληλης ισορροπίας όσον αφορά αυτή την πτυχή του κατανοητού χαρακτήρα των πληροφοριών εξετάζεται στη γνώμη της Ομάδας εργασίας του άρθρου 29 σχετικά με περισσότερο εναρμονισμένες διατάξεις πληροφόρησης. Σε αυτήν προάγεται η ιδέα των επονομαζόμενων σημειωμάτων πολλαπλών επιπέδων ⁵³⁹, τα οποία παρέχουν τη δυνατότητα στο υποκείμενο των δεδομένων να αποφασίζει για τον βαθμό λεπτομέρειας που προτιμά. Ωστόσο, αυτός ο τρόπος παρουσίασης των πληροφοριών δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από τις υποχρεώσεις που υπέχει βάσει των άρθρων 13 και 14 του ΓΚΠΔ. Ο υπεύθυνος επεξεργασίας εξακολουθεί να υποχρεούται να παρέχει όλες τις πληροφορίες στο υποκείμενο των δεδομένων.

Ένας από τους πιο αποτελεσματικούς τρόπους παροχής πληροφοριών είναι η ανάρτηση κατάλληλων ρητρών ενημέρωσης στην αρχική σελίδα του υπευθύνου επεξεργασίας, όπως η πολιτική απορρήτου του ιστότοπου. Ωστόσο, σημαντική μερίδα του πληθυσμού δεν χρησιμοποιεί το διαδίκτυο, και οι εταιρείες ή οι δημόσιες αρχές θα πρέπει να λαμβάνουν υπόψη το γεγονός αυτό στην πολιτική ενημέρωσης που εφαρμόζουν.

Το ενημερωτικό σημείωμα σχετικά με την πολιτική απορρήτου όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε ιστοσελίδα θα μπορούσε να έχει την ακόλουθη μορφή:

Ποιοι είμαστε;

Ο «υπεύθυνος επεξεργασίας» δεδομένων είναι η Bed and Breakfast C&U, με έδρα στ... [διεύθυνση: xxx], τηλ: xxx, φαξ: xxx, ηλ. ταχυδρομείο: info@c&u.com, στοιχεία επικοινωνίας υπευθύνου προστασίας δεδομένων: [xxx].

Το ενημερωτικό σημείωμα σχετικά με τα δεδομένα προσωπικού χαρακτήρα αποτελεί μέρος των όρων και προϋποθέσεων που διέπουν τις ξενοδοχειακές υπηρεσίες που παρέχουμε.

⁵³⁹ Ομάδα εργασίας του άρθρου 29 (2004), *Γνωμοδότηση 10/2004 σχετικά με περισσότερο εναρμονισμένες διατάξεις πληροφόρησης*, WP 100, Βρυξέλλες, 25 Νοεμβρίου 2004.

Ποια δεδομένα που σας αφορούν συλλέγουμε;

Συλλέγουμε από εσάς τα ακόλουθα δεδομένα προσωπικού χαρακτήρα: ονοματεπώνυμο, ταχυδρομική διεύθυνση, αριθμό τηλεφώνου, διεύθυνση ηλεκτρονικού ταχυδρομείου, πληροφορίες διαμονής, αριθμό πιστωτικής και χρεωστικής κάρτας και διευθύνσεις IP ή ονόματα χώρου των υπολογιστών που χρησιμοποιήσατε για να συνδεθείτε με τον ιστότοπό μας.

Γιατί συλλέγουμε τα δεδομένα σας;

Επεξεργαζόμαστε τα δεδομένα σας κατόπιν συγκατάθεσής σας και για σκοπούς όπως η πραγματοποίηση κρατήσεων, η σύναψη και εκτέλεση των συμβάσεων που σχετίζονται με τις υπηρεσίες που σας παρέχουμε και η συμμόρφωση με νόμιμες απαιτήσεις, για παράδειγμα, τον νόμο περί τοπικών τελών, ο οποίος μας υποχρεώνει να συλλέγουμε δεδομένα προσωπικού χαρακτήρα για την καταβολή του δημοτικού φόρου διαμονής.

Πώς επεξεργαζόμαστε τα δεδομένα σας;

Τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν θα διατηρηθούν για διάστημα τριών μηνών. Τα δεδομένα σας δεν υπόκεινται σε διαδικασίες αυτοματοποιημένης λήψης αποφάσεων.

Η Bed and Breakfast C&U εφαρμόζει αυστηρές διαδικασίες ασφάλειας, προκειμένου οι προσωπικές πληροφορίες σας να προστατεύονται από φθορά, καταστροφή ή κοινολόγηση σε τρίτο χωρίς τη συγκατάθεσή σας, και να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση σε αυτές. Οι ηλεκτρονικοί υπολογιστές στους οποίους αποθηκεύονται οι πληροφορίες φυλάσσονται σε ασφαλές περιβάλλον με περιορισμένη φυσική πρόσβαση. Χρησιμοποιούμε ασφαλή τείχη προστασίας και άλλα μέτρα για τον περιορισμό της ηλεκτρονικής πρόσβασης. Εάν τα δεδομένα πρέπει να διαβιβαστούν σε τρίτο, απαιτούμε από αυτόν να θεσπίζει παρόμοια μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα που σας αφορούν.

Κάθε πληροφορία που συλλέγουμε ή καταγράφουμε περιορίζεται στα γραφεία μας. Πρόσβαση στα δεδομένα προσωπικού χαρακτήρα παρέχεται μόνο σε πρόσωπα που χρειάζονται τις πληροφορίες για την εκτέλεση των καθηκόντων τους βάσει της παρούσας σύμβασης. Θα σας

ρωτήσουμε ρητώς όταν θα χρειαστούμε πληροφορίες για την εξακρίβωση της ταυτότητάς σας. Ενδέχεται να σας ζητήσουμε να συνεργαστείτε με τους ελέγχους ασφάλειας που διενεργούμε προτού σας κοινοποιήσουμε πληροφορίες. Μπορείτε να επικαιροποιήσετε τις πληροφορίες προσωπικού χαρακτήρα που μας παρέχετε οποτεδήποτε επικοινωνώντας απευθείας μαζί μας.

Ποια είναι τα δικαιώματά σας;

Έχετε το δικαίωμα να αποκτήσετε πρόσβαση στα δεδομένα που σας αφορούν, να λάβετε αντίγραφο των δεδομένων αυτών, να ζητήσετε τη διαγραφή ή τη διόρθωσή τους, ή τη μεταφορά των δεδομένων που σας αφορούν σε άλλον υπεύθυνο επεξεργασίας.

Μπορείτε να επικοινωνήσετε μαζί μας και να μας υποβάλετε τα αιτήματά σας στη διεύθυνση info@c&u.com. Είμαστε υποχρεωμένοι να απαντήσουμε στο αίτημά σας εντός ενός μήνα, αλλά εάν το αίτημά σας είναι υπερβολικά πολύπλοκο ή εάν λάβουμε υπερβολικά πολλά αιτήματα, θα σας ενημερώσουμε ότι η προθεσμία αυτή ενδέχεται να παραταθεί κατά δύο ακόμη μήνες.

Πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που σας αφορούν

Έχετε δικαίωμα πρόσβασης στα δεδομένα που σας αφορούν, δικαίωμα λήψης κατόπιν αιτήματος πληροφοριών σχετικά με τη συλλογιστική στην οποία βασίζεται η επεξεργασία δεδομένων, δικαίωμα να ζητήσετε τη διαγραφή ή τη διόρθωση των δεδομένων και δικαίωμα να μην αποτελέσετε αντικείμενο πλήρως αυτοματοποιημένης λήψης απόφασης χωρίς να ληφθούν υπόψη οι απόψεις σας. Μπορείτε να επικοινωνήσετε μαζί μας και να μας υποβάλετε τα αιτήματά σας στη διεύθυνση info@c&u.com. Έχετε επίσης το δικαίωμα να εναντιωθείτε στην επεξεργασία, να ανακαλέσετε τη συγκατάθεσή σας και να υποβάλετε καταγγελία στην εθνική εποπτική αρχή, εάν θεωρείτε ότι η εν λόγω επεξεργασία δεδομένων συνιστά παραβίαση της νομοθεσίας, και επίσης να αξιώσετε αποζημίωση για τη ζημία που προέκυψε ως αποτέλεσμα της παράνομης επεξεργασίας.

Το δικαίωμα υποβολής καταγγελίας

Ο ΓΚΠΔ υποχρεώνει τον υπεύθυνο επεξεργασίας να ενημερώνει τα υποκείμενα των δεδομένων σχετικά με τους μηχανισμούς επιβολής βάσει του εθνικού και του ενωσιακού δικαίου σε περίπτωση παραβίασης των δεδομένων προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει τα υποκείμενα των δεδομένων για το δικαίωμά τους να υποβάλουν καταγγελία σχετικά με παραβίαση των δεδομένων προσωπικού χαρακτήρα σε εποπτική αρχή και, εάν απαιτείται, ενώπιον εθνικού δικαστηρίου ⁵⁴⁰. Το δίκαιο του Συμβουλίου της Ευρώπης προβλέπει το δικαίωμα των υποκειμένων των δεδομένων να ενημερώνονται για τα μέσα άσκησης των δικαιωμάτων τους, συμπεριλαμβανομένου του δικαιώματος πραγματικής προσφυγής σύμφωνα με το άρθρο 9 παράγραφος 1 στοιχείο στ).

Εξαιρέσεις από την υποχρέωση ενημέρωσης

Ο ΓΚΠΔ προβλέπει εξαίρεση από την υποχρέωση ενημέρωσης. Βάσει του άρθρου 13 παράγραφος 4 και του άρθρου 14 παράγραφος 5 του ΓΚΠΔ, η υποχρέωση ενημέρωσης δεν ισχύει εάν το υποκείμενο των δεδομένων διαθέτει ήδη όλες τις σχετικές πληροφορίες ⁵⁴¹. Επιπλέον, όταν τα δεδομένα προσωπικού χαρακτήρα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων, η υποχρέωση ενημέρωσης δεν θα ισχύει εάν η παροχή πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια, ιδίως όταν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα αφορά σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς ⁵⁴².

Επιπλέον, τα κράτη μέλη διαθέτουν διακριτική ευχέρεια βάσει του ΓΚΠΔ όσον αφορά τον περιορισμό των υποχρεώσεων και των δικαιωμάτων που προβλέπονται για τα φυσικά πρόσωπα βάσει του κανονισμού, εάν αυτό είναι αναγκαίο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία· για παράδειγμα, για τη διαφύλαξη της εθνικής και δημόσιας ασφάλειας και της άμυνας, την προστασία δικαστικών ερευνών και διαδικασιών ή την προστασία οικονομικών και χρηματοοικονομικών

⁵⁴⁰ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο δ) και άρθρο 14 παράγραφος 2 στοιχείο ε)- Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 παράγραφος 1 στοιχείο στ).

⁵⁴¹ Ό.π., άρθρο 13 παράγραφος 4 και άρθρο 14 παράγραφος 5 στοιχείο α).

⁵⁴² Ό.π., άρθρο 14 παράγραφος 5 στοιχεία β) έως ε).

συμφερόντων καθώς και ιδιωτικών συμφερόντων τα οποία είναι πιο επιτακτικού χαρακτήρα από τα συμφέροντα προστασίας των δεδομένων ⁵⁴³.

Κάθε εξαίρεση ή περιορισμός πρέπει να είναι αναγκαίος σε μια δημοκρατική κοινωνία και ανάλογος προς τον επιδιωκόμενο σκοπό. Σε εξαιρετικές περιπτώσεις, για παράδειγμα λόγω ιατρικών ενδείξεων, η ίδια η προστασία του υποκειμένου των δεδομένων μπορεί να απαιτεί τον περιορισμό της διαφάνειας αυτό αφορά ειδικότερα τον περιορισμό του δικαιώματος πρόσβασης κάθε υποκειμένου δεδομένων ⁵⁴⁴. Ωστόσο, διασφαλίζοντας ένα ελάχιστο επίπεδο προστασίας, το εθνικό δίκαιο πρέπει να σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών που προστατεύονται από το δίκαιο της ΕΕ ⁵⁴⁵. Βάσει αυτού, το εθνικό δίκαιο πρέπει να περιέχει ειδικές διατάξεις που αποσαφηνίζουν τον σκοπό της επεξεργασίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται, τις εγγυήσεις και άλλες διαδικαστικές απαιτήσεις ⁵⁴⁶.

Όταν τα δεδομένα συλλέγονται για σκοπούς επιστημονικής ή ιστορικής έρευνας, στατιστικούς σκοπούς ή σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, το δίκαιο της Ένωσης ή των κρατών μελών μπορεί να προβλέπει παρεκκλίσεις από την υποχρέωση ενημέρωσης, εφόσον αυτή είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την επίτευξη των ειδικών σκοπών ⁵⁴⁷.

Παρόμοιοι περιορισμοί υπάρχουν στο δίκαιο του Συμβουλίου της Ευρώπης, όπου τα δικαιώματα που χορηγούνται σε υποκείμενα δεδομένων σύμφωνα με το άρθρο 9 της Εκσυγχρονισμένης Σύμβασης 108 μπορεί να υπόκεινται σε πιθανούς περιορισμούς σύμφωνα με το άρθρο 11 της Σύμβασης, υπό αυστηρές προϋποθέσεις. Επιπλέον, σύμφωνα με το άρθρο 8 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108 η υποχρέωση περί διαφάνειας της επεξεργασίας που επιβάλλεται στους υπευθύνους επεξεργασίας δεν έχει εφαρμογή όταν το υποκείμενο των δεδομένων έχει ήδη τις πληροφορίες.

543 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 23 παράγραφος 1.

544 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 15.

545 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 23 παράγραφος 1.

546 Ό.π., άρθρο 23 παράγραφος 2.

547 Ό.π., άρθρο 89 παράγραφοι 2 και 3.

Το δικαίωμα πρόσβασης του φυσικού προσώπου στα δεδομένα που το αφορούν

Στο δίκαιο του Συμβουλίου της Ευρώπης, το δικαίωμα πρόσβασης φυσικού προσώπου στα δεδομένα που το αφορούν αναγνωρίζεται ρητώς στο άρθρο 9 της Εκσυγχρονισμένης Σύμβασης 108. Αυτό προβλέπει ότι κάθε φυσικό πρόσωπο έχει δικαίωμα να αποκτήσει, κατόπιν αιτήματος, πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, οι οποίες ανακοινώνονται με κατανοητό τρόπο. Το δικαίωμα πρόσβασης έχει αναγνωριστεί όχι μόνο στις διατάξεις της Εκσυγχρονισμένης Σύμβασης 108, αλλά και στη νομολογία του ΕΔΔΑ. Το ΕΔΔΑ έχει αποφανθεί επανειλημμένως ότι τα φυσικά πρόσωπα έχουν δικαίωμα πρόσβασης σε πληροφορίες σχετικά με τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και ότι το εν λόγω δικαίωμα απορρέει από την ανάγκη σεβασμού της ιδιωτικής ζωής⁵⁴⁸. Ωστόσο, το δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα τα οποία αποθηκεύουν δημόσιοι ή ιδιωτικοί οργανισμοί μπορεί να περιορίζεται σε ορισμένες περιπτώσεις⁵⁴⁹.

Στο δίκαιο της ΕΕ, το δικαίωμα πρόσβασης του φυσικού προσώπου στα δεδομένα που το αφορούν αναγνωρίζεται ρητώς στο άρθρο 15 του ΓΚΠΔ και περιγράφεται επίσης ως στοιχείο του θεμελιώδους δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα στο άρθρο 8 παράγραφος 2 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ⁵⁵⁰. Το δικαίωμα του φυσικού προσώπου να έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που το αφορούν είναι βασικό στοιχείο του ευρωπαϊκού δικαίου για την προστασία δεδομένων⁵⁵¹.

Ο ΓΚΠΔ προβλέπει ότι κάθε υποκείμενο δεδομένων έχει δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που το αφορούν και σε ορισμένες πληροφορίες σχετικά με την επεξεργασία, τις οποίες οι υπεύθυνοι επεξεργασίας οφείλουν

548 ΕΔΔΑ, *Gaskin κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 10454/83, 7 Ιουλίου 1989· ΕΔΔΑ, *Odièvre κατά Γαλλίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 42326/98, 13 Φεβρουαρίου 2003· ΕΔΔΑ, *K.H. κ.λπ. κατά Σλοβακίας*, προσφυγή αριθ. 32881/04, 28 Απριλίου 2009· ΕΔΔΑ, *Godelli κατά Ιταλίας*, προσφυγή αριθ. 33783/09, 25 Σεπτεμβρίου 2012.

549 ΕΔΔΑ, *Leander κατά Σουηδίας*, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987.

550 Βλ. επίσης ΔΕΕ, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, *ΥΣ κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S*, 17 Ιουλίου 2014· ΔΕΕ, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) κατά Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων (EFSA), Ευρωπαϊκής Επιτροπής*, 16 Ιουλίου 2015.

551 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, *ΥΣ κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S*, 17 Ιουλίου 2014.

να παρέχουν⁵⁵². Ειδικότερα, κάθε υποκείμενο δεδομένων έχει δικαίωμα να λαμβάνει (από τον υπεύθυνο επεξεργασίας) επιβεβαίωση για το αν τα δεδομένα που το αφορούν υποβάλλονται σε επεξεργασία καθώς και, τουλάχιστον, τις ακόλουθες πληροφορίες:

- τους σκοπούς της επεξεργασίας
- τις κατηγορίες των σχετικών δεδομένων·
- τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινοποιούνται τα δεδομένα·
- το χρονικό διάστημα για το οποίο πρόκειται να αποθηκευτούν τα δεδομένα ή, όταν αυτό είναι αδύνατον, τα κριτήρια που χρησιμοποιούνται για τον καθορισμό του εν λόγω χρονικού διαστήματος
- την ύπαρξη δικαιωμάτων διόρθωσης ή διαγραφής δεδομένων προσωπικού χαρακτήρα ή περιορισμού της επεξεργασίας δεδομένων προσωπικού χαρακτήρα·
- το δικαίωμα υποβολής καταγγελίας στην εποπτική αρχή·
- κάθε διαθέσιμη πληροφορία σχετικά με την πηγή των δεδομένων που υποβάλλονται σε επεξεργασία εάν δεν ελήφθησαν από το υποκείμενο των δεδομένων·
- στην περίπτωση αυτοματοποιημένης λήψης απόφασης, τη λογική που ακολουθείται σε κάθε αυτοματοποιημένη επεξεργασία δεδομένων.

Ο υπεύθυνος επεξεργασίας οφείλει να παρέχει στο υποκείμενο των δεδομένων αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Κάθε πληροφορία η οποία ανακοινώνεται στο υποκείμενο των δεδομένων πρέπει να παρέχεται σε κατανοητή μορφή, το οποίο σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να βεβαιώνεται ότι το υποκείμενο των δεδομένων μπορεί να κατανοήσει τις πληροφορίες που του παρέχονται. Για παράδειγμα, η χρήση τεχνικών συντομογραφιών, κωδικοποιημένων όρων ή ακρωνυμίων σε απάντηση σε αίτημα πρόσβασης συνήθως δεν θα επαρκεί, εκτός εάν η έννοια

⁵⁵² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 15 παράγραφος 1.

των όρων αυτών εξηγείται. Όταν πραγματοποιείται αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, η γενική λογική που υιοθετείται θα πρέπει να εξηγείται, συμπεριλαμβανομένων των κριτηρίων που ελήφθησαν υπόψη κατά την αξιολόγηση του υποκειμένου των δεδομένων. Παρόμοιες απαιτήσεις προβλέπονται στο **δίκαιο του Συμβουλίου της Ευρώπης** ⁵⁵³.

Παράδειγμα: Η πρόσβαση του υποκειμένου των δεδομένων στα δεδομένα προσωπικού χαρακτήρα που το αφορούν θα το βοηθήσει να διαπιστώσει αν αυτά είναι ακριβή. Επομένως, είναι σημαντικό να ενημερώνεται το υποκείμενο των δεδομένων με κατανοητό τρόπο όχι μόνο για τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία αυτά καθαυτά, αλλά και για τις κατηγορίες υπό τις οποίες τα εν λόγω δεδομένα υποβάλλονται σε επεξεργασία, όπως ονοματεπώνυμο, διεύθυνση IP, συντεταγμένες γεωεντοπισμού, αριθμός πιστωτικής κάρτας κ.λπ.

Πληροφορίες σχετικά με την πηγή των δεδομένων –όταν αυτά δεν λαμβάνονται από το υποκείμενο των δεδομένων– πρέπει να παρέχονται κατόπιν αιτήματος, εφόσον οι πληροφορίες αυτές είναι διαθέσιμες. Η πρόβλεψη αυτή πρέπει να ερμηνεύεται στο πλαίσιο των αρχών της αντικειμενικότητας, της διαφάνειας και της λογοδοσίας. Ο υπεύθυνος επεξεργασίας δεν δικαιούται να καταστρέφει πληροφορίες σχετικά με την πηγή των δεδομένων προκειμένου να απαλλαγεί από την κοινοποίησή τους –εκτός εάν η διαγραφή πραγματοποιείται ανεξάρτητα από τη λήψη του αιτήματος πρόσβασης– και πρέπει να συμμορφώνεται προς τις γενικές υποχρεώσεις περί «λογοδοσίας».

Όπως προβλέπεται στη νομολογία του ΔΕΕ, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να περιορίζεται αδικαιολόγητα από χρονικές προθεσμίες. Πρέπει επίσης να παρέχεται εύλογη δυνατότητα στα υποκείμενα των δεδομένων να αποκτήσουν πληροφορίες σχετικά με πράξεις επεξεργασίας δεδομένων οι οποίες πραγματοποιήθηκαν στο παρελθόν.

Παράδειγμα: Στην υπόθεση *Rijkeboer* ⁵⁵⁴, ζητήθηκε από το ΔΕΕ να καθορίσει αν το δικαίωμα φυσικού προσώπου να αποκτήσει πρόσβαση σε πληροφορίες σχετικά με τους αποδέκτες ή τις κατηγορίες αποδεκτών

553 Βλ. Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 παράγραφος 1 στοιχείο γ).

554 ΔΕΕ, C-553/07, *College van burgemeester en wethouders van Rotterdam κατά E. E. Rijkeboer*, 7 Μαΐου 2009.

δεδομένων προσωπικού χαρακτήρα και στο περιεχόμενο των δεδομένων θα μπορούσε να περιοριστεί σε πληροφορίες μόνο για ένα έτος πριν από την υποβολή του αιτήματος πρόσβασης.

Προκειμένου να καθορίσει αν η νομοθεσία της ΕΕ επιτρέπει τέτοιο χρονικό περιορισμό, το ΔΕΕ αποφάσισε να ερμηνεύσει το άρθρο 12 λαμβανομένων υπόψη των σκοπών της οδηγίας. Το ΔΕΕ επισήμανε, κατ' αρχάς, ότι το δικαίωμα πρόσβασης είναι αναγκαίο για να μπορεί το υποκείμενο των δεδομένων να απαιτήσει από τον υπεύθυνο της επεξεργασίας να διορθώσει, να διαγράψει ή να κλειδώσει τα δεδομένα του, ή να απαιτήσει την κοινοποίηση σε τρίτους, στους οποίους έχουν γνωστοποιηθεί τα δεδομένα, της εν λόγω διόρθωσης, διαγραφής ή του κλειδώματος. Το δικαίωμα αποτελεσματικής πρόσβασης είναι επίσης αναγκαίο για να μπορέσει το υποκείμενο των δεδομένων να ασκήσει το δικαίωμα εναντίωσης στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν ή το δικαίωμα υποβολής καταγγελίας και αξίωσης αποζημίωσης⁵⁵⁵.

Για να εξασφαλίζεται η πρακτική αποτελεσματικότητα της άσκησης των δικαιωμάτων που παρέχονται στα υποκείμενα των δεδομένων, το ΔΕΕ αποφάνθηκε ότι το δικαίωμα αυτό «πρέπει οπωσδήποτε να αφορά το παρελθόν. Συγκεκριμένα, αν δεν συνέβαινε αυτό, ο ενδιαφερόμενος δεν θα μπορούσε να ασκήσει αποτελεσματικώς το δικαίωμά του να απαιτήσει τη διαγραφή, τη διόρθωση ή το κλείδωμα των δεδομένων που φέρονται να είναι παράνομα ή ανακριβή καθώς και το δικαίωμά του να ασκήσει αγωγή αποζημίωσης».

6.1.2. Δικαίωμα διόρθωσης

Βάσει του **δικαίου της ΕΕ** και του **δικαίου του Συμβουλίου της Ευρώπης**, τα υποκείμενα των δεδομένων έχουν το δικαίωμα διόρθωσης των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Η ακρίβεια των δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη προκειμένου να διασφαλίζεται υψηλό επίπεδο προστασίας για τα υποκείμενα των δεδομένων⁵⁵⁶.

⁵⁵⁵ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 15 παράγραφος 1 στοιχεία γ) και στ), άρθρο 16, άρθρο 17 παράγραφος 2 και άρθρο 21, και κεφάλαιο VIII.

⁵⁵⁶ Ό.π., άρθρο 16 και αιτιολογική σκέψη 65· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο ε).

Παράδειγμα: Στην υπόθεση *Ciubotaru κατά Μολδαβίας*⁵⁵⁷, ο προσφεύγων αδυνατούσε να αλλάξει την καταχώριση της εθνοτικής καταγωγής του στα επίσημα μητρώα από μολδαβική σε ρουμανική, επειδή δεν μπόρεσε να τεκμηριώσει το αίτημά του. Το ΕΔΔΑ έκρινε ότι είναι αποδεκτό να απαιτούν τα κράτη αντικειμενικές αποδείξεις όταν καταχωρίζουν την εθνοτική ταυτότητα φυσικού προσώπου. Όταν ένας τέτοιος ισχυρισμός βασίζεται σε αμιγώς υποκειμενικούς και αβάσιμους ισχυρισμούς, οι αρχές μπορούν να απορρίψουν το αίτημα. Ωστόσο, το αίτημα του προσφεύγοντος δεν βασιζόταν μόνο στην υποκειμενική αντίληψη της ταυτότητάς του από τον ίδιο· ο προσφεύγων κατέδειξε ότι είχε αντικειμενικά επαληθεύσιμους δεσμούς με τη ρουμανική εθνοτική ομάδα, όπως γλώσσα, όνομα, ενσυναίσθηση και άλλα. Παρ' όλα αυτά, βάσει του εθνικού δικαίου, ο προσφεύγων υποχρεούνταν να προσκομίσει αποδείξεις ότι οι γονείς του ήταν μέλη της ρουμανικής εθνοτικής ομάδας. Δεδομένης της ιστορικής πραγματικότητας της Μολδαβίας, μια τέτοια απαίτηση αποτελούσε ανυπέρβλητο εμπόδιο για την καταχώριση εθνοτικής ταυτότητας διαφορετικής από εκείνη την οποία είχαν καταχωρίσει για τους γονείς του προσφεύγοντος οι σοβιετικές αρχές. Εμποδίζοντας την εξέταση του ισχυρισμού του προσφεύγοντος υπό το πρίσμα αντικειμενικά επαληθεύσιμων αποδείξεων, το κράτος παρέβη τη θετική υποχρέωσή του να διασφαλίσει τον ουσιαστικό σεβασμό της ιδιωτικής ζωής του προσφεύγοντος. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Σε ορισμένες περιπτώσεις, αρκεί απλό αίτημα του υποκειμένου των δεδομένων για διόρθωση, για παράδειγμα, της ορθογραφίας ονόματος, της διεύθυνσης ή του αριθμού τηλεφώνου. Σύμφωνα με το **δίκαιο της ΕΕ** και το **δίκαιο του Συμβουλίου της Ευρώπης**, ανακριβή δεδομένα προσωπικού χαρακτήρα πρέπει να διορθώνονται χωρίς αδικαιολόγητη ή υπερβολική καθυστέρηση⁵⁵⁸. Εάν, ωστόσο, τέτοια αιτήματα συνδέονται με σημαντικά θέματα νομικής φύσης, όπως τη νόμιμη ταυτότητα του υποκειμένου των δεδομένων ή τον ορθό τρόπο διαμονής για την επίδοση νομικών εγγράφων, τα αιτήματα διόρθωσης ενδέχεται να μην επαρκούν και ο υπεύθυνος επεξεργασίας μπορεί να δικαιούται να απαιτήσει την απόδειξη της εικαζόμενης ανακρίβειας στα δεδομένα. Μια τέτοια απαίτηση δεν πρέπει να δημιουργεί αδικαιολόγητο βάρος απόδειξης για το υποκείμενο των δεδομένων

557 ΕΔΔΑ, *Ciubotaru κατά Μολδαβίας*, προσφυγή αριθ. 27138/04, 27 Απριλίου 2010, σκέψεις 51 και 59.

558 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 16· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1.

εμποδίζοντας με τον τρόπο αυτό τη διόρθωση των δεδομένων των φυσικών προσώπων. Το ΕΔΔΑ διαπίστωσε παραβάσεις του άρθρου 8 της ΕΣΔΑ σε αρκετές περιπτώσεις στις οποίες ο προσφεύγων δεν μπόρεσε να αμφισβητήσει την ακρίβεια πληροφοριών που τηρούνταν σε μυστικά μητρώα ⁵⁵⁹.

Παράδειγμα: Στην υπόθεση *Cemalettin Canli κατά Τουρκίας* ⁵⁶⁰, το ΕΔΔΑ διαπίστωσε παράβαση του άρθρου 8 της ΕΣΔΑ λόγω ανακριβούς έκθεσης της αστυνομίας σε ποινική διαδικασία.

Ο προσφεύγων είχε εμπλακεί σε ποινικές διαδικασίες δύο φορές, λόγω εικαζόμενης συμμετοχής σε παράνομες οργανώσεις, αλλά δεν είχε καταδικαστεί. Όταν ο προσφεύγων συνελήφθη εκ νέου και του απαγγέλλθηκαν κατηγορίες για άλλο ποινικό αδίκημα, η αστυνομία κατέθεσε στο ποινικό δικαστήριο έκθεση με τίτλο «*πληροφορίες σχετικά με άλλες αξιόποινες πράξεις*», στην οποία ο προσφεύγων εμφανιζόταν ως μέλος δύο παράνομων οργανώσεων. Το αίτημα του προσφεύγοντος περί τροποποίησης της έκθεσης και των αρχείων της αστυνομίας απορρίφθηκε. Το ΕΔΔΑ έκρινε ότι οι πληροφορίες που περιέχονταν στην αστυνομική έκθεση ενέπιπταν στο πεδίο εφαρμογής του άρθρου 8 της ΕΣΔΑ, καθώς δημόσιες πληροφορίες που συγκεντρώνονται και αποθηκεύονται συστηματικά σε αρχεία που τηρούν οι αρχές μπορούσαν επίσης να εμπίπτουν στην έννοια της «ιδιωτικής ζωής». Επιπλέον, η αστυνομική έκθεση ήταν ανακριβής στη σύνταξή της, και η υποβολή της στο ποινικό δικαστήριο δεν ήταν σύμφωνη προς το εθνικό δίκαιο. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8.

Ενόσω εκκρεμεί αστική αγωγή ή προσφυγή ενώπιον δημόσιας αρχής προκειμένου να αποφασιστεί αν τα δεδομένα είναι ορθά ή μη, το υποκείμενο των δεδομένων μπορεί να ζητήσει να προστεθεί στον φάκελό του καταχώριση ή σημείωση στην οποία θα αναφέρεται ότι η ακρίβειά αμφισβητείται και ότι εκκρεμεί η έκδοση επίσημης απόφασης ⁵⁶¹. Κατά το διάστημα αυτό, ο υπεύθυνος επεξεργασίας δεν πρέπει να παρουσιάζει τα δεδομένα ως ορθά ή μη υποκείμενα σε τροποποίηση, ιδίως σε τρίτους.

559 ΕΔΔΑ, *Rotaru κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000.

560 ΕΔΔΑ, *Cemalettin Canli κατά Τουρκίας*, προσφυγή αριθ. 22427/04, 18 Νοεμβρίου 2008, σκέψεις 33 και 42-43· ΕΔΔΑ, *Dalea κατά Γαλλίας*, προσφυγή αριθ. 964/07, 2 Φεβρουαρίου 2010.

561 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 18 και αιτιολογική σκέψη 67.

6.1.3. Δικαίωμα διαγραφής («δικαίωμα στη λήθη»)

Η παροχή στα υποκείμενα των δεδομένων του δικαιώματος διαγραφής των δεδομένων που τα αφορούν είναι ιδιαίτερα σημαντική για την αποτελεσματική εφαρμογή των αρχών περί προστασίας των δεδομένων, και ιδίως της αρχής της ελαχιστοποίησης των δεδομένων (τα δεδομένα προσωπικού χαρακτήρα πρέπει να περιορίζονται στα αναγκαία για τους σκοπούς για τους οποίους τα εν λόγω δεδομένα υποβάλλονται σε επεξεργασία). Επομένως, δικαίωμα διαγραφής προβλέπεται στις νομικές πράξεις τόσο του Συμβουλίου της Ευρώπης, όσο και της ΕΕ ⁵⁶².

Παράδειγμα: Στην υπόθεση *Segerstedt-Wiberg κ.λπ. κατά Σουηδίας* ⁵⁶³, οι προσφεύγοντες είχαν διατελέσει μέλη ορισμένων φιλελεύθερων και κομμουνιστικών πολιτικών κομμάτων. Είχαν υπόνοιες ότι πληροφορίες που τους αφορούν είχαν καταχωριστεί σε αρχεία ασφάλειας της αστυνομίας και ζήτησαν τη διαγραφή τους. Το ΕΔΔΑ διαπίστωσε ότι η αποθήκευση των επίμαχων δεδομένων είχε νομική βάση και επιδίωκε θεμιτό σκοπό. Ωστόσο, σε σχέση με ορισμένους από τους προσφεύγοντες, το ΕΔΔΑ διαπίστωσε ότι η συνεχιζόμενη διατήρηση των δεδομένων τους συνιστούσε υπέρμετρη επέμβαση στην ιδιωτική ζωή τους. Για παράδειγμα, στην περίπτωση ενός από τους προσφεύγοντες, οι αρχές διατηρούσαν την πληροφορία ότι το 1969 είχε υποστηρίξει τη βίαιη αντίσταση στον αστυνομικό έλεγχο κατά τη διάρκεια διαδηλώσεων. Το ΕΔΔΑ διαπίστωσε ότι οι πληροφορίες αυτές δεν μπορούσαν να έχουν κανένα σχετικό ενδιαφέρον για την εθνική ασφάλεια, λαμβανομένου υπόψη μάλιστα του ιστορικού χαρακτήρα τους. Το ΕΔΔΑ διαπίστωσε παράβαση του άρθρου 8 της ΕΣΔΑ σε σχέση με τέσσερις από τους πέντε προσφεύγοντες καθώς, λαμβανομένου υπόψη του μεγάλου χρονικού διαστήματος που είχε παρέλθει από τις εικαζόμενες πράξεις των προσφευγόντων, η συνεχιζόμενη αποθήκευση των δεδομένων τους στερούνταν νοήματος.

Παράδειγμα: Στην υπόθεση *Brunet κατά Γαλλίας* ⁵⁶⁴, ο προσφεύγων κατήγγειλε την αποθήκευση των προσωπικών του πληροφοριών σε βάση δεδομένων της αστυνομίας η οποία περιείχε πληροφορίες

⁵⁶² Ό.π., άρθρο 17.

⁵⁶³ ΕΔΔΑ, *Segerstedt-Wiberg κ.λπ. κατά Σουηδίας*, προσφυγή αριθ. 62332/00, 6 Ιουνίου 2006, σκέψεις 89 και 90· βλ. επίσης, για παράδειγμα, ΕΔΔΑ, *Μ.Κ. κατά Γαλλίας*, προσφυγή αριθ. 19522/09, 18 Απριλίου 2013.

⁵⁶⁴ ΕΔΔΑ, *Brunet κατά Γαλλίας*, προσφυγή αριθ. 21010/10, 18 Σεπτεμβρίου 2014.

για καταδικασθέντες, κατηγορηθέντες και θύματα. Παρότι η ποινική διαδικασία κατά του προσφεύγοντος δεν ολοκληρώθηκε, τα στοιχεία του εμφανίζονταν στη βάση δεδομένων. Το ΕΔΔΑ έκρινε ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ. Για να καταλήξει στο συμπέρασμά του, το ΕΔΔΑ έκρινε ότι, στην πράξη, δεν υπήρχε καμία δυνατότητα για τον προσφεύγοντα να επιτύχει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που τον αφορούσαν. Έλαβε επίσης υπόψη τη φύση των πληροφοριών που περιείχονταν στη βάση δεδομένων και εκτίμησε ότι συνιστούσαν επέμβαση στην ιδιωτική ζωή του προσφεύγοντος, καθώς περιείχαν στοιχεία της ταυτότητας και της προσωπικότητάς του. Επιπλέον, το ΕΔΔΑ έκρινε ότι η περίοδος διατήρησης των προσωπικών αρχείων στη βάση δεδομένων, η οποία ανερχόταν σε 20 έτη, ήταν υπερβολικά μακρά, δεδομένου μάλιστα ότι κανένα δικαστήριο δεν είχε καταδικάσει ποτέ τον προσφεύγοντα.

Στην Εκσυγχρονισμένη Σύμβαση 108 αναγνωρίζεται ρητώς ότι κάθε πρόσωπο έχει δικαίωμα στη διαγραφή ανακριβών, ψευδών ή παρανόμως υποβληθέντων σε επεξεργασία δεδομένων ⁵⁶⁵.

Στο δίκαιο της ΕΕ, το άρθρο 17 του ΓΚΠΔ προβλέπει το δικαίωμα των υποκειμένων των δεδομένων να ζητούν τη διαγραφή των δεδομένων που τα αφορούν. Το δικαίωμα του φυσικού προσώπου να ζητεί τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση ισχύει όταν:

- τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία,
- το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεση επί της οποίας βασίζεται η επεξεργασία και δεν υπάρχει άλλη νομική βάση για την επεξεργασία,
- το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία,
- τα δεδομένα προσωπικού χαρακτήρα υποβλήθηκαν σε επεξεργασία παράνομα,

⁵⁶⁵ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο ε).

- τα δεδομένα προσωπικού χαρακτήρα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους στην οποία υπόκειται ο υπεύθυνος επεξεργασίας,
- τα δεδομένα προσωπικού χαρακτήρα έχουν συλλεχθεί στο πλαίσιο της παροχής υπηρεσιών της κοινωνίας των πληροφοριών σε παιδιά βάσει του άρθρου 8 του ΓΚΠΔ ⁵⁶⁶.

Το βάρος της απόδειξης της νομιμότητας της επεξεργασίας των δεδομένων φέρουν οι υπεύθυνοι επεξεργασίας, καθώς είναι υπεύθυνοι για τη νομιμότητα της επεξεργασίας ⁵⁶⁷. Σύμφωνα με την αρχή της λογοδοσίας, ο υπεύθυνος επεξεργασίας οφείλει να είναι ανά πάσα στιγμή σε θέση να αποδείξει την ύπαρξη ορθής νομικής βάσης για την επεξεργασία των δεδομένων, διαφορετικά η επεξεργασία πρέπει να παύσει ⁵⁶⁸. Ο ΓΚΠΔ προβλέπει εξαιρέσεις στο δικαίωμα στη λήθη, για παράδειγμα όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι απαραίτητη για:

- την άσκηση του δικαιώματος ελευθερίας της έκφρασης και του δικαιώματος στην ενημέρωση,
- την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους στο οποίο υπάγεται ο υπεύθυνος επεξεργασίας ή για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο της επεξεργασίας,
- λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας,
- σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς,
- τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ⁵⁶⁹.

566 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 17 παράγραφος 1.

567 Ό.π.

568 Ό.π., άρθρο 5 παράγραφος 2.

569 Ό.π., άρθρο 17 παράγραφος 3.

Το ΔΕΕ επιβεβαίωσε τη σημασία του δικαιώματος διαγραφής για τη διασφάλιση υψηλού επιπέδου προστασίας των δεδομένων.

Παράδειγμα: Στην υπόθεση *Google Spain* ⁵⁷⁰, το ΔΕΕ εξέτασε αν η Google ήταν υποχρεωμένη να διαγράψει παρωχημένες πληροφορίες σχετικά με τις οικονομικές δυσκολίες του προσφεύγοντος από τον κατάλογο αποτελεσμάτων των αναζητήσεων. Μεταξύ άλλων, η Google αμφισβήτησε την ευθύνη της, υποστηρίζοντας ότι παρέχει απλώς έναν υπερσύνδεσμο προς την ιστοσελίδα του εκδότη στην οποία φιλοξενοούνται οι πληροφορίες, η οποία στην περίπτωση αυτή ήταν άρθρο εφημερίδας σχετικά με τα προβλήματα αφερεγγυότητας του προσφεύγοντος ⁵⁷¹. Η Google υποστήριξε ότι το αίτημα διαγραφής παρωχημένων πληροφοριών από ιστοσελίδα θα πρέπει να υποβάλλεται στον πάροχο υπηρεσιών φιλοξενίας της ιστοσελίδας και όχι στην Google, η οποία παρέχει απλώς σύνδεσμο προς την αρχική σελίδα. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι η Google, όταν πραγματοποιεί αναζήτηση στον Παγκόσμιο Ιστό σχετικά με πληροφορίες και ιστοσελίδες και όταν ευρετηριάζει περιεχόμενο για να παρέχει αποτελέσματα αναζήτησης, καθίσταται υπεύθυνος επεξεργασίας δεδομένων με τις ευθύνες και υποχρεώσεις που προβλέπονται στο δίκαιο της ΕΕ.

Το ΔΕΕ αποφάσισε ότι οι μηχανές αναζήτησης στο διαδίκτυο και τα αποτελέσματα αναζητήσεων τα οποία παρέχουν δεδομένα προσωπικού χαρακτήρα δίνουν τη δυνατότητα κατάρτισης λεπτομερούς προφίλ φυσικού προσώπου ⁵⁷². Οι μηχανές αναζήτησης καθιστούν τις πληροφορίες που περιέχονται σε τέτοιο κατάλογο αποτελεσμάτων προσβάσιμες ανά πάσα στιγμή και από οποιοδήποτε σημείο. Λαμβανομένης υπόψη της δυνητικής σοβαρότητάς της, η επέμβαση αυτή δεν μπορεί να δικαιολογείται

570 ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014, σκέψεις 55-58.

571 Η Google αμφισβήτησε επίσης την εφαρμογή των κανόνων της ΕΕ περί προστασίας δεδομένων, επειδή η Google Inc. είναι εγκατεστημένη στις ΗΠΑ και η επίμαχη επεξεργασία δεδομένων προσωπικού χαρακτήρα στην υπόθεση αυτή πραγματοποιήθηκε επίσης στις ΗΠΑ. Ως δεύτερο επιχείρημα για τη μη εφαρμογή της νομοθεσίας της ΕΕ για την προστασία δεδομένων πρόβαλε ότι οι μηχανές αναζήτησης δεν μπορούν να θεωρηθούν «υπεύθυνοι επεξεργασίας» σε σχέση με τα δεδομένα που εμφανίζονται στα αποτελέσματά τους, καθώς δεν έχουν γνώση των δεδομένων ούτε ασκούν έλεγχο επ' αυτών. Το ΔΕΕ απέρριψε αμφότερα τα επιχειρήματα, αποφάνθηκε ότι η οδηγία 95/46/ΕΚ εφαρμόζεται στην περίπτωση αυτή και, εν συνεχεία, εξέτασε το περιεχόμενο των κατοχυρωμένων δικαιωμάτων, και ιδίως του δικαιώματος διαγραφής των δεδομένων προσωπικού χαρακτήρα.

572 Ό.π., σκέψεις 36, 38, 80-81 και 97.

από το απλό οικονομικό συμφέρον του φορέα εκμετάλλευσης μιας τέτοιας μηχανής στη συγκεκριμένη επεξεργασία. Πρέπει να αναζητηθεί δίκαιη ισορροπία μεταξύ, αφενός, του έννομου συμφέροντος των χρηστών του διαδικτύου από την πρόσβαση στις πληροφορίες και, αφετέρου, των θεμελιωδών δικαιωμάτων των υποκειμένων των δεδομένων βάσει των άρθρων 7 και 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Σε μια ολοένα και περισσότερο ψηφιοποιημένη κοινωνία, η απαίτηση ακρίβειας των δεδομένων προσωπικού χαρακτήρα και περιορισμού τους εντός των ορίων του αναγκαίου (δηλαδή, για πληροφόρηση του κοινού) είναι θεμελιώδους σημασίας προκειμένου να διασφαλίζεται υψηλό επίπεδο προστασίας των δεδομένων για τα φυσικά πρόσωπα. Ο «υπεύθυνος της επεξεργασίας αυτής πρέπει να διασφαλίζει, στο πλαίσιο των ευθυνών, των ικανοτήτων και των δυνατοτήτων του, ότι η εν λόγω δραστηριότητα ανταποκρίνεται στις απαιτήσεις» της νομοθεσίας της ΕΕ, προκειμένου οι προβλεπόμενες νόμιμες εγγυήσεις να μπορούν να παράγουν πλήρως τα αποτελέσματά τους ⁵⁷³. Αυτό σημαίνει ότι το δικαίωμα του φυσικού προσώπου στη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν, όταν η επεξεργασία είναι παρωχημένη ή δεν είναι πλέον αναγκαία, καλύπτει επίσης υπευθύνους επεξεργασίας δεδομένων που αναπαράγουν τις πληροφορίες ⁵⁷⁴.

Όταν εξέτασε αν η Google υποχρεούται να αφαιρέσει τους σχετικούς με τον προσφεύγοντα συνδέσμους, το ΔΕΕ αποφάνθηκε ότι, υπό ορισμένες προϋποθέσεις, τα φυσικά πρόσωπα έχουν το δικαίωμα να ζητούν τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Το δικαίωμα αυτό μπορεί να προβληθεί όταν οι πληροφορίες που αφορούν το φυσικό πρόσωπο είναι ανακριβείς, ακατάλληλες, άσχετες ή υπερβολικές σε σχέση με τους σκοπούς της επεξεργασίας δεδομένων. Το ΔΕΕ αναγνώρισε ότι το δικαίωμα αυτό δεν είναι απόλυτο· πρέπει να σταθμίζεται με άλλα δικαιώματα και συμφέροντα, ιδίως δε με το συμφέρον και το δικαίωμα του ευρύτερου κοινού να έχει πρόσβαση σε ορισμένες πληροφορίες. Κάθε αίτημα διαγραφής πρέπει να αξιολογείται

⁵⁷³ Ό.π., σκέψεις 81-83.

⁵⁷⁴ ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014, σκέψη 88. Βλ. επίσης, Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Βρυξέλλες, 26 Νοεμβρίου 2014, και σύσταση CM/Rec 2012 (3) της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά τις μηχανές αναζήτησης, 4 Απριλίου 2012.

κατά περίπτωση ώστε να επιτυγχάνεται ισορροπία μεταξύ, αφενός, των θεμελιωδών δικαιωμάτων στην προστασία των δεδομένων προσωπικού χαρακτήρα και στον σεβασμό της ιδιωτικής ζωής του υποκειμένου των δεδομένων και, αφετέρου, των έννομων συμφερόντων των χρηστών του διαδικτύου, συμπεριλαμβανομένων των εκδοτών. Το ΔΕΕ παρείχε καθοδήγηση σχετικά με τους παράγοντες που πρέπει να λαμβάνονται υπόψη κατά την εν λόγω στάθμιση. Η φύση των επίμαχων πληροφοριών είναι ιδιαίτερα σημαντικός παράγοντας. Εάν οι πληροφορίες αφορούν την ιδιωτική ζωή του φυσικού προσώπου και δεν υπάρχει δημόσιο συμφέρον όσον αφορά τη διαθεσιμότητα των πληροφοριών, η προστασία των δεδομένων και της ιδιωτικής ζωής υπερισχύει του δικαιώματος του ευρύτερου κοινού να έχει πρόσβαση στις πληροφορίες. Εάν, αντιθέτως, φαίνεται ότι το υποκείμενο των δεδομένων είναι δημόσιο πρόσωπο ή ότι οι πληροφορίες είναι τέτοιας φύσης ώστε να δικαιολογείται η διάθεσή τους στο ευρύ κοινό, το υπέρτατο συμφέρον του ευρέος κοινού από την πρόσβαση στις πληροφορίες μπορεί να δικαιολογεί την επέμβαση στα θεμελιώδη δικαιώματα της προστασίας δεδομένων και της προστασίας της ιδιωτικής ζωής του υποκειμένου των δεδομένων.

Μετά την έκδοση της απόφασης αυτής, η Ομάδα εργασίας του άρθρου 29 εξέδωσε κατευθυντήριες γραμμές σχετικά με την εφαρμογή της απόφασης του ΔΕΕ ⁵⁷⁵. Στις κατευθυντήριες γραμμές περιλαμβάνεται κατάλογος κοινών κριτηρίων για χρήση από τις εποπτικές αρχές, όταν χειρίζονται καταγγελίες που αφορούν αιτήματα διαγραφής φυσικών προσώπων, εξηγούνται οι συνέπειες του δικαιώματος διαγραφής και παρέχεται καθοδήγηση για την ως άνω στάθμιση δικαιωμάτων. Στις κατευθυντήριες γραμμές επαναλαμβάνεται ότι οι εκτιμήσεις πρέπει να πραγματοποιούνται κατά περίπτωση. Καθώς το δικαίωμα στη λήθη δεν είναι απόλυτο, το αποτέλεσμα σχετικού αιτήματος μπορεί να διαφέρει ανάλογα με την υπό κρίση υπόθεση. Αυτό επισημαίνεται επίσης στη νομολογία του ΔΕΕ μετά την υπόθεση που αφορούσε την Google.

575 Ομάδα εργασίας του άρθρου 29 (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* C-131/12, WP 225, Βρυξέλλες, 26 Νοεμβρίου 2014.

Παράδειγμα: Στην υπόθεση *Camera di Commercio di Lecce κατά Manni*⁵⁷⁶, το ΔΕΕ κλήθηκε να εξετάσει αν φυσικό πρόσωπο είχε το δικαίωμα να εξασφαλίσει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούσαν τα οποία είχαν δημοσιευθεί σε δημόσιο μητρώο εταιρειών, αφού η εταιρεία του έπαυσε να υφίσταται. Ο S. Manni είχε ζητήσει από το εμπορικό επιμελητήριο του Λέτσε να διαγράψει από το οικείο μητρώο τα δεδομένα προσωπικού χαρακτήρα που τον αφορούσαν, καθώς ανακάλυψε ότι δυνητικοί πελάτες συμβουλευόνταν το μητρώο και διαπίστωναν ότι είχε διατελέσει διαχειριστής εταιρείας η οποία είχε κηρύξει πτώχευση πριν από περισσότερο από μια δεκαετία. Κατά τον προσφεύγοντα, οι πληροφορίες αυτές θα αποθάρρυναν δυνητικούς πελάτες.

Σταθμίζοντας το δικαίωμα του S. Manni στην προστασία των δεδομένων προσωπικού χαρακτήρα με το συμφέρον του ευρέος κοινού από την πρόσβαση σε πληροφορίες, το ΔΕΕ εξέτασε κατ' αρχάς τον σκοπό του δημόσιου μητρώου. Επισήμανε ότι η δημοσιότητα προβλεπόταν από τον νόμο, και ιδίως από οδηγία της ΕΕ η οποία αποσκοπεί στη διευκόλυνση της πρόσβασης τρίτων σε εταιρικές πληροφορίες. Επομένως, οι τρίτοι θα πρέπει να έχουν πρόσβαση και να είναι σε θέση να εξετάζουν τις ουσιώδεις καταστατικές πράξεις μιας εταιρείας και άλλες πληροφορίες που αφορούν την εταιρεία, «ιδίως δε τα στοιχεία ταυτότητας των ατόμων που έχουν την εξουσία να τη δεσμεύουν». Σκοπός της δημοσιότητας ήταν επίσης να παράσχει ασφάλεια δικαίου υπό την προοπτική αύξησης των οικονομικών συναλλαγών μεταξύ κρατών μελών, διασφαλίζοντας ότι οι τρίτοι θα έχουν πρόσβαση σε όλες τις πληροφορίες για τις εταιρείες σε ολόκληρη την ΕΕ.

Το ΔΕΕ επισήμανε περαιτέρω ότι, ακόμη και μετά την πάροδο του χρόνου και έστω και αν η εταιρεία λυθεί, τα δικαιώματα και οι έννομες υποχρεώσεις που σχετίζονται με την εταιρεία συχνά εξακολουθούν να υφίστανται. Οι διαφορές που σχετίζονται με τη λύση της εταιρείας μπορεί να έχουν μεγάλη διάρκεια και ερωτήματα σχετικά με την εταιρεία, τους διευθυντές και τους εκκαθαριστές της μπορούν να ανακύπτουν για πολλά χρόνια αφότου η εταιρεία παύσει να υφίσταται. Το ΔΕΕ έκρινε ότι, λαμβανομένων υπόψη της ποικιλομορφίας των περιστάσεων που ενδέχεται να ανακύψουν και των αποκλίσεων μεταξύ των προθεσμιών

⁵⁷⁶ ΔΕΕ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*, 9 Μαρτίου 2017.

παραγραφής που προβλέπονται στα κράτη μέλη, «στην παρούσα κατάσταση των πραγμάτων είναι αδύνατο να προσδιοριστεί ένα ενιαίο χρονικό διάστημα ύστερα από τη λύση μιας εταιρίας μετά το οποίο να μην απαιτείται πλέον η καταχώριση των εν λόγω δεδομένων στο μητρώο και η δημοσιότητά τους». Λόγω του νόμιμου σκοπού της δημοσιότητας και των δυσκολιών καθορισμού περιόδου στο πέρας της οποίας τα δεδομένα προσωπικού χαρακτήρα θα μπορούσαν να διαγραφούν από το μητρώο χωρίς να θιγούν τα συμφέροντα τρίτων, το ΔΕΕ αποφάνθηκε ότι οι κανόνες της ΕΕ περί προστασίας δεδομένων δεν εγγυώνται δικαίωμα διαγραφής των δεδομένων προσωπικού χαρακτήρα για πρόσωπα στην κατάσταση του S. Manni.

Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει δεδομένα προσωπικού χαρακτήρα και υποχρεούται να διαγράψει τις πληροφορίες, υποχρεούται και οφείλει να λάβει «εύλογα» μέτρα ώστε να ενημερώσει άλλους υπευθύνους επεξεργασίας των ίδιων δεδομένων σχετικά με το αίτημα διαγραφής του υποκειμένου των δεδομένων. Οι δραστηριότητες του υπευθύνου επεξεργασίας πρέπει να λαμβάνουν υπόψη τις διαθέσιμες τεχνολογίες και το κόστος εφαρμογής⁵⁷⁷.

6.1.4. Δικαίωμα περιορισμού της επεξεργασίας

Το άρθρο 18 του ΓΚΠΔ παρέχει στα υποκείμενα των δεδομένων το δικαίωμα να ζητήσουν από τον υπεύθυνο επεξεργασίας τον προσωρινό περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν. Τα υποκείμενα των δεδομένων μπορούν να ζητούν από τον υπεύθυνο επεξεργασίας να περιορίσει την επεξεργασία όταν:

- η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται·
- η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων ζητεί τον περιορισμό της χρήσης των δεδομένων προσωπικού χαρακτήρα αντί της διαγραφής αυτών·
- τα δεδομένα πρέπει να διατηρηθούν για την άσκηση ή την υποστήριξη νομικών αξιώσεων·

⁵⁷⁷ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 17 παράγραφος 2 και αιτιολογική σκέψη 66.

- εκκρεμεί απόφαση όσον αφορά το κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερσχύουν έναντι των λόγων του υποκειμένου των δεδομένων ⁵⁷⁸.

Οι μέθοδοι με τις οποίες ο υπεύθυνος επεξεργασίας μπορεί να περιορίσει την επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορούν να περιλαμβάνουν, για παράδειγμα, προσωρινή μετακίνηση των επιλεγμένων δεδομένων σε άλλο σύστημα επεξεργασίας, αποτροπή της προσβασιμότητας των δεδομένων από άλλους χρήστες ή προσωρινή αφαίρεση δεδομένων προσωπικού χαρακτήρα ⁵⁷⁹. Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο των δεδομένων πριν από την άρση του περιορισμού της επεξεργασίας ⁵⁸⁰.

Υποχρέωση γνωστοποίησης όσον αφορά τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας

Ο υπεύθυνος επεξεργασίας πρέπει να ανακοινώνει κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή κάθε περιορισμό της επεξεργασίας σε κάθε αποδέκτη στον οποίο έχει κοινολογήσει τα δεδομένα προσωπικού χαρακτήρα, εφόσον αυτό δεν είναι ανέφικτο ούτε συνεπάγεται δυσανάλογη προσπάθεια ⁵⁸¹. Εάν το υποκείμενο των δεδομένων ζητήσει πληροφορίες σχετικά με τους εν λόγω αποδέκτες, ο υπεύθυνος επεξεργασίας οφείλει να του παράσχει τις πληροφορίες αυτές ⁵⁸².

6.1.5. Δικαίωμα στη φορητότητα των δεδομένων

Σύμφωνα με τον ΓΚΠΔ, τα υποκείμενα των δεδομένων απολαύουν του δικαιώματος στη φορητότητα των δεδομένων σε περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα τα οποία έχουν παράσχει σε υπεύθυνο επεξεργασίας υποβάλλονται σε επεξεργασία με αυτοματοποιημένα μέσα βάσει συγκατάθεσης ή σε περιπτώσεις στις οποίες η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης και διενεργείται με αυτοματοποιημένα μέσα. Αυτό σημαίνει ότι το δικαίωμα στη φορητότητα των δεδομένων δεν εφαρμόζεται σε

⁵⁷⁸ Ό.π., άρθρο 18 παράγραφος 1.

⁵⁷⁹ Ό.π., αιτιολογική σκέψη 67.

⁵⁸⁰ Ό.π., άρθρο 18 παράγραφος 3.

⁵⁸¹ Ό.π., άρθρο 19.

⁵⁸² Ό.π.

περιπτώσεις στις οποίες η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται σε άλλη νομική βάση πλην της συγκατάθεσης ή της σύμβασης⁵⁸³.

Εάν είναι εφαρμοστέο το δικαίωμα στη φορητότητα των δεδομένων, τα υποκείμενα των δεδομένων δικαιούνται να ζητούν την απευθείας διαβίβαση των δεδομένων προσωπικού χαρακτήρα τους από έναν υπεύθυνο επεξεργασίας σε άλλον, εάν αυτό είναι τεχνικά εφικτό⁵⁸⁴. Προς διευκόλυνση της διαδικασίας αυτής, ο υπεύθυνος επεξεργασίας θα πρέπει να αναπτύξει διαλειτουργικούς μορφότευπους που επιτρέπουν τη φορητότητα των δεδομένων για τα υποκείμενα των δεδομένων⁵⁸⁵. Ο ΓΚΠΔ προσδιορίζει ότι οι μορφότευποι αυτοί πρέπει να είναι δομημένοι, κοινώς χρησιμοποιούμενοι και αναγνώσιμοι από μηχανήματα προκειμένου να διευκολύνουν τη διαλειτουργικότητα⁵⁸⁶. Η διαλειτουργικότητα μπορεί να οριστεί υπό ευρεία έννοια ως η ικανότητα των συστημάτων πληροφοριών να ανταλλάσσουν δεδομένα και να επιτρέπουν την κοινοχρησία πληροφοριών⁵⁸⁷. Παρότι ο σκοπός των μορφότευπων που χρησιμοποιούνται είναι η εξασφάλιση διαλειτουργικότητας, ο ΓΚΠΔ δεν επιβάλλει συγκεκριμένες συστάσεις σχετικά με τον ειδικό μορφότευπο που πρέπει να παρέχεται: οι μορφότευποι μπορούν να διαφέρουν από τομέα σε τομέα⁵⁸⁸.

Σύμφωνα με τις κατευθυντήριες γραμμές της Ομάδας εργασίας του άρθρου 29, το δικαίωμα στη φορητότητα των δεδομένων «αυξάνει τις δυνατότητες επιλογής των χρηστών, τον βαθμό ελέγχου των χρηστών και τη δύναμη των χρηστών», με στόχο να παρέχεται στα υποκείμενα των δεδομένων η δυνατότητα ελέγχου επί των δεδομένων προσωπικού χαρακτήρα που τα αφορούν⁵⁸⁹. Στις κατευθυντήριες γραμμές διευκρινίζονται τα βασικά στοιχεία της φορητότητας των δεδομένων, μεταξύ των οποίων περιλαμβάνονται τα εξής:

- το δικαίωμα των υποκειμένων των δεδομένων να λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και τα οποία υποβάλλονται σε

583 Ό.π., αιτιολογική σκέψη 68 και άρθρο 20 παράγραφος 1.

584 Ό.π., άρθρο 20 παράγραφος 2.

585 Ό.π., αιτιολογική σκέψη 68 και άρθρο 20 παράγραφος 1.

586 Ό.π., αιτιολογική σκέψη 68.

587 Ευρωπαϊκή Επιτροπή, Ανακοίνωση «Πιο Ισχυρά και Έξυπνα Συστήματα Πληροφοριών για τα Σύνορα και την Ασφάλεια», COM(2016) 205 final, 2 Απριλίου 2016.

588 Ομάδα εργασίας του άρθρου 29 (2016), *Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων*, WP 242, 13 Δεκεμβρίου 2016, αναθεωρήθηκαν στις 5 Απριλίου 2017, σ. 13.

589 Ό.π.

επεξεργασία από τον υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο·

- το δικαίωμα των υποκειμένων των δεδομένων να ζητούν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από έναν υπεύθυνο επεξεργασίας σε άλλον χωρίς αντίρρηση εάν αυτό είναι τεχνικά εφικτό·
- το καθεστώς των υπευθύνων επεξεργασίας –όταν ο υπεύθυνος επεξεργασίας ανταποκρίνεται σε αίτημα φορητότητας δεδομένων, ενεργεί βάσει των οδηγιών του υποκειμένου των δεδομένων, που σημαίνει ότι δεν ευθύνεται για τη συμμόρφωση του αποδέκτη με το δίκαιο για την προστασία των δεδομένων, καθώς το υποκείμενο των δεδομένων είναι εκείνο που αποφασίζει σε ποιον διαβιβάζονται αυτά·
- το δικαίωμα στη φορητότητα των δεδομένων ασκείται με την επιφύλαξη κάθε άλλου δικαιώματος όπως ισχύει και στην περίπτωση οποιωνδήποτε άλλων δικαιωμάτων που προβλέπονται στον ΓΚΠΔ.

6.1.6. Δικαίωμα εναντίωσης

Τα υποκείμενα των δεδομένων μπορούν να επικαλούνται το δικαίωμά τους να αντιτάσσονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή τους και στην επεξεργασία δεδομένων για σκοπούς απευθείας εμπορικής προώθησης. Το δικαίωμα εναντίωσης μπορεί να ασκείται με αυτοματοποιημένα μέσα.

Το δικαίωμα εναντίωσης για λόγους που σχετίζονται με την ιδιαίτερη κατάσταση των υποκειμένων των δεδομένων

Τα υποκείμενα των δεδομένων δεν έχουν γενικό δικαίωμα να αντιτάσσονται στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν⁵⁹⁰. Το άρθρο 21 παράγραφος 1 του ΓΚΠΔ παρέχει στο υποκείμενο των δεδομένων τη δυνατότητα να εγείρει αντιρρήσεις για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του όταν η νομική βάση για την επεξεργασία είναι η εκτέλεση καθήκοντος για λόγους δημόσιου συμφέροντος από τον υπεύθυνο επεξεργασίας

⁵⁹⁰ Βλ. επίσης ΕΔΔΑ, *M.S. κατά Σουηδίας*, προσφυγή αριθ. 20837/92, 27 Αυγούστου 1997 (υπόθεση στην οποία κοινοποιήθηκαν ιατρικά δεδομένα χωρίς τη συγκατάθεση ή τη δυνατότητα αντίταξης)· ΕΔΔΑ, *Leander κατά Σουηδίας*, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987· ΕΔΔΑ, *Mosley κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 48009/08, 10 Μαΐου 2011.

ή όταν η επεξεργασία βασίζεται στα έννομα συμφέροντα του υπευθύνου επεξεργασίας⁵⁹¹. Το δικαίωμα εναντίωσης εφαρμόζεται στις δραστηριότητες κατάρτισης προφίλ. Παρόμοιο δικαίωμα έχει αναγνωριστεί στην Εκσυγχρονισμένη Σύμβαση 108⁵⁹².

Το δικαίωμα εναντίωσης για λόγους που σχετίζονται με την ιδιαίτερη κατάσταση του υποκειμένου των δεδομένων αποσκοπεί στην επίτευξη της κατάλληλης ισορροπίας μεταξύ, αφενός, των δικαιωμάτων προστασίας δεδομένων του υποκειμένου των δεδομένων και, αφετέρου, των νόμιμων δικαιωμάτων των τρίτων για επεξεργασία των δεδομένων του. Ωστόσο, το ΔΕΕ έχει διευκρινίσει ότι τα δικαιώματα του υποκειμένου των δεδομένων υπερέχουν «κατά κανόνα» των οικονομικών συμφερόντων του υπευθύνου επεξεργασίας σε βαθμό που εξαρτάται από «τη φύση της επίμαχης πληροφορίας και από τον ευαίσθητο χαρακτήρα της για την ιδιωτική ζωή του υποκειμένου των δεδομένων καθώς και από το συμφέρον του κοινού να διαθέτει την πληροφορία αυτή»⁵⁹³. Σύμφωνα με τον ΓΚΠΔ, το βάρος της απόδειξης το φέρουν οι υπεύθυνοι επεξεργασίας, οι οποίοι πρέπει να καταδείξουν επιτακτικούς λόγους για τη συνέχιση της επεξεργασίας⁵⁹⁴. Ομοίως, στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 διευκρινίζεται ότι οι νόμιμοι λόγοι για την επεξεργασία δεδομένων (οι οποίοι ενδέχεται να υπερσχύουν του δικαιώματος εναντίωσης του υποκειμένου των δεδομένων) θα πρέπει να καταδεικνύονται σε κάθε μεμονωμένη περίπτωση⁵⁹⁵.

Παράδειγμα: Στην απόφαση *Manni*⁵⁹⁶, το ΔΕΕ έκρινε ότι λόγω του νόμιμου σκοπού της δημοσιοποίησης δεδομένων προσωπικού χαρακτήρα στο μητρώο εταιρειών, και ειδικότερα της ανάγκης για προστασία των συμφερόντων τρίτων και ασφάλεια δικαίου, καταρχήν, ο S. Manni δεν είχε δικαίωμα να ζητήσει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα

591 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 69: άρθρο 6 παράγραφος 1 στοιχεία ε) και στ).

592 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο δ), σύσταση σχετικά με την κατάρτιση προφίλ, άρθρο 5 παράγραφος 3.

593 ΔΕΕ, C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014, σκέψη 81.

594 Βλ. επίσης Εκσυγχρονισμένη Σύμβαση 108, άρθρο 8 παράγραφος 1 στοιχείο δ), που ορίζει ότι το υποκείμενο των δεδομένων μπορεί να αντιταχθεί στην επεξεργασία των δεδομένων του «εκτός εάν ο υπεύθυνος επεξεργασίας καταδείξει νόμιμους λόγους για την επεξεργασία που υπερσχύουν των συμφερόντων ή των δικαιωμάτων και των θεμελιωδών ελευθεριών του».

595 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 78.

596 ΔΕΕ, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*, 9 Μαρτίου 2017, σκέψεις 47 και 60.

που τον αφορούσαν από το μητρώο εταιρειών. Ωστόσο, αναγνώρισε την ύπαρξη δικαιώματος αντίταξης στην επεξεργασία, δηλώνοντας ότι «όταν έχει παρέλθει ένα αρκούντως μακρύ χρονικό διάστημα [...], δεν μπορεί να αποκλειστεί το ενδεχόμενο να υπάρξουν ιδιαίτερες καταστάσεις στις οποίες επιτακτικοί και νόμιμοι λόγοι συνδεόμενοι με τη συγκεκριμένη περίπτωση του ενδιαφερομένου να δικαιολογούν όλως εξαιρετικώς να περιορίζεται η πρόσβαση στα καταχωρισμένα στο μητρώο δεδομένα προσωπικού χαρακτήρα που τον αφορούν εκ μέρους τρίτων οι οποίοι έχουν ειδικό συμφέρον να λάβουν γνώση των δεδομένων αυτών».

Το ΔΕΕ θεώρησε ότι αποτελεί αρμοδιότητα των εθνικών δικαστηρίων να εκτιμήσουν κάθε επιμέρους υπόθεση, λαμβάνοντας υπόψη το σύνολο των κρίσιμων περιστάσεων του ατόμου και το κατά πόσον υπάρχουν θεμιτοί και επιτακτικοί λόγοι ικανοί να δικαιολογήσουν όλως εξαιρετικώς την περιορισμένη πρόσβαση τρίτων σε δεδομένα προσωπικού χαρακτήρα που περιέχονται σε μητρώα εταιρειών. Ωστόσο, το ΔΕΕ διευκρίνισε ότι, στην περίπτωση του S. Μαννί, μόνη η προβαλλόμενη περίσταση ότι η δημοσιοποίηση των δεδομένων προσωπικού χαρακτήρα που τον αφορούσαν στο μητρώο επηρέαζε την πελατεία του δεν μπορεί να θεωρηθεί τέτοιος νόμιμος και επιτακτικός λόγος. Οι δυνητικοί πελάτες του S. Μαννί έχουν έννομο συμφέρον σε ό,τι αφορά την πρόσβαση στις πληροφορίες που αφορούν την πτώχευση της παλαιότερης εταιρείας του.

Το αποτέλεσμα της επιτυχούς εναντίωσης είναι ότι ο υπεύθυνος επεξεργασίας δεν επιτρέπεται πλέον να επεξεργάζεται τα επίμαχα δεδομένα. Ωστόσο, οι πράξεις επεξεργασίας που έχουν εκτελεστεί επί των δεδομένων αυτών παραμένουν νόμιμες.

Το δικαίωμα εναντίωσης στην επεξεργασία δεδομένων για σκοπούς απευθείας εμπορικής προώθησης

Το άρθρο 21 παράγραφος 2 του ΓΚΠΔ προβλέπει ειδικό δικαίωμα εναντίωσης στη χρήση δεδομένων προσωπικού χαρακτήρα για σκοπούς απευθείας εμπορικής προώθησης, αποσαφηνίζοντας περαιτέρω το άρθρο 13 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες. Το εν λόγω δικαίωμα προβλέπεται επίσης στην Εκσυγχρονισμένη Σύμβαση 108, καθώς και στη σύσταση του Συμβουλίου της Ευρώπης σχετικά με την απευθείας εμπορική

προώθηση ⁵⁹⁷. Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 διευκρινίζεται ότι οι αντιρρήσεις στην επεξεργασία δεδομένων για σκοπούς απευθείας εμπορικής προώθησης θα πρέπει να συνεπάγονται την άνευ όρων διαγραφή ή αφαίρεση των επίμαχων δεδομένων προσωπικού χαρακτήρα ⁵⁹⁸.

Το υποκείμενο των δεδομένων έχει το δικαίωμα να αντιτάσσεται ανά πάσα στιγμή και χωρίς επιβάρυνση στη χρήση των δεδομένων προσωπικού χαρακτήρα που το αφορούν για σκοπούς απευθείας εμπορικής προώθησης. Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για το εν λόγω δικαίωμα με σαφή τρόπο, ξέχωρα από κάθε άλλη πληροφόρηση.

Άσκηση του δικαιώματος εναντίωσης με αυτοματοποιημένα μέσα

Σε περίπτωση χρήσης και επεξεργασίας πληροφοριών προσωπικού χαρακτήρα για σκοπούς υπηρεσιών της κοινωνίας των πληροφοριών, το υποκείμενο των δεδομένων μπορεί να ασκεί το δικαίωμά του να αντισταχθεί στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν με αυτοματοποιημένα μέσα.

Ως υπηρεσία της κοινωνίας των πληροφοριών ορίζεται κάθε υπηρεσία που συνήθως παρέχεται έναντι αμοιβής, με ηλεκτρονικά μέσα εξ αποστάσεως και κατόπιν προσωπικής επιλογής ενός αποδέκτη υπηρεσιών ⁵⁹⁹.

Οι υπεύθυνοι επεξεργασίας δεδομένων που παρέχουν υπηρεσίες της κοινωνίας των πληροφοριών πρέπει να εφαρμόζουν κατάλληλες τεχνικές ρυθμίσεις και διαδικασίες για να διασφαλίζουν ότι το δικαίωμα εναντίωσης μπορεί να ασκείται αποτελεσματικά με αυτοματοποιημένα μέσα ⁶⁰⁰. Για παράδειγμα, μπορεί να απαιτείται φραγή των cookies σε ιστοσελίδες ή απενεργοποίηση του εντοπισμού της πλοήγησης στο διαδίκτυο.

597 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1985), Σύσταση Rec (85)20 προς τα κράτη μέλη της ΕΕ σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται για τους σκοπούς της απευθείας εμπορικής προώθησης, 25 Οκτωβρίου 1985, άρθρο 4 παράγραφος 1.

598 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 79.

599 Οδηγία 98/34/ΕΚ όπως τροποποιήθηκε με την οδηγία 98/48/ΕΚ για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προτύπων και προδιαγραφών, άρθρο 1 παράγραφος 2.

600 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 21 παράγραφος 5.

Το δικαίωμα εναντίωσης για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς

Βάσει του δικαίου της ΕΕ, η επιστημονική έρευνα θα πρέπει να ερμηνεύεται διασταλτικά, δηλαδή να περιλαμβάνει παραδείγματα χάριν τεχνολογική ανάπτυξη και επίδειξη, βασική έρευνα, εφαρμοσμένη έρευνα και ιδιωτικά χρηματοδοτούμενη έρευνα ⁶⁰¹. Στην ιστορική έρευνα συμπεριλαμβάνεται επίσης η έρευνα για γενεαλογικούς σκοπούς, έχοντας κατά νουν ότι ο κανονισμός δεν θα πρέπει να ισχύει για τους θανόντες ⁶⁰². Ο όρος «στατιστικοί σκοποί» σημαίνει κάθε πράξη συλλογής και την επεξεργασία δεδομένων προσωπικού χαρακτήρα που είναι αναγκαία για την πραγματοποίηση στατιστικών ερευνών ή για την παραγωγή στατιστικών αποτελεσμάτων ⁶⁰³. Και σε αυτή την περίπτωση, η ιδιαίτερη κατάσταση του υποκειμένου των δεδομένων αποτελεί τη νομική βάση όσον αφορά το δικαίωμα εναντίωσης στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς έρευνας ⁶⁰⁴. Η μόνη εξαίρεση είναι η αναγκαιότητα της επεξεργασίας για την εκτέλεση καθήκοντος που ασκείται για λόγους δημόσιου συμφέροντος. Ωστόσο, το δικαίωμα διαγραφής δεν εφαρμόζεται όταν η επεξεργασία είναι απαραίτητη (είτε υφίστανται λόγοι δημόσιου συμφέροντος είτε όχι) για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς ⁶⁰⁵.

Ο ΓΚΠΔ εξισορροπεί τις απαιτήσεις της επιστημονικής, στατιστικής ή ιστορικής έρευνας και τα δικαιώματα των υποκειμένων των δεδομένων με ειδικές διασφαλίσεις και παρεκκλίσεις που προβλέπονται στο άρθρο 89. Κατά συνέπεια, το δίκαιο της Ένωσης ή των κρατών μελών μπορεί να προβλέπει παρεκκλίσεις του δικαιώματος εναντίωσης στον βαθμό που το εν λόγω δικαίωμα είναι πιθανό να καταστήσει αδύνατη ή να παρακωλύσει σοβαρά την επίτευξη των σκοπών της έρευνας, και εφόσον οι εν λόγω παρεκκλίσεις είναι απαραίτητες για την εκπλήρωση των εν λόγω σκοπών.

Βάσει του **δικαίου του Συμβουλίου της Ευρώπης**, το άρθρο 9 παράγραφος 2 της Εκσυγχρονισμένης Σύμβασης 108 ορίζει ότι μπορούν να προβλέπονται από τον νόμο περιορισμοί επί των δικαιωμάτων των υποκειμένων των δεδομένων, συμπεριλαμβανομένου του δικαιώματος εναντίωσης, όσον αφορά την επεξεργασία

601 Ό.π., αιτιολογική σκέψη 159.

602 Ό.π., αιτιολογική σκέψη 160.

603 Ό.π., αιτιολογική σκέψη 162.

604 Ό.π., άρθρο 21 παράγραφος 6.

605 Ό.π., άρθρο 17 παράγραφος 3 στοιχείο δ).

δεδομένων για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς όταν δεν υφίσταται αναγνωρίσιμος κίνδυνος παράβασης των δικαιωμάτων και των θεμελιωδών ελευθεριών των υποκειμένων των δεδομένων.

Ωστόσο, στην Αιτιολογική Έκθεση (σημείο 41) αναγνωρίζεται επίσης ότι τα υποκείμενα των δεδομένων θα πρέπει να έχουν τη δυνατότητα να δίνουν τη συγκατάθεσή τους μόνο σε ορισμένους τομείς έρευνας ή σε τμήματα ερευνητικών προγραμμάτων στον βαθμό που ο επιδιωκόμενος σκοπός το επιτρέπει, και να αντιτάσσονται σε περίπτωση που αντιληφθούν ότι η επεξεργασία καταπατά σε υπέρμετρο βαθμό τα δικαιώματα και τις ελευθερίες τους χωρίς νόμιμο λόγο.

Με άλλα λόγια, η εν λόγω επεξεργασία θα θεωρείται, συνεπώς, εκ των προτέρων συμβατή, υπό την προϋπόθεση ότι υφίστανται άλλες εγγυήσεις και ότι οι πράξεις, καταρχήν, αποκλείουν οποιαδήποτε χρήση των πληροφοριών που έχουν ληφθεί για αποφάσεις ή μέτρα που αφορούν συγκεκριμένο φυσικό πρόσωπο.

6.1.7. Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ

Οι αυτοματοποιημένες αποφάσεις είναι αποφάσεις οι οποίες λαμβάνονται με τη χρήση δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία αποκλειστικά με αυτόματα μέσα, χωρίς ανθρώπινη παρέμβαση. **Βάσει του δικαίου της ΕΕ**, τα υποκείμενα των δεδομένων δεν πρέπει να υπόκεινται σε αυτοματοποιημένες αποφάσεις που παράγουν έννομα αποτελέσματα ή έχουν παρόμοιες σημαντικές συνέπειες. Εάν οι εν λόγω αποφάσεις είναι πιθανό να έχουν σημαντικό αντίκτυπο στη ζωή των φυσικών προσώπων επειδή σχετίζονται, για παράδειγμα, με την πιστοληπτική ικανότητα, τις ηλεκτρονικές προσλήψεις, τις επιδόσεις στην εργασία ή την ανάλυση συμπεριφοράς ή αξιοπιστίας, τότε απαιτείται ειδική προστασία για να αποφευχθούν αρνητικές επιπτώσεις. Η λήψη αυτοματοποιημένων αποφάσεων περιλαμβάνει την κατάρτιση προφίλ, η οποία συνίσταται σε οποιαδήποτε μορφή αυτόματης αξιολόγησης «προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία,

τις προσωπικές προτιμήσεις ή τα ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή τις μετακινήσεις του υποκειμένου των δεδομένων»⁶⁰⁶.

Παράδειγμα: Για την ταχεία αξιολόγηση της πιστοληπτικής ικανότητας ενός μελλοντικού πελάτη, οι υπηρεσίες πληροφοριών πιστοληπτικής ικανότητας συγκεντρώνουν ορισμένα δεδομένα, όπως την κατάσταση των πιστωτικών λογαριασμών και των λογαριασμών υπηρεσιών/παροχών κοινής ωφέλειας του πελάτη, τα στοιχεία των προηγούμενων διευθύνσεων του πελάτη, καθώς και πληροφορίες από δημόσιες πηγές, όπως εκλογικούς καταλόγους, δημόσια μητρώα (συμπεριλαμβανομένων δικαστικών αποφάσεων) ή δεδομένα πτώχευσης και αφερεγγυότητας. Τα εν λόγω δεδομένα προσωπικού χαρακτήρα εισάγονται στη συνέχεια σε έναν αλγόριθμο βαθμολόγησης, ο οποίος υπολογίζει τη συνολική αξία της πιστοληπτικής ικανότητας του δυνητικού πελάτη.

Σύμφωνα με την Ομάδα εργασίας του άρθρου 29, το δικαίωμα να μην υπόκειται κάποιος σε αποφάσεις που λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και οι οποίες ενδέχεται να παράγουν έννομα αποτελέσματα που αφορούν ή επηρεάζουν σημαντικά το υποκείμενο των δεδομένων ισοδυναμεί με γενική απαγόρευση και δεν απαιτεί από το υποκείμενο των δεδομένων να αντιταχθεί προληπτικά σε μια τέτοια απόφαση⁶⁰⁷.

Ωστόσο, σύμφωνα με τον ΓΚΠΔ, η αυτοματοποιημένη λήψη αποφάσεων που παράγουν έννομα αποτελέσματα ή επηρεάζουν σημαντικά τα φυσικά πρόσωπα ενδέχεται να είναι αποδεκτή εάν είναι αναγκαία για τη σύναψη ή την εκτέλεση σύμβασης μεταξύ του υπευθύνου επεξεργασίας δεδομένων και του υποκειμένου των δεδομένων ή εάν το υποκείμενο των δεδομένων έχει παράσχει τη ρητή συγκατάθεσή του. Επίσης, η αυτοματοποιημένη λήψη αποφάσεων είναι αποδεκτή εάν επιτρέπεται από τον νόμο και εάν προστατεύονται δεόντως τα δικαιώματα, οι ελευθερίες και τα έννομα συμφέροντα του υποκειμένου των δεδομένων⁶⁰⁸.

606 Ό.π., αιτιολογική σκέψη 71, άρθρο 4 παράγραφος 4 και άρθρο 22.

607 Ομάδα εργασίας του άρθρου 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 Οκτωβρίου 2017, σ. 15.

608 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 22 παράγραφος 2.

Ο ΓΚΠΔ προβλέπει επίσης ότι στο πλαίσιο των υποχρεώσεων του υπευθύνου επεξεργασίας όσον αφορά τις πληροφορίες που πρέπει να παρέχονται κατά τη συλλογή δεδομένων προσωπικού χαρακτήρα, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ ⁶⁰⁹. Δεν τίθεται το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα τα οποία επεξεργάζεται ο υπεύθυνος επεξεργασίας ⁶¹⁰. Στην ενημέρωση θα πρέπει να αναφέρεται όχι μόνο το γεγονός ότι θα πραγματοποιηθεί κατάρτιση προφίλ, αλλά και σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται κατά την κατάρτιση προφίλ και τις προβλεπόμενες συνέπειες της επεξεργασίας για τα φυσικά πρόσωπα ⁶¹¹. Για παράδειγμα, μια εταιρεία ασφάλισης υγείας που εφαρμόζει αυτοματοποιημένη λήψη αποφάσεων σχετικά με αιτήσεις θα πρέπει να παρέχει στα υποκείμενα των δεδομένων γενικές πληροφορίες όσον αφορά το πώς λειτουργεί ο αλγόριθμος και ποιους παράγοντες χρησιμοποιεί ο αλγόριθμος για τον υπολογισμό των ασφαλιστρών τους. Ομοίως, κατά την άσκηση του «δικαιώματος πρόσβασης», τα υποκείμενα των δεδομένων μπορούν να ζητούν πληροφορίες από τον υπεύθυνο επεξεργασίας όσον αφορά την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων και σημαντικά στοιχεία σχετικά με τη λογική που υιοθετείται ⁶¹².

Οι πληροφορίες που παρέχονται στα υποκείμενα των δεδομένων έχουν ως στόχο τη διασφάλιση της διαφάνειας και της δυνατότητας των υποκειμένων των δεδομένων να δίνουν τη συγκατάθεσή τους εν πλήρει επιγνώσει, εφόσον συντρέχει μια τέτοια περίπτωση, ή να εξασφαλίζουν ανθρώπινη παρέμβαση. Ο υπεύθυνος επεξεργασίας υποχρεούται να εφαρμόζει κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων των υποκειμένων των δεδομένων. Στο πλαίσιο αυτό περιλαμβάνεται τουλάχιστον το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης εκ μέρους του υπευθύνου επεξεργασίας και η δυνατότητα του υποκειμένου των δεδομένων να εκφράσει την άποψή του και να αμφισβητήσει απόφαση που βασίζεται στην αυτοματοποιημένη επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν ⁶¹³.

609 'Ο.π., άρθρο 12.

610 'Ο.π., άρθρο 15.

611 'Ο.π., άρθρο 13 παράγραφος 2 στοιχείο στ).

612 'Ο.π., άρθρο 15 παράγραφος 1 στοιχείο η).

613 'Ο.π., άρθρο 22 παράγραφος 3.

Η Ομάδα εργασίας του άρθρου 29 παρείχε περαιτέρω καθοδήγηση σχετικά με τη χρήση αυτοματοποιημένης λήψης αποφάσεων δυνάμει του ΓΚΠΔ ⁶¹⁴.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, τα φυσικά πρόσωπα έχουν δικαίωμα να μην υπόκεινται σε απόφαση η οποία θα τα επηρεάσει σημαντικά και η οποία βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία χωρίς να ληφθούν υπόψη οι απόψεις τους ⁶¹⁵. Η απαίτηση συνεκτίμησης των απόψεων του υποκειμένου των δεδομένων όταν οι αποφάσεις βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία σημαίνει ότι τα υποκείμενα των δεδομένων έχουν δικαίωμα να προσβάλουν τις εν λόγω αποφάσεις, και θα πρέπει να έχουν τη δυνατότητα να θέσουν υπό αμφισβήτηση οποιαδήποτε ανακρίβεια στα δεδομένα προσωπικού χαρακτήρα τα οποία χρησιμοποιεί ο υπεύθυνος επεξεργασίας, καθώς και τη συνάφεια οποιουδήποτε προφίλ που εφαρμόστηκε στην περίπτωση τους ⁶¹⁶. Ωστόσο, ένα φυσικό πρόσωπο δεν μπορεί να ασκήσει αυτό το δικαίωμα εάν η αυτοματοποιημένη απόφαση επιτρέπεται βάσει νόμου στον οποίο υπόκειται ο υπεύθυνος επεξεργασίας και ο οποίος νόμος προβλέπει επίσης κατάλληλα μέτρα για τη διασφάλιση των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων των υποκειμένων των δεδομένων. Επιπλέον, τα υποκείμενα των δεδομένων έχουν το δικαίωμα, κατόπιν αιτήματος, να λαμβάνουν γνώση του σκεπτικού στο οποίο βασίζεται η διενεργούμενη επεξεργασία δεδομένων ⁶¹⁷. Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 παρατίθεται το παράδειγμα της βαθμολόγησης της πιστοληπτικής ικανότητας. Τα φυσικά πρόσωπα θα πρέπει να δικαιούνται να γνωρίζουν όχι μόνον τη θετική ή αρνητική απόφαση βαθμολόγησης αυτή καθαυτή, αλλά και τη λογική στην οποία βασίζεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, η οποία οδήγησε στην εν λόγω απόφαση. «Η κατανόηση των στοιχείων αυτών συμβάλλει στην αποτελεσματική άσκηση άλλων ουσιαστών εγγυήσεων όπως το δικαίωμα εναντίωσης και το δικαίωμα υποβολής καταγγελίας σε αρμόδια αρχή» ⁶¹⁸.

Η σύσταση σχετικά με την κατάρτιση προφίλ, παρότι δεν είναι νομικά δεσμευτική, καθορίζει τις προϋποθέσεις για τη συλλογή και επεξεργασία

614 Ομάδα εργασίας του άρθρου 29 (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3 Οκτωβρίου 2017.

615 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο α).

616 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 75.

617 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 9 παράγραφος 1 στοιχείο γ).

618 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 77.

δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της κατάρτισης προφίλ ⁶¹⁹. Περιλαμβάνει διατάξεις σχετικά με την ανάγκη να διασφαλίζεται ότι η επεξεργασία στο πλαίσιο της κατάρτισης προφίλ θα είναι δίκαιη, σύννομη και αναλογική και θα πραγματοποιείται για καθορισμένους και νόμιμους σκοπούς. Η σύσταση περιλαμβάνει επίσης διατάξεις σχετικά με τις πληροφορίες τις οποίες θα πρέπει να παρέχουν οι υπεύθυνοι επεξεργασίας στα υποκείμενα των δεδομένων. Η αρχή της ποιότητας των δεδομένων –βάσει της οποίας οι υπεύθυνοι επεξεργασίας οφείλουν να λαμβάνουν μέτρα για τη διόρθωση ανακρίβειών των δεδομένων, προκειμένου να περιορίζουν τους κινδύνους ή τα σφάλματα που ενδεχομένως συνεπάγεται η κατάρτιση προφίλ, καθώς και να αξιολογούν σε περιοδική βάση την ποιότητα των δεδομένων και των αλγορίθμων που χρησιμοποιούνται– περιλαμβάνεται επίσης στη σύσταση.

6.2. Προσφυγές, ευθύνη, κυρώσεις και αποζημίωση

Κύρια σημεία

- Σύμφωνα με την Εκσυγχρονισμένη Σύμβαση 108, το εθνικό δίκαιο των συμβαλλόμενων μερών πρέπει να ορίζει κατάλληλες προσφυγές και κυρώσεις κατά των παραβάσεων του δικαιώματος στην προστασία των δεδομένων.
- Στην ΕΕ, ο ΓΚΠΔ προβλέπει δυνατότητες προσφυγής για τα υποκείμενα των δεδομένων σε περιπτώσεις παραβίασης των δικαιωμάτων τους, καθώς και κυρώσεις σε βάρος των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία που δεν συμμορφώνονται με τις διατάξεις του κανονισμού. Προβλέπει επίσης δικαίωμα αποζημίωσης και ευθύνη.
- Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να υποβάλουν καταγγελία σε εποπτική αρχή για εικαζόμενες παραβάσεις του κανονισμού, το δικαίωμα πραγματικής δικαστικής προσφυγής και το δικαίωμα αποζημίωσης.
- Κατά την άσκηση του δικαιώματος πραγματικής δικαστικής προσφυγής, τα υποκείμενα των δεδομένων μπορούν να εκπροσωπούνται από μη κυβερνητικές οργανώσεις που δραστηριοποιούνται στον τομέα της προστασίας δεδομένων.
- Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ευθύνεται για τυχόν υλική και μη υλική ζημία που προκύπτει ως αποτέλεσμα της παράβασης.

⁶¹⁹ Συμβούλιο της Ευρώπης, Σύσταση CM/Rec (2010)13 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την προστασία των φυσικών προσώπων έναντι της αυτόματης επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της κατάρτισης προφίλ, άρθρο 5 παράγραφος 5.

- Οι εποπτικές αρχές έχουν την εξουσία να επιβάλλουν διοικητικά πρόστιμα για παραβάσεις του κανονισμού έως 20 000 000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών –ανάλογα με το ποιο είναι υψηλότερο.
- Τα υποκείμενα των δεδομένων μπορούν, ως έσχατη λύση και υπό ορισμένες προϋποθέσεις, να προσφεύγουν ενώπιον του ΕΔΔΑ για παραβάσεις του δικαίου για την προστασία των δεδομένων.
- Κάθε φυσικό ή νομικό πρόσωπο έχει το δικαίωμα να υποβάλει καταγγελία εναντίον οποιασδήποτε απόφασης του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων ενώπιον του ΔΕΕ σύμφωνα με τους όρους που προβλέπονται στις Συνθήκες.

Η έκδοση νομικών πράξεων δεν επαρκεί για να διασφαλίσει την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ευρώπη. Προκειμένου να καταστούν αποτελεσματικοί οι ευρωπαϊκοί κανόνες περί προστασίας δεδομένων, είναι απαραίτητο να δημιουργηθούν μηχανισμοί που επιτρέπουν στα φυσικά πρόσωπα να προσφεύγουν κατά των παραβιάσεων των δικαιωμάτων τους και να ζητούν αποζημίωση για τυχόν προκληθείσα ζημία. Είναι επίσης σημαντικό οι εποπτικές αρχές να διαθέτουν την εξουσία να επιβάλλουν κυρώσεις αποτελεσματικές, αποτρεπτικές και ανάλογες προς την εκάστοτε παράβαση.

Τα δικαιώματα δυνάμει του δικαίου για την προστασία των δεδομένων μπορούν να ασκούνται από το πρόσωπο του οποίου τα δικαιώματα διακυβεύονται: το πρόσωπο αυτό είναι το υποκείμενο των δεδομένων. Ωστόσο, μπορούν και άλλα πρόσωπα –που πληρούν τις αναγκαίες προϋποθέσεις βάσει του εθνικού δικαίου– να εκπροσωπούν τα υποκείμενα των δεδομένων κατά την άσκηση των δικαιωμάτων τους. Σύμφωνα με διάφορες εθνικές νομοθεσίες, τα παιδιά και τα πρόσωπα με νοητικές αναπηρίες πρέπει να εκπροσωπούνται από τους κηδεμόνες τους ⁶²⁰. Σύμφωνα με το δίκαιο της ΕΕ για την προστασία των δεδομένων, μια ένωση –της οποίας ο νόμιμος σκοπός είναι η προώθηση των δικαιωμάτων προστασίας των δεδομένων– μπορεί να εκπροσωπεί τα υποκείμενα των δεδομένων ενώπιον εποπτικής αρχής ή δικαστηρίου ⁶²¹.

620 FRA (2015), *Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για τα δικαιώματα του παιδιού*, Λουξεμβούργο, Υπηρεσία Εκδόσεων· FRA (2013), *Δικαιοπρακτική ικανότητα ατόμων με νοητική αναπηρία και ατόμων με προβλήματα ψυχικής υγείας*, Λουξεμβούργο, Υπηρεσία Εκδόσεων.

621 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 80.

6.2.1. Δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή

Σύμφωνα με το **δικαίωμα τόσο του Συμβουλίου της Ευρώπης όσο και της ΕΕ**, τα φυσικά πρόσωπα έχουν δικαίωμα υποβολής αιτημάτων και καταγγελιών στην αρμόδια εποπτική αρχή εάν θεωρούν ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν δεν πραγματοποιείται σύμφωνα με τον νόμο.

Η Εκσυγχρονισμένη Σύμβαση 108 αναγνωρίζει το δικαίωμα των υποκειμένων των δεδομένων να επωφελούνται από τη συνδρομή εποπτικής αρχής κατά την άσκηση των δικαιωμάτων τους δυνάμει της Σύμβασης, ανεξαρτήτως της ιθαγένειας ή της κατοικίας τους ⁶²². Η αίτηση συνδρομής μπορεί να απορριφθεί μόνο σε εξαιρετικές περιπτώσεις, και τα υποκείμενα των δεδομένων δεν θα πρέπει να υποχρεούνται να καλύψουν τα έξοδα και τέλη που σχετίζονται με τη συνδρομή ⁶²³.

Παρόμοιες διατάξεις περιλαμβάνονται και στο νομικό σύστημα της ΕΕ. Ο ΓΚΠΔ απαιτεί από τις εποπτικές αρχές να λάβουν μέτρα για τη διευκόλυνση της υποβολής καταγγελιών, όπως είναι η δημιουργία ηλεκτρονικού εντύπου υποβολής καταγγελίας ⁶²⁴. Το υποκείμενο των δεδομένων μπορεί να υποβάλει την καταγγελία στην εποπτική αρχή του κράτους μέλους της συνήθους διαμονής του, του τόπου εργασίας του ή του τόπου της εικαζόμενης παράβασης ⁶²⁵. Οι καταγγελίες πρέπει να διερευνώνται, και η εποπτική αρχή πρέπει να ενημερώνει το ενδιαφερόμενο πρόσωπο για την έκβαση της διαδικασίας που αφορά την αξίωση ⁶²⁶.

Πιθανές παραβάσεις εκ μέρους θεσμικών οργάνων ή οργανισμών της ΕΕ μπορούν να γνωστοποιούνται στον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων ⁶²⁷. Η έλλειψη απάντησης του ΕΕΠΔ εντός προθεσμίας έξι μηνών ισοδυναμεί με απόφαση απόρριψης της καταγγελίας. Προσφυγές κατά αποφάσεων του ΕΕΠΔ μπορούν να ασκούνται ενώπιον του ΔΕΕ εντός του πλαισίου του

622 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 18.

623 Ό.π., άρθρα 16-17.

624 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 57 παράγραφος 2.

625 Ό.π., άρθρο 77 παράγραφος 1.

626 Ό.π., άρθρο 77 παράγραφος 2.

627 Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

κανονισμού (ΕΚ) αριθ. 45/2001 που θέτει στα θεσμικά όργανα και στους οργανισμούς της ΕΕ την υποχρέωση να συμμορφώνονται με τους κανόνες περί προστασίας δεδομένων.

Πρέπει να υπάρχει η δυνατότητα προσφυγής στα δικαστήρια κατά των αποφάσεων εθνικής εποπτικής αρχής. Αυτό ισχύει τόσο για το υποκείμενο των δεδομένων, όσο και για τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία που έχουν αποτελέσει μέρη διαδικασίας ενώπιον εποπτικής αρχής.

Παράδειγμα: Τον Σεπτέμβριο του 2017 η ισπανική Αρχή Προστασίας Δεδομένων επέβαλε πρόστιμο στη Facebook για παράβαση διαφόρων κανονισμών για την προστασία δεδομένων. Η εποπτική αρχή καταδίκασε το μέσο κοινωνικής δικτύωσης για τη συλλογή, αποθήκευση και επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων ειδικών κατηγοριών, για σκοπούς διαφήμισης και χωρίς εξασφάλιση της συγκατάθεσης του υποκειμένου των δεδομένων. Η απόφαση βασίστηκε σε έρευνα που διεξήχθη κατόπιν ιδίας πρωτοβουλίας της εποπτικής αρχής.

6.2.2. Δικαίωμα πραγματικής δικαστικής προσφυγής

Πέραν του δικαιώματος υποβολής καταγγελίας στην εποπτική αρχή, τα φυσικά πρόσωπα πρέπει να έχουν δικαίωμα πραγματικής δικαστικής προσφυγής και το δικαίωμα να φέρουν την υπόθεσή τους ενώπιον δικαστηρίου. Το δικαίωμα δικαστικής προσφυγής κατοχυρώνεται σαφώς στην ευρωπαϊκή νομική παράδοση και αναγνωρίζεται ως θεμελιώδες δικαίωμα τόσο βάσει του άρθρου 47 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, όσο και βάσει του άρθρου 13 της ΕΣΔΑ ⁶²⁸.

Στο δίκαιο της ΕΕ, η σημασία της παροχής δυνατοτήτων πραγματικής δικαστικής προσφυγής στα υποκείμενα των δεδομένων σε περίπτωση παραβίασης των δικαιωμάτων τους προκύπτει σαφώς τόσο από τις διατάξεις του ΓΚΠΔ –που θεσπίζει το δικαίωμα πραγματικής δικαστικής προσφυγής κατά εποπτικών αρχών, υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία–, όσο και από τη νομολογία του ΔΕΕ.

628 Βλ., για παράδειγμα, ΕΔΔΑ, *Karabeyoğlu κατά Τουρκίας*, προσφυγή αριθ. 30083/10, 7 Ιουνίου 2016· ΕΔΔΑ, *Mustafa Sezgin Tanrikulu κατά Τουρκίας*, προσφυγή αριθ. 27473/06, 18 Ιουλίου 2017.

Παράδειγμα: Στην υπόθεση *Schrems*⁶²⁹, το ΔΕΕ κήρυξε ανίσχυρη την απόφαση σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα. Βάσει της εν λόγω απόφασης είχαν επιτραπεί διεθνείς διαβιβάσεις δεδομένων από την ΕΕ σε οργανισμούς στις ΗΠΑ που είχαν αυτοπιστοποιηθεί βάσει του συστήματος ασφαλούς λιμένα. Το ΔΕΕ έκρινε ότι το σύστημα ασφαλούς λιμένα έχει αρκετά κενά, τα οποία υπονομεύουν τα θεμελιώδη δικαιώματα των πολιτών της ΕΕ στην προστασία της ιδιωτικής ζωής, την προστασία των δεδομένων προσωπικού χαρακτήρα και το δικαίωμα πραγματικής δικαστικής προσφυγής.

Όσον αφορά την παραβίαση των δικαιωμάτων στον σεβασμό της ιδιωτικής ζωής και στην προστασία δεδομένων, το ΔΕΕ τόνισε ότι η νομοθεσία των ΗΠΑ επιτρέπει σε ορισμένες δημόσιες αρχές να έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από τα κράτη μέλη στις ΗΠΑ και να τα επεξεργάζονται κατά τρόπο ασυμβίβαστο με τους αρχικούς σκοπούς της διαβίβασής τους και καθ' υπέρβαση των ορίων του απολύτως αναγκαίου και του αναλογικού σε σχέση με την προστασία της εθνικής ασφάλειας. Όσον αφορά το δικαίωμα πραγματικής προσφυγής, το ΔΕΕ επισήμανε ότι τα υποκείμενα των δεδομένων δεν είχαν δυνατότητα μέσω της διοικητικής ή της δικαστικής οδού να αποκτήσουν πρόσβαση στα δεδομένα που τα αφορούσαν, και εφόσον χρειαζόταν να εξασφαλίσουν την τροποποίηση ή τη διαγραφή τους. Το ΔΕΕ κατέληξε στο συμπέρασμα ότι η νομοθεσία που δεν προβλέπει ένδικο βοήθημα προκειμένου οι ενδιαφερόμενοι να έχουν δυνατότητα πρόσβασης, διόρθωσης ή διαγραφής των δεδομένων προσωπικού χαρακτήρα που τους αφορούν «δεν σέβεται το ουσιαστικό περιεχόμενο του θεμελιώδους δικαιώματος αποτελεσματικής δικαστικής προστασίας, όπως αυτό κατοχυρώνεται στο άρθρο 47 του Χάρτη». Υπογράμμισε δε ότι η δυνατότητα δικαστικής προσφυγής που εγγυάται τη συμμόρφωση με τους κανόνες δικαίου είναι αναπόσπαστα συνδεδεμένη με το κράτος δικαίου.

Φυσικά πρόσωπα, υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία που επιδιώκουν να προσβάλουν μια νομικώς δεσμευτική απόφαση εποπτικής αρχής μπορούν να κινήσουν διαδικασία ενώπιον δικαστηρίου⁶³⁰. Ο όρος «απόφαση» θα πρέπει να ερμηνεύεται διασταλτικά, καλύπτοντας την άσκηση των εξουσιών

629 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015.

630 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 78.

έρευνας, επιβολής κυρώσεων και αδειοδότησης τις οποίες διαθέτουν οι εποπτικές αρχές, καθώς και τις αποφάσεις με τις οποίες κρίνουν απαράδεκτη ή απορρίπτουν μια καταγγελία. Ωστόσο, μέτρα που δεν είναι νομικώς δεσμευτικά, όπως οι γνωμοδοτήσεις ή οι συμβουλές που παρέχονται από την εποπτική αρχή, δεν μπορούν να αποτελέσουν αντικείμενο προσφυγής ενώπιον δικαστηρίου⁶³¹. Η δικαστική προσφυγή πρέπει να ασκείται ενώπιον των δικαστηρίων του κράτους μέλους στο οποίο είναι εγκατεστημένη η οικεία εποπτική αρχή⁶³².

Σε περιπτώσεις παραβίασης των δικαιωμάτων του υποκειμένου των δεδομένων από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, τα υποκείμενα των δεδομένων δικαιούνται να υποβάλουν καταγγελία ενώπιον δικαστηρίου⁶³³. Για διαδικασίες που κινούνται κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία, είναι ιδιαίτερα σημαντικό να παρέχεται στα φυσικά πρόσωπα η δυνατότητα να επιλέξουν πού θα ασκήσουν την προσφυγή. Μπορεί να επιλέξουν να το πράξουν είτε στο κράτος μέλος στο οποίο ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχουν εγκατάσταση είτε στο κράτος μέλος στο οποίο τα ενδιαφερόμενα υποκείμενα των δεδομένων έχουν τη συνήθη διαμονή τους⁶³⁴. Η δεύτερη δυνατότητα διευκολύνει σε μεγάλο βαθμό τα φυσικά πρόσωπα στην άσκηση των δικαιωμάτων τους, καθώς τους επιτρέπει να ασκούν προσφυγές στο κράτος στο οποίο διαμένουν και εντός οικείας δικαιοδοσίας. Ο περιορισμός του τόπου για τις διαδικασίες κατά υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία στο κράτος μέλος στο οποίο οι τελευταίοι έχουν εγκατάσταση θα μπορούσε να αποθαρρύνει την άσκηση προσφυγής ενώπιον δικαστηρίου από υποκείμενα των δεδομένων που διαμένουν σε άλλα κράτη μέλη, καθώς κάτι τέτοιο θα συνεπαγόταν μετακινήσεις και πρόσθετα έξοδα, ενώ και οι διαδικασίες θα διεξάγονταν σε ξένη γλώσσα και δικαιοδοσία. Η μόνη εξαίρεση αφορά περιπτώσεις στις οποίες ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσιες αρχές και η επεξεργασία πραγματοποιείται κατά την άσκηση των δημόσιων εξουσιών τους. Σε αυτή την περίπτωση, μόνο τα δικαστήρια του κράτους της οικείας δημόσιας αρχής είναι αρμόδια για τις σχετικές αξιώσεις⁶³⁵.

Παρότι, στις περισσότερες περιπτώσεις, οι υποθέσεις που αφορούν τους κανόνες περί προστασίας δεδομένων εκδικάζονται στα δικαστήρια των κρατών μελών,

631 Ό.π., αιτιολογική σκέψη 143.

632 Ό.π., άρθρο 78 παράγραφος 3.

633 Ό.π., άρθρο 79.

634 Ό.π., άρθρο 79 παράγραφος 2.

635 Ό.π.

ορισμένες υποθέσεις μπορούν να παραπεμφθούν ενώπιον του ΔΕΕ. Η πρώτη δυνατή περίπτωση είναι όταν το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία ή η εποπτική αρχή ασκεί προσφυγή για την ακύρωση απόφασης του ΕΣΠΔ. Ωστόσο, η προσφυγή υπόκειται στις προϋποθέσεις του άρθρου 263 της ΣΛΕΕ, που σημαίνει ότι, για να είναι παραδεκτή, τα εν λόγω πρόσωπα και οι προαναφερθείσες οντότητες πρέπει να καταδείξουν ότι η απόφαση του ΕΣΠΔ τους αφορά άμεσα και ατομικά.

Το δεύτερο σενάριο αφορά περιπτώσεις παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα από θεσμικά όργανα ή οργανισμούς της ΕΕ. Σε περιπτώσεις στις οποίες τα θεσμικά όργανα της ΕΕ παραβαίνουν το δίκαιο για την προστασία των δεδομένων, τα υποκείμενα των δεδομένων μπορούν να ασκήσουν προσφυγή απευθείας ενώπιον του Γενικού Δικαστηρίου της ΕΕ (το Γενικό Δικαστήριο αποτελεί μέρος του ΔΕΕ). Το Γενικό Δικαστήριο είναι, σε πρώτο βαθμό, αρμόδιο να αποφαινεται επί καταγγελιών για παραβάσεις του δικαίου της ΕΕ από θεσμικά της όργανα. Ως εκ τούτου, καταγγελίες κατά του ΕΕΠΔ –ως θεσμικού οργάνου της ΕΕ– μπορούν επίσης να υποβάλλονται ενώπιον του Γενικού Δικαστηρίου ⁶³⁶.

Παράδειγμα: Στην υπόθεση *Bavarian Lager* ⁶³⁷, η εταιρεία ζήτησε από την Ευρωπαϊκή Επιτροπή να της παράσχει πρόσβαση στα πλήρη πρακτικά συνεδρίασης της Επιτροπής η οποία φέρεται ότι σχετιζόταν με νομικά ζητήματα που αφορούσαν την εταιρεία. Η Επιτροπή απέρριψε την αίτηση πρόσβασης για λόγους υπερισχυόντων συμφερόντων προστασίας δεδομένων ⁶³⁸. Η *Bavarian Lager*, δυνάμει του άρθρου 32 του κανονισμού για την προστασία δεδομένων από τα όργανα της ΕΕ, άσκησε προσφυγή ενώπιον του Πρωτοδικείου (νυν Γενικού Δικαστηρίου) κατά της εν λόγω απόφασης. Στην απόφασή του (υπόθεση T-194/04, *The Bavarian Lager Co. Ltd κατά Επιτροπής των Ευρωπαϊκών Κοινοτήτων*), το Πρωτοδικείο ακύρωσε την απόφαση της Επιτροπής με την οποία απορρίφθηκε η αίτηση πρόσβασης. Η Ευρωπαϊκή Επιτροπή υπέβαλε αίτηση αναιρέσεως κατά της απόφασης αυτής στο ΔΕΕ.

636 Κανονισμός (ΕΚ) αριθ. 45/2001, άρθρο 32 παράγραφος 3.

637 ΔΕΕ, C-28/08 P, *Ευρωπαϊκή Επιτροπή κατά The Bavarian Lager Co. Ltd* [τμήμα μείζονος συνθέσεως], 2010.

638 Για ανάλυση του επιχειρήματος, βλ. ΕΕΠΔ (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Βρυξέλλες, ΕΕΠΔ.

Το ΔΕΕ (τμήμα μείζονος συνθέσεως) εξέδωσε απόφαση με την οποία αναιρέθηκε η απόφαση του Πρωτοδικείου και επικυρώθηκε η εκ μέρους της Ευρωπαϊκής Επιτροπής απόρριψη της αίτησης πρόσβασης στα πλήρη πρακτικά της συνεδρίασης, με στόχο την προστασία των δεδομένων προσωπικού χαρακτήρα αυτών που μετείχαν στη συνεδρίαση. Το ΔΕΕ έκρινε ορθή την άρνηση της Επιτροπής να γνωστοποιήσει τις εν λόγω πληροφορίες, δεδομένου ότι οι συμμετέχοντες δεν είχαν δώσει τη συγκατάθεσή τους στη γνωστοποίηση των δεδομένων προσωπικού χαρακτήρα που τους αφορούσαν. Επιπροσθέτως, η Bavarian Lager δεν είχε αποδείξει την αναγκαιότητα να αποκτήσει πρόσβαση σε αυτές τις πληροφορίες.

Τέλος, τα υποκείμενα των δεδομένων, οι εποπτικές αρχές, οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία μπορούν, κατά τη διάρκεια των εθνικών διαδικασιών, να υποβάλουν αίτημα στο εθνικό δικαστήριο ώστε να ζητήσει διευκρινίσεις από το ΔΕΕ σχετικά με την ερμηνεία και το κύρος των πράξεων των θεσμικών και λοιπών οργάνων και οργανισμών της ΕΕ. Οι διευκρινίσεις αυτές είναι γνωστές ως προδικαστικές αποφάσεις. Αυτό δεν αποτελεί απευθείας προσφυγή του καταγγέλλοντος, αλλά παρέχει στα εθνικά δικαστήρια τη δυνατότητα να διασφαλίζουν την ορθή ερμηνεία του δικαίου της ΕΕ. Μέσω ακριβώς αυτού του μηχανισμού προδικαστικών αποφάσεων, σημαντικές υποθέσεις –όπως οι *Digital Rights Ireland* και *Kärntner Landesregierung* κ.λπ.⁶³⁹ καθώς και η υπόθεση *Schrems*⁶⁴⁰– κατέληξαν στο ΔΕΕ. Οι υποθέσεις αυτές επηρέασαν σε μεγάλο βαθμό την ανάπτυξη του δικαίου της ΕΕ για την προστασία των δεδομένων.

Παράδειγμα: Οι συνεκδικασθείσες υποθέσεις *Digital Rights Ireland* και *Kärntner Landesregierung* κ.λπ.⁶⁴¹ είχαν υποβληθεί από το High Court της Ιρλανδίας και το Verfassungsgerichtshof (Συνταγματικό Δικαστήριο) της Αυστρίας και αφορούσαν τη συμβατότητα της οδηγίας 2006/24/ΕΚ (οδηγία για τη διατήρηση δεδομένων) με το δίκαιο της ΕΕ για την προστασία των δεδομένων. Το αυστριακό Συνταγματικό Δικαστήριο υπέβαλε

639 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources* κ.λπ. και *Kärntner Landesregierung* κ.λπ. [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

640 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015.

641 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources* κ.λπ. και *Kärntner Landesregierung* κ.λπ. [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

ερωτήματα στο ΔΕΕ όσον αφορά το κύρος των άρθρων 3 έως 9 της οδηγίας 2006/24/ΕΚ υπό το φως των άρθρων 7, 9 και 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Αυτά περιλάμβαναν το ερώτημα αν ορισμένες διατάξεις του αυστριακού ομοσπονδιακού νόμου περί τηλεπικοινωνιών με τον οποίο μεταφέρθηκε στο εθνικό δίκαιο η οδηγία για τη διατήρηση δεδομένων ήταν ή όχι ασύμβατες με πτυχές της πρώην Οδηγίας για την Προστασία Δεδομένων και του κανονισμού για την προστασία δεδομένων από τα όργανα της ΕΕ.

Στην υπόθεση *Kärntner Landesregierung κ.λπ.*, ο Μ. Seitlinger –ένας από τους προσφεύγοντες στη δίκη ενώπιον του Συνταγματικού Δικαστηρίου– υποστήριξε ότι χρησιμοποιούσε το τηλέφωνο, το διαδίκτυο και το ηλεκτρονικό ταχυδρομείο τόσο για τους σκοπούς της εργασίας του, όσο και στην ιδιωτική του ζωή. Κατά συνέπεια, οι πληροφορίες τις οποίες απέστειλε και λάμβανε διέρχονταν μέσω δημόσιων δικτύων τηλεπικοινωνιών. Βάσει του αυστριακού νόμου του 2003 περί τηλεπικοινωνιών, ο πάροχος υπηρεσιών τηλεπικοινωνιών του Μ. Seitlinger είχε νόμιμη υποχρέωση να συλλέγει και να αποθηκεύει δεδομένα σχετικά με την εκ μέρους του χρήση του δικτύου. Ο Μ. Seitlinger θεωρούσε ότι η εν λόγω συλλογή και αποθήκευση δεδομένων προσωπικού χαρακτήρα που τον αφορούσαν δεν ήταν απαραίτητη για τους τεχνικούς σκοπούς της αποστολής και λήψης πληροφοριών μέσω του δικτύου. Στην πραγματικότητα, η συλλογή και αποθήκευση των δεδομένων αυτών δεν ήταν καν απαραίτητη για σκοπούς τιμολόγησης. Ο Μ. Seitlinger δήλωσε ότι δεν είχε συγκατατεθεί σε αυτή τη χρήση των δεδομένων προσωπικού χαρακτήρα που τον αφορούσαν, τα οποία συλλέγονταν και αποθηκεύονταν αποκλειστικά βάσει του αυστριακού νόμου του 2003 περί τηλεπικοινωνιών.

Κατά συνέπεια, ο Μ. Seitlinger άσκησε προσφυγή ενώπιον του αυστριακού Συνταγματικού Δικαστηρίου, στην οποία ισχυρίστηκε ότι οι εκ του νόμου υποχρεώσεις του φορέα παροχής υπηρεσιών τηλεπικοινωνιών παραβίαζαν τα θεμελιώδη δικαιώματά του δυνάμει του άρθρου 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Δεδομένου ότι η αυστριακή νομοθεσία εφάρμοζε το δίκαιο της ΕΕ (την τότε οδηγία για τη διατήρηση δεδομένων), το αυστριακό Συνταγματικό Δικαστήριο παρέπεμψε την υπόθεση στο ΔΕΕ προκειμένου να αποφανθεί σχετικά με τη συμβατότητα της οδηγίας με τα δικαιώματα στον σεβασμό της ιδιωτικής ζωής και στην προστασία δεδομένων που κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Η υπόθεση εκδικάστηκε από το τμήμα μείζονος συνθέσεως του ΔΕΕ, με αποτέλεσμα την ακύρωση της οδηγίας της ΕΕ για τη διατήρηση δεδομένων. Το ΔΕΕ αποφάνθηκε ότι η οδηγία συνεπαγόταν ιδιαιτέρως σοβαρή επέμβαση στα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας δεδομένων, χωρίς η εν λόγω επέμβαση να περιορίζεται στον απολύτως αναγκαίο βαθμό. Η οδηγία επεδίωκε νόμιμο σκοπό, καθώς παρείχε στις εθνικές αρχές πρόσθετες δυνατότητες έρευνας και δίωξης σοβαρών ποινικών αδικημάτων και ως εκ τούτου αποτελούσε χρήσιμο εργαλείο για τις ποινικές έρευνες. Ωστόσο, το ΔΕΕ επισήμανε ότι περιορισμοί στα θεμελιώδη δικαιώματα θα πρέπει να εφαρμόζονται μόνον εάν αυτό είναι απολύτως αναγκαίο, και θα πρέπει να συνοδεύονται από σαφείς και ακριβείς κανόνες όσον αφορά το πεδίο εφαρμογής τους, καθώς και από εγγυήσεις για τα φυσικά πρόσωπα.

Κατά το ΔΕΕ, η οδηγία δεν πληρούσε αυτό το κριτήριο της αναγκαιότητας. Κατ' αρχάς, δεν προέβλεπε σαφείς και ακριβείς κανόνες που να περιορίζουν την έκταση της επέμβασης. Αντί να απαιτεί την ύπαρξη σχέσης μεταξύ διατηρούμενων δεδομένων και σοβαρών ποινικών αδικημάτων, η οδηγία εφαρμοζόταν σε όλα τα δεδομένα όλων των χρηστών όλων των μέσων ηλεκτρονικών επικοινωνιών. Ως εκ τούτου, συνιστούσε επέμβαση στα δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας δεδομένων σχεδόν του συνόλου του πληθυσμού της ΕΕ, γεγονός που θα μπορούσε να θεωρηθεί δυσανάλογο. Δεν περιείχε προϋποθέσεις για τον περιορισμό των προσώπων στα οποία επιτρέπεται η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα, ούτε προβλέπονταν διαδικαστικές προϋποθέσεις που να διέπουν την εν λόγω πρόσβαση, όπως η απαίτηση να εξασφαλίζεται η έγκριση διοικητικής αρχής ή δικαστηρίου πριν από την πρόσβαση. Τέλος, η οδηγία δεν προέβλεπε σαφείς εγγυήσεις για την προστασία των διατηρούμενων δεδομένων. Ως εκ τούτου, δεν διασφάλιζε την αποτελεσματική προστασία των δεδομένων κατά των κινδύνων κατάχρησης, καθώς και κατά κάθε αθέμιτης πρόσβασης σε αυτά και χρήσης τους ⁶⁴².

Καταρχήν, το ΔΕΕ οφείλει να απαντά στα προδικαστικά ερωτήματα και δεν δύναται να αρνηθεί να εκδώσει την προδικαστική απόφασή του με την

⁶⁴² ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ.* και *Kärntner Landesregierung κ.λπ.* [Τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014, σκέψη 69.

αιτιολογία ότι η εν λόγω απάντηση δεν θα ήταν ούτε λυσιτελής ούτε έγκαιρη σε σχέση με την κύρια δίκη. Μπορεί, ωστόσο, να αρνηθεί εάν το ερώτημα δεν εμπίπτει στη σφαίρα αρμοδιότητάς του ⁶⁴³. Το ΔΕΕ αποφαινεται μόνον επί των συστατικών στοιχείων του αιτήματος που παραπέμπεται για προδικαστική απόφαση, ενώ το εθνικό δικαστήριο παραμένει αρμόδιο να αποφανθεί επί της υπόθεσης της κύριας δίκης ⁶⁴⁴.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, τα συμβαλλόμενα μέρη πρέπει να καθορίσουν κατάλληλες δικαστικές και μη δικαστικές προσφυγές για τις παραβάσεις των διατάξεων της Εκσυγχρονισμένης Σύμβασης 108 ⁶⁴⁵. Προσφυγές που αφορούν ισχυρισμούς για παραβιάσεις των δικαιωμάτων προστασίας δεδομένων, κατά παράβαση του άρθρου 8 της ΕΣΔΑ, σε βάρος συμβαλλόμενου μέρους της ΕΣΔΑ, μπορούν, επιπλέον, να ασκούνται ενώπιον του ΕΔΔΑ εφόσον έχουν εξαντληθεί όλα τα διαθέσιμα εσωτερικά ένδικα μέσα. Ο ισχυρισμός για παράβαση του άρθρου 8 της ΕΣΔΑ ενώπιον του ΕΔΔΑ πρέπει επίσης να πληροί και άλλα κριτήρια παραδεκτού (άρθρα 34-35 της ΕΣΔΑ) ⁶⁴⁶.

Παρότι οι προσφυγές στο ΕΔΔΑ μπορούν να στρέφονται μόνο κατά συμβαλλόμενων μερών, μπορούν επίσης να αφορούν έμμεσα πράξεις ή παραλείψεις ιδιωτών εφόσον ένα συμβαλλόμενο μέρος δεν έχει εκπληρώσει τις θετικές υποχρεώσεις τις οποίες υπέχει δυνάμει της ΕΣΔΑ και δεν έχει παράσχει επαρκή προστασία έναντι παραβιάσεων των δικαιωμάτων προστασίας δεδομένων στο εθνικό του δίκαιο.

Παράδειγμα: Στην υπόθεση *Κ.Υ. κατά Φινλανδίας* ⁶⁴⁷, ο προσφεύγων –ένας ανήλικος– κατήγγειλε ότι είχε αναρτηθεί σε ιστότοπο γνωριμιών αγγελία σεξουαλικού χαρακτήρα που αφορούσε τον ίδιο. Ο φορέας παροχής διαδικτυακών υπηρεσιών δεν αποκάλυψε την ταυτότητα του προσώπου που είχε αναρτήσει τις πληροφορίες, λόγω υποχρέωσης τήρησης του απορρήτου βάσει της φινλανδικής νομοθεσίας. Ο προσφεύγων ισχυρίστηκε ότι η φινλανδική νομοθεσία δεν παρείχε επαρκή προστασία έναντι τέτοιου

643 ΔΕΕ, C-244/80, *Pasquale Foglia κατά Mariella Novello* (αριθ. 2), 16 Δεκεμβρίου 1981· ΔΕΕ, C-467/04, *Ποινική δίκη κατά Gasparini κ.λπ.*, 28 Σεπτεμβρίου 2006.

644 ΔΕΕ, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union κατά Viking Line ABP, OÜ Viking Line Eesti* [τμήμα μείζονος συνθέσεως], 11 Δεκεμβρίου 2007, σκέψη 85.

645 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 12.

646 ΕΣΔΑ, άρθρα 34-37.

647 ΕΔΔΑ, *Κ.Υ. κατά Φινλανδίας*, προσφυγή αριθ. 2872/02, 2 Δεκεμβρίου 2008.

είδους πράξεων ιδιώτη ο οποίος δημοσιεύει στο διαδίκτυο δυσφημιστικές αναρτήσεις για τον προσφεύγοντα. Το ΕΔΔΑ έκρινε ότι τα κράτη δεν είναι μόνον υποχρεωμένα να απέχουν από αυθαίρετες επεμβάσεις στην ιδιωτική ζωή των φυσικών προσώπων, αλλά ενδέχεται να υπόκεινται και σε θετικές υποχρεώσεις που περιλαμβάνουν «τη θέσπιση μέτρων που είναι σχεδιασμένα κατά τρόπον ώστε να διασφαλίζουν τον σεβασμό της ιδιωτικής ζωής, ακόμη και στη σφαίρα των σχέσεων μεταξύ των φυσικών προσώπων». Στη συγκεκριμένη υπόθεση, η αποτελεσματική και έμπρακτη προστασία του προσφεύγοντος απαιτούσε τη λήψη αποτελεσματικών μέτρων για τη διαπίστωση της ταυτότητας και τη δίωξη του δράστη. Ωστόσο, το κράτος δεν είχε παράσχει τέτοια προστασία, και το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Παράδειγμα: Στην υπόθεση *Körke κατά Γερμανίας*⁶⁴⁸, η προσφεύγουσα είχε θεωρηθεί ύποπτη για κλοπή στον χώρο εργασίας της και είχε υποβληθεί σε κρυφή βιντεοεπιτήρηση. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι δεν υπήρχε «η παραμικρή ένδειξη ότι οι εθνικές αρχές δεν στάθμισαν ορθά, εντός του περιθωρίου εκτίμησης που διαθέτουν, μεταξύ, αφενός, του δικαιώματος της προσφεύγουσας στον σεβασμό της ιδιωτικής της ζωής δυνάμει του άρθρου 8 και, αφετέρου, του συμφέροντος του εργοδότη της όσον αφορά την προστασία των δικαιωμάτων ιδιοκτησίας του και του δημόσιου συμφέροντος όσον αφορά την ορθή απονομή δικαιοσύνης». Κατά συνέπεια, η προσφυγή κηρύχθηκε απαράδεκτη.

Εάν το ΕΔΔΑ διαπιστώσει ότι συμβαλλόμενο μέρος έχει παραβιάσει οποιοδήποτε από τα δικαιώματα που προστατεύονται από την ΕΣΔΑ, το εν λόγω συμβαλλόμενο μέρος υποχρεούται να εκτελέσει την απόφαση του ΕΔΔΑ (άρθρο 46 της ΕΣΔΑ). Τα μέτρα εκτέλεσης πρέπει κατ' αρχάς να θέτουν τέρμα στην παραβίαση και να απαλείφουν, στο μέτρο του δυνατού, τις αρνητικές συνέπειές της για τον προσφεύγοντα. Η εκτέλεση των δικαστικών αποφάσεων ενδέχεται επίσης να απαιτεί γενικά μέτρα για την πρόληψη παραβάσεων παρόμοιων με εκείνες τις οποίες διαπίστωσε το ΕΔΔΑ, μέσω αλλαγών στη νομοθεσία, μέσω της νομολογίας ή μέσω άλλων μέτρων.

⁶⁴⁸ ΕΔΔΑ, *Körke κατά Γερμανίας* (διάταξη), προσφυγή αριθ. 420/07, 5 Οκτωβρίου 2010.

Σε περίπτωση που το ΕΔΔΑ διαπιστώσει παράβαση της ΕΣΔΑ, το άρθρο 41 της ΕΣΔΑ προβλέπει ότι μπορεί να επιδικάσει «δίκαιη ικανοποίηση» στον προσφεύγοντα εις βάρος του συμβαλλόμενου μέρους.

Δικαίωμα ανάθεσης σε μη κερδοσκοπικό φορέα, οργάνωση ή ένωση

Ο ΓΚΠΔ παρέχει στα φυσικά πρόσωπα που υποβάλλουν καταγγελία σε εποπτική αρχή ή ασκούν δικαστική προσφυγή ενώπιον δικαστηρίου το δικαίωμα να αναθέσουν την εκπροσώπησή τους σε μη κερδοσκοπικό φορέα, οργάνωση ή ένωση⁶⁴⁹. Οι εν λόγω μη κερδοσκοπικές οντότητες πρέπει να διαθέτουν καταστατικούς σκοπούς γενικού συμφέροντος και να δραστηριοποιούνται στον τομέα της προστασίας δεδομένων. Μπορούν να υποβάλουν την καταγγελία ή να ασκήσουν το δικαίωμα δικαστικής προσφυγής εξ ονόματος των υποκειμένων των δεδομένων. Ο κανονισμός παρέχει στα κράτη μέλη τη δυνατότητα να αποφασίσουν –σύμφωνα με το εθνικό δίκαιο– αν ένας φορέας δύναται να υποβάλλει καταγγελίες για λογαριασμό υποκειμένων των δεδομένων χωρίς σχετική ανάθεση από τα εν λόγω υποκείμενα των δεδομένων.

Αυτό το δικαίωμα εκπροσώπησης παρέχει στα φυσικά πρόσωπα τη δυνατότητα να επωφελούνται από την εμπειρογνωσία και την οργανωτική και οικονομική ικανότητα των εν λόγω μη κερδοσκοπικών οντοτήτων, διευκολύνοντάς τα σημαντικά, ως εκ τούτου, κατά την άσκηση των δικαιωμάτων τους. Ο ΓΚΠΔ επιτρέπει στις εν λόγω οντότητες να ασκούν συλλογικές προσφυγές εξ ονόματος πολλών υποκειμένων των δεδομένων. Το στοιχείο αυτό ωφελεί επίσης τη λειτουργία και την αποδοτικότητα του δικαστικού συστήματος, καθώς παρεμφερείς αξιώσεις ομαδοποιούνται και εξετάζονται από κοινού.

6.2.3. Ευθύνη και δικαίωμα αποζημίωσης

Το δικαίωμα πραγματικής προσφυγής πρέπει να παρέχει στα φυσικά πρόσωπα τη δυνατότητα να αξιώνουν αποζημίωση για τυχόν ζημία την οποία υφίστανται ως αποτέλεσμα επεξεργασίας δεδομένων προσωπικού χαρακτήρα που τα αφορούν κατά τρόπο που συνιστά παράβαση της εφαρμοστέας νομοθεσίας. Η ευθύνη για παράνομη επεξεργασία, την οποία υπέχουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία, αναγνωρίζεται ρητά στον ΓΚΠΔ⁶⁵⁰.

649 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 80.

650 Ό.π., άρθρο 82.

Ο κανονισμός παρέχει στα φυσικά πρόσωπα το δικαίωμα να λαμβάνουν αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία τόσο για υλικές, όσο και για μη υλικές ζημίες, ενώ στις αιτιολογικές σκέψεις του κανονισμού ορίζεται ότι «η έννοια της ζημίας θα πρέπει να ερμηνεύεται διασταλτικά με γνώμονα τη νομολογία του Δικαστηρίου κατά τρόπον ώστε να λαμβάνονται πλήρως υπόψη οι στόχοι του παρόντος κανονισμού»⁶⁵¹. Οι υπεύθυνοι επεξεργασίας ευθύνονται και θα μπορούσαν να υπόκεινται σε αξιώσεις αποζημίωσης εάν δεν τηρούν τις υποχρεώσεις τους δυνάμει του κανονισμού. Οι εκτελούντες την επεξεργασία δεδομένων προσωπικού χαρακτήρα ευθύνονται για τη ζημία που προκάλεσε η επεξεργασία μόνο εφόσον δεν ανταποκρίθηκαν στις υποχρεώσεις εκ του κανονισμού που αφορούν ειδικότερα τους εκτελούντες την επεξεργασία ή υπερέβησαν ή ενήργησαν αντίθετα προς τις νόμιμες εντολές του υπευθύνου επεξεργασίας. Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει καταβάλει πλήρη αποζημίωση, ο ΓΚΠΔ προβλέπει ότι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί να ζητήσει –από άλλους υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία που εμπλέκονται στην ίδια επεξεργασία– την ανάκτηση μέρους της αποζημίωσης που αντιστοιχεί στο μέρος της ευθύνης τους για τη ζημία⁶⁵². Ταυτόχρονα, οι όροι απαλλαγής από την ευθύνη είναι πολύ αυστηροί και προϋποθέτουν την απόδειξη ότι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν φέρει καμία ευθύνη για το γενεσιουργό της ζημίας γεγονός.

Η αποζημίωση πρέπει να είναι «πλήρης και ουσιαστική» για την προκληθείσα ζημία. Σε περίπτωση που η ζημία προκαλείται από την επεξεργασία την οποία πραγματοποιούν περισσότεροι υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία, καθένας από αυτούς πρέπει να ευθύνεται για τη συνολική ζημία. Ο κανόνας αυτός επιδιώκει να διασφαλίσει ουσιαστική αποζημίωση για τα υποκείμενα των δεδομένων και μια συντονισμένη προσέγγιση της συμμόρφωσης από την πλευρά των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία που εμπλέκονται σε δραστηριότητες επεξεργασίας.

Παράδειγμα: Τα υποκείμενα των δεδομένων δεν είναι απαραίτητο να ασκήσουν προσφυγή και να αξιώσουν αποζημίωση από όλες τις οντότητες που ευθύνονται για τη ζημία, καθώς κάτι τέτοιο ενδέχεται να συνεπάγεται δαπανηρές και χρονοβόρες διαδικασίες. Αρκεί να ασκήσουν προσφυγή κατά ενός εκ των από κοινού υπευθύνων επεξεργασίας, ο οποίος

651 Ό.π., αιτιολογική σκέψη 146.

652 Ό.π., άρθρο 82 παράγραφοι 2 και 5.

ενδέχεται σε αυτή την περίπτωση να ευθύνεται για τη συνολική ζημία. Σε αυτές τις περιπτώσεις, ο υπεύθυνος της επεξεργασίας ή ο εκτελών την επεξεργασία που καταβάλλει την αποζημίωση δικαιούται στη συνέχεια να ανακτήσει το καταβληθέν ποσό από τις άλλες οντότητες που εμπλέκονται στην επεξεργασία και ευθύνονται για την παράβαση, κατά το μέρος της ευθύνης που τους αναλογεί για τη ζημία. Οι διαδικασίες που αφορούν τους διάφορους από κοινού υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία λαμβάνουν χώρα αφού καταβληθεί η αποζημίωση στο υποκείμενο των δεδομένων, το οποίο δεν συμμετέχει σε αυτές.

Στο νομικό πλαίσιο του Συμβουλίου της Ευρώπης, το άρθρο 12 της Εκσυγχρονισμένης Σύμβασης 108 απαιτεί από τα συμβαλλόμενα μέρη να καθορίσουν κατάλληλα μέσα προσφυγής για τις παραβάσεις των διατάξεων του εθνικού δικαίου, θέτοντας έτσι σε εφαρμογή τις απαιτήσεις της Σύμβασης. Στην Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108 αναφέρεται ότι οι προσφυγές πρέπει να συμπεριλαμβάνουν τη δυνατότητα δικαστικής προσφυγής κατά απόφασης ή πρακτικής, ενώ πρέπει να προβλέπονται και μη δικαστικές προσφυγές⁶⁵³. Οι λεπτομέρειες και οι διάφοροι κανόνες που αφορούν την πρόσβαση στις εν λόγω προσφυγές, παράλληλα με τη διαδικασία που πρέπει να ακολουθείται, επαφίενται στη διακριτική ευχέρεια κάθε συμβαλλόμενου μέρους. Τα συμβαλλόμενα μέρη και τα εθνικά δικαστήρια θα πρέπει επίσης να εξετάσουν το ενδεχόμενο να θεσπίσουν διατάξεις περί χρηματικής αποζημίωσης για υλικές και μη υλικές ζημίες που προκαλούνται από την επεξεργασία, καθώς και τη δυνατότητα άσκησης συλλογικών αγωγών⁶⁵⁴.

6.2.4. Κυρώσεις

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, το άρθρο 12 της Εκσυγχρονισμένης Σύμβασης 108 προβλέπει ότι κάθε συμβαλλόμενο μέρος πρέπει να ορίσει κατάλληλες κυρώσεις και προσφυγές για τις παραβάσεις των διατάξεων του εσωτερικού δικαίου που θέτουν σε εφαρμογή βασικές αρχές για την προστασία των πληροφοριών οι οποίες αναφέρονται στη Σύμβαση 108. Η Σύμβαση δεν καθορίζει ούτε επιβάλλει συγκεκριμένο σύνολο κυρώσεων. Αντιθέτως, αναφέρει σαφώς ότι κάθε συμβαλλόμενο μέρος έχει τη διακριτική ευχέρεια να καθορίσει τη φύση των δικαστικών ή μη δικαστικών κυρώσεων, οι οποίες μπορεί να είναι ποινικές, διοικητικές ή αστικές. Η αιτιολογική έκθεση της

653 Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 100.

654 Ό.π.

Εκσυγχρονισμένης Σύμβασης 108 προβλέπει ότι οι κυρώσεις πρέπει να είναι αποτελεσματικές, αναλογικές και αποτρεπτικές ⁶⁵⁵. Τα συμβαλλόμενα μέρη πρέπει να τηρούν την αρχή αυτή κατά τον καθορισμό της φύσης και της αυστηρότητας των κυρώσεων που προβλέπονται στην εσωτερική έννομη τάξη τους.

Βάσει του δικαίου της ΕΕ, το άρθρο 83 του ΓΚΠΔ παρέχει στις εποπτικές αρχές των κρατών μελών την εξουσία να επιβάλλουν διοικητικά πρόστιμα για παραβάσεις του κανονισμού. Το ύψος των προστίμων και οι περιστάσεις τις οποίες λαμβάνουν υπόψη οι εθνικές αρχές κατά τη λήψη απόφασης σχετικά με την επιβολή προστίμου, καθώς και τα συνολικά ανώτατα όρια του εν λόγω προστίμου, προβλέπονται επίσης στο άρθρο 83. Με τον τρόπο αυτόν, το καθεστώς επιβολής κυρώσεων εναρμονίζεται σε ολόκληρη την ΕΕ.

Ο ΓΚΠΔ ακολουθεί κλιμακωτή προσέγγιση για τα πρόστιμα. Οι εποπτικές αρχές έχουν την εξουσία να επιβάλλουν διοικητικά πρόστιμα για παραβάσεις του κανονισμού έως 20 000 000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών τους –ανάλογα με το ποιο είναι υψηλότερο. Οι παραβάσεις που μπορούν να επισύρουν το συγκεκριμένο ύψος προστίμου περιλαμβάνουν παραβιάσεις των βασικών αρχών για την επεξεργασία και των προϋποθέσεων για συγκατάθεση, καθώς και παραβιάσεις των δικαιωμάτων των υποκειμένων των δεδομένων και των διατάξεων του κανονισμού που διέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αποδέκτες σε τρίτες χώρες. Για άλλες παραβάσεις, οι εποπτικές αρχές μπορούν να επιβάλλουν πρόστιμα έως 10 000 000 ευρώ ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών τους –ανάλογα με το ποιο είναι υψηλότερο.

Κατά τον καθορισμό του είδους και του ύψους του προστίμου που θα πρέπει να επιβληθεί, οι εποπτικές αρχές πρέπει να λαμβάνουν υπόψη σειρά παραγόντων ⁶⁵⁶. Για παράδειγμα, πρέπει να συνεκτιμούν δεόντως τη φύση, τη βαρύτητα και τη διάρκεια της παράβασης, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάστηκαν, καθώς και τον δόλο ή την αμέλεια που προκάλεσε την παράβαση. Όταν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει προβεί σε ενέργειες για να μετριάσει τη ζημία που υπέστησαν τα υποκείμενα των δεδομένων, αυτό θα πρέπει επίσης να λαμβάνεται υπόψη. Ομοίως, ο βαθμός συνεργασίας με την εποπτική αρχή μετά την παράβαση και ο τρόπος με τον

⁶⁵⁵ Ό.π.

⁶⁵⁶ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 83 παράγραφος 2.

οποίο η εποπτική αρχή πληροφορήθηκε την παράβαση (για παράδειγμα, αν αναφέρθηκε από την οντότητα που είναι υπεύθυνη για την επεξεργασία ή από υποκείμενο των δεδομένων του οποίου τα δικαιώματα παραβιάστηκαν) είναι άλλοι δύο σημαντικοί παράγοντες που καθοδηγούν τις εποπτικές αρχές στην απόφασή τους⁶⁵⁷.

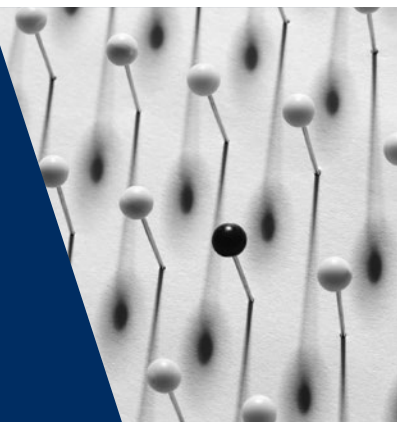
Πέραν της δυνατότητας επιβολής διοικητικών προστίμων, οι εποπτικές αρχές διαθέτουν επίσης ευρύ φάσμα άλλων διορθωτικών εξουσιών. Οι αποκαλούμενες «διορθωτικές» εξουσίες των εποπτικών αρχών καθορίζονται στο άρθρο 58 του ΓΚΠΔ. Αυτές εκτείνονται από την έκδοση εντολών, προειδοποιήσεων και επιπλήξεων προς τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία έως την επιβολή προσωρινών ή ακόμη και μόνιμων απαγορεύσεων των δραστηριοτήτων επεξεργασίας.

Όσον αφορά τις κυρώσεις έναντι παραβάσεων του δικαίου της ΕΕ από θεσμικά όργανα ή οργανισμούς της ΕΕ, λόγω του ειδικού πεδίου εφαρμογής του κανονισμού για την προστασία δεδομένων από τα όργανα της ΕΕ μπορεί να εξεταστεί η επιβολή ποινών υπό μορφή πειθαρχικών μέτρων. Σύμφωνα με το άρθρο 49 του κανονισμού, «[κ]άθε παράλειψη των υποχρεώσεων τις οποίες υπέχει υπάλληλος ή άλλο μέλος του προσωπικού των Ευρωπαϊκών Κοινοτήτων δυνάμει του παρόντος κανονισμού, η οποία διαπράττεται εκ προθέσεως ή εξ αμελείας, επισύρει πειθαρχική κύρωση [...]».

657 Ομάδα εργασίας του άρθρου 29 (2017), *Κατευθυντήριες γραμμές για την εφαρμογή και τον καθορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού 2016/679*, WP 253, 3 Οκτωβρίου 2017.

7

Διεθνείς διαβιβάσεις δεδομένων και ροές δεδομένων προσωπικού χαρακτήρα



ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 44	Έννοια	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφοι 1 και 2
Ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 1 παράγραφος 3 και αιτιολογική σκέψη 170	Μεταξύ κρατών μελών της ΕΕ	
	Μεταξύ συμβαλλόμενων μερών της Σύμβασης 108	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 1
Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς		
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 45 <i>C-362/14, Maximilian Schrems κατά Data Protection Commissioner</i> [τμήμα μείζονος συνθέσεως], 2015	Απόφαση επάρκειας / τρίτες χώρες ή διεθνείς οργανισμοί με κατάλληλα επίπεδα προστασίας	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 2

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46 παράγραφοι 1 και 2	Κατάλληλες εγγυήσεις, συμπεριλαμβανομένων εκτελεστών δικαιωμάτων και ένδικων μέσων για τα υποκείμενα των δεδομένων, οι οποίες παρέχονται μέσω τυποποιημένων συμβατικών ρητρών, δεσμευτικών εταιρικών κανόνων, κωδίκων δεοντολογίας και μηχανισμών πιστοποίησης	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφοι 2, 3, 5 και 6
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46 παράγραφος 3	Με την επιφύλαξη της άδειας από την αρμόδια εποπτική αρχή: συμβατικές ρήτρες και διατάξεις που περιλαμβάνονται σε διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46 παράγραφος 5	Υφιστάμενες άδειες βάσει της οδηγίας 95/46	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 47	Δεσμευτικοί εταιρικοί κανόνες	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 49	Παρεκκλίσεις για ειδικές καταστάσεις	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 4
Παραδείγματα: Συμφωνία ΕΕ-ΗΠΑ για τις καταστάσεις με τα ονόματα των επιβατών (PNR) Συμφωνία ΕΕ-ΗΠΑ για τη SWIFT	Διεθνείς συμφωνίες	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 3 στοιχείο α)

Βάσει του δικαίου της ΕΕ, ο Γενικός Κανονισμός για την Προστασία Δεδομένων προβλέπει την ελεύθερη ροή των δεδομένων εντός της Ευρωπαϊκής Ένωσης. Ωστόσο, περιλαμβάνει ειδικές απαιτήσεις που αφορούν τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός ΕΕ και σε διεθνείς οργανισμούς. Ο κανονισμός αναγνωρίζει τη σημασία των εν λόγω διαβιβάσεων, ειδικότερα για τους σκοπούς του διεθνούς εμπορίου και της διεθνούς συνεργασίας, αλλά ταυτόχρονα και τον αυξημένο κίνδυνο για τα δεδομένα προσωπικού χαρακτήρα. Συνεπώς, σκοπός του κανονισμού είναι να παράσχει στα δεδομένα προσωπικού

χαρακτήρα που διαβιβάζονται σε τρίτες χώρες το ίδιο επίπεδο προστασίας που προβλέπεται και εντός της ΕΕ ⁶⁵⁸. Στο δίκαιο του Συμβουλίου της Ευρώπης αναγνωρίζεται επίσης η σημασία της εφαρμογής κανόνων για τις διασυνοριακές ροές δεδομένων, με βάση την ελεύθερη ροή μεταξύ των μερών και ειδικές απαιτήσεις για διαβιβάσεις σε μη μέλη.

7.1. Φύση των διαβιβάσεων δεδομένων προσωπικού χαρακτήρα

Κύρια σημεία

- Στο δίκαιο της ΕΕ και στο δίκαιο του Συμβουλίου της Ευρώπης προβλέπονται κανόνες σχετικά με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε αποδέκτες σε τρίτες χώρες ή σε διεθνείς οργανισμούς.
- Με τη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων που διαβιβάζονται εκτός ΕΕ, καθίσταται δυνατό η προστασία που παρέχεται από το δίκαιο της ΕΕ να ακολουθεί τα δεδομένα προσωπικού χαρακτήρα που προέρχονται από την ΕΕ.

Βάσει του **δικαίου του Συμβουλίου της Ευρώπης**, οι διασυνοριακές ροές δεδομένων περιγράφονται ως διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε αποδέκτες που υπάγονται σε αλλοδαπή δικαιοδοσία ⁶⁵⁹. Οι διασυνοριακές ροές δεδομένων προς αποδέκτη ο οποίος δεν υπάγεται σε δικαιοδοσία συμβαλλόμενου μέρους επιτρέπονται μόνον εάν υπάρχει κατάλληλο επίπεδο προστασίας ⁶⁶⁰.

Το **δίκαιο της ΕΕ** ρυθμίζει τις διαβιβάσεις «δεδομένων προσωπικού χαρακτήρα τα οποία υποβάλλονται σε επεξεργασία ή προορίζονται να υποβληθούν σε επεξεργασία μετά από τη διαβίβασή τους σε τρίτη χώρα ή διεθνή οργανισμό [...]» ⁶⁶¹. Τέτοιου είδους ροές δεδομένων επιτρέπονται μόνον εφόσον συμμορφώνονται με τους κανόνες που καθορίζονται στο κεφάλαιο V του ΓΚΠΔ.

⁶⁵⁸ Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογικές σκέψεις 101 και 116.

⁶⁵⁹ Αιτιολογική Έκθεση της Εκσυγχρονισμένης Σύμβασης 108, σημείο 102.

⁶⁶⁰ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 2.

⁶⁶¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 44.

Οι διασυνοριακές ροές δεδομένων προσωπικού χαρακτήρα προς αποδέκτη ο οποίος υπάγεται στη δικαιοδοσία συμβαλλόμενου μέρους ή κράτους μέλους επιτρέπονται βάσει του δικαίου του Συμβουλίου της Ευρώπης ή του δικαίου της ΕΕ, αντίστοιχα. Και τα δύο νομικά συστήματα επιτρέπουν επίσης τη διαβίβαση δεδομένων προς χώρα που δεν είναι συμβαλλόμενο μέρος ή κράτος μέλος, εφόσον πληρούνται ορισμένες προϋποθέσεις.

7.2. Ελεύθερη κυκλοφορία/ροή δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών ή συμβαλλόμενων μερών

Κύρια σημεία

- Η ροή δεδομένων προσωπικού χαρακτήρα σε ολόκληρη την ΕΕ και οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ των συμβαλλόμενων μερών της Εκσυγχρονισμένης Σύμβασης 108 δεν πρέπει να υπόκεινται σε περιορισμούς. Ωστόσο, δεδομένου ότι δεν είναι όλα τα συμβαλλόμενα μέρη της Εκσυγχρονισμένης Σύμβασης 108 κράτη μέλη της ΕΕ, οι διαβιβάσεις από ένα κράτος μέλος της ΕΕ σε τρίτη χώρα η οποία είναι, ωστόσο, συμβαλλόμενο μέρος της Σύμβασης 108 δεν επιτρέπονται εάν δεν πληρούνται οι προϋποθέσεις που προβλέπονται στον ΓΚΠΔ.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, η ροή δεδομένων προσωπικού χαρακτήρα μεταξύ των συμβαλλόμενων μερών της Εκσυγχρονισμένης Σύμβασης 108 πρέπει να είναι ελεύθερη. Ωστόσο, η διαβίβαση μπορεί να απαγορεύεται εάν υπάρχει «πραγματικός και σοβαρός κίνδυνος η μεταφορά σε άλλο μέρος να οδηγήσει στην καταστρατήγηση των διατάξεων της Σύμβασης» ή εάν ένα συμβαλλόμενο μέρος δεσμεύεται να προβεί σε αυτό «βάσει εναρμονισμένων κανόνων προστασίας που ισχύουν σε κράτη τα οποία ανήκουν σε περιφερειακό διεθνή οργανισμό»⁶⁶².

Βάσει του δικαίου της ΕΕ, δεν επιτρέπεται η επιβολή περιορισμών ή απαγορεύσεων στην ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών της ΕΕ για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων

⁶⁶² Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 1.

προσωπικού χαρακτήρα⁶⁶³. Ο χώρος ελεύθερης ροής δεδομένων επεκτάθηκε με τη συμφωνία για τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ)⁶⁶⁴, με την οποία η Ισλανδία, το Λιχτενστάιν και η Νορβηγία προσχώρησαν στην εσωτερική αγορά.

Παράδειγμα: Εάν η θυγατρική διεθνούς ομίλου εταιρειών ο οποίος έχει εγκαταστάσεις σε αρκετά κράτη μέλη, μεταξύ των οποίων η Σλοβενία και η Γαλλία, αποστέλλει δεδομένα προσωπικού χαρακτήρα από τη Σλοβενία στη Γαλλία, η εν λόγω ροή δεδομένων δεν πρέπει να περιορίζεται ή να απαγορεύεται από το εθνικό δίκαιο της Σλοβενίας για λόγους που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα.

Εάν, ωστόσο, η ίδια σλοβενική θυγατρική επιθυμεί να διαβιβάσει τα ίδια δεδομένα προσωπικού χαρακτήρα στη μητρική εταιρεία στη Μαλαισία, τότε το πρόσωπο στη Σλοβενία που είναι αρμόδιο για την εξαγωγή των δεδομένων πρέπει να λάβει υπόψη τους κανόνες του κεφαλαίου V του ΓΚΠΔ. Στόχος των διατάξεων αυτών είναι η διαφύλαξη τα δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων που υπάγονται στη δικαιοδοσία της ΕΕ.

Βάσει του δικαίου της ΕΕ, οι ροές δεδομένων προσωπικού χαρακτήρα προς κράτη μέλη του ΕΟΧ για σκοπούς που σχετίζονται με την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων διέπονται από την οδηγία 2016/680⁶⁶⁵. Με τον τρόπο αυτό διασφαλίζεται επίσης ότι η ανταλλαγή δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές εντός της Ένωσης δεν περιορίζεται ούτε απαγορεύεται για λόγους προστασίας των δεδομένων. Βάσει του δικαίου του Συμβουλίου της Ευρώπης, η επεξεργασία όλων των δεδομένων προσωπικού χαρακτήρα (συμπεριλαμβανομένης της διασυνοριακής ροής τους προς άλλα μέρη της Σύμβασης 108), χωρίς εξαιρέσεις

663 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 1 παράγραφος 3.

664 Απόφαση του Συμβουλίου και της Επιτροπής, της 13ης Δεκεμβρίου 1993, για τη σύναψη συμφωνίας σχετικά με τον Ευρωπαϊκό Οικονομικό Χώρο μεταξύ των Ευρωπαϊκών Κοινοτήτων, των κρατών μελών αυτών και της Δημοκρατίας της Αυστρίας, της Δημοκρατίας της Φινλανδίας, της Δημοκρατίας της Ισλανδίας, του Πριγκιπάτου του Λιχτενστάιν, του Βασιλείου της Νορβηγίας, του Βασιλείου της Σουηδίας και της Ελβετικής Συνομοσπονδίας (ΕΕ 1994 L 1).

665 **Οδηγία (ΕΕ) 2016/680** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (ΕΕ L 119 της 4.5.2016, σ. 89).

με βάση τους σκοπούς ή τα πεδία δράσης, συμπεριλαμβάνεται στο πεδίο εφαρμογής της Σύμβασης 108, παρότι τα συμβαλλόμενα μέρη δύνανται να προβλέπουν εξαιρέσεις. Όλα τα μέλη του ΕΟΧ είναι επίσης συμβαλλόμενα μέρη της Σύμβασης 108.

7.3. Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες / μη συμβαλλόμενα μέρη ή σε διεθνείς οργανισμούς

Κύρια σημεία

- Τόσο το **Συμβούλιο της Ευρώπης**, όσο και η **ΕΕ** επιτρέπουν τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς εφόσον πληρούνται ορισμένες προϋποθέσεις για την προστασία των δεδομένων αυτών.
- **Βάσει του δικαίου του Συμβουλίου της Ευρώπης**, κατάλληλο επίπεδο προστασίας μπορεί να εξασφαλιστεί μέσω του δικαίου του κράτους ή του διεθνούς οργανισμού ή μέσω της εφαρμογής κατάλληλων προτύπων.
- **Βάσει του δικαίου της ΕΕ**, μπορούν να πραγματοποιούνται διαβιβάσεις εάν η τρίτη χώρα διασφαλίζει επαρκές επίπεδο προστασίας ή εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία των δεδομένων παρέχει κατάλληλες εγγυήσεις, συμπεριλαμβανομένων εκτελεστών δικαιωμάτων των υποκειμένων των δεδομένων και ένδικων μέσων, χρησιμοποιώντας μέσα όπως οι τυποποιημένες ρήτρες προστασίας δεδομένων ή οι δεσμευτικοί εταιρικοί κανόνες.
- **Τόσο στο δίκαιο του Συμβουλίου της Ευρώπης, όσο και στο δίκαιο της ΕΕ** προβλέπονται ρήτρες παρέκκλισης που επιτρέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε ειδικές περιστάσεις ακόμη και αν δεν εξασφαλίζεται επαρκές επίπεδο προστασίας ούτε υπάρχουν κατάλληλες εγγυήσεις.

Παρότι το δίκαιο του Συμβουλίου της Ευρώπης και το δίκαιο της ΕΕ επιτρέπουν και τα δύο ροές δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς, θέτουν διαφορετικές προϋποθέσεις. Σε κάθε σύνολο προϋποθέσεων λαμβάνονται υπόψη η διαφορετική δομή και οι διαφορετικοί σκοποί του αντίστοιχου οργανισμού.

Βάσει του **δικαίου της ΕΕ**, υπάρχουν, καταρχήν, δύο τρόποι για να επιτραπεί η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή σε διεθνείς

οργανισμούς. Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μπορούν να πραγματοποιούνται βάσει: απόφασης επάρκειας της Ευρωπαϊκής Επιτροπής⁶⁶⁶ ή, απουσία απόφασης επάρκειας, όταν ο υπεύθυνος της επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις, συμπεριλαμβανομένων εκτελεστών δικαιωμάτων και ένδικων μέσων για το υποκείμενο των δεδομένων⁶⁶⁷. Απουσία είτε απόφασης επάρκειας είτε κατάλληλων εγγυήσεων, ισχύουν διάφορες παρεκκλίσεις.

Βάσει του δικαίου του **Συμβουλίου της Ευρώπης**, ωστόσο, οι ελεύθερες διαβιβάσεις δεδομένων προς μη συμβαλλόμενα μέρη της Σύμβασης επιτρέπονται μόνο με βάση:

- το δίκαιο του κράτους ή του διεθνούς οργανισμού, συμπεριλαμβανομένων των εφαρμοστέων διεθνών συνθηκών ή συμφωνιών που διασφαλίζουν κατάλληλες εγγυήσεις
- ειδικές ή εγκεκριμένες τυποποιημένες εγγυήσεις που παρέχονται από νομικώς δεσμευτικά και εκτελεστά μέσα τα οποία θεσπίζονται και εφαρμόζονται από τα πρόσωπα που συμμετέχουν στη διαβίβαση και την περαιτέρω επεξεργασία⁶⁶⁸.

Όπως και στο δίκαιο της ΕΕ, απουσία επαρκούς επιπέδου προστασίας των δεδομένων ισχύουν διάφορες παρεκκλίσεις.

7.3.1. Διαβιβάσεις βάσει απόφασης επάρκειας

Βάσει του δικαίου της ΕΕ, η ελεύθερη ροή δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες με επαρκές επίπεδο προστασίας των δεδομένων προβλέπεται στο άρθρο 45 του ΓΚΠΔ. Το ΔΕΕ έχει διευκρινίσει ότι ο όρος «επαρκές επίπεδο προστασίας» απαιτεί από την τρίτη χώρα να διασφαλίζει επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών «ουσιαστικά ισοδύναμο»⁶⁶⁹ με τις εγγυήσεις που εξασφαλίζει το δίκαιο της ΕΕ. Ταυτόχρονα, τα μέσα τα οποία χρησιμοποιεί η τρίτη χώρα για να εξασφαλίσει αυτό το επίπεδο προστασίας

666 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 45.

667 Ό.π., άρθρο 46.

668 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 3 (στοιχεία α) και β).

669 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015, σκέψη 96.

μπορούν να διαφέρουν από αυτά που εφαρμόζονται εντός της Ένωσης. Το πρότυπο της επάρκειας δεν θέτει ως όρο την αυτολεξεί αναπαραγωγή των ενωσιακών κανόνων ⁶⁷⁰.

Η Ευρωπαϊκή Επιτροπή αξιολογεί το επίπεδο προστασίας των δεδομένων σε τρίτες χώρες εξετάζοντας το εθνικό τους δίκαιο και τις εφαρμοστέες διεθνείς υποχρεώσεις. Η συμμετοχή μιας χώρας σε πολυμερή ή περιφερειακά συστήματα, ιδιαίτερα όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα, πρέπει επίσης να λαμβάνεται υπόψη. Εάν η Ευρωπαϊκή Επιτροπή διαπιστώσει ότι η τρίτη χώρα ή ο διεθνής οργανισμός διασφαλίζει επαρκές επίπεδο προστασίας, δύναται να εκδώσει απόφαση επάρκειας η οποία έχει δεσμευτική ισχύ ⁶⁷¹. Ωστόσο, το ΔΕΕ έχει αποφανθεί ότι οι εθνικές εποπτικές αρχές εξακολουθούν να είναι αρμόδιες για την εξέταση αιτήματος προσώπου σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα του που διαβιβάζονται σε τρίτη χώρα για την οποία η Επιτροπή έχει κρίνει ότι διασφαλίζει επαρκές επίπεδο προστασίας, όταν το πρόσωπο αυτό υποστηρίζει ότι η νομοθεσία και η πρακτική στη χώρα αυτή δεν εξασφαλίζουν επαρκές επίπεδο προστασίας ⁶⁷².

Η Ευρωπαϊκή Επιτροπή μπορεί επίσης να αξιολογήσει την επάρκεια της προστασίας που παρέχεται σε έδαφος τρίτης χώρας, ή να περιοριστεί σε συγκεκριμένους τομείς, όπως στην περίπτωση της εμπορικής νομοθεσίας του Καναδά για τον ιδιωτικό τομέα ⁶⁷³. Αποφάσεις επάρκειας εκδίδονται επίσης για διαβιβάσεις βάσει συμφωνιών μεταξύ ΕΕ και τρίτων χωρών. Οι αποφάσεις αυτές αφορούν αποκλειστικά ένα μόνο είδος διαβίβασης δεδομένων, όπως είναι η διαβίβαση κατάστασης με τα ονόματα επιβατών (PNR) από αεροπορική εταιρεία στις αρχές συνοριακού ελέγχου τρίτης χώρας, όταν η εταιρεία πραγματοποιεί πτήσεις από την ΕΕ σε ορισμένους προορισμούς εκτός ΕΕ (βλ. [ενότητα 7.3.4](#)).

670 Ό.π., σκέψη 74. Βλ. επίσης Ευρωπαϊκή Επιτροπή (2017), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο «Ανταλλαγή και προστασία των δεδομένων προσωπικού χαρακτήρα σε έναν παγκοσμιοποιημένο κόσμο», COM(2017) 7 final της 10ης Ιανουαρίου 2017, σ. 6.

671 Ο κατάλογος των χωρών για τις οποίες έχει εκδοθεί απόφαση επάρκειας επικαιροποιείται συνεχώς και διατίθεται στην αρχική σελίδα της Ευρωπαϊκής Επιτροπής, Γενική Διεύθυνση Δικαιοσύνης.

672 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μειζονος συνθέσεως], 6 Οκτωβρίου 2015, σκέψεις 63 και 65-66.

673 Ευρωπαϊκή Επιτροπή (2002), Απόφαση 2002/2/EK, της 20ής Δεκεμβρίου 2001, βάσει της οδηγίας 95/46/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα του καναδικού νόμου περί προστασίας των δεδομένων προσωπικού χαρακτήρα και ηλεκτρονικών εγγράφων (ΕΕ 2002 L 2).

Οι αποφάσεις επάρκειας παρακολουθούνται σε συνεχή βάση. Η Ευρωπαϊκή Επιτροπή επανεξετάζει ανά τακτά διαστήματα τις αποφάσεις αυτές προκειμένου να εντοπίζει εξελίξεις που μπορούν να επηρεάσουν το κύρος τους. Ως εκ τούτου, εάν η Ευρωπαϊκή Επιτροπή διαπιστώσει ότι η τρίτη χώρα ή ο διεθνής οργανισμός δεν πληροί πλέον τις προϋποθέσεις που δικαιολογούν την απόφαση επάρκειας, μπορεί να τροποποιήσει, να αναστείλει ή να καταργήσει την απόφαση. Η Επιτροπή μπορεί επίσης να προβεί σε διαπραγματεύσεις με την αντίστοιχη τρίτη χώρα ή τον αντίστοιχο διεθνή οργανισμό με σκοπό την επανόρθωση της κατάστασης που οδήγησε στην απόφαση.

Οι αποφάσεις επάρκειας που εκδόθηκαν από την Ευρωπαϊκή Επιτροπή βάσει της οδηγίας 95/46/EK παραμένουν σε ισχύ έως ότου τροποποιηθούν, αντικατασταθούν ή καταργηθούν με απόφαση της Επιτροπής η οποία εκδίδεται σύμφωνα με τους κανόνες του άρθρου 45 του ΓΚΠΔ.

Έως σήμερα, η Ευρωπαϊκή Επιτροπή έχει αναγνωρίσει την Ανδόρα, την Αργεντινή, τον Καναδά [εμπορικοί οργανισμοί που εμπίπτουν στο πεδίο εφαρμογής του νόμου περί δεδομένων προσωπικού χαρακτήρα και ηλεκτρονικών εγγράφων (Personal Information and Electronic Documents Act – PIPEDA)], το Γκέρνζι, την Ελβετία, το Ισραήλ, τη Νέα Ζηλανδία, τη Νήσο του Μαν, την Ουρουγουάη, το Τζέρζι και τις Φερόες Νήσους ως χώρες/περιοχές που παρέχουν επαρκή προστασία. Όσον αφορά τις διαβιβάσεις δεδομένων στις Ηνωμένες Πολιτείες της Αμερικής, η Ευρωπαϊκή Επιτροπή εξέδωσε απόφαση επάρκειας το 2000 η οποία επέτρεπε τις διαβιβάσεις δεδομένων σε εταιρείες που έχουν αυτοπιστοποιηθεί όσον αφορά την προστασία την οποία παρέχουν στα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από την ΕΕ και τη συμμόρφωση με τις αποκαλούμενες «αρχές ασφαλούς λιμένα»⁶⁷⁴. Το ΔΕΕ έκρινε ανίσχυρη την απόφαση αυτή το 2015 και εκδόθηκε νέα απόφαση επάρκειας τον Ιούλιο του 2016, η οποία παρείχε τη δυνατότητα στις επιχειρήσεις να προσχωρήσουν σε αυτήν από την 1η Αυγούστου του 2016.

⁶⁷⁴ Απόφαση 2000/520/EK της Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ (ΕΕ L 215 της 25.8.2000, σ. 7). Η απόφαση κρίθηκε ανίσχυρη από το ΔΕΕ στην απόφαση για την υπόθεση C-632/14, *Maximilian Schrems κατά Data Protection Commission* [Τμήμα μείζονος συνθέσεως].

Παράδειγμα: Στην υπόθεση *Schrems*⁶⁷⁵, ο Maximilian Schrems, αυστριακός υπήκοος, ήταν χρήστης του Facebook για πολλά χρόνια. Ορισμένα ή όλα τα δεδομένα που ο κ. Schrems παρείχε στο Facebook διαβιβάζονταν από την ιρλανδική θυγατρική εταιρεία της Facebook σε διακομιστές εγκατεστημένους στις ΗΠΑ, όπου υποβάλλονταν σε επεξεργασία. Ο κ. Schrems υπέβαλε καταγγελία στην ιρλανδική Αρχή Προστασίας Δεδομένων στην οποία διατύπωνε την άποψη ότι, δεδομένων των αποκαλύψεων που έκανε ο μάρτυρας δημοσίου συμφέροντος Edward Snowden σχετικά με τις δραστηριότητες παρακολούθησης των υπηρεσιών πληροφοριών των Ηνωμένων Πολιτειών, το δίκαιο και η πρακτική των ΗΠΑ δεν διασφαλίζουν επαρκή προστασία για τα δεδομένα που διαβιβάζονται στην εν λόγω χώρα. Η ιρλανδική αρχή απέρριψε την καταγγελία, με την αιτιολογία ότι στην απόφαση που είχε εκδώσει στις 26 Ιουλίου 2000 η Επιτροπή είχε κρίνει ότι, στο πλαίσιο του συστήματος «ασφαλούς λιμένα», οι ΗΠΑ διασφαλίζουν επαρκές επίπεδο προστασίας των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα. Η υπόθεση παραπέμφθηκε στο Ανώτατο Δικαστήριο της Ιρλανδίας (High Court), το οποίο την παρέπεμψε στο ΔΕΕ για την έκδοση προδικαστικής απόφασης.

Το ΔΕΕ αποφάνθηκε ότι η απόφαση της Επιτροπής σχετικά με την επάρκεια του πλαισίου ασφαλούς λιμένα ήταν ανίσχυρη. Επισήμανε αρχικά ότι η απόφαση επέτρεπε τον περιορισμό της εφαρμογής των αρχών ασφαλούς λιμένα σχετικά με την προστασία δεδομένων για λόγους εθνικής ασφάλειας, δημοσίου συμφέροντος ή απαιτήσεων επιβολής του νόμου ή βάσει της εγχώριας νομοθεσίας των ΗΠΑ. Ως εκ τούτου, η απόφαση παρείχε τη δυνατότητα επέμβασης στα θεμελιώδη δικαιώματα των προσώπων εκείνων των οποίων τα δεδομένα προσωπικού χαρακτήρα είχαν διαβιβαστεί ή μπορούσαν να διαβιβαστούν στις ΗΠΑ⁶⁷⁶. Επιπλέον, επισημαινόταν ότι η απόφαση δεν συμπεριλάμβανε καμία διαπίστωση σχετικά με την ύπαρξη στις ΗΠΑ κανόνων για τον περιορισμό τυχόν επεμβάσεων στα θεμελιώδη δικαιώματα, ούτε σχετικά με την ύπαρξη αποτελεσματικής δικαστικής προστασίας κατά τέτοιων επεμβάσεων⁶⁷⁷. Το ΔΕΕ επισήμανε ότι το επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών εντός της Ένωσης απαιτεί οποιαδήποτε ρύθμιση που

675 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015.

676 Ό.π., σκέψη 84.

677 Ό.π., σκέψεις 88-89.

συνεπάγεται επέμβαση στα θεμελιώδη δικαιώματα που διαφυλάσσονται από τα άρθρα 7 και 8 του Χάρτη να προβλέπει σαφείς και ακριβείς κανόνες που να διέπουν την έκταση και την εφαρμογή του οικείου μέτρου και να επιβάλλουν έναν ελάχιστο αριθμό απαιτήσεων, παρεκκλίσεων και περιορισμών όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα ⁶⁷⁸. Δεδομένου ότι στην απόφαση της Επιτροπής δεν αναφερόταν ότι οι ΗΠΑ εξασφαλίζουν πραγματικά ικανοποιητικό επίπεδο προστασίας με την εσωτερική τους νομοθεσία ή με τις διεθνείς δεσμεύσεις που έχουν αναλάβει, το ΔΕΕ κατέληγε στο συμπέρασμα ότι η απόφαση δεν ικανοποιούσε τις απαιτήσεις της σχετικής διάταξης της οδηγίας για την προστασία των δεδομένων που αφορά τις διαβιβάσεις και ήταν, ως εκ τούτου, άκυρη ⁶⁷⁹.

Το επίπεδο προστασίας στις ΗΠΑ δεν ήταν συνεπώς «ουσιαστικά ισοδύναμο» με αυτό των θεμελιωδών δικαιωμάτων και των ελευθεριών που διασφαλίζονται από την ΕΕ ⁶⁸⁰. Το ΔΕΕ υποστήριξε ότι παραβιάζονταν διάφορα άρθρα του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ. Πρώτον, επρόκειτο για προσβολή του ουσιαστικού περιεχομένου του δικαιώματος που κατοχυρώνεται στο άρθρο 7, δεδομένου ότι η νομοθεσία των ΗΠΑ επέτρεπε «στις δημόσιες αρχές την πρόσβαση κατά γενικευμένο τρόπο στο περιεχόμενο των ηλεκτρονικών επικοινωνιών». Δεύτερον, δεν γινόταν σεβαστό το ουσιαστικό περιεχόμενο του άρθρου 47, δεδομένου ότι η νομοθεσία δεν παρείχε στα φυσικά πρόσωπα δυνατότητα δικαστικής προσφυγής όσον αφορά την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα ή τη διόρθωση ή διαγραφή των δεδομένων αυτών. Τέλος, δεδομένου ότι η συμφωνία ασφαλούς λιμένα παραβίαζε τα ανωτέρω άρθρα, τα δεδομένα προσωπικού χαρακτήρα δεν υποβάλλονταν πλέον νόμιμα σε επεξεργασία, με αποτέλεσμα να σημειώνεται παράβαση του άρθρου 8.

Αφού το ΔΕΕ κήρυξε ανίσχυρη τη συμφωνία ασφαλούς λιμένα, η Επιτροπή και οι ΗΠΑ κατέληξαν σε συμφωνία σχετικά με νέο πλαίσιο, την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ. Στις 12 Ιουλίου 2016 η Επιτροπή εξέδωσε απόφαση στην οποία δήλωνε ότι οι ΗΠΑ εξασφαλίζουν επαρκές επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από την Ένωση

⁶⁷⁸ Ό.π., σκέψεις 91-92.

⁶⁷⁹ Ό.π., σκέψεις 96-97.

⁶⁸⁰ Ό.π., σκέψεις 73-74 και 96.

σε οργανισμούς στις ΗΠΑ στο πλαίσιο της ασπίδας προστασίας της ιδιωτικής ζωής⁶⁸¹.

Ομοίως προς τη συμφωνία ασφαλούς λιμένα, στόχος του πλαισίου της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ είναι η προστασία των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται από την ΕΕ στις ΗΠΑ για εμπορικούς σκοπούς⁶⁸². Οι επιχειρήσεις των ΗΠΑ μπορούν να αυτοπιστοποιούνται σε εθελοντική βάση με την ένταξή τους στον κατάλογο της ασπίδας προστασίας, μέσω της οποίας δεσμεύονται να πληρούν τα πρότυπα προστασίας δεδομένων του πλαισίου. Οι αρμόδιες αρχές των ΗΠΑ παρακολουθούν και επιβεβαιώνουν τη συμμόρφωση των πιστοποιημένων επιχειρήσεων με τα εν λόγω πρότυπα.

Ειδικότερα, το σύστημα της ασπίδας προστασίας της ιδιωτικής ζωής προβλέπει τα εξής:

- επιβολή υποχρέωσης προστασίας δεδομένων σε επιχειρήσεις που λαμβάνουν δεδομένα προσωπικού χαρακτήρα από την ΕΕ·
- παροχή προστασίας και δυνατότητας προσφυγής για τα φυσικά πρόσωπα, και ειδικότερα σύσταση μηχανισμού διαμεσολαβητή, ο οποίος είναι ανεξάρτητος από τις υπηρεσίες πληροφοριών των ΗΠΑ και χειρίζεται καταγγελίες από φυσικά πρόσωπα τα οποία πιστεύουν ότι τα προσωπικά τους δεδομένα έχουν χρησιμοποιηθεί παράνομα από τις αρχές των ΗΠΑ στον τομέα της εθνικής ασφάλειας·

681 Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ (ΕΕ L 207 της 1.8.2016, σ. 1). Η Ομάδα εργασίας του άρθρου 29 επιδοκίμασε τις βελτιώσεις που επήλθαν με τον μηχανισμό της ασπίδας προστασίας σε σχέση με την απόφαση για τον ασφαλή λιμένα και συνεχάρη την Επιτροπή και τις αρχές των ΗΠΑ για το γεγονός ότι έλαβαν υπόψη στην τελική έκδοση των εγγράφων της ασπίδας προστασίας τους προβληματισμούς που είχε εκφράσει στη γνώμη WP238 σχετικά με το σχέδιο απόφασης επάρκειας της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ. Ωστόσο, επισήμανε ότι εξακολουθούσαν να υπάρχουν διάφορες ανησυχίες. Για περισσότερες λεπτομέρειες, βλ. Ομάδα εργασίας του άρθρου 29, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, που εκδόθηκε στις 13 Απριλίου 2016, 16/EN WP 238.

682 Για περισσότερες πληροφορίες, βλ. το ενημερωτικό δελτίο για την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ.

- τη διενέργεια ετήσιας κοινής επανεξέτασης για την παρακολούθηση της εφαρμογής του πλαισίου ⁶⁸³, η πρώτη ετήσια επανεξέταση πραγματοποιήθηκε τον Σεπτέμβριο του 2017 ⁶⁸⁴.

Η κυβέρνηση των ΗΠΑ παρέχει έγγραφες δεσμεύσεις και διαβεβαιώσεις οι οποίες συνοδεύουν την απόφαση για την ασπίδα προστασίας της ιδιωτικής ζωής. Σε αυτές προβλέπονται περιορισμοί και διασφαλίσεις όσον αφορά την πρόσβαση της κυβέρνησης των ΗΠΑ σε δεδομένα προσωπικού χαρακτήρα για σκοπούς επιβολής του νόμου και εθνικής ασφάλειας.

7.3.2. Διαβιβάσεις που υπόκεινται σε κατάλληλες εγγυήσεις

Τόσο το **δίκαιο της ΕΕ**, όσο και το **δίκαιο του Συμβουλίου της Ευρώπης** αναγνωρίζουν τις κατάλληλες εγγυήσεις μεταξύ του υπευθύνου της επεξεργασίας που εξάγει τα δεδομένα και του αποδέκτη στην τρίτη χώρα ή διεθνή οργανισμό ως πιθανά μέσα εξασφάλισης επαρκούς επιπέδου προστασίας για τον αποδέκτη.

Βάσει του **δικαίου της ΕΕ**, οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό επιτρέπονται εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και εκτελεστά δικαιώματα, και εάν υφίστανται αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων ⁶⁸⁵. Ο κατάλογος των «κατάλληλων εγγυήσεων» που είναι αποδεκτές προβλέπεται αποκλειστικά στο δίκαιο της ΕΕ για την προστασία δεδομένων. Κατάλληλες εγγυήσεις μπορούν να προβλέπονται μέσω:

- ενός νομικά δεσμευτικού και εκτελεστού μέσου για δημόσιες αρχές ή φορείς,
- δεσμευτικών εταιρικών κανόνων,
- τυποποιημένων ρητρών προστασίας δεδομένων που εκδίδονται είτε από την Ευρωπαϊκή Επιτροπή είτε από εποπτική αρχή,

683 Για περισσότερες πληροφορίες, βλ. την ιστοσελίδα της Ευρωπαϊκής Επιτροπής για την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ.

684 Ευρωπαϊκή Επιτροπή, Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο για την πρώτη ετήσια επανεξέταση της λειτουργίας της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ, COM(2017) 611 final της 18ης Οκτωβρίου 2017. Βλ. επίσης Ομάδα εργασίας του άρθρου 29, *EU-U.S. Privacy Shield – First annual Joint Review*, που εκδόθηκε στις 28 Νοεμβρίου 2017, 17/EN WP 255.

685 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46.

- κωδίκων δεοντολογίας,
- μηχανισμών πιστοποίησης ⁶⁸⁶.

Οι εξατομικευμένες συμβατικές ρήτρες μεταξύ του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία στην ΕΕ και του αποδέκτη των δεδομένων σε τρίτη χώρα αποτελούν ένα ακόμη μέσο παροχής κατάλληλων εγγυήσεων. Οι εν λόγω συμβατικές ρήτρες, ωστόσο, πρέπει να εγκρίνονται από την αρμόδια εποπτική αρχή προκειμένου να μπορούν να χρησιμοποιηθούν ως μέσο στο οποίο μπορεί να βασιστεί η διαβίβαση δεδομένων προσωπικού χαρακτήρα. Ομοίως, οι δημόσιες αρχές μπορούν να χρησιμοποιούν διατάξεις περί προστασίας των δεδομένων που περιλαμβάνονται στις διοικητικές ρυθμίσεις τους υπό τον όρο ότι έχουν εγκριθεί από την εποπτική αρχή ⁶⁸⁷.

Βάσει του δικαίου του Συμβουλίου της Ευρώπης, επιτρέπονται οι ροές δεδομένων προς ένα κράτος ή διεθνή οργανισμό που δεν είναι μέρος της Εκσυγχρονισμένης Σύμβασης 108, υπό τον όρο ότι διασφαλίζεται επαρκές επίπεδο προστασίας. Αυτό μπορεί να επιτευχθεί μέσω:

- του δικαίου του κράτους ή του διεθνούς οργανισμού ή
- ειδικών ή τυποποιημένων εγγυήσεων που ενσωματώνονται σε νομικά δεσμευτικό έγγραφο ⁶⁸⁸.

Διαβιβάσεις που υπόκεινται σε συμβατικές ρήτρες

Τόσο το **δίκαιο του Συμβουλίου της Ευρώπης**, όσο και το **δίκαιο της ΕΕ** αναγνωρίζουν τις συμβατικές ρήτρες μεταξύ του υπευθύνου της επεξεργασίας που εξάγει τα δεδομένα και του αποδέκτη στην τρίτη χώρα ως πιθανά μέσα εξασφάλισης επαρκούς επιπέδου προστασίας για τον αποδέκτη ⁶⁸⁹.

Στο **επίπεδο της ΕΕ**, η Ευρωπαϊκή Επιτροπή, με τη συνδρομή της Ομάδας εργασίας του άρθρου 29, κατάρτισε τυποποιημένες ρήτρες προστασίας δεδομένων οι

⁶⁸⁶ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46 παράγραφος 1 στοιχεία γ), δ), παράγραφος 2 στοιχεία α), β), ε), στ) και άρθρο 47.

⁶⁸⁷ Ό.π., άρθρο 46 παράγραφος 3.

⁶⁸⁸ Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 3 στοιχείο β).

⁶⁸⁹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46 παράγραφος 3· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 3 στοιχείο β).

οποίες πιστοποιήθηκαν επισήμως με απόφαση της Επιτροπής ως αποδεικτικά μέσα επαρκούς προστασίας δεδομένων⁶⁹⁰. Δεδομένου ότι οι αποφάσεις της Επιτροπής είναι δεσμευτικές στο σύνολό τους για τα κράτη μέλη, οι εθνικές αρχές που εποπτεύουν τις διαβιβάσεις δεδομένων πρέπει να αναγνωρίζουν τις τυποποιημένες αυτές συμβατικές ρήτρες στο πλαίσιο των διαδικασιών τους⁶⁹¹. Ως εκ τούτου, εάν ο υπεύθυνος επεξεργασίας ο οποίος εξάγει τα δεδομένα και ο αποδέκτης της τρίτης χώρας συμφωνήσουν και υπογράψουν τις εν λόγω ρήτρες, η συμφωνία αυτή θα πρέπει να συνιστά για την εποπτική αρχή επαρκή απόδειξη ότι εφαρμόζονται κατάλληλες εγγυήσεις. Ωστόσο, στην υπόθεση *Schrems* το ΔΕΕ αποφάνθηκε ότι η Ευρωπαϊκή Επιτροπή δεν έχει την αρμοδιότητα να περιορίσει τις εξουσίες των εθνικών εποπτικών αρχών σε ό,τι αφορά τον έλεγχο της διαβίβασης δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα η οποία έχει αποτελέσει αντικείμενο απόφασης επάρκειας της Επιτροπής⁶⁹². Κατά συνέπεια, δεν παρεμποδίζεται η άσκηση των εξουσιών των εθνικών εποπτικών αρχών, συμπεριλαμβανομένης της εξουσίας αναστολής ή απαγόρευσης διαβίβασης δεδομένων προσωπικού χαρακτήρα, όταν η διαβίβαση πραγματοποιείται κατά παράβαση του δικαίου της ΕΕ ή του εθνικού δικαίου στον τομέα της προστασίας των δεδομένων, όπως, για παράδειγμα, σε περίπτωση που ο εισαγωγέας των δεδομένων δεν τηρεί τις τυποποιημένες συμβατικές ρήτρες⁶⁹³.

Η ύπαρξη τυποποιημένων ρητρών προστασίας δεδομένων στο νομικό πλαίσιο της ΕΕ δεν εμποδίζει τους υπευθύνους επεξεργασίας να καταρτίσουν άλλες ειδικές, μεμονωμένες συμβατικές ρήτρες, υπό τον όρο ότι η εποπτική αρχή εγκρίνει τις εν λόγω ρήτρες⁶⁹⁴. Θα πρέπει, ωστόσο, οι ρήτρες αυτές να διασφαλίζουν το ίδιο επίπεδο προστασίας με αυτό που παρέχεται από τις τυποποιημένες ρήτρες προστασίας των δεδομένων. Κατά την έγκριση των ειδικών ρητρών, οι εποπτικές αρχές υποχρεούνται να εφαρμόζουν τον μηχανισμό συνεκτικότητας, ώστε να

690 Ό.π., άρθρο 46 παράγραφος 2 στοιχείο β) και άρθρο 46 παράγραφος 5.

691 Ό.π., άρθρο 46 παράγραφος 2 στοιχείο γ)- Συνθήκη για τη Λειτουργία της Ευρωπαϊκής Ένωσης, άρθρο 288.

692 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015, σκέψεις 96-98 και 102-105.

693 Προκειμένου να ληφθεί υπόψη η στάση του ΔΕΕ στην υπόθεση *Schrems*, η Επιτροπή τροποποίησε την απόφασή της σχετικά με τις τυποποιημένες συμβατικές ρήτρες: **Εκτελεστική απόφαση (ΕΕ) 2016/2297 της Επιτροπής**, της 16ης Δεκεμβρίου 2016, για την τροποποίηση των αποφάσεων 2001/497/ΕΚ και 2010/87/ΕΕ σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες και σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ 2016 L 344).

694 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 46 παράγραφος 3 στοιχείο α).

διασφαλίζεται μια συνεκτική ρυθμιστική προσέγγιση σε ολόκληρη την ΕΕ ⁶⁹⁵. Αυτό σημαίνει ότι η αρμόδια εποπτική αρχή πρέπει να κοινοποιήσει το σχέδιο απόφασής της σχετικά με τις ρήτρες στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ). Το ΕΣΠΔ θα εκδώσει γνώμη επί του ζητήματος και η εποπτική αρχή πρέπει να λάβει ιδιαίτερως υπόψη τη γνώμη αυτή κατά τη λήψη απόφασης. Εάν δεν προτίθεται να ακολουθήσει τη γνώμη του ΕΣΠΔ, θα ενεργοποιηθεί ο μηχανισμός επίλυσης διαφορών εντός του ΕΣΠΔ και το Συμβούλιο Προστασίας Δεδομένων θα εκδώσει δεσμευτική απόφαση ⁶⁹⁶.

Τα πιο σημαντικά χαρακτηριστικά της τυποποιημένης συμβατικής ρήτρας είναι τα εξής:

- ρήτρα δικαιούχου τρίτου η οποία παρέχει τη δυνατότητα στα υποκείμενα των δεδομένων να ασκούν συμβατικά δικαιώματα παρότι δεν είναι μέρη της σύμβασης
- συμφωνία εκ μέρους του αποδέκτη ή εισαγωγέα των δεδομένων ότι, σε περίπτωση διαφοράς, υπάγεται στη δικαιοδοσία της εθνικής εποπτικής αρχής και/ή των δικαστηρίων της χώρας του υπευθύνου επεξεργασίας που εξάγει τα δεδομένα.

Διατίθενται επί του παρόντος δύο σύνολα τυποποιημένων ρητρών για τις διαβιβάσεις μεταξύ υπευθύνων επεξεργασίας, από τα οποία μπορεί να επιλέξει ο υπεύθυνος επεξεργασίας που εξάγει τα δεδομένα ⁶⁹⁷. Για διαβιβάσεις μεταξύ υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, υπάρχει μόνο ένα σύνολο τυποποιημένων συμβατικών ρητρών ⁶⁹⁸. Ωστόσο, αυτές οι τυποποιημένες συμβατικές ρήτρες αποτελούν επί του παρόντος αντικείμενο δικαστικών προσφυγών.

⁶⁹⁵ Ό.π., άρθρο 63 και άρθρο 64 παράγραφος 1 στοιχείο ε).

⁶⁹⁶ Ό.π., άρθρο 64 και άρθρο 65.

⁶⁹⁷ Η δέσμη I περιέχεται στο παράρτημα της απόφασης 2001/497/ΕΚ της Επιτροπής, της 15ης Ιουνίου 2001, σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες δυνάμει του άρθρου 26 παράγραφος 4 της οδηγίας 95/46/ΕΚ (ΕΕ 2001 L 181)· η δέσμη II περιέχεται στο παράρτημα της απόφασης 2004/915/ΕΚ της Επιτροπής, της 27ης Δεκεμβρίου 2004, για την τροποποίηση της απόφασης 2001/497/ΕΚ όσον αφορά την εισαγωγή μιας εναλλακτικής δέσμης τυποποιημένων συμβατικών ρητρών για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες (ΕΕ 2004 L 385).

⁶⁹⁸ Ευρωπαϊκή Επιτροπή (2010), Απόφαση 2010/87 της Επιτροπής, της 5ης Φεβρουαρίου 2010, σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (ΕΕ 2010 L 39).

Παράδειγμα: Αφού το ΔΕΕ κήρυξε την απόφαση για τον ασφαλή λιμένα άκυρη ⁶⁹⁹, οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα στις ΗΠΑ δεν μπορούσαν πλέον να πραγματοποιούνται βάσει της εν λόγω απόφασης επάρκειας. Ενώ βρίσκονταν σε εξέλιξη διαπραγματεύσεις με τις αρχές των ΗΠΑ και εν αναμονή της έκδοσης νέας απόφασης επάρκειας (η οποία εντέλει εκδόθηκε στις 12 Ιουλίου 2016) ⁷⁰⁰, οι διαβιβάσεις μπορούσαν να πραγματοποιούνται μόνο δυνάμει άλλων νομικών βάσεων, όπως είναι οι τυποποιημένες συμβατικές ρήτρες ή οι δεσμευτικοί εταιρικοί κανόνες. Αρκετές επιχειρήσεις, συμπεριλαμβανομένης της Facebook Ιρλανδίας (η επιχείρηση η οποία εμπλεκόταν στην υπόθεση που οδήγησε στην ακύρωση της απόφασης για τον ασφαλή λιμένα), άρχισαν να χρησιμοποιούν τις τυποποιημένες συμβατικές ρήτρες για να συνεχίσουν τις διαβιβάσεις δεδομένων μεταξύ ΕΕ-ΗΠΑ.

Ο κ. Schrems υπέβαλε καταγγελία στην ιρλανδική εποπτική αρχή στην οποία ζητούσε την αναστολή των διαβιβάσεων δεδομένων στις ΗΠΑ βάσει τυποποιημένων συμβατικών ρητρών. Στην ουσία, ισχυριζόταν ότι όταν τα προσωπικά του δεδομένα διαβιβάζονται από την ιρλανδική θυγατρική της Facebook στη Facebook Inc. και σε διακομιστές που βρίσκονται στις ΗΠΑ, δεν υφίσταται καμία εγγύηση για την προστασία τους. Η Facebook Inc. δεσμεύεται από αμερικανικούς νόμους οι οποίοι ενδέχεται να την υποχρεώσουν να αποκαλύψει δεδομένα προσωπικού χαρακτήρα στις αρχές επιβολής του νόμου των ΗΠΑ, και δεν διατίθεται ένδικο βοήθημα στα ευρωπαϊκά φυσικά πρόσωπα για να αντισταχθούν στην πρακτική αυτή ⁷⁰¹. Για τους λόγους αυτούς το ΔΕΕ κατέληξε στο συμπέρασμα ότι η απόφαση για τον ασφαλή λιμένα ήταν ανίσχυρη και, παρότι η απόφαση του δικαστηρίου περιοριζόταν στην εξέταση εκείνης της απόφασης, ο προσφεύγων θεωρούσε ότι τα ζητήματα αυτά ήταν συναφή και στην περίπτωση της διαβίβασης βάσει συμβατικών ρητρών. Κατά τον χρόνο κατάρτισης του εγχειριδίου, η υπόθεση εξετάζεται ενώπιον του High Court της Ιρλανδίας. Ο προσφεύγων προφανώς προτίθεται να απευθυνθεί στο ΔΕΕ, και στόχος του είναι να αμφισβητήσει την εγκυρότητα της απόφασης

699 ΔΕΕ, C-362/14, *Maximilian Schrems κατά Data Protection Commissioner* [τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015.

700 Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ (ΕΕ L 207 της 1.8.2016, σ. 1).

701 Για περισσότερες πληροφορίες, βλ. την *αναθεωρημένη καταγγελία* του Ιρλανδού επιτρόπου προστασίας δεδομένων κατά της Facebook Ireland Ltd την 1η Δεκεμβρίου 2015.

της Επιτροπής σχετικά με τις τυποποιημένες συμβατικές ρήτρες. Όπως περιγράφεται στο [κεφάλαιο 5](#), μόνο το ΔΕΕ έχει την αρμοδιότητα να κηρύξει ανίσχυρη πράξη της ΕΕ.

Διαβιβάσεις που υπόκεινται σε δεσμευτικούς εταιρικούς κανόνες

Το δίκαιο της ΕΕ παρέχει επίσης τη δυνατότητα πραγματοποίησης διεθνών διαβιβάσεων βάσει δεσμευτικών εταιρικών κανόνων, όταν οι διαβιβάσεις πραγματοποιούνται εντός του ιδίου ομίλου επιχειρήσεων ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα ⁷⁰². Για να αποτελέσουν οι δεσμευτικοί εταιρικοί κανόνες μέσο στο οποίο μπορεί να βασιστεί η διαβίβαση δεδομένων προσωπικού χαρακτήρα, η αρμόδια εποπτική αρχή πρέπει να τους εγκρίνει, σύμφωνα με δεσμευτικούς εταιρικούς κανόνες και με χρήση του μηχανισμού συνεκτικότητας.

Για την έγκριση των δεσμευτικών εταιρικών κανόνων, οι κανόνες αυτοί πρέπει να είναι νομικά δεσμευτικοί, να καλύπτουν όλες τις ουσιαστικές αρχές προστασίας των δεδομένων και να εφαρμόζονται –καθώς και να επιβάλλονται– από κάθε μέλος του ομίλου. Πρέπει να απονέμουν ρητώς εκτελεστά δικαιώματα στα υποκείμενα των δεδομένων, να περιλαμβάνουν όλες τις ουσιαστικές αρχές προστασίας των δεδομένων και να συμμορφώνονται με ορισμένες τυπικές απαιτήσεις, όπως αναφορά της δομής της επιχείρησης, περιγραφή των διαβιβάσεων και του τρόπου εφαρμογής των αρχών προστασίας των δεδομένων. Στις υποχρεώσεις αυτές περιλαμβάνεται και η παροχή των πληροφοριών αυτών στα υποκείμενα των δεδομένων. Στους δεσμευτικούς εταιρικούς κανόνες πρέπει να προσδιορίζονται, μεταξύ άλλων, τα δικαιώματα των υποκειμένων των δεδομένων και οι διατάξεις περί ευθύνης για τυχόν παράβαση των κανόνων ⁷⁰³. Κατά την έγκριση δεσμευτικών εταιρικών κανόνων, θα ενεργοποιείται ο μηχανισμός συνεκτικότητας για τη συνεργασία των εποπτικών αρχών (περιγράφεται στο [κεφάλαιο 5](#)).

Στο πλαίσιο του μηχανισμού συνεκτικότητας, η επικεφαλής εποπτική αρχή εξετάζει τους προτεινόμενους δεσμευτικούς εταιρικούς κανόνες, εκδίδει σχέδιο απόφασης και το κοινοποιεί στο ΕΣΠΔ. Το ΕΣΠΔ εκδίδει γνώμη επί του θέματος, και η επικεφαλής εποπτική αρχή μπορεί επισημώς να εγκρίνει τους δεσμευτικούς εταιρικούς κανόνες, λαμβάνοντας «ιδιαίτερως» υπόψη τη γνώμη του Συμβουλίου Προστασίας Δεδομένων. Η γνώμη αυτή δεν είναι νομικά δεσμευτική, αλλά εάν η εποπτική αρχή προτίθεται να μην τη λάβει υπόψη, τότε ο μηχανισμός επίλυσης

⁷⁰² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 47.

⁷⁰³ Για λεπτομερέστερη περιγραφή, βλ. Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 47.

διαφορών ενεργοποιείται και το Συμβούλιο Προστασίας Δεδομένων θα κληθεί να εκδώσει νομικά δεσμευτική απόφαση, με πλειοψηφία δύο τρίτων των μελών του ⁷⁰⁴.

Βάσει του **δικαίου του Συμβουλίου της Ευρώπης**, στις ειδικές ή τυποποιημένες εγγυήσεις, οι οποίες ενσωματώνονται σε νομικά δεσμευτικό έγγραφο ⁷⁰⁵, περιλαμβάνονται επίσης οι εταιρικοί δεσμευτικοί κανόνες.

7.3.3. Παρεκκλίσεις για ειδικές καταστάσεις

Βάσει του δικαίου της ΕΕ, οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα μπορούν να δικαιολογηθούν, ακόμη και απουσία απόφασης επάρκειας ή εγγυήσεων, όπως τυποποιημένες συμβατικές ρήτρες ή δεσμευτικοί εταιρικοί κανόνες, σε οποιαδήποτε από τις ακόλουθες περιστάσεις:

- το υποκείμενο των δεδομένων συγκατατίθεται ρητώς στη διαβίβαση των δεδομένων·
- το υποκείμενο των δεδομένων συνάπτει –ή πρόκειται να συνάψει– συμβατική σχέση στο πλαίσιο της οποίας είναι απαραίτητη η διαβίβαση των δεδομένων στο εξωτερικό·
- για τη σύναψη σύμβασης μεταξύ υπευθύνου επεξεργασίας δεδομένων και τρίτου μέρους προς όφελος του υποκειμένου των δεδομένων·
- για σημαντικούς λόγους δημόσιου συμφέροντος·
- για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων·
- για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων·
- για τη διαβίβαση δεδομένων από δημόσια μητρώα (πρόκειται για περίπτωση στην οποία προέχουν τα συμφέροντα του ευρύτερου κοινού ώστε να μπορεί να έχει πρόσβαση σε πληροφορίες που αποθηκεύονται σε δημόσια μητρώα) ⁷⁰⁶.

704 Ό.π., άρθρο 57 παράγραφος 1 στοιχείο ιθ), άρθρο 58 παράγραφος 1 στοιχείο ι), άρθρο 64 παράγραφος 1 στοιχείο στ), άρθρο 65 παράγραφοι 1 και 2.

705 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 3 στοιχείο β).

706 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 49.

Στην περίπτωση που δεν ισχύει καμία από αυτές τις προϋποθέσεις, και οι διαβιβάσεις δεν μπορούν να πραγματοποιηθούν βάσει απόφασης επάρκειας ή κατάλληλων εγγυήσεων, η διαβίβαση μπορεί να πραγματοποιηθεί μόνον εάν δεν είναι επαναλαμβανόμενη, αφορά μόνο περιορισμένο αριθμό υποκειμένων των δεδομένων, είναι απαραίτητη για τους σκοπούς επιτακτικών έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας, υπό τον όρο ότι τα δικαιώματα του υποκειμένου των δεδομένων δεν υπερισχύουν των συμφερόντων αυτών ⁷⁰⁷. Στις περιπτώσεις αυτές, ο υπεύθυνος επεξεργασίας πρέπει να αξιολογήσει τις περιστάσεις γύρω από τη διαβίβαση και να παράσχει εγγυήσεις. Πρέπει επίσης να ενημερώσει την εποπτική αρχή και τα υποκείμενα των δεδομένων για τη διαβίβαση και για τα έννομα συμφέροντα που την δικαιολογούν.

Το γεγονός ότι οι παρεκκλίσεις αποτελούν την έσχατη λύση για τις νόμιμες διαβιβάσεις ⁷⁰⁸ (και πρέπει να χρησιμοποιούνται απουσία απόφασης επάρκειας και εάν δεν υφίσταται καμία άλλη εγγύηση) τονίζει τον εξαιρετικό χαρακτήρα τους, ο οποίος επισημαίνεται περαιτέρω στις αιτιολογικές σκέψεις του ΓΚΠΔ ⁷⁰⁹. Ως εκ τούτου, οι παρεκκλίσεις είναι αποδεκτές ως «δυνατότητα διαβιβάσεων σε ορισμένες περιπτώσεις» βάσει συγκατάθεσης, και εφόσον «η διαβίβαση είναι περιστασιακή και αναγκαία» ⁷¹⁰ στο πλαίσιο σύμβασης ή νομικής αξίωσης.

Επιπλέον, σύμφωνα με τις κατευθύνσεις της Ομάδας εργασίας του άρθρου 29, η χρήση των παρεκκλίσεων για ειδικές καταστάσεις πρέπει να γίνεται σε εξαιρετικές και μεμονωμένες περιπτώσεις και όχι για μαζικές ή επαναλαμβανόμενες διαβιβάσεις ⁷¹¹. Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων υπογράμμισε επίσης τον εξαιρετικό χαρακτήρα των παρεκκλίσεων που χρησιμοποιούνται ως νομική βάση για διαβιβάσεις στο πλαίσιο του κανονισμού 45/2001, επισημαίνοντας ότι αυτή η λύση θα πρέπει να χρησιμοποιείται «σε περιορισμένες περιπτώσεις» και «για περιστασιακές διαβιβάσεις» ⁷¹².

707 Ό.π.

708 Ό.π., άρθρο 49 παράγραφος 1.

709 Βλ. Γενικό Κανονισμό για την Προστασία Δεδομένων, άρθρο 49, παράγραφος 1 στοιχ. α), β) και ε) και αιτιολογική σκέψη 113.

710 Ό.π., άρθρο 49 παράγραφος 1.

711 Ομάδα εργασίας του άρθρου 29 (2005), Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995, WP 114, Βρυξέλλες, 25 Νοεμβρίου 2005.

712 Ευρωπαίος Επόπτης Προστασίας Δεδομένων, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, έγγραφο θέσης, Βρυξέλλες, 14 Ιουλίου 2014, σ. 15.

Παράδειγμα: Εταιρεία παροχής υπηρεσιών παγκόσμιου συστήματος διανομής (Global Distribution System, GDS), με έδρα στις ΗΠΑ, παρέχει διαδικτυακό σύστημα κρατήσεων για πολλές αεροπορικές εταιρείες, ξενοδοχεία και κρουαζιέρες σε ολόκληρο τον κόσμο, υποβάλλοντας σε επεξεργασία τα δεδομένα δεκάδων εκατομμυρίων προσώπων στην ΕΕ. Για την αρχική διαβίβαση δεδομένων στους διακομιστές της στις ΗΠΑ, η εταιρεία GDS χρησιμοποιεί μια παρέκκλιση ως νόμιμη βάση για τις διαβιβάσεις, η οποία παρέκκλιση αφορά την ανάγκη σύναψης σύμβασης. Ως εκ τούτου, δεν παρέχει καμία άλλη εγγύηση για τα δεδομένα προσωπικού χαρακτήρα που προέρχονται από την Ευρώπη, διαβιβάζονται στις ΗΠΑ και στη συνέχεια αναδιανέμονται σε ξενοδοχεία σε ολόκληρο τον κόσμο (δηλαδή δεν παρέχονται εγγυήσεις ούτε για περαιτέρω διαβιβάσεις). Η εταιρεία GDS δεν συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ όσον αφορά τις νόμιμες διεθνείς διαβιβάσεις δεδομένων, διότι χρησιμοποιεί μια παρέκκλιση ως νόμιμη βάση για να πραγματοποιεί μαζικές διαβιβάσεις.

Εάν δεν υφίσταται απόφαση επάρκειας, η ΕΕ ή τα κράτη μέλη της έχουν την εξουσία να θέτουν όρια σχετικά με τη διαβίβαση συγκεκριμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα για σημαντικούς λόγους δημόσιου συμφέροντος, παρά την εκπλήρωση άλλων προϋποθέσεων για τις διαβιβάσεις αυτές. Τα όρια αυτά θα πρέπει να θεωρούνται ως εξαιρετικά μέτρα και τα κράτη μέλη οφείλουν να κοινοποιούν τις σχετικές διατάξεις στην Επιτροπή⁷¹³.

Το δικαίο του Συμβουλίου της Ευρώπης επιτρέπει τις ροές δεδομένων προς εδάφη τα οποία δεν εξασφαλίζουν επαρκή προστασία δεδομένων στις ακόλουθες περιπτώσεις:

- όταν το υποκείμενο των δεδομένων έχει δώσει τη ρητή συγκατάθεσή του·
- όταν τα συμφέροντα του υποκειμένου των δεδομένων απαιτούν μια τέτοια διαβίβαση·
- όταν υπάρχουν έννομα συμφέροντα που προέχουν, και ειδικότερα σημαντικά δημόσια συμφέροντα, τα οποία προβλέπονται από τον νόμο·
- όταν πρόκειται για αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία⁷¹⁴.

713 Βλ. Γενικό Κανονισμό για την Προστασία Δεδομένων, άρθρο 49 παράγραφος 5.

714 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 14 παράγραφος 4.

7.3.4. Διαβιβάσεις βάσει διεθνών συμφωνιών

Η ΕΕ δύναται να συνάπτει διεθνείς συμφωνίες με τρίτες χώρες οι οποίες διέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα για συγκεκριμένους σκοπούς. Οι συμφωνίες αυτές πρέπει να περιλαμβάνουν κατάλληλες εγγυήσεις ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα των σχετικών προσώπων. Ο ΓΚΠΔ ισχύει με την επιφύλαξη των εν λόγω διεθνών συμφωνιών ⁷¹⁵.

Τα κράτη μέλη μπορούν επίσης να συνάπτουν διεθνείς συμφωνίες με τρίτες χώρες ή διεθνείς οργανισμούς που παρέχουν κατάλληλο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, στον βαθμό που οι συμφωνίες αυτές δεν θίγουν την εφαρμογή του ΓΚΠΔ.

Παρόμοιος κανόνας προβλέπεται στο άρθρο 12 παράγραφος 3 στοιχείο α) της Εκσυγχρονισμένης Σύμβασης 108.

Παραδείγματα διεθνών συμφωνιών που αφορούν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι οι συμφωνίες για τις καταστάσεις ονομάτων επιβατών (passenger name records, PNR).

Καταστάσεις ονομάτων επιβατών

Τα δεδομένα που περιέχονται στις καταστάσεις με ονόματα επιβατών συλλέγονται από τους αερομεταφορείς κατά τη διάρκεια της διαδικασίας κράτησης αεροπορικού εισιτηρίου και περιλαμβάνουν, μεταξύ άλλων, τα ονόματα, τις διευθύνσεις, τα στοιχεία πιστωτικής κάρτας και τους αριθμούς θέσεων των επιβατών. Οι αερομεταφορείς συλλέγουν επίσης τις πληροφορίες αυτές για να εξυπηρετούν τους δικούς τους εμπορικούς σκοπούς. Η ΕΕ έχει συνάψει συμφωνίες με ορισμένες τρίτες χώρες (Αυστραλία, Καναδάς και ΗΠΑ) για τη διαβίβαση των δεδομένων PNR για τους σκοπούς της πρόληψης, της ανίχνευσης, της διερεύνησης και της δίωξης τρομοκρατικών και σοβαρών εγκλημάτων. Επιπλέον, η Ένωση εξέδωσε την οδηγία (ΕΕ) 2016/861 –γνωστή ως οδηγία PNR της ΕΕ– ⁷¹⁶ το 2016. Η οδηγία αυτή παρέχει το νομικό πλαίσιο για τη διαβίβαση δεδομένων PNR από

⁷¹⁵ Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 102.

⁷¹⁶ Οδηγία (ΕΕ) 2016/681 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων (ΕΕ L 119 της 4.5.2016, σ. 132).

τα κράτη μέλη της ΕΕ σε αρμόδιες αρχές άλλων τρίτων χωρών, με σκοπό ομοίως την πρόληψη, την ανίχνευση, τη διερεύνηση ή τη δίωξη τρομοκρατικών και σοβαρών εγκλημάτων. Οι διαβιβάσεις δεδομένων PNR σε αρχές τρίτων χωρών πραγματοποιούνται κατά περίπτωση και κατόπιν επιμέρους αξιολόγησης της αναγκαιότητας της διαβίβασης για τους σκοπούς που προσδιορίζονται στην οδηγία και υπό τον όρο του σεβασμού των θεμελιωδών δικαιωμάτων.

Όσον αφορά τις συμφωνίες PNR μεταξύ της ΕΕ και τρίτων χωρών, η συμβατότητά τους με τα θεμελιώδη δικαιώματα στην προστασία της ιδιωτικής ζωής και στην προστασία δεδομένων που κατοχυρώνονται στον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ έχει αμφισβητηθεί. Όταν –κατόπιν διαπραγματεύσεων με τον Καναδά– η ΕΕ υπέγραψε συμφωνία σχετικά με τη διαβίβαση και την επεξεργασία δεδομένων PNR το 2014, το Ευρωπαϊκό Κοινοβούλιο αποφάσισε να παραπέμψει το ζήτημα στο ΔΕΕ ώστε να εξεταστεί η νομιμότητα της συμφωνίας με βάση το δίκαιο της ΕΕ, και ειδικότερα με βάση τα άρθρα 7 και 8 του Χάρτη.

Παράδειγμα: Στη Γνωμοδότησή του σχετικά με τη νομιμότητα της συμφωνίας PNR μεταξύ ΕΕ-Καναδά ⁷¹⁷, το ΔΕΕ αποφάνθηκε ότι η σχεδιαζόμενη συμφωνία, με τη μορφή που είχε την περίοδο εκείνη, δεν ήταν συμβατή με τα θεμελιώδη δικαιώματα που αναγνωρίζονται στον Χάρτη και, ως εκ τούτου, δεν μπορούσε να συναφθεί. Δεδομένου ότι αφορούσε την επεξεργασία δεδομένων προσωπικού χαρακτήρα, η συμφωνία συνιστούσε επέμβαση στο δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που παρέχεται βάσει του άρθρου 8 του Χάρτη. Ταυτόχρονα, η συμφωνία περιορίζει το δικαίωμα στον σεβασμό της ιδιωτικής ζωής, όπως κατοχυρώνεται στο άρθρο 7, δεδομένου ότι στο σύνολό τους, τα δεδομένα PNR μπορούν να συγκεντρωθούν και να αναλυθούν κατά τρόπο που να αποκαλύπτουν ταξιδιωτικές συνήθειες, σχέσεις μεταξύ διαφόρων ατόμων, πληροφορίες σχετικά με την οικονομική τους κατάσταση, τις διατροφικές συνήθειες και την κατάσταση της υγείας τους, παρεμβαίνοντας με τον τρόπο αυτό στην ιδιωτική τους ζωή.

⁷¹⁷ ΔΕΕ, *Γνωμοδότηση 1/15 του Δικαστηρίου* [τμήμα μείζονος συνθέσεως], της 26ης Ιουλίου 2017.

Η επέμβαση στα θεμελιώδη δικαιώματα που συνεπαγόταν η σχεδιαζόμενη συμφωνία εξυπηρετούσε έναν στόχο γενικού ενδιαφέροντος, δηλαδή τη δημόσια ασφάλεια και την καταπολέμηση της τρομοκρατίας και των σοβαρών διεθνικών εγκλημάτων. Ωστόσο, το ΔΕΕ υπενθύμισε ότι για να είναι δικαιολογημένη η επέμβαση πρέπει να περιορίζεται σε ό,τι είναι απολύτως αναγκαίο για την επίτευξη του επιδιωκόμενου σκοπού. Μετά την ανάλυση των διατάξεων της συμφωνίας, το ΔΕΕ κατέληξε στο συμπέρασμα ότι η σχεδιαζόμενη συμφωνία δεν πληρούσε το κριτήριο της «απόλυτης αναγκαιότητας». Μεταξύ των παραγόντων που έλαβε υπόψη το ΔΕΕ για να καταλήξει στο συμπέρασμα αυτό συμπεριλαμβάνονται οι εξής:

- Το γεγονός ότι η σχεδιαζόμενη συμφωνία συνεπαγόταν τη διαβίβαση ευαίσθητων δεδομένων. Τα δεδομένα PNR που θα συλλέγονταν δυνάμει της σχεδιαζόμενης συμφωνίας μπορούσαν να περιλαμβάνουν ευαίσθητα δεδομένα, όπως πληροφορίες που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα ή την κατάσταση της υγείας ενός επιβάτη. Η διαβίβαση και η επεξεργασία ευαίσθητων δεδομένων από τις καναδικές αρχές θα μπορούσε να αποτελέσει κίνδυνο για την αρχή της απαγόρευσης των διακρίσεων και, ως εκ τούτου, απαιτείται ακριβής και βάσιμη αιτιολόγηση, αντλούμενη από άλλους λόγους εκτός της δημόσιας ασφάλειας και την καταπολέμηση του σοβαρού εγκλήματος. Η σχεδιαζόμενη συμφωνία δεν παρείχε τέτοιου είδους αιτιολόγηση ⁷¹⁸.
- Η συνεχόμενη αποθήκευση των δεδομένων PNR όλων των επιβατών για χρονική περίοδο πέντε ετών, ακόμη και μετά την αναχώρηση των επιβατών από τον Καναδά θεωρήθηκε επίσης ότι υπερβαίνει τα όρια του απολύτως αναγκαίου. Το ΔΕΕ έκρινε ότι θα μπορούσε να επιτραπεί στις καναδικές αρχές να διατηρούν τα δεδομένα επιβατών για τους οποίους υπάρχουν αντικειμενικά στοιχεία που υποδεικνύουν ότι οι συγκεκριμένοι επιβάτες ενδέχεται να αποτελούν απειλή για τη δημόσια ασφάλεια, ακόμη και μετά την αναχώρησή τους από τον Καναδά. Αντιθέτως, η αποθήκευση των δεδομένων προσωπικού χαρακτήρα όλων των επιβατών, για τους οποίους δεν υφίστανται καν έμμεσα στοιχεία που να υποδεικνύουν ότι αποτελούν κίνδυνο για τη δημόσια ασφάλεια, δεν δικαιολογείται ⁷¹⁹.

⁷¹⁸ Ό.π., σκέψη 165.

⁷¹⁹ Ό.π., σκέψεις 204-207.

Η Συμβουλευτική Επιτροπή της Σύμβασης 108 εξέδωσε Γνωμοδότηση σχετικά με τις επιπτώσεις των συμφωνιών PNR βάσει του δικαίου του Συμβουλίου της Ευρώπης⁷²⁰.

Δεδομένα μηνυμάτων

Η Εταιρεία Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT), με έδρα στο Βέλγιο, η οποία διεκπεραιώνει τις περισσότερες διεθνείς μεταφορές χρηματικών ποσών από ευρωπαϊκές τράπεζες, διατηρούσε αντίστοιχο επιχειρησιακό κέντρο στις ΗΠΑ και της ζητήθηκε να κοινοποιήσει δεδομένα στο Υπουργείο Οικονομικών των ΗΠΑ για σκοπούς διερεύνησης τρομοκρατικών εγκλημάτων στο πλαίσιο του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας⁷²¹.

Από την άποψη της ΕΕ, δεν αποτελούσε επαρκή νομική βάση για την κοινοποίηση των δεδομένων αυτών –κυρίως για τους πολίτες της ΕΕ– στις ΗΠΑ, το γεγονός απλώς ότι ένα από τα κέντρα επεξεργασίας δεδομένων της SWIFT ήταν εγκατεστημένο στις ΗΠΑ.

Το 2010 συνάφθηκε ειδική συμφωνία μεταξύ της ΕΕ και των ΗΠΑ, γνωστή ως συμφωνία SWIFT, για να εξασφαλιστεί η απαραίτητη νομική βάση και να διασφαλιστούν πρότυπα επαρκούς προστασίας των δεδομένων⁷²².

Βάσει της εν λόγω συμφωνίας, τα χρηματοπιστωτικά δεδομένα που αποθηκεύονται από τη SWIFT συνεχίζουν να κοινοποιούνται στο Υπουργείο Οικονομικών των ΗΠΑ για τους σκοπούς της πρόληψης, της διερεύνησης, της

720 Συμβούλιο της Ευρώπης, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19 Αυγούστου 2016.

721 Βλ., σε αυτό το πλαίσιο, Ομάδα εργασίας του άρθρου 29 (2011), Γνώμη 14/2011 σχετικά με θέματα προστασίας δεδομένων που συνδέονται με την πρόληψη της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας, WP 186, Βρυξέλλες, 13 Ιουνίου 2011· Ομάδα εργασίας του άρθρου 29 (2006), Γνώμη 10/2006 σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από την Εταιρεία Παγκόσμιων Διατραπεζικών Χρηματοπιστωτικών Τηλεπικοινωνιών (SWIFT), WP 128, Βρυξέλλες, 22 Νοεμβρίου 2006· Βελγική Επιτροπή προστασίας της ιδιωτικής ζωής (Commission de la protection de la vie privée) (2008), «Contrôle et procédure de recommandation initiés à l'égard de la société SWIFT srl» (Ελεγχος και διαδικασία έκδοσης σύστασης που κινήθηκαν για την εταιρεία SWIFT srl), απόφαση της 9ης Δεκεμβρίου 2008.

722 Απόφαση 2010/412/ΕΕ του Συμβουλίου, της 13ης Ιουλίου 2010, για τη σύναψη της συμφωνίας μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών της Αμερικής σχετικά με την επεξεργασία και τη διαβίβαση δεδομένων χρηματοπιστωτικών μηνυμάτων από την Ευρωπαϊκή Ένωση στις Ηνωμένες Πολιτείες της Αμερικής για σκοπούς του προγράμματος παρακολούθησης της χρηματοδότησης της τρομοκρατίας (ΕΕ 2010 L 195, σ. 3 και 4). Το κείμενο της συμφωνίας επισυνάπτεται στην εν λόγω απόφαση (ΕΕ 2010 L 195, σ. 5-14).

ανίχνευσης ή της δίωξης της τρομοκρατίας ή της χρηματοδότησης της τρομοκρατίας. Το Υπουργείο Οικονομικών των ΗΠΑ δύναται να ζητεί χρηματοπιστωτικά δεδομένα από τη SWIFT, υπό τον όρο ότι η σχετική αίτηση:

- προσδιορίζει με τον σαφέστερο δυνατό τρόπο τα χρηματοπιστωτικά δεδομένα·
- τεκμηριώνει σαφώς την αναγκαιότητα των δεδομένων·
- περιορίζεται στα απολύτως απαραίτητα ούτως ώστε να ελαχιστοποιείται ο όγκος των αιτούμενων δεδομένων·
- δεν ζητά δεδομένα που αφορούν τον ενιαίο χώρο πληρωμών σε ευρώ (SEPA)⁷²³.

Η Ευρωπόλ πρέπει να λαμβάνει αντίγραφο κάθε αίτησης που υποβάλλεται από το Υπουργείο Οικονομικών των ΗΠΑ και να εξακριβώνει αν η αίτηση συμμορφώνεται με τις αρχές της συμφωνίας SWIFT⁷²⁴. Εάν επιβεβαιωθεί ότι εξασφαλίζεται η συμμόρφωση, η SWIFT πρέπει να παρέχει τα χρηματοπιστωτικά δεδομένα απευθείας στο Υπουργείο Οικονομικών των ΗΠΑ. Το Υπουργείο πρέπει να αποθηκεύει τα χρηματοπιστωτικά δεδομένα σε ασφαλές φυσικό περιβάλλον, όπου πρόσβαση έχουν μόνον οι αναλυτές που διεξάγουν έρευνες για την τρομοκρατία ή τη χρηματοδότησή της, και τα χρηματοπιστωτικά δεδομένα δεν πρέπει να διασυνδέονται με καμία άλλη βάση δεδομένων. Εν γένει, τα χρηματοπιστωτικά δεδομένα που λαμβάνονται από τη SWIFT πρέπει να διαγράφονται το αργότερο πέντε έτη από τη λήψη τους. Τα χρηματοπιστωτικά δεδομένα που είναι σημαντικά για συγκεκριμένες έρευνες ή διώξεις μπορούν να διατηρούνται μόνο για το χρονικό διάστημα που τα δεδομένα είναι αναγκαία για τους σκοπούς αυτών των ερευνών ή διώξεων.

Το Υπουργείο Οικονομικών των ΗΠΑ δύναται να διαβιβάζει στοιχεία από τα δεδομένα που λαμβάνει από τη SWIFT σε ειδικές αρχές επιβολής του νόμου, αρχές δημόσιας ασφάλειας ή αρχές καταπολέμησης της τρομοκρατίας, εντός ή εκτός των ΗΠΑ, αποκλειστικά για τους σκοπούς της διερεύνησης, της ανίχνευσης, της πρόληψης ή της δίωξης της τρομοκρατίας και της χρηματοδότησής της.

⁷²³ Ό.π., άρθρο 4 παράγραφος 2.

⁷²⁴ Η Κοινή Εποπτική Αρχή της Ευρωπόλ έχει διενεργήσει ελέγχους σχετικά με τις δραστηριότητες της Ευρωπόλ στον τομέα αυτόν.

Όταν η περαιτέρω διαβίβαση χρηματοπιστωτικών δεδομένων αφορά πολίτη ή κάτοικο κράτους μέλους της ΕΕ, οποιαδήποτε διαβίβαση των δεδομένων στις αρχές τρίτης χώρας υπόκειται στην προηγούμενη έγκριση των αρμόδιων αρχών του ενδιαφερόμενου κράτους μέλους. Είναι δυνατή η εφαρμογή εξαιρέσεων στις περιπτώσεις που η διαβίβαση των δεδομένων είναι ουσιώδης για την πρόληψη άμεσης και σοβαρής απειλής κατά της δημόσιας ασφάλειας.

Ανεξάρτητοι επόπτες, συμπεριλαμβανομένου προσώπου που διορίζεται από την Ευρωπαϊκή Επιτροπή, παρακολουθούν τη συμμόρφωση με τις αρχές της συμφωνίας SWIFT. Έχουν τη δυνατότητα να επανεξετάζουν σε πραγματικό χρόνο και αναδρομικά όλες τις αναζητήσεις που έγιναν στα παρεχόμενα δεδομένα, να ζητούν πρόσθετες πληροφορίες για την αιτιολόγηση του συνδέσμου των αναζητήσεων αυτών με την τρομοκρατία, καθώς και την εξουσία να εμποδίζουν μερικές ή όλες τις αναζητήσεις που φαίνεται να παραβιάζουν τις εγγυήσεις που ορίζονται στη συμφωνία.

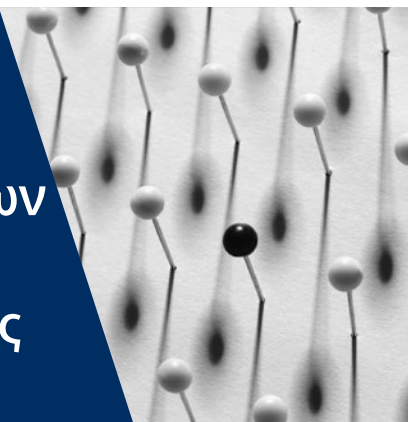
Τα υποκείμενα των δεδομένων έχουν το δικαίωμα να λαμβάνουν επιβεβαίωση από την αρμόδια εποπτική αρχή της ΕΕ ότι έχει εξασφαλιστεί η συμμόρφωση με τα δικαιώματά τους όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα. Τα υποκείμενα των δεδομένων έχουν επίσης το δικαίωμα διόρθωσης, διαγραφής ή κλειδώματος των δεδομένων τους τα οποία έχουν συλλεχθεί και αποθηκευτεί από το Υπουργείο Οικονομικών των ΗΠΑ βάσει της συμφωνίας SWIFT. Ωστόσο, τα δεδομένα πρόσβασης των υποκειμένων των δεδομένων μπορεί να υπόκεινται σε ορισμένους νομικούς περιορισμούς. Όταν απορρίπτεται αίτηση πρόσβασης, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται γραπτώς για την απόρριψη της αίτησής του και για το δικαίωμά του όσον αφορά την άσκηση διοικητικής ή δικαστικής προσφυγής στις ΗΠΑ.

Η συμφωνία SWIFT ισχύει για πέντε έτη, και η πρώτη περίοδος ισχύος της διήρκεσε έως τον Αύγουστο του 2015. Παρατείνεται αυτόματα για μεταγενέστερες χρονικές περιόδους ενός έτους, εκτός εάν ένα μέρος κοινοποιήσει στο άλλο, τουλάχιστον έξι μήνες πριν, την πρόθεση του να μην παρατείνει τη συμφωνία. Η αυτόματη παράταση εφαρμόστηκε τον Αύγουστο του 2015, του 2016 και του 2017 και διασφαλίζει την ισχύ της συμφωνίας SWIFT έως τουλάχιστον το τέλος Αυγούστου 2018 ⁷²⁵.

725 Ό.π., άρθρο 23 παράγραφος 2.

8

Προστασία των δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης



ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης	Γενικά	Εκσυγχρονισμένη Σύμβαση 108
	Αστυνομία	Σύσταση για τον αστυνομικό τομέα Πρακτικός Οδηγός για τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα
	Παρακολούθηση	ΕΔΔΑ, <i>B. B. κατά Γαλλίας</i> , προσφυγή αριθ. 5335/06, 2009 ΕΔΔΑ, <i>S. και Marper κατά Ηνωμένου Βασιλείου</i> [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 2008 ΕΔΔΑ, <i>Allan κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 48539/99, 2002 ΕΔΔΑ, <i>Malone κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 8691/79, 1984 ΕΔΔΑ, <i>Klass κ.λπ. κατά Γερμανίας</i> , προσφυγή αριθ. 5029/71, 1978 ΕΔΔΑ, <i>Szabó και Vissy κατά Ουγγαρίας</i> , προσφυγή αριθ. 37138/14, 2016 ΕΔΔΑ, <i>Vetter κατά Γαλλίας</i> , προσφυγή αριθ. 59842/00, 2005

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
	Έγκλημα στον κυβερνοχώρο	Σύμβαση για το έγκλημα στον κυβερνοχώρο
Άλλες ειδικές νομικές πράξεις		
Απόφαση Prüm	Για ειδικές κατηγορίες δεδομένων: δακτυλικά αποτυπώματα, DNA, χουλιγκανισμός, πληροφορίες επιβατών αεροπορικών μεταφορών, δεδομένα τηλεπικοινωνιών, κ.λπ.	Εκσυγχρονισμένη Σύμβαση 108, άρθρο 6 Σύσταση για τον αστυνομικό τομέα, Πρακτικός Οδηγός για τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα
Συνηδική πρωτοβουλία (Απόφαση-πλαίσιο 2006/960/ΔΕΥ του Συμβουλίου)	Απλούστευση της ανταλλαγής πληροφοριών και στοιχείων μεταξύ των αρχών επιβολής του νόμου	ΕΔΔΑ, <i>S. και Marper κατά Ηνωμένου Βασιλείου</i> [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 2008
Οδηγία (ΕΕ) 2016/681 σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις με τα ονόματα των επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, <i>Digital Rights Ireland</i> και <i>Kärntner Landesregierung</i> κ.λπ. [τμήμα μείζονος συνθέσεως], 2014 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, <i>Tele2 Sverige</i> και <i>Home Department κατά Tom Watson</i> κ.λπ. [τμήμα μείζονος συνθέσεως], 2016	Διατήρηση δεδομένων προσωπικού χαρακτήρα	ΕΔΔΑ, <i>B.B. κατά Γαλλίας</i> , προσφυγή αριθ. 5335/06, 2009
Κανονισμός Ευρωπαϊκή Απόφαση Eurojust	Από ειδικούς οργανισμούς	Σύσταση για τον αστυνομικό τομέα
Απόφαση Σένγκεν II Κανονισμός VIS Κανονισμός Eurodac Απόφαση CIS	Από ειδικά κοινά συστήματα πληροφοριών	Σύσταση τον αστυνομικό τομέα ΕΔΔΑ, <i>Dalea κατά Γαλλίας</i> , προσφυγή αριθ. 964/07, 2010

Προκειμένου να διασφαλίζεται η εξισορρόπηση των ατομικών συμφερόντων ως προς την προστασία των δεδομένων με τα συμφέροντα της κοινωνίας ως προς τη συλλογή δεδομένων για τους σκοπούς της καταπολέμησης του εγκλήματος και της διαφύλαξης της εθνικής και δημόσιας ασφάλειας, το Συμβούλιο της Ευρώπης και η ΕΕ έχουν θεσπίσει ειδικές νομικές πράξεις. Στην παρούσα ενότητα παρουσιάζεται επισκόπηση του δικαίου του Συμβουλίου της Ευρώπης (ενότητα 8.1) και της ΕΕ (ενότητα 8.2) σε σχέση με την προστασία των δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης.

8.1. Το δίκαιο του Συμβουλίου της Ευρώπης για την προστασία των δεδομένων και την εθνική ασφάλεια, τον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης

Κύρια σημεία

- Η Εκσυγχρονισμένη Σύμβαση 108 και η σύσταση του Συμβουλίου της Ευρώπης για τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα καλύπτουν την προστασία των δεδομένων σε όλους τους τομείς δράσης των αστυνομικών αρχών.
- Η Σύμβαση για το έγκλημα στον κυβερνοχώρο (Σύμβαση της Βουδαπέστης) είναι μια δεσμευτική διεθνής νομική πράξη η οποία αφορά τα εγκλήματα που διαπράττονται κατά ή μέσω ηλεκτρονικών δικτύων. Αφορά επίσης τη διερεύνηση εγκλημάτων τα οποία δεν διαπράττονται στον κυβερνοχώρο, αλλά περιλαμβάνουν ηλεκτρονικά αποδεικτικά στοιχεία.

Σημαντική διάκριση μεταξύ του δικαίου του Συμβουλίου της Ευρώπης και του δικαίου της ΕΕ αποτελεί το γεγονός ότι, σε αντίθεση με το δίκαιο της ΕΕ, το **δίκαιο του Συμβουλίου της Ευρώπης** εφαρμόζεται και στον τομέα της εθνικής ασφάλειας. Αυτό σημαίνει ότι τα συμβαλλόμενα μέρη πρέπει να παραμένουν εντός του πεδίου εφαρμογής του άρθρου 8 της ΕΣΔΑ, ακόμη και όταν πρόκειται για δραστηριότητες σχετικές με την εθνική ασφάλεια. Αρκετές από τις αποφάσεις

του ΕΔΔΑ αφορούν κρατικές δραστηριότητες στους ευαίσθητους τομείς της νομοθεσίας και της πρακτικής σε θέματα εθνικής ασφάλειας ⁷²⁶.

Όσον αφορά τον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης σε ευρωπαϊκό επίπεδο, η Εκσυγχρονισμένη Σύμβαση 108 καλύπτει όλα τα πεδία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, οι δε διατάξεις της έχουν ως στόχο τη ρύθμιση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα εν γένει. Κατά συνέπεια, η Εκσυγχρονισμένη Σύμβαση 108 έχει εφαρμογή στην προστασία των δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης. Η επεξεργασία γενετικών δεδομένων, δεδομένων προσωπικού χαρακτήρα που αφορούν αδικήματα, ποινικές διαδικασίες και καταδικαστικές αποφάσεις, αλλά και κάθε σχετικό μέτρο ασφαλείας, βιομετρικών δεδομένων που ταυτοποιούν πλήρως κάποιο πρόσωπο, καθώς και τυχόν ευαίσθητων δεδομένων προσωπικού χαρακτήρα, επιτρέπεται μόνον εάν υπάρχουν κατάλληλες εγγυήσεις έναντι των κινδύνων που μπορεί να ενέχει η επεξεργασία των εν λόγω δεδομένων για τα συμφέροντα, τα δικαιώματα και τις θεμελιώδεις ελευθερίες του υποκειμένου των δεδομένων, κυρίως δε έναντι του κινδύνου εισαγωγής διακρίσεων ⁷²⁷.

Για την εκπλήρωση των νομίμων καθηκόντων τους, οι αστυνομικές και δικαστικές αρχές καλούνται συχνά να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, γεγονός που μπορεί να έχει σοβαρές συνέπειες για τον ενδιαφερόμενο. Η σύσταση για τη χρήση προσωπικών δεδομένων στον αστυνομικό τομέα, η οποία εκδόθηκε από το Συμβούλιο της Ευρώπης το 1987, παρέχει στα κράτη μέλη του κατευθυντήριες οδηγίες σχετικά με τους τρόπους εφαρμογής των αρχών της Σύμβασης 108 στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τις αστυνομικές αρχές ⁷²⁸. Η σύσταση συμπληρώθηκε από έναν Πρακτικό Οδηγό για τη χρήση των προσωπικών δεδομένων στον αστυνομικό τομέα, ο οποίος υιοθετήθηκε από τη Συμβουλευτική Επιτροπή της Σύμβασης 108 ⁷²⁹.

726 Βλ., για παράδειγμα, ΕΔΔΑ, *Klass κ.λπ. κατά Γερμανίας*, προσφυγή αριθ. 5029/71, 6 Σεπτεμβρίου 1978· ΕΔΔΑ, *Rotaru κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000 και ΕΔΔΑ, *Szabó και Vissy κατά Ουγγαρίας*, προσφυγή αριθ. 37138/14, 12 Ιανουαρίου 2016.

727 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 6.

728 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1987), Σύσταση Rec (87)15 προς τα κράτη μέλη σχετικά με τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα, 17 Σεπτεμβρίου 1987.

729 Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή για τη Σύμβαση 108, Πρακτικός Οδηγός για τη χρήση των προσωπικών δεδομένων στον αστυνομικό τομέα., T-PD(2018)1.

Παράδειγμα: Στην υπόθεση *D.L. κατά Βουλγαρίας*⁷³⁰, οι κοινωνικές υπηρεσίες τοποθέτησαν την προσφεύγουσα σε κλειστό εκπαιδευτικό ίδρυμα βάσει δικαστικής απόφασης. Κάθε γραπτή αλληλογραφία και τηλεφωνική συνομιλία είχε τεθεί υπό γενικευμένη και αδιάκριτη παρακολούθηση από το ίδρυμα. Το ΕΔΔΑ αποφάνθηκε ότι παραβιάστηκε το άρθρο 8, δεδομένου ότι το επίμαχο μέτρο δεν ήταν απαραίτητο σε μια δημοκρατική κοινωνία. Το ΕΔΔΑ δήλωσε ότι έπρεπε να καταβάλλεται κάθε δυνατή προσπάθεια ώστε να παρέχεται στους ανηλίκους που είναι έγκλειστοι σε ιδρύματα η δυνατότητα επαρκούς επικοινωνίας με τον έξω κόσμο, δεδομένου ότι η επικοινωνία αυτή αποτελεί αναπόσπαστο μέρος του δικαιώματός τους σε αξιοπρεπή μεταχείριση και είναι απολύτως αναγκαία για την προετοιμασία της επανένταξής τους στην κοινωνία. Αυτό ισχύει εξίσου για τις επισκέψεις και για τη γραπτή αλληλογραφία ή τις τηλεφωνικές συνομιλίες. Επιπλέον, στο πλαίσιο της παρακολούθησης δεν γινόταν διάκριση μεταξύ της επικοινωνίας των ανηλίκων με τις οικογένειές τους και της επικοινωνίας τους με τις ΜΚΟ που εκπροσωπούσαν τα δικαιώματα του παιδιού ή με τους δικηγόρους. Πέραν αυτού, η απόφαση σχετικά με την υποκλοπή της επικοινωνίας δεν είχε ληφθεί κατόπιν εξατομικευμένης ανάλυσης των κινδύνων σε κάθε περίπτωση χωριστά.

Παράδειγμα: Στην υπόθεση *Dragojević κατά Κροατίας*⁷³¹, ο προσφεύγων ήταν ύποπτος για συμμετοχή σε δραστηριότητες διακίνησης ναρκωτικών. Κρίθηκε ένοχος μετά τη λήψη μέτρων κρυφής παρακολούθησης, κατόπιν σχετικής άδειας από ανακριτή, με σκοπό την υποκλοπή των τηλεφωνικών συνδιαλέξεων του προσφεύγοντος. Το ΕΔΔΑ αποφάνθηκε ότι το μέτρο, κατά του οποίου ασκήθηκε προσφυγή, συνιστούσε επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής και της αλληλογραφίας. Η άδεια που εξέδωσε ο ανακριτής βασιζόταν αποκλειστικά και μόνο στη δήλωση της εισαγγελικής αρχής ότι «η έρευνα δεν μπορούσε να διεξαχθεί με άλλα μέσα». Επίσης, το ΕΔΔΑ επισήμανε ότι τα ποινικά δικαστήρια είχαν περιορίσει την εξέταση της προσφυγής στη χρήση των μέτρων παρακολούθησης και έκρινε ότι η κυβέρνηση δεν είχε θέσει σε εφαρμογή τα ένδικα μέσα που ήταν διαθέσιμα. Συνεπώς, παραβιάστηκε το άρθρο 8.

⁷³⁰ ΕΔΔΑ, *D.L. κατά Βουλγαρίας*, προσφυγή αριθ. 7472/14, 19 Μαΐου 2016.

⁷³¹ ΕΔΔΑ, *Dragojević κατά Κροατίας*, προσφυγή αριθ. 68955/11, 15 Ιανουαρίου 2015.

8.1.1. Η σύσταση στον αστυνομικό τομέα

Κατά πάγια νομολογία του ΕΔΔΑ, η αποθήκευση και η διατήρηση δεδομένων προσωπικού χαρακτήρα από αστυνομικές αρχές ή αρχές εθνικής ασφάλειας συνιστά επέμβαση στα δικαιώματα του άρθρου 8 παράγραφος 1 της ΕΣΔΑ. Πολλές αποφάσεις του ΕΔΔΑ άπτονται της αιτιολόγησης της συγκεκριμένης επέμβασης⁷³².

Παράδειγμα: Στην υπόθεση *B.B. κατά Γαλλίας*⁷³³, ο προσφεύγων καταδικάστηκε για τη διάπραξη σεξουαλικών αδικημάτων εις βάρος ανηλίκων 15 ετών ως πρόσωπο ευρισκόμενο σε θέση εμπιστοσύνης. Εξέτισε την ποινή φυλάκισης που του επιβλήθηκε το 2000. Το επόμενο έτος υπέβαλε αίτημα για τη διαγραφή της εν λόγω καταδικαστικής απόφασης από το ποινικό του μητρώο, αλλά το αίτημά του απορρίφθηκε. Το 2004 θεσπίστηκε γαλλικός νόμος για τη δημιουργία εθνικής δικαστικής βάσης δεδομένων με δράστες σεξουαλικών αδικημάτων και ο προσφεύγων ενημερώθηκε για την καταχώριση των στοιχείων του σε αυτή. Το ΕΔΔΑ αποφάνθηκε ότι η καταχώριση των στοιχείων καταδικασθέντων δραστών σεξουαλικών αδικημάτων σε εθνική δικαστική βάση δεδομένων εμπίπτει στο πεδίο εφαρμογής του άρθρου 8 της ΕΣΔΑ. Ωστόσο, δεδομένου ότι παρέχονταν επαρκείς εγγυήσεις για την προστασία των δεδομένων, όπως το δικαίωμα του υποκειμένου των δεδομένων να ζητήσει τη διαγραφή των δεδομένων, η περιορισμένη χρονική διάρκεια διατήρησης των δεδομένων και η περιορισμένη πρόσβαση στα εν λόγω δεδομένα, είχε επιτευχθεί ορθή στάθμιση των αντιτιθέμενων ιδιωτικών και δημοσίων συμφερόντων που διακυβεύονταν. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι δεν παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Παράδειγμα: Στην υπόθεση *S. και Marger κατά Ηνωμένου Βασιλείου*⁷³⁴, και οι δύο προσφεύγοντες είχαν κατηγορηθεί, αλλά δεν είχαν καταδικαστεί, για ποινικά αδικήματα. Ωστόσο, οι αστυνομικές αρχές διατήρησαν και αποθήκευσαν τα δακτυλικά τους αποτυπώματα, το

⁷³² Βλ., για παράδειγμα, ΕΔΔΑ, *Leander κατά Σουηδίας*, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987· ΕΔΔΑ, *M.M. κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 24029/07, 13 Νοεμβρίου 2012· ΕΔΔΑ, *M.K. κατά Γαλλίας*, προσφυγή αριθ. 19522/09, 18 Απριλίου 2013, ή ΕΔΔΑ, *Aycaguer κατά Γαλλίας*, προσφυγή αριθ. 8806/12, 22 Ιουνίου 2017.

⁷³³ ΕΔΔΑ, *B.B. κατά Γαλλίας*, προσφυγή αριθ. 5335/06, 17 Δεκεμβρίου 2009.

⁷³⁴ ΕΔΔΑ, *S. και Marger κατά Ηνωμένου Βασιλείου* [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008, σκέψεις 119 και 125.

βιολογικό υλικό και το προφίλ του DNA τους. Η επ' αόριστον διατήρηση των προαναφερόμενων βιομετρικών δεδομένων υπόπτων για την τέλεση ποινικών αδικημάτων επιτρεπόταν από τον νόμο, ακόμη και αν οι ύποπτοι αθωνώνονταν ή απαλλάσσονταν στη συνέχεια από τις σχετικές κατηγορίες. Το ΕΔΔΑ αποφάνθηκε ότι η γενικευμένη και αδιάκριτη διατήρηση δεδομένων προσωπικού χαρακτήρα, χωρίς χρονικά όρια και με περιορισμένη δυνατότητα άσκησης του δικαιώματος διαγραφής τους από τους αθωωθέντες, συνιστούσε δυσανάλογη επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής των προσφευγόντων. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Καίριο ζήτημα στο πλαίσιο των ηλεκτρονικών επικοινωνιών αποτελεί η επέμβαση των κρατικών αρχών στα δικαιώματα της προστασίας της ιδιωτικής ζωής και της προστασίας των δεδομένων. Η χρήση μέσων παρακολούθησης ή υποκλοπής των επικοινωνιών, όπως οι συσκευές ακρόασης ή υποκλοπής, επιτρέπεται μόνον εάν προβλέπονται σχετικές νομοθετικές διατάξεις και εφόσον συνιστά απαραίτητο μέτρο σε μια δημοκρατική κοινωνία για την εξυπηρέτηση των ακόλουθων σκοπών:

- προστασία της εθνικής ασφάλειας
- δημόσια ασφάλεια
- οικονομικά συμφέροντα του κράτους
- πάταξη ποινικών αδικημάτων· ή
- προστασία του υποκειμένου των δεδομένων ή των δικαιωμάτων και των ελευθεριών τρίτων.

Πολλές περαιτέρω αποφάσεις του ΕΔΔΑ αφορούν την αιτιολόγηση της επέμβασης στο δικαίωμα προστασίας της ιδιωτικής ζωής μέσω μέτρων παρακολούθησης.

Παράδειγμα: Στην υπόθεση *Allan κατά Ηνωμένου Βασιλείου*⁷³⁵, οι αρχές ηχογράφησαν κρυφά ιδιωτικές συνομιλίες ενός κρατουμένου με φίλο του στον χώρο του επισκεπτηρίου της φυλακής, καθώς και με συγκατηγορούμενό του σε κελί της φυλακής. Το ΕΔΔΑ αποφάνθηκε ότι η χρήση συσκευών καταγραφής ήχου και εικόνας στο κελί του προσφεύγοντος, στον χώρο επισκεπτηρίου της φυλακής και στο κελί συγκαταφυγμένου συνιστούσε επέμβαση στο δικαίωμα του προσφεύγοντος στην προστασία της ιδιωτικής ζωής. Δεδομένου ότι εκείνη τη χρονική στιγμή δεν υπήρχε νομοθεσία η οποία να διέπει τη χρήση κρυφών συσκευών καταγραφής από τις αστυνομικές αρχές, η εν λόγω επέμβαση δεν ήταν σύμφωνη με τον νόμο. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Παράδειγμα: Στην υπόθεση *Roman Zakharov κατά Ρωσίας*⁷³⁶, ο προσφεύγων κίνησε δικαστική διαδικασία εναντίον τριών παρόχων κινητής τηλεφωνίας. Ισχυρίστηκε ότι είχε παραβιαστεί το δικαίωμά του στην τήρηση του απορρήτου των τηλεφωνικών του συνδιαλέξεων, διότι οι πάροχοι είχαν εγκαταστήσει εξοπλισμό ο οποίος επέτρεπε στην Ομοσπονδιακή Υπηρεσία Ασφαλείας να υποκλέπτει τις τηλεφωνικές του συνδιαλέξεις χωρίς προηγούμενη δικαστική άδεια. Το ΕΔΔΑ έκρινε ότι οι εθνικές νομοθετικές διατάξεις που διέπουν την υποκλοπή των επικοινωνιών δεν παρείχαν επαρκείς και αποτελεσματικές εγγυήσεις έναντι της αυθαιρεσίας και του κινδύνου κατάχρησης. Ειδικότερα, η εθνική νομοθεσία δεν επέβαλλε τη διαγραφή των αποθηκευμένων δεδομένων μετά την εκπλήρωση του σκοπού της αποθήκευσης. Επιπλέον, παρότι ήταν απαραίτητη η έκδοση σχετικής δικαστικής άδειας, ο δικαστικός έλεγχος ήταν περιορισμένος.

Παράδειγμα: Στην υπόθεση *Szabó και Vissy κατά Ουγγαρίας*⁷³⁷, οι προσφεύγοντες ισχυρίστηκαν ότι η νομοθεσία της Ουγγαρίας συνιστούσε παράβαση του άρθρου 8 της ΕΣΔΑ, διότι δεν ήταν επαρκώς λεπτομερής ή ακριβής. Επιπλέον, ισχυρίστηκαν ότι η νομοθεσία δεν παρείχε επαρκείς εγγυήσεις έναντι της κατάχρησης και της αυθαιρεσίας. Το ΕΔΔΑ έκρινε ότι η νομοθεσία της Ουγγαρίας δεν επέβαλλε την υποχρέωση

735 ΕΔΔΑ, *Allan κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 48539/99, 5 Νοεμβρίου 2002.

736 ΕΔΔΑ, *Roman Zakharov κατά Ρωσίας* [Τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 47143/06, 4 Δεκεμβρίου 2015.

737 ΕΔΔΑ, *Szabó και Vissy κατά Ουγγαρίας*, προσφυγή αριθ. 37138/14, 12 Ιανουαρίου 2016.

έκδοσης δικαστικής άδειας για σκοπούς παρακολούθησης. Επισήμανε, ωστόσο, ότι, παρά το γεγονός ότι η εν λόγω παρακολούθηση υπόκειται στη χορήγηση άδειας από τον υπουργό Δικαιοσύνης, ήταν κατεξοχήν πολιτικού χαρακτήρα και δεν μπορούσε να διασφαλίσει την απαιτούμενη αξιολόγηση του κριτηρίου της «απόλυτης αναγκαιότητας». Επιπλέον, η εθνική νομοθεσία δεν προέβλεπε την άσκηση δικαστικού ελέγχου, δεδομένου ότι δεν επρόκειτο να αποσταλεί καμία γνωστοποίηση στα υποκείμενα των δεδομένων. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι είχε σημειωθεί παράβαση του άρθρου 8 της ΕΣΔΑ.

Λαμβανομένου υπόψη ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αστυνομικές αρχές ενδέχεται να έχει σημαντικό αντίκτυπο στον ενδιφερόμενο, είναι απολύτως αναγκαίο να προβλέπονται λεπτομερείς κανόνες για την προστασία των δεδομένων όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον εν λόγω τομέα. Με τη σύστασή του για τον αστυνομικό τομέα, το Συμβούλιο της Ευρώπης επιδίωξε να επιλύσει το θέμα αυτό παρέχοντας κατευθυντήριες γραμμές σχετικά με τα εξής: τους τρόπους με τους οποίους θα πρέπει να συλλέγονται τα δεδομένα προσωπικού χαρακτήρα από τις αστυνομικές αρχές και να τηρούνται τα αρχεία δεδομένων· τα πρόσωπα τα οποία μπορούν να έχουν πρόσβαση στα εν λόγω αρχεία, συμπεριλαμβανομένων των προϋποθέσεων για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε αλλοδαπές αστυνομικές αρχές· τους τρόπους με τους οποίους τα υποκείμενα των δεδομένων θα πρέπει να είναι σε θέση να ασκούν τα δικαιώματά τους· και τους τρόπους με τους οποίους θα πρέπει να ασκείται ο έλεγχος από τις ανεξάρτητες αρχές. Εξετάστηκε επίσης η υποχρέωση παροχής ικανοποιητικού επιπέδου ασφάλειας των δεδομένων.

Η σύσταση δεν προβλέπει την άνευ ορίων, αδιάκριτη συλλογή δεδομένων προσωπικού χαρακτήρα από τις αστυνομικές αρχές. Περιορίζει τη συλλογή των δεδομένων προσωπικού χαρακτήρα από τις αστυνομικές αρχές στον βαθμό που είναι αναγκαία για την πρόληψη υπαρκτού κινδύνου ή για τη δίωξη συγκεκριμένης αξιόποινης πράξης. Κάθε πρόσθετη συλλογή δεδομένων θα πρέπει να βασίζεται σε συγκεκριμένη εθνική νομοθεσία. Η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα θα πρέπει να περιορίζεται στα απολύτως αναγκαία στο πλαίσιο συγκεκριμένης έρευνας.

Όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται εν αγνοία του υποκειμένου των δεδομένων, το υποκείμενο των δεδομένων πρέπει να

ενημερώνεται για τη συλλογή των δεδομένων που το αφορούν από τη στιγμή που η ανακοίνωση αυτή παύει πλέον να επηρεάζει την έρευνα. Η συλλογή δεδομένων προσωπικού χαρακτήρα μέσω παρακολούθησης με τεχνικά ή άλλα αυτοματοποιημένα μέσα πρέπει να στηρίζεται σε ειδική νομική βάση.

Παράδειγμα: Στην υπόθεση *Versini-Campinchi και Crasnianski κατά Γαλλίας*⁷³⁸, η προσφεύγουσα, δικηγόρος στο επάγγελμα, είχε μια τηλεφωνική συνομιλία με πελάτη του οποίου η τηλεφωνική γραμμή τελούσε υπό παρακολούθηση κατόπιν αιτήματος ανακριτή. Από την απομαγνητοφώνηση της συνομιλίας αποδείχθηκε ότι είχε αποκαλύψει πληροφορίες που καλύπτονταν από το δικηγορικό απόρρητο. Ο εισαγγελέας διαβίβασε τις εν λόγω πληροφορίες στον Δικηγορικό Σύλλογο, ο οποίος επέβαλε ποινή στην προσφεύγουσα. Το ΕΔΔΑ αναγνώρισε την ύπαρξη επέμβασης στο δικαίωμα σεβασμού της ιδιωτικής ζωής και της αλληλογραφίας, όχι μόνο του προσώπου του οποίου το τηλέφωνο τελούσε υπό παρακολούθηση, αλλά και της προσφεύγουσας της οποίας οι επικοινωνίες είχαν τεθεί υπό παρακολούθηση και απομαγνητοφώνηση. Η επέμβαση αυτή ήταν σύμφωνη με τον νόμο και επιδίωκε τον νόμιμο σκοπό της πρόληψης της διασάλευσης της τάξης. Η προσφεύγουσα είχε επιτύχει τον δικαστικό έλεγχο της νομιμότητας της υποβολής των υποκλαπέντων αρχείων από τις τηλεφωνικές συνδιαλέξεις που είχαν μαγνητοφωνηθεί στο πλαίσιο της πειθαρχικής διαδικασίας που κινήθηκε εις βάρος της. Μολονότι δεν είχε τη δυνατότητα να αιτηθεί την ακύρωση της απομαγνητοφώνησης της τηλεφωνικής συνδιάλεξης, το ΕΔΔΑ εκτίμησε ότι είχε διεξαχθεί αποτελεσματικός έλεγχος, ικανός να περιορίσει την καταγγελλθείσα επέμβαση στον βαθμό που κρίνεται αναγκαία σε μια δημοκρατική κοινωνία. Το ΕΔΔΑ αποφάνθηκε ότι το επιχείρημα, σύμφωνα με το οποίο η δυνατότητα άσκησης ποινικής δίωξης κατά δικηγόρου βάσει της απομαγνητοφώνησης θα μπορούσε να έχει αποτρεπτικό αποτέλεσμα στην ελευθερία της επικοινωνίας μεταξύ δικηγόρου και πελάτη και, κατ' επέκταση, στην άσκηση των δικαιωμάτων υπεράσπισης του πελάτη, δεν ήταν αξιόπιστο εάν η κοινοποίηση στην οποία προέβη η ίδια η δικηγόρος μπορούσε να εκληφθεί ως παράνομη συμπεριφορά εκ μέρους της. Συνεπώς, δεν διαπιστώθηκε παραβίαση του άρθρου 8.

⁷³⁸ ΕΔΔΑ, *Versini-Campinchi και Crasnianski κατά Γαλλίας*, προσφυγή αριθ. 49176/11, 16 Ιουνίου 2016.

Η σύσταση του Συμβουλίου της Ευρώπης για τον αστυνομικό τομέα προβλέπει ότι κατά την αποθήκευση δεδομένων προσωπικού χαρακτήρα θα πρέπει να γίνεται σαφής διάκριση: μεταξύ των διοικητικών δεδομένων και των αστυνομικών δεδομένων· μεταξύ των δεδομένων προσωπικού χαρακτήρα διαφόρων κατηγοριών υποκειμένων των δεδομένων, π.χ. υπόπτων, καταδίκων, θυμάτων και μαρτύρων· και, τέλος, μεταξύ των δεδομένων που θεωρούνται αδιάσειστα αποδεικτικά στοιχεία και των δεδομένων που βασίζονται σε υπόνοιες ή εικασίες.

Ο σκοπός για τον οποίο μπορούν να χρησιμοποιούνται τα αστυνομικά δεδομένα πρέπει να είναι αυστηρά περιορισμένος. Ο περιορισμός αυτός έχει επιπτώσεις όσον αφορά την κοινοποίηση αστυνομικών δεδομένων σε τρίτους: κριτήριο για τη διαβίβαση ή κοινοποίηση των εν λόγω δεδομένων στον αστυνομικό τομέα θα πρέπει να αποτελεί η διαπίστωση της ύπαρξης ή μη έννομου συμφέροντος για την κοινοποίησή τους. Η διαβίβαση ή κοινοποίηση των εν λόγω δεδομένων εκτός του αστυνομικού τομέα θα πρέπει να επιτρέπεται μόνον όταν υφίσταται σαφής εκ του νόμου υποχρέωση ή εξουσιοδότηση.

Παράδειγμα: Στην υπόθεση *Karabeyoğlu κατά Τουρκίας*⁷³⁹, οι τηλεφωνικές γραμμές του προσφεύγοντος, δικαστή στο επάγγελμα, παρακολουθούνταν στο πλαίσιο ποινικής έρευνας σε υπόθεση παράνομης οργάνωσης, στην οποία είτε υπήρχαν υπόνοιες ότι συμμετείχε και ο ίδιος είτε εικάζόταν ότι παρείχε βοήθεια και στήριξη. Κατόπιν της απόφασης να μην ασκηθεί δίωξη, ο αρμόδιος εισαγγελέας για τη διεξαγωγή της ποινικής έρευνας κατέστρεψε τις επίμαχες ηχογραφήσεις. Ωστόσο, είχε παραμείνει ένα αντίγραφο στην κατοχή των ανακριτών, οι οποίοι χρησιμοποίησαν στη συνέχεια το σχετικό υλικό στο πλαίσιο πειθαρχικής έρευνας που κινήθηκε εις βάρος του προσφεύγοντος. Το ΕΔΔΑ αποφάνθηκε ότι υπήρξε παράβαση της σχετικής νομοθεσίας διότι οι πληροφορίες είχαν χρησιμοποιηθεί για διαφορετικούς σκοπούς από εκείνους για τους οποίους είχαν συγκεντρωθεί και δεν είχαν καταστραφεί εντός της εκ του νόμου προβλεπόμενης προθεσμίας. Η επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής του προσφεύγοντος δεν ήταν σύμφωνη με τον νόμο, τουλάχιστον όσον αφορά τις πειθαρχικές διαδικασίες που κινήθηκαν εις βάρος του.

Η διεθνής διαβίβαση ή κοινοποίηση θα πρέπει να περιορίζεται στις αλλοδαπές αστυνομικές αρχές και να βασίζεται σε ειδικές νομικές διατάξεις, ενδεχομένως

⁷³⁹ ΕΔΔΑ, *Karabeyoğlu κατά Τουρκίας*, προσφυγή αριθ. 30083/10, 7 Ιουνίου 2016.

διεθνείς συμφωνίες, εκτός εάν κρίνεται αναγκαία για την αποτροπή σοβαρού και επικείμενου κινδύνου.

Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τις αστυνομικές αρχές πρέπει να υπόκειται σε ανεξάρτητη εποπτεία, ούτως ώστε να διασφαλίζεται η συμμόρφωση προς το εθνικό δίκαιο σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Το υποκείμενο των δεδομένων πρέπει να χαίρει όλων των δικαιωμάτων πρόσβασης που προβλέπονται στην Εκσυγχρονισμένη Σύμβαση 108. Όταν το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων περιορίζεται, σύμφωνα με το άρθρο 9 της Σύμβασης 108, προς όφελος της αποτελεσματικής αστυνομικής έρευνας και εκτέλεσης ποινικών κυρώσεων, το εθνικό δίκαιο πρέπει να παρέχει στο υποκείμενο των δεδομένων το δικαίωμα προσφυγής ενώπιον της εθνικής αρχής προστασίας των δεδομένων ή άλλου ανεξάρτητου φορέα.

8.1.2. Η Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο

Δεδομένου ότι τα ηλεκτρονικά συστήματα επεξεργασίας δεδομένων προσωπικού χαρακτήρα αποτελούν ολοένα και περισσότερο είτε στόχο είτε εργαλείο εγκληματικών δραστηριοτήτων, απαιτούνται νέες διατάξεις του ποινικού δικαίου για την αντιμετώπιση της συγκεκριμένης πρόκλησης. Για τον λόγο αυτό, το Συμβούλιο της Ευρώπης εξέδωσε διεθνή νομική πράξη, τη Σύμβαση για το έγκλημα στον Κυβερνοχώρο, γνωστή και ως Σύμβαση της Βουδαπέστης, προκειμένου να αντιμετωπιστεί το ζήτημα των εγκληματικών πράξεων που διαπράττονται κατά και μέσω των ηλεκτρονικών δικτύων⁷⁴⁰. Δικαίωμα προσχώρησης στην εν λόγω Σύμβαση έχουν και κράτη τα οποία δεν είναι μέλη του Συμβουλίου της Ευρώπης. Στις αρχές του 2018 14 κράτη εκτός Συμβουλίου της Ευρώπης⁷⁴¹ συμμετείχαν στη Σύμβαση, ενώ 7 ακόμη μη μέλη του Συμβουλίου της Ευρώπης είχαν προσκληθεί να προσχωρήσουν σε αυτή.

Η Σύμβαση για το έγκλημα στον Κυβερνοχώρο εξακολουθεί να αποτελεί τη σημαντικότερη διεθνή συνθήκη που άπτεται των παραβιάσεων της νομοθεσίας

⁷⁴⁰ Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2001), Σύμβαση για το έγκλημα στον κυβερνοχώρο, CETS αριθ. 185, Βουδαπέστη, 23 Νοεμβρίου 2001, τέθηκε σε ισχύ την 1η Ιουλίου 2004.

⁷⁴¹ Αυστραλία, Καναδάς, Χιλή, Κολομβία, Δομινικανή Δημοκρατία, Ισραήλ, Ιαπωνία, Μαυρίκιος, Παναμάς, Σενεγάλη, Σρι Λάνκα, Τόνγκα, Τυνησία και Ηνωμένες Πολιτείες Αμερικής. Βλ. Διάγραμμα υπογραφών και κυρώσεων της Σύμβασης 185, ως είχε την 1η Ιουλίου 2017.

μέσω του διαδικτύου ή άλλων δικτύων πληροφοριών. Επιβάλλει στα συμβαλλόμενα μέρη την υποχρέωση να επικαιροποιούν και να εναρμονίζουν την ποινική νομοθεσία τους για την καταπολέμηση του hacking και άλλων παραβιάσεων ασφαλείας, μεταξύ των οποίων και οι παραβιάσεις των πνευματικών δικαιωμάτων, η απάτη με χρήση ηλεκτρονικών υπολογιστών, η παιδική πορνογραφία και άλλες παράνομες δραστηριότητες στον κυβερνοχώρο. Η Σύμβαση προβλέπει επίσης δικονομικές αρμοδιότητες οι οποίες καλύπτουν την έρευνα δικτύων ηλεκτρονικών υπολογιστών και την υποκλοπή επικοινωνιών στο πλαίσιο της καταπολέμησης του εγκλήματος στον κυβερνοχώρο. Τέλος, παρέχει τη δυνατότητα αποτελεσματικής διεθνούς συνεργασίας. Το πρόσθετο πρωτόκολλο στη Σύμβαση αφορά την ποινικοποίηση της ρατσιστικής και ξενοφοβικής προπαγάνδας μέσω των δικτύων ηλεκτρονικών υπολογιστών.

Παρότι η Σύμβαση δεν αποσκοπεί ουσιαστικά στην προώθηση της προστασίας των δεδομένων προσωπικού χαρακτήρα, ποινικοποιεί δραστηριότητες οι οποίες είναι πιθανό να παραβιάζουν το δικαίωμα του υποκειμένου των δεδομένων στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν. Περαιτέρω, επιβάλλει στα συμβαλλόμενα μέρη την υποχρέωση να θεσπίσουν νομοθετικά μέτρα τα οποία θα επιτρέπουν στις οικείες εθνικές αρχές να υποκλέπτουν δεδομένα κίνησης και περιεχομένου ⁷⁴². Επιτάσσει επίσης στα συμβαλλόμενα μέρη να προβλέπουν, κατά την εφαρμογή της Σύμβασης, επαρκές επίπεδο προστασίας των δικαιωμάτων και των ελευθεριών του ανθρώπου, περιλαμβανομένων των δικαιωμάτων που κατοχυρώνονται με την ΕΣΔΑ, όπως το δικαίωμα προστασίας των προσωπικών δεδομένων ⁷⁴³. Τα συμβαλλόμενα μέρη δεν είναι υποχρεωμένα να προσχωρήσουν στη Σύμβαση 108 προκειμένου να είναι σε θέση να προσχωρήσουν στη Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο.

742 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2001), Σύμβαση για το έγκλημα στον κυβερνοχώρο, CETS αριθ. 185, Βουδαπέστη, 23 Νοεμβρίου 2001, άρθρα 20 και 21.

743 Ό.π., άρθρο 15 παράγραφος 1.

8.2. Το δίκαιο της ΕΕ για την προστασία των δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης

Κύρια σημεία

- Εντός της ΕΕ, η προστασία των δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης ρυθμίζεται στο πλαίσιο τόσο της εθνικής όσο και της διασυννοριακής επεξεργασίας τους από τις αστυνομικές και δικαστικές αρχές των κρατών μελών και των φορέων της ΕΕ.
- Σε επίπεδο κρατών μελών, η οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης πρέπει να ενσωματωθεί στο εθνικό δίκαιο.
- Η προστασία των δεδομένων στο πλαίσιο της διασυννοριακής συνεργασίας μεταξύ των αστυνομικών αρχών και των αρχών επιβολής του νόμου διέπεται από ειδικές νομοθετικές πράξεις, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυννοριακού εγκλήματος.
- Προβλέπονται ειδικοί κανόνες προστασίας των δεδομένων για την Ευρωπαϊκή Αστυνομική Υπηρεσία (Ευρωπόλ), την Ευρωπαϊκή Μονάδα Δικαστικής Συνεργασίας (Eurojust) και τη νεοσυσταθείσα Ευρωπαϊκή Εισαγγελία, δηλαδή για τους οργανισμούς της ΕΕ οι οποίοι επικουρούν και προάγουν τη διασυννοριακή επιβολή του νόμου.
- Ειδικοί κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα υπάρχουν επίσης για τα κοινά συστήματα πληροφοριών, τα οποία έχουν αναπτυχθεί σε επίπεδο ΕΕ για τη διασυννοριακή ανταλλαγή πληροφοριών μεταξύ των αρμόδιων αστυνομικών και δικαστικών αρχών. Σημαντικά παραδείγματα αποτελούν το Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II), το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) και το Eurodac, ένα κεντρικό σύστημα το οποίο περιέχει δεδομένα δακτυλικών αποτυπωμάτων των υπηκόων τρίτων χωρών και των απάτριδων που υποβάλλουν αίτηση ασύλου σε κράτος μέλος της ΕΕ.
- Η ΕΕ βρίσκεται στη διαδικασία επικαιροποίησης των προαναφερόμενων διατάξεων για την προστασία των δεδομένων, ώστε να συνάδουν με τις διατάξεις της οδηγίας για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης.

8.2.1. Η οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης

Η οδηγία 2016/680 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (η οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης)⁷⁴⁴ έχει ως στόχο την προστασία των δεδομένων προσωπικού χαρακτήρα που συλλέγονται και υπόκεινται σε επεξεργασία για σκοπούς που αφορούν την ποινική δικαιοσύνη και περιλαμβάνουν μεταξύ άλλων:

- την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, καθώς και την προστασία από απειλές κατά της δημόσιας ασφάλειας και την αποτροπή τους
- την εκτέλεση ποινικής κύρωσης και
- περιπτώσεις όπου η αστυνομία ή άλλες αρχές επιβολής του νόμου ενεργούν για την τήρηση του νόμου και για την αποτροπή ή για την προστασία από απειλές κατά της δημόσιας ασφάλειας και κατά θεμελιωδών δικαιωμάτων της κοινωνίας οι οποίες ενδέχεται να συνιστούν ποινικό αδίκημα.

Η οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης προστατεύει τα δεδομένα προσωπικού χαρακτήρα διαφόρων κατηγοριών ατόμων που εμπλέκονται σε ποινικές διαδικασίες, π.χ. μάρτυρες, πληροφοριοδότες, θύματα, ύποπτοι και συνεργοί. Οι αστυνομικές και οι δικαστικές αρχές υποχρεούνται να συμμορφώνονται με τις διατάξεις της οδηγίας κάθε φορά που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα αυτού

⁷⁴⁴ Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (ΕΕ L 119 της 4.5.2016, σ. 89) (οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης).

του είδους για τους σκοπούς της επιβολής του νόμου, τόσο στο προσωπικό όσο και στο καθ' ύλην πεδίο εφαρμογής της οδηγίας⁷⁴⁵.

Ωστόσο, η χρήση δεδομένων επιτρέπεται και για διαφορετικό σκοπό, αλλά υπό ορισμένες προϋποθέσεις. Η επεξεργασία δεδομένων για διαφορετικούς σκοπούς επιβολής του νόμου από τον σκοπό για τον οποίο έχουν συλλεχθεί επιτρέπεται μόνον εάν αυτό είναι νόμιμο, αναγκαίο και αναλογικό σύμφωνα με το δίκαιο κράτους μέλους ή το δίκαιο της ΕΕ⁷⁴⁶. Για άλλους σκοπούς, εφαρμόζονται οι κανόνες του Γενικού Κανονισμού για την Προστασία Δεδομένων. Η καταχώριση και τεκμηρίωση την κοινοχρησίας των δεδομένων συγκαταλέγεται στα ειδικά καθήκοντα των αρμόδιων αρχών για τη διευκόλυνση της απόδοσης των ευθυνών σε περίπτωση καταγγελίας.

Οι αρμόδιες αρχές που εργάζονται στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης είναι δημόσιες αρχές ή αρχές στις οποίες εκχωρούνται – δυνάμει του εθνικού δικαίου και από δημόσιες εξουσίες – αρμοδιότητες άσκησης των καθηκόντων δημόσιας αρχής⁷⁴⁷, π.χ. φυλακές υπό ιδιωτική διαχείριση⁷⁴⁸. Η ισχύς της οδηγίας εκτείνεται τόσο στην επεξεργασία δεδομένων σε εθνικό επίπεδο όσο και στη διασυνοριακή επεξεργασία μεταξύ των αστυνομικών και δικαστικών αρχών των κρατών μελών, καθώς και στη διεθνή διαβίβαση δεδομένων από τις αρμόδιες αρχές προς τρίτες χώρες και διεθνείς οργανισμούς⁷⁴⁹. Η οδηγία δεν καλύπτει την εθνική ασφάλεια ή την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ⁷⁵⁰.

Η οδηγία βασίζεται, σε μεγάλο βαθμό, στις αρχές και τους ορισμούς που περιέχονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων ενώ λαμβάνει

745 Οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, άρθρο 2 παράγραφος 1.

746 Ό.π., άρθρο 4 παράγραφος 2.

747 Ό.π., άρθρο 3 παράγραφος 7.

748 Ευρωπαϊκή Επιτροπή (2016), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο σύμφωνα με το άρθρο 294 παράγραφος 6 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης σχετικά με τη θέση του Συμβουλίου όσον αφορά την έγκριση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου, COM(2016) 213 final, Βρυξέλλες, 11 Απριλίου 2016.

749 Οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, κεφάλαιο V.

750 Ό.π., άρθρο 2 παράγραφος 3.

επίσης υπόψη την ιδιαίτερη φύση του αστυνομικού τομέα και του τομέα της ποινικής δικαιοσύνης. Η εποπτεία μπορεί να ασκείται από τις ίδιες αρχές των κρατών μελών οι οποίες είναι αρμόδιες και για την άσκηση της δυνάμει του Γενικού Κανονισμού για την Προστασία Δεδομένων. Ο διορισμός υπευθύνων προστασίας δεδομένων και η διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων προβλέπονται στην οδηγία ως νέες υποχρεώσεις για τις αστυνομικές και δικαστικές αρχές⁷⁵¹. Παρότι οι έννοιες αυτές είναι εμπνευσμένες από τον Γενικό Κανονισμό για την Προστασία Δεδομένων, η οδηγία πραγματεύεται την ιδιαίτερη φύση των αστυνομικών και δικαστικών αρχών. Σε σύγκριση με την επεξεργασία δεδομένων για εμπορικούς σκοπούς, η οποία ρυθμίζεται από τον κανονισμό, η επεξεργασία δεδομένων για λόγους ασφάλειας ενδέχεται να προϋποθέτει ορισμένο βαθμό ευελιξίας. Για παράδειγμα, η παροχή του ίδιου επιπέδου προστασίας στα υποκείμενα των δεδομένων, όσον αφορά το δικαίωμα πληροφόρησης, πρόσβασης ή διαγραφής των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, με το επίπεδο προστασίας που προβλέπεται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων θα μπορούσε να σημαίνει ότι κάθε δραστηριότητα παρακολούθησης που πραγματοποιείται για τους σκοπούς της επιβολής του νόμου θα καθίστατο αλυσιτελής στο πλαίσιο της επιβολής του νόμου. Για τον λόγο αυτό, στην οδηγία δεν περιλαμβάνεται η αρχή της διαφάνειας. Ομοίως, οι αρχές της ελαχιστοποίησης των δεδομένων και του περιορισμού του σκοπού, οι οποίες επιβάλλουν την υποχρέωση, αφενός, του περιορισμού των δεδομένων προσωπικού χαρακτήρα μόνο στον βαθμό που είναι αναγκαία για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, και, αφετέρου, της επεξεργασίας τους για καθορισμένους και σαφείς σκοπούς, πρέπει επίσης να εφαρμόζονται με ευέλικτο τρόπο στο πλαίσιο της επεξεργασίας δεδομένων για λόγους ασφάλειας. Οι πληροφορίες που συλλέγονται και αποθηκεύονται από τις αρμόδιες αρχές για συγκεκριμένη υπόθεση ενδέχεται να αποβούν ιδιαιτέρως χρήσιμες κατά την επίλυση μελλοντικών υποθέσεων.

Αρχές που διέπουν την επεξεργασία

Η οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης καθορίζει ορισμένες βασικές διασφαλίσεις όσον αφορά τη χρήση δεδομένων προσωπικού χαρακτήρα. Επίσης, διατυπώνει τις αρχές που διέπουν την επεξεργασία των δεδομένων αυτών. Τα κράτη μέλη πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα:

⁷⁵¹ Ό.π., άρθρο 32 και άρθρο 27, αντίστοιχα.

- υποβάλλονται σε σύννομη και δίκαιη επεξεργασία·
- συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς·
- είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία·
- είναι ακριβή και, όταν απαιτείται, επικαιροποιούνται, λαμβάνονται όλα τα εύλογα μέτρα που διασφαλίζουν τη χωρίς καθυστέρηση διαγραφή ή διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα, λαμβανομένων υπόψη των σκοπών της επεξεργασίας·
- διατηρούνται υπό μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων των δεδομένων για χρονικό διάστημα όχι μεγαλύτερο από αυτό που είναι αναγκαίο για την επίτευξη των σκοπών για τους οποίους υποβάλλονται σε επεξεργασία·
- υποβάλλονται σε επεξεργασία κατά τρόπο που να εγγυάται τη δέουσα ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία από μη εγκεκριμένη ή παράνομη επεξεργασία ή τυχαία απώλεια, καταστροφή ή φθορά, με χρήση κατάλληλων τεχνικών ή οργανωτικών μέτρων ⁷⁵².

Σύμφωνα με την οδηγία, η επεξεργασία είναι σύννομη μόνο στον βαθμό που είναι αναγκαία για την εκτέλεση του σχετικού καθήκοντος. Επιπλέον, η επεξεργασία θα πρέπει να πραγματοποιείται από αρμόδια αρχή με σκοπό την επίτευξη των στόχων που καθορίζονται στην οδηγία και να βασίζεται στο δίκαιο της ΕΕ ή στο εθνικό δίκαιο ⁷⁵³. Τα δεδομένα δεν πρέπει να διατηρούνται για μεγαλύτερο διάστημα από αυτό που απαιτείται και πρέπει να διαγράφονται ή να επανεξετάζονται ανά τακτά χρονικά διαστήματα εντός συγκεκριμένων προθεσμιών. Τα δεδομένα πρέπει να χρησιμοποιούνται μόνο από αρμόδια αρχή και για τους σκοπούς για τους οποίους συλλέγονται, διαβιβάζονται ή καθίστανται διαθέσιμα.

⁷⁵² Ό.π., άρθρο 4 παράγραφος 1.

⁷⁵³ Ό.π., άρθρο 8.

Δικαιώματα του υποκειμένου των δεδομένων

Η οδηγία καθορίζει επίσης τα δικαιώματα του υποκειμένου των δεδομένων. Σε αυτά περιλαμβάνονται τα εξής:

- Το δικαίωμα λήψης πληροφοριών. Τα κράτη μέλη πρέπει να υποχρεώνουν τον υπεύθυνο επεξεργασίας των δεδομένων να παρέχει στο υποκείμενο των δεδομένων 1) τα στοιχεία ταυτότητας και επικοινωνίας του υπευθύνου επεξεργασίας, 2) τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, 3) τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα, 4) το δικαίωμα να υποβάλει καταγγελία στην εποπτική αρχή, καθώς και τα στοιχεία επικοινωνίας της αρχής, και 5) το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα, διόρθωσης ή διαγραφής τους, καθώς και το δικαίωμα περιορισμού της επεξεργασίας των δεδομένων ⁷⁵⁴. Επιπλέον αυτών των γενικών απαιτήσεων πληροφόρησης, η οδηγία προβλέπει ότι, σε ειδικές περιπτώσεις και προκειμένου να καθίσταται δυνατή η άσκηση των δικαιωμάτων τους, τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται από τους υπευθύνους επεξεργασίας για τη νομική βάση της επεξεργασίας και τη διάρκεια αποθήκευσης των δεδομένων. Σε περίπτωση διαβίβασης των δεδομένων προσωπικού χαρακτήρα σε άλλους αποδέκτες, μεταξύ άλλων σε τρίτες χώρες ή διεθνείς οργανισμούς, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται για τις κατηγορίες των εν λόγω αποδεκτών. Τέλος, οι υπεύθυνοι επεξεργασίας πρέπει να παρέχουν περαιτέρω πληροφορίες, λαμβάνοντας υπόψη τις ειδικές περιστάσεις υπό τις οποίες τα δεδομένα υποβάλλονται σε επεξεργασία, για παράδειγμα, όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται κατά τη διάρκεια κρυφής παρακολούθησης, δηλαδή εν αγνοία του υποκειμένου των δεδομένων. Με αυτόν τον τρόπο εξασφαλίζεται η θεμιτή επεξεργασία έναντι του υποκειμένου των δεδομένων ⁷⁵⁵.
- Το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα. Τα κράτη μέλη πρέπει να διασφαλίζουν ότι το υποκείμενο των δεδομένων έχει το δικαίωμα να γνωρίζει αν τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υποβάλλονται σε επεξεργασία. Εάν υποβάλλονται σε επεξεργασία, το υποκείμενο των δεδομένων θα πρέπει να έχει πρόσβαση σε ορισμένες πληροφορίες, όπως οι κατηγορίες των δεδομένων που υποβάλλονται σε

⁷⁵⁴ Ό.π., άρθρο 13 παράγραφος 1.

⁷⁵⁵ Ό.π., άρθρο 13 παράγραφος 2.

επεξεργασία ⁷⁵⁶. Ωστόσο, το δικαίωμα αυτό μπορεί να περιορίζεται, π.χ., για την αποφυγή της παρακώλυσης έρευνας ή της παρεμπόδισης δίωξης ποινικών αδικημάτων ή για την προστασία της δημόσιας ασφάλειας και των δικαιωμάτων και των ελευθεριών τρίτων ⁷⁵⁷.

- Το δικαίωμα διόρθωσης των δεδομένων προσωπικού χαρακτήρα. Τα κράτη μέλη υποχρεούνται να διασφαλίζουν ότι το υποκείμενο των δεδομένων δύναται να ασκεί, χωρίς αδικαιολόγητη καθυστέρηση, το δικαίωμά του να απαιτεί τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα. Επιπλέον, το υποκείμενο των δεδομένων έχει επίσης το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα ⁷⁵⁸.
- Το δικαίωμα διαγραφής δεδομένων προσωπικού χαρακτήρα και περιορισμού της επεξεργασίας. Σε ορισμένες περιπτώσεις, ο υπεύθυνος επεξεργασίας χρειάζεται να διαγράψει δεδομένα προσωπικού χαρακτήρα. Επιπλέον, το υποκείμενο έχει το δικαίωμα να εξασφαλίσει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν μόνο σε περίπτωση που η επεξεργασία τους δεν είναι σύννομη ⁷⁵⁹. Σε ορισμένες περιπτώσεις παρέχεται η δυνατότητα περιορισμού της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα αντί της διαγραφής τους. Αυτό μπορεί να συμβεί στις ακόλουθες περιπτώσεις: 1) εάν η ακρίβεια των δεδομένων προσωπικού χαρακτήρα έχει αμφισβητηθεί, αλλά δεν μπορεί να διαπιστωθεί ή 2) εάν τα δεδομένα προσωπικού χαρακτήρα είναι αναγκαία για σκοπούς απόδειξης ⁷⁶⁰.

Οποτεδήποτε ο υπεύθυνος επεξεργασίας αρνείται να διορθώσει ή να διαγράψει δεδομένα προσωπικού χαρακτήρα, ή να περιορίσει την επεξεργασία τους, το υποκείμενο των δεδομένων πρέπει να ενημερώνεται εγγράφως για την άρνηση αυτή. Τα κράτη μέλη δύνανται να περιορίζουν το εν λόγω δικαίωμα ενημέρωσης για τους σκοπούς, μεταξύ άλλων, της προστασίας της δημόσιας ασφάλειας ή των δικαιωμάτων και των ελευθεριών τρίτων, για τους ίδιους λόγους για τους οποίους περιορίζουν και το δικαίωμα πρόσβασης ⁷⁶¹.

⁷⁵⁶ Ό.π., άρθρο 14.

⁷⁵⁷ Ό.π., άρθρο 15.

⁷⁵⁸ Ό.π., άρθρο 16 παράγραφος 1.

⁷⁵⁹ Ό.π., άρθρο 16 παράγραφος 2.

⁷⁶⁰ Ό.π., άρθρο 16 παράγραφος 3.

⁷⁶¹ Ό.π., άρθρο 16 παράγραφος 4.

Το υποκείμενο των δεδομένων έχει συνήθως δικαίωμα πληροφόρησης σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, καθώς και δικαίωμα πρόσβασης, διόρθωσης, διαγραφής ή περιορισμού της επεξεργασίας, το οποίο μπορεί να ασκήσει άμεσα μέσω του υπευθύνου επεξεργασίας. Εναλλακτικά, η οδηγία για την προστασία δεδομένων στον αστυνομικό τομέα και τον τομέα της ποινικής δικαιοσύνης προβλέπει επίσης τη δυνατότητα έμμεσης άσκησης των δικαιωμάτων του υποκειμένου των δεδομένων, μέσω της εποπτικής αρχής προστασίας των δεδομένων, η οποία αρχίζει να ισχύει όταν ο υπεύθυνος επεξεργασίας περιορίζει το δικαίωμα του υποκειμένου των δεδομένων ⁷⁶². Σύμφωνα με το άρθρο 17 της οδηγίας, τα κράτη μέλη θεσπίζουν μέτρα που διασφαλίζουν ότι τα δικαιώματα των υποκειμένων των δεδομένων είναι επίσης δυνατόν να ασκούνται μέσω της εθνικής εποπτικής αρχής. Για τον λόγο αυτό, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει το υποκείμενο των δεδομένων σχετικά με τη δυνατότητα έμμεσης πρόσβασης.

Υποχρεώσεις του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία

Στο πλαίσιο της οδηγίας για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, οι υπεύθυνοι επεξεργασίας των δεδομένων είναι αρμόδιες δημόσιες αρχές ή άλλοι φορείς με σχετικές δημόσιες εξουσίες που καθορίζουν τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η οδηγία επιβάλλει στους υπευθύνους επεξεργασίας των δεδομένων διάφορες υποχρεώσεις, ούτως ώστε να διασφαλίζεται υψηλό επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για τους σκοπούς της επιβολής του νόμου.

Οι αρμόδιες αρχές πρέπει να τηρούν καταχωρίσεις για τις πράξεις επεξεργασίας που εκτελούν σε συστήματα αυτοματοποιημένης επεξεργασίας. Καταχωρίσεις πρέπει να τηρούνται τουλάχιστον για πράξεις συλλογής, μεταβολής, αναζήτησης πληροφοριών, κοινολόγησης, περιλαμβανομένων των διαβιβάσεων, συνδυασμού και διαγραφής των δεδομένων προσωπικού χαρακτήρα ⁷⁶³. Η οδηγία προβλέπει ότι οι καταχωρίσεις της αναζήτησης πληροφοριών και της κοινολόγησης πρέπει να επιτρέπουν τον προσδιορισμό της ημερομηνίας και της ώρας των πράξεων, της αιτιολόγησής τους και, στον βαθμό του εφικτού, της ταυτότητας του προσώπου που αναζήτησε πληροφορίες στο σύστημα ή κοινολόγησε δεδομένα

⁷⁶² Ό.π., άρθρο 17.

⁷⁶³ Ό.π., άρθρο 25 παράγραφος 1.

προσωπικού χαρακτήρα, καθώς και της ταυτότητας των αποδεκτών των εν λόγω δεδομένων προσωπικού χαρακτήρα. Οι καταχωρίσεις πρέπει να χρησιμοποιούνται αποκλειστικά και μόνο για λόγους επαλήθευσης της νομιμότητας της επεξεργασίας, αυτοπαρακολούθησης, διαφύλαξης της ακεραιότητας και της ασφάλειας των δεδομένων προσωπικού χαρακτήρα, καθώς και στο πλαίσιο ποινικών διαδικασιών ⁷⁶⁴. Κατόπιν αιτήματος από την εποπτική αρχή, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να θέτουν τα αρχεία καταχωρήσεων στη διάθεσή της.

Ειδικότερα, προβλέπεται γενική υποχρέωση βάσει της οποίας οι υπεύθυνοι επεξεργασίας πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζουν ότι η επεξεργασία εκτελείται σύμφωνα με την οδηγία και ότι είναι σε θέση να αποδείξουν τη νομιμότητα της εν λόγω επεξεργασίας ⁷⁶⁵. Κατά τον σχεδιασμό των εν λόγω μέτρων, οι υπεύθυνοι επεξεργασίας πρέπει να λαμβάνουν υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο της επεξεργασίας και, κυρίως, τους πιθανούς κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων. Οι υπεύθυνοι επεξεργασίας θα πρέπει να υιοθετούν εσωτερικές πολιτικές και να εφαρμόζουν μέτρα που διευκολύνουν την τήρηση των αρχών προστασίας δεδομένων, ιδίως της αρχής της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού ⁷⁶⁶. Σε περίπτωση που η επεξεργασία είναι πιθανό να συνεπάγεται υψηλό κίνδυνο για τα δικαιώματα των ατόμων, λόγω, π.χ., της χρήσης νέων τεχνολογιών, οι υπεύθυνοι επεξεργασίας πρέπει να διενεργούν εκτίμηση αντικτύπου όσον αφορά την προστασία των δεδομένων πριν από την έναρξη της επεξεργασίας ⁷⁶⁷. Στην οδηγία απαριθμούνται επίσης τα μέτρα που πρέπει να εφαρμόζουν οι υπεύθυνοι επεξεργασίας για τη διαφύλαξη της ασφάλειας της επεξεργασίας. Τα μέτρα αυτά περιλαμβάνουν την απαγόρευση της μη εξουσιοδοτημένης πρόσβασης στα δεδομένα προσωπικού χαρακτήρα τα οποία υποβάλλονται σε επεξεργασία από τους υπευθύνους επεξεργασίας, την εξασφάλιση της πρόσβασης των εξουσιοδοτημένων προσώπων μόνο στα δεδομένα προσωπικού χαρακτήρα τα οποία καλύπτει η σχετική εξουσιοδότηση πρόσβασης, τη διασφάλιση της ορθής εκτέλεσης των λειτουργιών του συστήματος, καθώς και την εξάλειψη της δυνατότητας αλλοίωσης των αποθηκευμένων δεδομένων προσωπικού χαρακτήρα λόγω δυσλειτουργίας του συστήματος ⁷⁶⁸.

⁷⁶⁴ Ό.π., άρθρο 25 παράγραφος 2.

⁷⁶⁵ Ό.π., άρθρο 19.

⁷⁶⁶ Ό.π., άρθρο 20.

⁷⁶⁷ Ό.π., άρθρο 27.

⁷⁶⁸ Ό.π., άρθρο 29.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, οι υπεύθυνοι επεξεργασίας πρέπει να γνωστοποιούν στην εποπτική αρχή εντός τριών ημερών, περιγράφοντας τη φύση της παραβίασης, τις ενδεχόμενες επιπτώσεις της, τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα που εμπλέκονται και τον κατά προσέγγιση αριθμό των θιγόμενων υποκειμένων των δεδομένων. Η παραβίαση των δεδομένων προσωπικού χαρακτήρα πρέπει επίσης να γνωστοποιείται «αμελλητί» στο υποκείμενο των δεδομένων, σε περίπτωση που η παραβίαση αυτή είναι πιθανό να προκαλέσει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες του ⁷⁶⁹.

Η οδηγία περιέχει την αρχή της λογοδοσίας, καθώς αναθέτει στους υπευθύνους επεξεργασίας το καθήκον εφαρμογής μέτρων για τη διασφάλιση της τήρησης της εν λόγω αρχής. Οι υπεύθυνοι επεξεργασίας πρέπει να τηρούν αρχεία για όλες τις κατηγορίες δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνοι: το αναλυτικό περιεχόμενο των εν λόγω αρχείων διευκρινίζεται στο άρθρο 24 της οδηγίας. Τα αρχεία πρέπει να τίθενται στη διάθεση της εποπτικής αρχής, κατόπιν σχετικού αιτήματος, ούτως ώστε να παρέχεται η δυνατότητα παρακολούθησης των δραστηριοτήτων επεξεργασίας του υπευθύνου επεξεργασίας. Άλλο ένα σημαντικό μέτρο για την ενίσχυση της λογοδοσίας είναι ο ορισμός του υπευθύνου προστασίας δεδομένων. Οι υπεύθυνοι επεξεργασίας πρέπει να διορίζουν υπεύθυνο προστασίας δεδομένων, παρότι η οδηγία επιτρέπει στα κράτη μέλη να απαλλάσσουν από την υποχρέωση αυτή τα δικαστήρια και άλλες ανεξάρτητες δικαστικές αρχές ⁷⁷⁰. Τα καθήκοντα του υπευθύνου προστασίας δεδομένων είναι παρόμοια με τα καθήκοντα που προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων. Ο υπεύθυνος προστασίας δεδομένων παρακολουθεί τη συμμόρφωση προς τις διατάξεις της οδηγίας και παρέχει στους υπαλλήλους που πραγματοποιούν την επεξεργασία δεδομένων πληροφορίες και συμβουλές σχετικά με τις υποχρεώσεις που υπέχουν σύμφωνα με τη νομοθεσία για την προστασία των δεδομένων. Ο υπεύθυνος προστασίας δεδομένων παρέχει επίσης συμβουλές σχετικά με την ανάγκη να διενεργηθεί εκτίμηση επιπτώσεων όσον αφορά την προστασία των δεδομένων και ενεργεί ως σημείο επαφής για την εποπτική αρχή.

⁷⁶⁹ Ό.π., άρθρα 30 και 31.

⁷⁷⁰ Ό.π., άρθρο 32.

Διαβιβάσεις προς τρίτες χώρες ή διεθνείς οργανισμούς

Ομοίως με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, η οδηγία καθορίζει τις προϋποθέσεις για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες ή διεθνείς οργανισμούς. Εάν τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονταν ελεύθερα εκτός της δικαιοδοσίας της ΕΕ, θα υπήρχε ο κίνδυνος υπονόμησης των εγγυήσεων και της ισχυρής προστασίας που παρέχονται βάσει του δικαίου της ΕΕ. Ωστόσο, οι προϋποθέσεις αυτές καθαυτές διαφοροποιούνται σε αρκετά μεγάλο βαθμό από τις προϋποθέσεις που προβλέπονται στον Γενικό Κανονισμό για την Προστασία Δεδομένων. Η διαβίβαση δεδομένων προς τρίτες χώρες ή διεθνείς οργανισμούς επιτρέπεται στις ακόλουθες περιπτώσεις ⁷⁷¹:

- Η διαβίβαση είναι αναγκαία για τους σκοπούς της οδηγίας.
- Τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε αρμόδια, κατά την έννοια της οδηγίας, αρχή της τρίτης χώρας ή του διεθνούς οργανισμού, αν και προβλέπεται παρέκκλιση από τον συγκεκριμένο κανόνα σε μεμονωμένες και ειδικές περιπτώσεις ⁷⁷².
- Η διαβίβαση δεδομένων προσωπικού χαρακτήρα που λαμβάνονται στο πλαίσιο διασυννοριακής συνεργασίας προς τρίτες χώρες ή διεθνείς οργανισμούς προϋποθέτει την έγκριση του κράτους μέλους από το οποίο προέρχονται τα δεδομένα, αν και προβλέπονται εξαιρέσεις σε επείγουσες περιπτώσεις.
- Η Ευρωπαϊκή Επιτροπή έχει εκδώσει απόφαση επάρκειας, έχουν θεσπιστεί κατάλληλες εγγυήσεις ή ισχύει η παρέκκλιση για τις διαβιβάσεις σε ειδικές περιπτώσεις.
- Η περαιτέρω διαβίβαση δεδομένων προσωπικού χαρακτήρα προς άλλη τρίτη χώρα ή διεθνή οργανισμό προϋποθέτει την προηγούμενη έγκριση της αρμόδιας αρχής προέλευσης, η οποία λαμβάνει υπόψη, μεταξύ άλλων, τη σοβαρότητα του αδικήματος και το επίπεδο προστασίας των δεδομένων στη χώρα προορισμού της δεύτερης διεθνούς διαβίβασης ⁷⁷³.

⁷⁷¹ 'Ο.π., άρθρο 35.

⁷⁷² 'Ο.π., άρθρο 39.

⁷⁷³ 'Ο.π., άρθρο 35 παράγραφος 1.

Βάσει της οδηγίας, η διαβίβαση δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον εάν πληρούται μία από τις ακόλουθες τρεις προϋποθέσεις: πρώτον, σε περίπτωση που η Ευρωπαϊκή Επιτροπή έχει εκδώσει απόφαση επάρκειας δυνάμει της οδηγίας. Η απόφαση μπορεί να ισχύει για ολόκληρη την επικράτεια τρίτης χώρας ή για συγκεκριμένους τομείς τρίτης χώρας ή για διεθνή οργανισμό. Εντούτοις, αυτό είναι δυνατόν μόνον εάν διασφαλίζεται επαρκές επίπεδο προστασίας και πληρούνται οι προϋποθέσεις που καθορίζονται στην οδηγία ⁷⁷⁴. Στις περιπτώσεις αυτές, η διαβίβαση των δεδομένων προσωπικού χαρακτήρα δεν υπόκειται στη χορήγηση έγκρισης από το κράτος μέλος ⁷⁷⁵. Η Ευρωπαϊκή Επιτροπή πρέπει να παρακολουθεί τις εξελίξεις που θα μπορούσαν να επηρεάσουν τη λειτουργία των αποφάσεων επάρκειας. Επιπλέον, η απόφαση πρέπει να περιλαμβάνει μηχανισμό περιοδικής επανεξέτασης. Η Επιτροπή μπορεί επίσης να ανακαλέσει, να τροποποιήσει ή να αναστείλει μια απόφαση σε περίπτωση που, βάσει των διαθέσιμων πληροφοριών, αποκαλυφθεί ότι οι συνθήκες στην τρίτη χώρα ή στον διεθνή οργανισμό δεν διασφαλίζουν πλέον επαρκές επίπεδο προστασίας. Στην περίπτωση αυτή, η Επιτροπή πρέπει να ξεκινήσει διαβουλεύσεις με την τρίτη χώρα ή τον διεθνή οργανισμό σε μια προσπάθεια επανόρθωσης της κατάστασης.

Ελλείψει απόφασης επάρκειας, οι διαβιβάσεις υπόκεινται σε κατάλληλες εγγυήσεις. Οι εγγυήσεις μπορούν να προβλέπονται σε νομικά δεσμευτικές πράξεις ή ο υπεύθυνος επεξεργασίας μπορεί να διενεργήσει αυτοαξιολόγηση όσον αφορά τις περιστάσεις που πλασιώνουν τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα και να καταλήξει στο συμπέρασμα ότι υπάρχουν κατάλληλες εγγυήσεις. Η αυτοαξιολόγηση θα πρέπει να λαμβάνει υπόψη πιθανές συμφωνίες συνεργασίας που έχουν συναφθεί μεταξύ της Ευρώπης ή της Eurojust και της τρίτης χώρας ή του διεθνούς οργανισμού, την ύπαρξη υποχρεώσεων τήρησης του απορρήτου και τον περιορισμό του σκοπού, καθώς και διασφαλίσεις σύμφωνα με τις οποίες τα δεδομένα δεν θα χρησιμοποιηθούν για καμία μορφή βάνουσης και απάνθρωπης μεταχείρισης, συμπεριλαμβανομένης της θανατικής ποινής ⁷⁷⁶. Στη δεύτερη περίπτωση, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει την αρμόδια εποπτική αρχή για τις κατηγορίες διαβιβάσεων που εμπίπτουν στη συγκεκριμένη κατηγορία ⁷⁷⁷.

⁷⁷⁴ Ό.π., άρθρο 36.

⁷⁷⁵ Ό.π., άρθρο 36 παράγραφος 1.

⁷⁷⁶ Ό.π., αιτιολογική σκέψη 71.

⁷⁷⁷ Ό.π., άρθρο 37 παράγραφος 1.

Σε περίπτωση που δεν έχει εκδοθεί απόφαση επάρκειας ούτε έχουν προβλεφθεί κατάλληλες εγγυήσεις, εξακολουθεί να επιτρέπεται η εκτέλεση διαβιβάσεων σε ειδικές περιπτώσεις, οι οποίες περιγράφονται συνοπτικά στην οδηγία. Οι περιπτώσεις αυτές περιλαμβάνουν, μεταξύ άλλων, την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή τρίτου προσώπου, καθώς και την πρόληψη άμεσης και σοβαρής απειλής κατά της δημόσιας ασφάλειας του οικείου κράτους μέλους ή τρίτης χώρας ⁷⁷⁸.

Σε μεμονωμένες και ειδικές περιπτώσεις παρέχεται η δυνατότητα διαβιβάσεων δεδομένων από αρμόδιες αρχές προς αποδέκτες οι οποίοι είναι εγκατεστημένοι σε τρίτες χώρες και δεν συνιστούν αρμόδιες αρχές, υπό τον όρο ότι πληρούνται μία από τις τρεις προϋποθέσεις που περιγράφονται ανωτέρω, αλλά και οι επιπλέον προϋποθέσεις που καθορίζονται στο άρθρο 39 της οδηγίας. Ειδικότερα, η διαβίβαση πρέπει να είναι απολύτως αναγκαία για την εκτέλεση καθήκοντος της διαβιβάζουσας αρμόδιας αρχής, η οποία είναι επίσης αρμόδια να κρίνει ότι τα θεμελιώδη δικαιώματα ή οι ελευθερίες των ατόμων δεν υπερισχύουν του δημοσίου συμφέροντος που αιτιολογεί τη διαβίβαση. Οι εν λόγω διαβιβάσεις πρέπει να τεκμηριώνονται και η διαβιβάζουσα αρμόδια αρχή θα πρέπει να ενημερώνει την αρμόδια εποπτική αρχή ⁷⁷⁹.

Τέλος, όσον αφορά τρίτες χώρες και διεθνείς οργανισμούς, η οδηγία επιβάλλει επίσης την ανάπτυξη μηχανισμών διεθνούς συνεργασίας για τη διευκόλυνση της αποτελεσματικής επιβολής της νομοθεσίας και, κατ' επέκταση, της συνεργασίας των εποπτικών αρχών προστασίας δεδομένων με τους διεθνείς ομολόγους τους ⁷⁸⁰.

Ανεξάρτητη εποπτεία και δυνατότητες προσφυγής για τα υποκείμενα των δεδομένων

Κάθε κράτος μέλος πρέπει να διασφαλίζει ότι μία ή περισσότερες ανεξάρτητες εθνικές εποπτικές αρχές είναι αρμόδιες για την παροχή συμβουλών και την παρακολούθηση της εφαρμογής των διατάξεων που θεσπίζονται δυνάμει της οδηγίας ⁷⁸¹. Παρότι η εποπτική αρχή που ιδρύεται για τους σκοπούς της οδηγίας μπορεί να είναι η ίδια με την εποπτική αρχή που έχει ιδρυθεί δυνάμει του Γενικού

⁷⁷⁸ 'Ο.π., άρθρο 38 παράγραφος 1.

⁷⁷⁹ 'Ο.π., άρθρο 37 παράγραφος 3.

⁷⁸⁰ 'Ο.π., άρθρο 40.

⁷⁸¹ 'Ο.π., άρθρο 41.

Κανονισμού για την Προστασία Δεδομένων, τα κράτη μέλη δύνανται να ορίσουν διαφορετική αρχή, υπό την προϋπόθεση ότι πληροί τα κριτήρια ανεξαρτησίας. Οι εποπτικές αρχές επιλαμβάνονται επίσης των καταγγελιών που υποβάλλονται από οποιοδήποτε πρόσωπο σχετικά με την προστασία των δικαιωμάτων και των ελευθεριών του όσον αφορά την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές.

Σε περίπτωση άρνησης του αιτήματος άσκησης των δικαιωμάτων του υποκειμένου των δεδομένων για επιτακτικούς λόγους, το υποκείμενο των δεδομένων πρέπει να έχει δικαίωμα προσφυγής ενώπιον της αρμόδιας εθνικής εποπτικής αρχής και/ή δικαστηρίου. Κάθε πρόσωπο το οποίο έχει υποστεί ζημία λόγω παραβίασης της εθνικής νομοθεσίας με την οποία εφαρμόζεται η οδηγία δικαιούται αποζημίωση από τον υπεύθυνο επεξεργασίας ή από άλλη αρμόδια αρχή σύμφωνα με το δίκαιο του οικείου κράτους μέλους⁷⁸². Κατά γενικό κανόνα, τα υποκείμενα των δεδομένων πρέπει να έχουν το δικαίωμα δικαστικής προσφυγής για κάθε παραβίαση των δικαιωμάτων τους, όπως κατοχυρώνονται από την εθνική νομοθεσία με την οποία εφαρμόζεται η οδηγία⁷⁸³.

8.3. Άλλες ειδικές νομικές πράξεις σχετικά με την προστασία δεδομένων στον τομέα της επιβολής του νόμου

Πέραν της οδηγίας για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, η ανταλλαγή πληροφοριών που πραγματοποιείται από τα κράτη μέλη σε συγκεκριμένους τομείς ρυθμίζεται και από άλλες νομικές πράξεις, όπως η απόφαση-πλαίσιο 2009/315/ΔΕΥ του Συμβουλίου σχετικά με τη διοργάνωση και το περιεχόμενο της ανταλλαγής πληροφοριών που προέρχονται από το ποινικό μητρώο μεταξύ των κρατών μελών, η απόφαση 2000/642/ΔΕΥ του Συμβουλίου σχετικά με τη θέσπιση ρυθμίσεων για τη συνεργασία μεταξύ των μονάδων χρηματοοικονομικών πληροφοριών των κρατών μελών όσον αφορά την ανταλλαγή πληροφοριών, και η απόφαση-πλαίσιο 2006/960/ΔΕΥ του Συμβουλίου, της 18ης Δεκεμβρίου 2006, για την απλούστευση

782 Ό.π., άρθρο 56.

783 Ό.π., άρθρο 54.

της ανταλλαγής πληροφοριών και στοιχείων μεταξύ των αρχών επιβολής του νόμου των κρατών μελών της Ευρωπαϊκής Ένωσης⁷⁸⁴.

Είναι σημαντικό να αναφερθεί ότι η διασυνοριακή συνεργασία⁷⁸⁵ μεταξύ των αρμόδιων αρχών αφορά ολόένα και περισσότερο την ανταλλαγή δεδομένων μετανάστευσης. Ο συγκεκριμένος τομέας του δικαίου δεν θεωρείται ότι εμπίπτει στον τομέα της αστυνομίας και της ποινικής δικαιοσύνης, αλλά άπτεται, από πολλές απόψεις, του έργου των αστυνομικών και δικαστικών αρχών. Το ίδιο ισχύει και για τα δεδομένα σχετικά με τα εμπορεύματα που εισάγονται στην ΕΕ ή εξάγονται από αυτή. Η απουσία ελέγχων στα εσωτερικά σύνορα του χώρου Σένγκεν έχει εντείνει τον κίνδυνο απάτης, καθιστώντας αναγκαία την εντατικοποίηση της συνεργασίας μεταξύ των κρατών μελών, κυρίως με την ενίσχυση της διασυνοριακής ανταλλαγής πληροφοριών, με σκοπό την αποτελεσματικότερη ανίχνευση και δίωξη παραβιάσεων της εθνικής και ενωσιακής τελωνειακής νομοθεσίας. Επιπλέον, τα τελευταία έτη έχει σημειωθεί αύξηση του σοβαρού και οργανωμένου εγκλήματος και της τρομοκρατίας, εξέλιξη που μπορεί να συνεπάγεται διεθνείς μετακινήσεις, και έχει αναδειχθεί η ανάγκη ενισχυμένης διασυνοριακής συνεργασίας μεταξύ των αστυνομικών αρχών και των αρχών επιβολής του νόμου σε πολλές περιπτώσεις⁷⁸⁶.

Η απόφαση Prüm

Σημαντικό παράδειγμα της θεσμοθετημένης διασυνοριακής συνεργασίας με τη μορφή ανταλλαγής δεδομένων τα οποία κατέχουν τα κράτη μέλη αποτελεί η απόφαση 2008/615/ΔΕΥ του Συμβουλίου, καθώς και οι διατάξεις εφαρμογής της που περιλαμβάνονται στην απόφαση 2008/615/ΔΕΥ, σχετικά με την αναβάθμιση

784 Συμβούλιο της Ευρωπαϊκής Ένωσης (2009), Απόφαση-πλαίσιο 2009/315/ΔΕΥ του Συμβουλίου, της 26ης Φεβρουαρίου 2009, σχετικά με τη διοργάνωση και το περιεχόμενο της ανταλλαγής πληροφοριών που προέρχονται από το ποινικό μητρώο μεταξύ των κρατών μελών (ΕΕ L 93 της 7.4.2009, σ. 23)- Συμβούλιο της Ευρωπαϊκής Ένωσης (2000), απόφαση 2000/642/ΔΕΥ του Συμβουλίου, της 17ης Οκτωβρίου 2000, σχετικά με τη θέσπιση ρυθμίσεων για τη συνεργασία μεταξύ των μονάδων χρηματοοικονομικών πληροφοριών των κρατών μελών όσον αφορά την ανταλλαγή πληροφοριών (ΕΕ L 271 της 24.10.2000, σ. 4)- απόφαση-πλαίσιο 2006/960/ΔΕΥ του Συμβουλίου, της 18ης Δεκεμβρίου 2006, για την απλούστευση της ανταλλαγής πληροφοριών και στοιχείων μεταξύ των αρχών επιβολής του νόμου των κρατών μελών της Ευρωπαϊκής Ένωσης (ΕΕ L 386 της 29.12.2006, σ. 89).

785 Ευρωπαϊκή Επιτροπή (2012), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο – Ενίσχυση της συνεργασίας για την επιβολή του νόμου στην ΕΕ: το ευρωπαϊκό πρότυπο ανταλλαγής πληροφοριών (EIXM), COM(2012) 735 final, Βρυξέλλες, 7 Δεκεμβρίου 2012.

786 Βλ. Ευρωπαϊκή Επιτροπή (2011), Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις με τα ονόματα επιβατών (δεδομένα PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και άλλων σοβαρών εγκλημάτων, COM(2011) 32 τελικό, Βρυξέλλες, 2 Φεβρουαρίου 2011, σ. 1.

της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος (απόφαση Prüm), με την οποία η συνθήκη του Prüm ενσωματώθηκε το 2008 στο δίκαιο της ΕΕ ⁷⁸⁷. Η συνθήκη του Prüm ήταν μια συμφωνία διεθνούς αστυνομικής συνεργασίας που υπογράφηκε το 2005 από την Αυστρία, το Βέλγιο, τη Γαλλία, τη Γερμανία, την Ισπανία, τις Κάτω Χώρες και το Λουξεμβούργο ⁷⁸⁸.

Στόχος της απόφασης Prüm είναι να βοηθήσει τα συμβαλλόμενα κράτη μέλη να βελτιώσουν την ανταλλαγή πληροφοριών με σκοπό την πρόληψη και την καταπολέμηση του εγκλήματος σε τρεις τομείς: τρομοκρατία, διασυνοριακό έγκλημα και παράνομη μετανάστευση. Για τον σκοπό αυτό, η απόφαση θεσπίζει διατάξεις σχετικά με:

- την αυτοματοποιημένη πρόσβαση σε προφίλ DNA, δεδομένα σχετικά με δακτυλικά αποτυπώματα και ορισμένα δεδομένα σχετικά με άδειες κυκλοφορίας οχημάτων·
- την παροχή δεδομένων σε σχέση με σημαντικά γεγονότα που έχουν διασυνοριακή διάσταση·
- την παροχή πληροφοριών για την πρόληψη τρομοκρατικών πράξεων·
- άλλα μέτρα για την αναβάθμιση της διασυνοριακής αστυνομικής συνεργασίας.

Οι βάσεις δεδομένων που καθίστανται διαθέσιμες δυνάμει της απόφασης Prüm διέπονται αποκλειστικά από την εθνική νομοθεσία, αλλά η ανταλλαγή δεδομένων διέπεται επιπροσθέτως από την απόφαση, της οποίας η συμβατότητα με την οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης θα πρέπει να αξιολογηθεί. Αρμόδιοι φορείς για την εποπτεία των εν λόγω ροών δεδομένων είναι οι εθνικές εποπτικές αρχές προστασίας δεδομένων.

787 Συμβούλιο της Ευρωπαϊκής Ένωσης (2008), απόφαση 2008/615/ΔΕΥ του Συμβουλίου, της 23ης Ιουνίου 2008, σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος (ΕΕ 2008 L 210).

788 Σύμβαση μεταξύ του Βασιλείου του Βελγίου, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, του Βασιλείου της Ισπανίας, της Γαλλικής Δημοκρατίας, του Μεγάλου Δουκάτου του Λουξεμβούργου, του Βασιλείου των Κάτω Χωρών και της Αυστριακής Δημοκρατίας σχετικά με την αναβάθμιση της διασυνοριακής συνεργασίας, ιδίως όσον αφορά την καταπολέμηση της τρομοκρατίας, του διασυνοριακού εγκλήματος και της παράνομης μετανάστευσης

Απόφαση-πλαίσιο 2006/960/ΔΕΥ – η Σουηδική Πρωτοβουλία

Η απόφαση-πλαίσιο 2006/960/ΔΕΥ (σουηδική πρωτοβουλία)⁷⁸⁹ αποτελεί ένα ακόμη παράδειγμα διασυννοριακής συνεργασίας όσον αφορά την ανταλλαγή δεδομένων που κατέχονται σε εθνικό επίπεδο από τις αρχές επιβολής του νόμου. Η σουηδική πρωτοβουλία εστιάζει ειδικά στην ανταλλαγή πληροφοριών και στοιχείων και προβλέπει ειδικούς κανόνες για την προστασία των δεδομένων στο άρθρο 8.

Σύμφωνα με την εν λόγω νομοθετική πράξη, η χρήση των πληροφοριών και στοιχείων που ανταλλάσσονται πρέπει να υπάγεται στους εθνικούς κανόνες περί προστασίας των δεδομένων του κράτους μέλους που λαμβάνει την αίτηση, σύμφωνα με τους ίδιους κανόνες όπως εάν είχαν συγκεντρωθεί στο συγκεκριμένο κράτος μέλος. Το άρθρο 8 ορίζει περαιτέρω ότι κατά την παροχή πληροφοριών και στοιχείων, η αρμόδια αρχή επιβολής του νόμου μπορεί, σύμφωνα με την εθνική της νομοθεσία, να θέτει στην αρμόδια αρχή επιβολής του νόμου προς την οποία παρέχει τις εν λόγω πληροφορίες, όρους όσον αφορά τη χρήση τους. Οι όροι αυτοί μπορούν επίσης να ισχύουν για τη γνωστοποίηση των αποτελεσμάτων της διερεύνησης του εγκλήματος ή των επιχειρήσεων συλλογής στοιχείων σχετικά με το έγκλημα στο πλαίσιο των οποίων ζητήθηκε η ανταλλαγή πληροφοριών και στοιχείων. Ωστόσο, όταν η εθνική νομοθεσία προβλέπει εξαιρέσεις στους περιορισμούς της χρήσης (π.χ. για δικαστικές αρχές, νομοθετικά σώματα, κ.λπ.), οι πληροφορίες και τα στοιχεία μπορούν να χρησιμοποιηθούν μόνο κατόπιν διαβουλεύσεων με το κράτος μέλος που τα διαβίβασε.

Οι πληροφορίες και τα στοιχεία που παρέχονται επιτρέπεται να χρησιμοποιούνται:

- για τους σκοπούς για τους οποίους έχουν παρασχεθεί· ή
- για την αποτροπή άμεσης και σοβαρής απειλής της δημόσιας ασφάλειας.

Η επεξεργασία τους για άλλους σκοπούς μπορεί να επιτραπεί, αλλά μόνο κατόπιν άδειας του κράτους μέλους που τα διαβίβασε.

⁷⁸⁹ Συμβούλιο της Ευρωπαϊκής Ένωσης (2006), Απόφαση-πλαίσιο 2006/960/ΔΕΥ του Συμβουλίου, της 18ης Δεκεμβρίου 2006, για την απλούστευση της ανταλλαγής πληροφοριών και στοιχείων μεταξύ των αρχών επιβολής του νόμου των κρατών μελών της Ευρωπαϊκής Ένωσης (ΕΕ L 386 της 29.12.2006, σ. 89).

Η σουηδική πρωτοβουλία ορίζει περαιτέρω ότι τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία πρέπει να προστατεύονται σύμφωνα με διεθνείς πράξεις, όπως:

- η Σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα ⁷⁹⁰.
- το πρόσθετο πρωτόκολλο της 8ης Νοεμβρίου 2001 στην προαναφερθείσα Σύμβαση, όσον αφορά τις εποπτικές αρχές και τη διασυνοριακή κυκλοφορία δεδομένων ⁷⁹¹.
- η σύσταση αριθ. R(87) 15 του Συμβουλίου της Ευρώπης που διέπει τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα ⁷⁹².

Η οδγία PNR της ΕΕ

Τα δεδομένα που περιέχονται στις καταστάσεις ονομάτων επιβατών (PNR) αφορούν πληροφορίες σχετικά με επιβάτες πτήσεων οι οποίες συλλέγονται και φυλάσσονται στα συστήματα κράτησης και ελέγχου αναχωρήσεων των αερομεταφορέων για δική τους εμπορική χρήση. Τα εν λόγω δεδομένα περιλαμβάνουν διάφορα είδη πληροφοριών, όπως την ημερομηνία ταξιδιού, το δρομολόγιο, τα στοιχεία εισιτηρίου, τα στοιχεία επικοινωνίας, τον ταξιδιωτικό πράκτορα μέσω του οποίου πραγματοποιήθηκε η κράτηση της πτήσης, τα μέσα πληρωμής που χρησιμοποιήθηκαν, τον αριθμό θέσης και πληροφορίες σχετικά με τις αποσκευές ⁷⁹³. Η επεξεργασία των δεδομένων PNR μπορεί να διευκολύνει τις αρχές επιβολής του νόμου στον εντοπισμό γνωστών ή πιθανών υπόπτων και στη διενέργεια αξιολογήσεων με βάση τα πρότυπα μετακινήσεων και άλλους δείκτες που συνδέονται συνήθως με εγκληματικές δραστηριότητες. Η ανάλυση

⁷⁹⁰ Συμβούλιο της Ευρώπης (1981), Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, CETS αριθ. 108.

⁷⁹¹ Συμβούλιο της Ευρώπης (2001), Πρόσθετο πρωτόκολλο της Σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα σχετικά με τις εποπτικές αρχές και τις διασυνοριακές ροές δεδομένων, CETS αριθ. 108.

⁷⁹² Συμβούλιο της Ευρώπης (1987), Σύσταση αριθ. R (87)15 της Επιτροπής Υπουργών προς τα κράτη μέλη που ρυθμίζουν τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα (εκδόθηκε από την Επιτροπή Υπουργών στις 17 Σεπτεμβρίου 1987, κατά την 410η συνεδρίαση των αντιπροσώπων των υπουργών).

⁷⁹³ Ευρωπαϊκή Επιτροπή (2011), Πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις με τα ονόματα των επιβατών (δεδομένα PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και άλλων σοβαρών εγκλημάτων, COM(2011) 32 τελικό, Βρυξέλλες, 2 Φεβρουαρίου 2011, σ. 1.

των δεδομένων PNR καθιστά επίσης δυνατή την αναδρομική παρακολούθηση των διαδρομών και των επαφών προσώπων για τα οποία υπάρχουν υπόνοιες ότι έχουν συμμετάσχει σε εγκληματικές δραστηριότητες, στοιχείο που μπορεί να διευκολύνει τις αρχές επιβολής του νόμου στον εντοπισμό εγκληματικών δικτύων ⁷⁹⁴. Όπως διευκρινίζεται στην **ενότητα 7**, η ΕΕ έχει συνάψει ορισμένες συμφωνίες με τρίτες χώρες για την ανταλλαγή δεδομένων PNR. Επιπλέον, έχει θεσπίσει την επεξεργασία δεδομένων PNR στο εσωτερικό της ΕΕ μέσω της οδηγίας 2016/681/ΕΕ σχετικά με τη χρήση των δεδομένων PNR για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων (οδηγία PNR της ΕΕ) ⁷⁹⁵. Η οδηγία αυτή επιβάλλει στους αερομεταφορείς την υποχρέωση να διαβιβάζουν δεδομένα PNR στις αρμόδιες αρχές και θεσπίζει αυστηρές εγγυήσεις για την προστασία των δεδομένων όσον αφορά την επεξεργασία και συλλογή των εν λόγω δεδομένων. Η οδηγία PNR της ΕΕ εφαρμόζεται σε διεθνείς πτήσεις προς και από την ΕΕ, καθώς και σε πτήσεις εντός της ΕΕ εάν ένα κράτος μέλος λάβει σχετική απόφαση ⁷⁹⁶.

Στα δεδομένα PNR που συλλέγονται πρέπει να περιλαμβάνονται μόνο οι πληροφορίες που επιτρέπονται βάσει της οδηγίας PNR της ΕΕ. Πρέπει δε να διατηρούνται σε μία και μόνη μονάδα στοιχείων, σε ασφαλή χώρο σε κάθε κράτος μέλος. Τα δεδομένα PNR πρέπει να ανωνυμοποιούνται μετά την παρέλευση έξι μηνών από τη διαβίβασή τους από τον αερομεταφορέα και να διατηρούνται για μέγιστη περίοδο πέντε ετών ⁷⁹⁷. Τα δεδομένα PNR ανταλλάσσονται μεταξύ των κρατών μελών, μεταξύ των κρατών μελών και της Ευρωπαϊκής, καθώς και με τρίτες χώρες, αλλά μόνο κατά περίπτωση.

Η διαβίβαση και επεξεργασία των δεδομένων PNR και η διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων πρέπει, αφενός, να συνάδουν με την οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης και, αφετέρου, να διασφαλίζουν το υψηλό επίπεδο προστασίας της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα που απαιτείται από τον Χάρτη, την Εκσυγχρονισμένη Σύμβαση 108 και την ΕΣΔΑ.

⁷⁹⁴ Ευρωπαϊκή Επιτροπή (2015), Ενημερωτικό δελτίο Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives, Βρυξέλλες, 11 Ιανουαρίου 2015.

⁷⁹⁵ **Οδηγία (ΕΕ) 2016/681** του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, σχετικά με τη χρήση των δεδομένων που περιέχονται στις καταστάσεις με τα ονόματα των επιβατών (PNR) για την πρόληψη, ανίχνευση, διερεύνηση και δίωξη τρομοκρατικών και σοβαρών εγκλημάτων (ΕΕ L 119 της 4.5.2016, σ. 132).

⁷⁹⁶ Οδηγία PNR (ΕΕ L 119 της 4.5.2016, σ. 132), άρθρο 1 παράγραφος 1 και άρθρο 2 παράγραφος 1.

⁷⁹⁷ Ό.π., άρθρο 12 παράγραφοι 1 και 2.

Οι ανεξάρτητες εθνικές εποπτικές αρχές οι οποίες είναι αρμόδιες βάσει της οδηγίας για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης είναι επίσης υπεύθυνες για την παροχή συμβουλών και την παρακολούθηση της εφαρμογής των διατάξεων που θεσπίζονται από τα κράτη μέλη δυνάμει της οδηγίας PNR της ΕΕ.

Διατήρηση δεδομένων τηλεπικοινωνιών

Η οδηγία για τη διατήρηση δεδομένων ⁷⁹⁸ –η οποία κηρύχθηκε ανίσχυρη στην απόφαση της 8ης Απριλίου 2014 στην υπόθεση *Digital Rights Ireland*– υποχρέωνε τους παρόχους υπηρεσιών επικοινωνιών να διατηρούν τα μεταδεδομένα διαθέσιμα για τον ειδικό σκοπό της καταπολέμησης του σοβαρού εγκλήματος για τουλάχιστον έξι αλλά όχι περισσότερους από 24 μήνες, ανεξάρτητα από το αν ο πάροχος εξακολουθούσε να χρειάζεται τα δεδομένα αυτά για σκοπούς τιμολόγησης ή για την παροχή της υπηρεσίας από τεχνική άποψη.

Η διατήρηση δεδομένων τηλεπικοινωνιών συνιστά καταφανή επέμβαση στο δικαίωμα προστασίας των δεδομένων ⁷⁹⁹. Το ερώτημα σχετικά με το αν η επέμβαση αυτή είναι αιτιολογημένη έχει αποτελέσει αντικείμενο πολλών δικαστικών διαδικασιών σε κράτη μέλη της ΕΕ ⁸⁰⁰.

Παράδειγμα: Στις υποθέσεις *Digital Rights Ireland* και *Kärntner Landesregierung κ.λπ.* ⁸⁰¹, η ομάδα Digital Rights και ο M. Seitlinger άσκησαν ενώπιον του ιρλανδικού Ανώτατου Δικαστηρίου και του αυστριακού συνταγματικού δικαστηρίου, αντίστοιχα, προσφυγή κατά της νομιμότητας των εθνικών μέτρων που επέτρεπαν τη διατήρηση δεδομένων ηλεκτρονικών τηλεπικοινωνιών. Η ομάδα Digital Rights ζήτησε από το

798 Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006, για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ (ΕΕ L 105 της 13.4.2006, σ. 54).

799 ΕΕΠΔ (2011), Γνωμοδότηση της 31ης Μαΐου 2011 σχετικά με την έκθεση αξιολόγησης της οδηγίας για τη διατήρηση δεδομένων (οδηγία 2006/24/ΕΚ) της Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο, 31 Μαΐου 2011.

800 Γερμανία, Ομοσπονδιακό Συνταγματικό Δικαστήριο (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 Μαρτίου 2010· Ρουμανία, Ομοσπονδιακό Συνταγματικό Δικαστήριο (*Curtea Constituțională a României*), αριθ. 1258, 8 Οκτωβρίου 2009· Τσεχική Δημοκρατία, Συνταγματικό Δικαστήριο (*Ústavní soud České republiky*), 94/2011 Coll., 22 Μαρτίου 2011.

801 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ.* και *Kärntner Landesregierung κ.λπ.* [Τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014, σκέψη 65.

ιρλανδικό δικαστήριο να κηρύξει ανίσχυρη την οδηγία 2006/24/EK και τις διατάξεις του εθνικού ποινικού δικαίου σχετικά με τα τρομοκρατικά εγκλήματα. Παρομοίως, ο κ. Seitlinger και περισσότεροι από 11 000 ακόμη προσφεύγοντες αμφισβήτησαν διάταξη της αυστριακής νομοθεσίας σχετικά με τις τηλεπικοινωνίες για τη μεταφορά της οδηγίας 2006/24/EK στο εθνικό δίκαιο και ζήτησαν την ακύρωσή της.

Στο πλαίσιο της εξέτασης των εν λόγω αιτήσεων έκδοσης προδικαστικής απόφασης, το ΔΕΕ κήρυξε ανίσχυρη την οδηγία για τη διατήρηση δεδομένων. Κατά το ΔΕΕ, τα δεδομένα που μπορούσαν να διατηρηθούν βάσει της οδηγίας παρείχαν, στο σύνολό τους, ακριβείς πληροφορίες σχετικά με φυσικά πρόσωπα. Επιπλέον, το ΔΕΕ εξέτασε τη σοβαρότητα της επέμβασης στα θεμελιώδη δικαιώματα του σεβασμού της ιδιωτικής ζωής και της προστασίας των δεδομένων προσωπικού χαρακτήρα. Έκρινε ότι η διατήρηση ανταποκρίνεται σε στόχο δημόσιου συμφέροντος, δηλαδή στην καταπολέμηση σοβαρού εγκλήματος και, συνεπώς, στη διαφύλαξη της δημόσιας ασφάλειας. Ωστόσο, το ΔΕΕ αποφάνθηκε ότι η έκδοση της οδηγίας συνιστούσε παραβίαση της αρχής της αναλογικότητας από τον νομοθέτη της ΕΕ. Παρότι η οδηγία μπορεί να είναι κατάλληλη για την επίτευξη του απαιτούμενου στόχου, «συνεπάγεται μια τεράστιας εκτάσεως και ιδιαιτέρως μεγάλης βαρύτητας στο πλαίσιο της έννομης τάξεως της Ένωσης επέμβαση σε αυτά τα θεμελιώδη δικαιώματα χωρίς η επέμβαση αυτή να οριοθετείται επακριβώς μέσω διατάξεων δυνάμενων να διασφαλίσουν ότι πράγματι περιορίζεται στον απολύτως αναγκαίο βαθμό».

Η διατήρηση δεδομένων επιτρέπεται, ελλείψει ειδικής νομοθεσίας σχετικά με τη διατήρηση δεδομένων, υπό τη μορφή εξαίρεσης από το απόρρητο των δεδομένων τηλεπικοινωνιών βάσει της οδηγίας 2002/58/EK (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)⁸⁰², ως προληπτικό μέτρο, αλλά αποκλειστικά και μόνο για τον σκοπό της καταπολέμησης σοβαρών μορφών εγκλήματος. Η εν λόγω διατήρηση πρέπει να περιορίζεται σε ό,τι είναι απολύτως αναγκαίο όσον αφορά τις κατηγορίες διατηρούμενων δεδομένων, τα χρησιμοποιούμενα μέσα επικοινωνίας, τα πρόσωπα των οποίων τα δεδομένα

⁸⁰² Οδηγία 2002/58/EK του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

διατηρούνται, καθώς και την επιλεγείσα διάρκεια της διατήρησης. Οι εθνικές αρχές μπορούν να έχουν πρόσβαση στα διατηρούμενα δεδομένα υπό αυστηρές προϋποθέσεις, συμπεριλαμβανομένου του προηγούμενου ελέγχου από ανεξάρτητη αρχή. Τα δεδομένα πρέπει να διατηρούνται εντός της ΕΕ.

Παράδειγμα: Μετά την έκδοση της απόφασης στις υποθέσεις *Digital Rights Ireland* και *Kärntner Landesregierung* κ.λπ.⁸⁰³, ασκήθηκαν ενώπιον του ΔΕΕ δύο ακόμη προσφυγές σε σχέση με τη γενική υποχρέωση που επέβαλλαν η Σουηδία και το Ηνωμένο Βασίλειο στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών να διατηρούν δεδομένα τηλεπικοινωνιών, κατ'εφαρμογή της οδηγίας για τη διατήρηση δεδομένων που κηρύχθηκε ανίσχυρη. Στις υποθέσεις *Tele2 Sverige* και *Home Department κατά Tom Watson* κ.λπ.⁸⁰⁴, το ΔΕΕ αποφάνθηκε ότι εθνική νομοθεσία η οποία επιβάλλει τη γενική και χωρίς διάκριση διατήρηση δεδομένων χωρίς να απαιτεί να υφίσταται σχέση μεταξύ των δεδομένων που πρέπει να διατηρούνται και κάποιας απειλής για τη δημόσια ασφάλεια, και χωρίς να προσδιορίζει τυχόν προϋποθέσεις –π.χ. χρονική περίοδος διατήρησης, γεωγραφική ζώνη, κύκλος προσώπων που θα μπορούσαν να είναι αναμειγνύμενοι σε κάποια σοβαρή παράβαση– υπερβαίνει τα όρια του απολύτως αναγκαίου και δεν μπορεί να θεωρηθεί δικαιολογημένη σε μια δημοκρατική κοινωνία όπως απαιτεί η οδηγία 2002/58/ΕΚ, ερμηνευόμενη υπό το πρίσμα του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Προοπτικές

Τον Ιανουάριο του 2017, η Ευρωπαϊκή Επιτροπή δημοσίευσε πρόταση κανονισμού για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες, με σκοπό την κατάργηση και αντικατάσταση της οδηγίας 2002/58/ΕΚ⁸⁰⁵. Στην πρόταση δεν περιλαμβάνονται

803 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources* κ.λπ. και *Kärntner Landesregierung* κ.λπ. [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

804 ΔΕΕ, συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, *Tele2 Sverige AB κατά Post- och telestyrelsen* και *Secretary of State for the Home Department κατά Tom Watson* κ.λπ. [τμήμα μείζονος συνθέσεως], 21 Δεκεμβρίου 2016.

805 Ευρωπαϊκή Επιτροπή (2017), πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), COM(2017) 10 final, Βρυξέλλες, 10 Ιανουαρίου 2017.

ειδικές διατάξεις σχετικά με τη διατήρηση δεδομένων. Ωστόσο, στην πρόταση κανονισμού ορίζεται ότι τα κράτη μέλη μπορούν να περιορίσουν δια νόμου ορισμένες υποχρεώσεις και δικαιώματα που προβλέπονται στον κανονισμό όταν ο περιορισμός αυτός συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για να διασφαλιστούν ειδικά δημόσια συμφέροντα, μεταξύ άλλων για σκοπούς εθνικής ασφάλειας, άμυνας, δημόσιας ασφάλειας και πρόληψης, διερεύνησης, ανίχνευσης και δίωξης ποινικών αδικημάτων ή εκτέλεσης ποινικών κυρώσεων ⁸⁰⁶. Ως εκ τούτου, τα κράτη μέλη μπορούν να διατηρήσουν ή να δημιουργήσουν εθνικά πλαίσια διατήρησης των δεδομένων τα οποία παρέχουν στοχευμένα μέτρα για τη διατήρηση, στον βαθμό που τα πλαίσια αυτά συμμορφώνονται με το δίκαιο της Ένωσης, λαμβάνοντας υπόψη τη νομολογία του ΔΕΕ όσον αφορά την ερμηνεία της οδηγίας για την προστασία της ιδιωτικής ζωής και τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ ⁸⁰⁷. Κατά τον χρόνο σύνταξης του παρόντος εγχειριδίου, οι συζητήσεις σχετικά με την έκδοση του κανονισμού βρίσκονταν σε εξέλιξη.

Συμφωνία-πλαίσιο ΕΕ-ΗΠΑ σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που ανταλλάσσονται για σκοπούς επιβολής του νόμου

Την 1η Φεβρουαρίου 2017 τέθηκε σε ισχύ η συμφωνία-πλαίσιο ΕΕ-ΗΠΑ για την επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό την πρόληψη, διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων από κοινού με τις ΗΠΑ ⁸⁰⁸. Στόχος της συμφωνίας-πλαίσιο ΕΕ-ΗΠΑ είναι να διασφαλιστεί υψηλό επίπεδο προστασίας των δεδομένων για τους πολίτες της ΕΕ, με παράλληλη ενίσχυση της συνεργασίας μεταξύ των αρχών επιβολής του νόμου της ΕΕ και των ΗΠΑ. Η συμφωνία αυτή συμπληρώνει τις υφιστάμενες συμφωνίες τόσο μεταξύ της ΕΕ και των ΗΠΑ όσο και μεταξύ των κρατών μελών και των ΗΠΑ, ενώ συμβάλλει παράλληλα στην εφαρμογή σαφών και εναρμονισμένων κανόνων προστασίας των δεδομένων για τη σύναψη μελλοντικών συμφωνιών στον συγκεκριμένο τομέα. Σε αυτό το πνεύμα, η συμφωνία αποσκοπεί στη δημιουργία ενός διαρκούς νομικού πλαισίου για τη διευκόλυνση της ανταλλαγής πληροφοριών.

⁸⁰⁶ Ό.π., αιτιολογική σκέψη 26.

⁸⁰⁷ Βλ. την αιτιολογική έκθεση της πρότασης κανονισμού για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες COM(2017) 10 final, σημείο 1.3.

⁸⁰⁸ Βλ. Συμβούλιο της ΕΕ (2016), «Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign ‘Umbrella agreement’», δελτίο Τύπου 305/16, 2 Ιουνίου 2016.

Η συμφωνία δεν παρέχει από μόνη της κατάλληλη νομική βάση για την ανταλλαγή δεδομένων προσωπικού χαρακτήρα· αντ' αυτού, προσφέρει στα ενδιαφερόμενα φυσικά πρόσωπα κατάλληλες εγγυήσεις για την προστασία των δεδομένων. Καλύπτει κάθε μορφή επεξεργασίας δεδομένων προσωπικού χαρακτήρα που είναι αναγκαία για την πρόληψη, διερεύνηση, ανίχνευση και δίωξη ποινικών αδικημάτων, συμπεριλαμβανομένης της τρομοκρατίας⁸⁰⁹.

Η συμφωνία ορίζει πολλαπλές διασφαλίσεις ώστε τα δεδομένα προσωπικού χαρακτήρα να χρησιμοποιούνται μόνο για τους σκοπούς που καθορίζονται στη συμφωνία. Ειδικότερα, προβλέπει τις ακόλουθες μορφές προστασίας για τους πολίτες της ΕΕ:

- περιορισμούς στη χρήση δεδομένων: τα δεδομένα προσωπικού χαρακτήρα μπορούν να χρησιμοποιούνται μόνο για σκοπούς πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων·
- προστασία έναντι αυθαίρετων και αδικαιολόγητων διακρίσεων·
- περαιτέρω διαβιβάσεις: κάθε περαιτέρω διαβίβαση σε χώρα εκτός ΗΠΑ, χώρα εκτός ΕΕ ή διεθνή οργανισμό πρέπει να υπόκειται στην προηγούμενη έγκριση της αρμόδιας αρχής της χώρας που διαβίβασε αρχικά τα δεδομένα·
- ποιότητα των δεδομένων: τα δεδομένα προσωπικού χαρακτήρα πρέπει να τηρούνται με τη δέουσα μέριμνα ώστε να είναι ακριβή, σχετικά, επίκαιρα και πλήρη·
- ασφάλεια της επεξεργασίας, συμπεριλαμβανομένης της γνωστοποίησης παραβιάσεων δεδομένων προσωπικού χαρακτήρα·
- η επεξεργασία ευαίσθητων δεδομένων επιτρέπεται μόνον εφόσον υπάρχουν κατάλληλες εγγυήσεις σύμφωνα με τον νόμο·

809 Συμφωνία μεταξύ των Ηνωμένων Πολιτειών της Αμερικής και της Ευρωπαϊκής Ένωσης σχετικά με την προστασία των πληροφοριών προσωπικού χαρακτήρα για την πρόληψη, τη διερεύνηση, την ανίχνευση και τη δίωξη ποινικών αδικημάτων της 18ης Μαΐου 2016 (OR.en) 8557/16, άρθρο 3 παράγραφος 1. Βλ. επίσης την κοινοποίηση της Επιτροπής της 26ης Μαΐου 2010 σχετικά με τις διαπραγματεύσεις για τη συμφωνία προστασίας δεδομένων ΕΕ-ΗΠΑ, MEMO/10/216 και το δελτίο Τύπου της Επιτροπής της 26ης Μαΐου 2010 για τη θέσπιση υψηλών κανόνων προστασίας της ιδιωτικής ζωής στη συμφωνία προστασίας δεδομένων ΕΕ-ΗΠΑ, IP/10/609.

- περίοδοι διατήρησης: τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα από ό,τι είναι αναγκαίο ή σκόπιμο·
- δικαιώματα πρόσβασης και διόρθωσης: κάθε άτομο έχει δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που το αφορούν, υπό ορισμένες προϋποθέσεις, και είναι σε θέση να ζητεί τη διόρθωση των δεδομένων εάν είναι ανακριβή·
- οι αυτοματοποιημένες αποφάσεις προϋποθέτουν κατάλληλες εγγυήσεις που περιλαμβάνουν τη δυνατότητα ανθρώπινης παρέμβασης·
- αποτελεσματική εποπτεία, συμπεριλαμβανομένης της συνεργασίας μεταξύ εποπτικών αρχών της ΕΕ και των ΗΠΑ· και
- δικαστική προσφυγή και εκτελεστότητα: οι πολίτες της ΕΕ έχουν το δικαίωμα ⁸¹⁰ να ασκούν δικαστική προσφυγή ενώπιον δικαστηρίων των ΗΠΑ σε περιπτώσεις στις οποίες οι αρχές των ΗΠΑ αρνούνται την πρόσβαση των πολιτών στα δεδομένα προσωπικού χαρακτήρα που τους αφορούν ή τη διόρθωση των δεδομένων αυτών ή προβαίνουν σε παράνομη κοινολόγησή τους.

Βάσει της συμφωνίας-πλαίσιου, δημιουργήθηκε επίσης σύστημα ενημέρωσης της αρμόδιας εποπτικής αρχής στο κράτος μέλος διαμονής των θιγόμενων φυσικών προσώπων σχετικά με τυχόν παραβιάσεις της προστασίας δεδομένων, όπου απαιτείται. Οι νομικές εγγυήσεις που προβλέπονται στη συμφωνία διασφαλίζουν την ίση μεταχείριση των πολιτών της ΕΕ στις ΗΠΑ σε περίπτωση παραβίασης της προστασίας της ιδιωτικής ζωής ⁸¹¹.

810 Ο αμερικανικός νόμος περί δικαστικής προσφυγής (*US Judicial Redress Act*) υπογράφηκε από τον πρόεδρο Obama στις 24 Φεβρουαρίου 2016.

811 Ο Ευρωπαϊός Επόπτης Προστασίας Δεδομένων εξέδωσε Γνωμοδότηση σχετικά με τη συμφωνία ΕΕ-ΗΠΑ συνιστώντας, μεταξύ άλλων, τις ακόλουθες προσαρμογές: 1) την προσθήκη της φράσης «για τους ειδικούς σκοπούς για τους οποίους διαβιβάζονται» στο άρθρο που αφορά τη διατήρηση των δεδομένων για διάστημα που δεν υπερβαίνει το αναγκαίο και σκόπιμο και 2) τον αποκλεισμό της μαζικής διαβίβασης δεδομένων ευαίσθητου χαρακτήρα, που μπορεί να είναι πιθανή. Βλ. Ευρωπαϊός Επόπτης Προστασίας Δεδομένων, *Γνωμοδότηση 1/2016, Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, παράγραφος 35.

8.3.1. Προστασία δεδομένων στις δικαστικές υπηρεσίες και στις υπηρεσίες επιβολής του νόμου της ΕΕ

Ευρωπαϊκή

Η Ευρωπαϊκή, ο οργανισμός επιβολής του νόμου της ΕΕ, έχει έδρα στη Χάγη, με εθνικές μονάδες της Ευρωπαϊκής (ENU) σε κάθε κράτος μέλος. Η Ευρωπαϊκή ιδρύθηκε το 1998· το σημερινό νομικό καθεστώς της ως θεσμικού οργάνου της ΕΕ βασίζεται στον κανονισμό για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (κανονισμός Ευρωπαϊκή)⁸¹². Σκοπός της Ευρωπαϊκής είναι να παρέχει συνδρομή στην πρόληψη και διερεύνηση του οργανωμένου εγκλήματος, της τρομοκρατίας και άλλων μορφών σοβαρού εγκλήματος, όπως παρατίθενται στο παράρτημα Ι του κανονισμού Ευρωπαϊκή, που επηρεάζουν δύο ή περισσότερα κράτη μέλη. Στο πλαίσιο αυτό, ανταλλάσσει πληροφορίες και λειτουργεί ως κόμβος πληροφόρησης της ΕΕ, παρέχοντας αναλύσεις πληροφοριών και αξιολογήσεις απειλών.

Για την επίτευξη των σκοπών της, η Ευρωπαϊκή έχει δημιουργήσει το σύστημα πληροφοριών Ευρωπαϊκή, το οποίο παρέχει στα κράτη μέλη μια βάση δεδομένων για την ανταλλαγή πληροφοριών και στοιχείων σχετικά με αξιόπινες πράξεις μέσω των αντίστοιχων ΕΝΥ. Το σύστημα πληροφοριών Ευρωπαϊκή μπορεί να χρησιμοποιείται για τη διάθεση δεδομένων που αφορούν πρόσωπα τα οποία είναι ύποπτα ή έχουν καταδικαστεί για διάπραξη αξιόπινης πράξης που εμπίπτει στην αρμοδιότητα της Ευρωπαϊκής ή πρόσωπα για τα οποία υπάρχουν πραγματικές ενδείξεις ότι πρόκειται να διαπράξουν τέτοια αξιόπινη πράξη. Η Ευρωπαϊκή και οι ΕΝΥ μπορούν να εισάγουν δεδομένα απευθείας στο σύστημα πληροφοριών της Ευρωπαϊκής και να ανακτούν δεδομένα από αυτό. Μόνο το μέρος που εισήγαγε τα δεδομένα στο σύστημα μπορεί να προβεί σε τροποποίηση, διόρθωση ή διαγραφή των δεδομένων αυτών. Πληροφορίες στην Ευρωπαϊκή μπορούν επίσης να παρέχουν φορείς της ΕΕ, τρίτες χώρες και διεθνείς οργανισμοί.

Η Ευρωπαϊκή μπορεί επίσης να εξασφαλίζει πληροφορίες, μεταξύ των οποίων δεδομένα προσωπικού χαρακτήρα, από διαθέσιμες στο κοινό πηγές, όπως το

⁸¹² Κανονισμός (ΕΕ) 2016/794 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαΐου 2016, για τον Οργανισμό της Ευρωπαϊκής Ένωσης για τη Συνεργασία στον Τομέα της Επιβολής του Νόμου (Ευρωπαϊκή) και την αντικατάσταση και κατάργηση των αποφάσεων του Συμβουλίου 2009/371/ΔΕΥ, 2009/934/ΔΕΥ, 2009/935/ΔΕΥ, 2009/936/ΔΕΥ και 2009/968/ΔΕΥ (ΕΕ L 135 της 24.5.2016, σ. 53).

διαδίκτυο. Οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε φορείς της ΕΕ επιτρέπονται μόνον εάν είναι αναγκαίες για την εκτέλεση του καθήκοντος της Ευρωπαϊκής ή του φορέα-αποδέκτη της ΕΕ. Οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες ή διεθνείς οργανισμούς επιτρέπονται μόνον εάν η Ευρωπαϊκή Επιτροπή αποφασίσει ότι η σχετική χώρα ή ο σχετικός διεθνής οργανισμός διασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων («απόφαση περί επάρκειας») ή εάν υπάρχει διεθνής συμφωνία ή συμφωνία συνεργασίας. Η Ευρωπαϊκή Επιτροπή μπορεί να λαμβάνει και να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα προερχόμενα από ιδιωτικούς φορείς και ιδιώτες, υπό την αυστηρή προϋπόθεση ότι τα δεδομένα αυτά διαβιβάζονται από ΕΝΥ σύμφωνα με την εθνική της νομοθεσία, από σημείο επαφής σε τρίτη χώρα ή από διεθνή οργανισμό, με τον οποίο υπάρχει παγιωμένη συνεργασία βάσει συμφωνίας συνεργασίας που επιτρέπει την ανταλλαγή δεδομένων προσωπικού χαρακτήρα, ή από αρχή τρίτης χώρας ή από διεθνή οργανισμό που υπόκειται σε απόφαση περί επάρκειας ή με τον οποίο η ΕΕ έχει συνάψει διεθνή συμφωνία. Οι ανταλλαγές πληροφοριών πραγματοποιούνται στο σύνολό τους μέσω της ασφαλούς εφαρμογής του δικτύου ανταλλαγής πληροφοριών (SIENA).

Στο πλαίσιο της Ευρωπαϊκής Ένωσης έχουν ιδρυθεί εξειδικευμένα κέντρα ως απόκριση στις νέες εξελίξεις. Το Ευρωπαϊκό Κέντρο για εγκλήματα στον κυβερνοχώρο ιδρύθηκε στους κόλπους της Ευρωπαϊκής Ένωσης το 2013⁸¹³. Το εν λόγω κέντρο λειτουργεί ως κόμβος πληροφόρησης της ΕΕ για τα εγκλήματα στον κυβερνοχώρο, ενώ συμβάλλει παράλληλα στην ταχύτερη αντίδραση σε περιπτώσεις ηλεκτρονικών εγκλημάτων, αναπτύσσει και αξιοποιεί ψηφιακές εγκληματολογικές ικανότητες και αναπτύσσει βέλτιστες πρακτικές διερεύνησης εγκλημάτων στον κυβερνοχώρο. Το κέντρο εστιάζει στα εγκλήματα στον κυβερνοχώρο τα οποία:

- διαπράττονται από οργανωμένες ομάδες με σκοπό να αποφέρουν τεράστια κέρδη, όπως η επιγραμμική απάτη·
- προκαλούν σοβαρές βλάβες στο θύμα, όπως η επιγραμμική σεξουαλική εκμετάλλευση παιδιών·
- επηρεάζουν βασικά συστήματα υποδομών και πληροφοριών στην ΕΕ.

813 Βλ. επίσης ΕΕΠΔ (2012), Γνωμοδότηση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων επί της ανακοίνωσης της Ευρωπαϊκής Επιτροπής προς το Συμβούλιο και το Ευρωπαϊκό Κοινοβούλιο σχετικά με την ίδρυση του ευρωπαϊκού κέντρου για εγκλήματα στον κυβερνοχώρο, Βρυξέλλες, 29 Ιουνίου 2012.

Το Ευρωπαϊκό Αντιτρομοκρατικό Κέντρο (ECTC) δημιουργήθηκε τον Ιανουάριο του 2016 με σκοπό την επιχειρησιακή στήριξη των κρατών μελών στις έρευνες που αφορούν τρομοκρατικά εγκλήματα. Διασταυρώνει επιχειρησιακά δεδομένα που συλλέγονται σε πραγματικό χρόνο με τα δεδομένα που έχει ήδη στη διάθεσή της η Ευρωπόλ, φέρνοντας άμεσα στο φως χρηματοοικονομικά στοιχεία, και αναλύει όλα τα διαθέσιμα στοιχεία της έρευνας με σκοπό να βοηθήσει στη διαμόρφωση δομημένης εικόνας για ένα τρομοκρατικό δίκτυο ⁸¹⁴.

Το Ευρωπαϊκό Κέντρο κατά της Παράνομης Διακίνησης Μεταναστών (EMSC) ιδρύθηκε τον Φεβρουάριο του 2016, κατόπιν συνεδρίασης του Συμβουλίου τον Νοέμβριο του 2015, με σκοπό τη στήριξη των κρατών μελών για την αντιμετώπιση και εξάρθρωση εγκληματικών δικτύων που εμπλέκονται στην παράνομη διακίνηση μεταναστών. Λειτουργεί ως κόμβος πληροφόρησης, παρέχοντας στήριξη στα γραφεία της περιφερειακής ειδικής ομάδας της ΕΕ στην Κατάνια (Ιταλία) και στον Πειραιά (Ελλάδα), τα οποία συνδράμουν τις εθνικές αρχές σε διάφορους τομείς, μεταξύ άλλων στην ανταλλαγή πληροφοριών, στις ποινικές έρευνες και στη δίωξη εγκληματικών δικτύων παράνομης διακίνησης ανθρώπων ⁸¹⁵.

Το καθεστώς προστασίας δεδομένων που διέπει τις δραστηριότητες της Ευρωπόλ είναι ενισχυμένο και βασίζεται στις αρχές του κανονισμού για την προστασία δεδομένων από τα όργανα της ΕΕ ⁸¹⁶, ενώ συνάδει επίσης με την οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, την Εκσυγχρονισμένη Σύμβαση 108 και τη σύσταση για τον αστυνομικό τομέα.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θυμάτων αξιόποινων πράξεων, μαρτύρων ή άλλων προσώπων που μπορούν να δώσουν πληροφορίες για αξιόποινες πράξεις, ή προσώπων ηλικίας κάτω των 18 ετών, επιτρέπεται εάν είναι απολύτως αναγκαία και αναλογική για την αποτροπή ή την καταπολέμηση αξιόποινων πράξεων αρμοδιότητας της Ευρωπόλ ⁸¹⁷. Η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα απαγορεύεται, εκτός εάν είναι απολύτως αναγκαία και αναλογική για την αποτροπή ή την καταπολέμηση αξιόποινων

814 Βλ. την [ιστοσελίδα για το ECTC](#) στον ιστότοπο της Ευρωπόλ.

815 Βλ. την [ιστοσελίδα για το EMSC](#) στον ιστότοπο της Ευρωπόλ.

816 Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

817 Κανονισμός Ευρωπόλ, άρθρο 30 παράγραφος 1.

πράξεων αρμοδιότητας της Ευρωπόλ και εάν τα δεδομένα αυτά συμπληρώνουν άλλα δεδομένα προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία από την Ευρωπόλ ⁸¹⁸. Και στις δύο αυτές περιπτώσεις, μόνο η Ευρωπόλ μπορεί να έχει πρόσβαση στα σχετικά δεδομένα ⁸¹⁹.

Η αποθήκευση δεδομένων επιτρέπεται μόνο για το χρονικό διάστημα που είναι αναγκαίο και αναλογικό και η συνέχισή της υπόκειται σε επανεξέταση ανά τριετία, ελλείψει της οποίας διαγράφονται αυτομάτως ⁸²⁰.

Η Ευρωπόλ επιτρέπεται, υπό ορισμένες προϋποθέσεις, να διαβιβάζει δεδομένα προσωπικού χαρακτήρα απευθείας σε φορέα της ΕΕ ή σε αρχή τρίτης χώρας ή σε διεθνή οργανισμό ⁸²¹. Όταν παραβιάσεις δεδομένων ενδέχεται να επηρεάσουν σοβαρά και αρνητικά τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, πρέπει να γνωστοποιούνται στα εν λόγω πρόσωπα χωρίς αδικαιολόγητη καθυστέρηση ⁸²². Σε επίπεδο κρατών μελών, ορίζεται εθνική εποπτική αρχή για την παρακολούθηση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από την Ευρωπόλ ⁸²³.

Ο ΕΕΠΔ είναι αρμόδιος για την παρακολούθηση και τη διασφάλιση της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από την Ευρωπόλ, καθώς και για παροχή συμβουλών προς την Ευρωπόλ και στα υποκείμενα των δεδομένων για κάθε θέμα που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Για τον σκοπό αυτόν, ο ΕΕΠΔ ενεργεί ως φορέας εξέτασης και διερεύνησης καταγγελιών, ενώ συνεργάζεται στενά με τις εθνικές εποπτικές αρχές ⁸²⁴. Ο ΕΕΠΔ και οι εθνικές εποπτικές αρχές θα συνεδριάζουν τουλάχιστον δύο φορές τον χρόνο στο πλαίσιο του συμβουλίου συνεργασίας, το οποίο έχει συμβουλευτικά καθήκοντα ⁸²⁵. Τα κράτη μέλη υποχρεούνται να ορίζουν δια νόμου μια εποπτική αρχή αρμόδια να ελέγχει τη νομιμότητα της διαβίβασης δεδομένων προσωπικού χαρακτήρα από το κράτος στην Ευρωπόλ, καθώς και τη νομιμότητα της ανάκτησης και κάθε κοινοποίησης δεδομένων προσωπικού

818 Ό.π., άρθρο 30 παράγραφος 2.

819 Ό.π., άρθρο 30 παράγραφος 3.

820 Ό.π., άρθρο 31.

821 Ό.π., άρθρο 24 και άρθρο 25, αντίστοιχα.

822 Ό.π., άρθρο 35.

823 Κανονισμός Ευρωπόλ, άρθρο 42.

824 Ό.π., άρθρο 43 και άρθρο 44.

825 Ό.π., άρθρο 45.

χαρακτήρα στην Ευρωπόλ από το κράτος μέλος ⁸²⁶. Τα κράτη μέλη απαιτείται επίσης να διασφαλίζουν τη δυνατότητα της εθνικής εποπτικής αρχής να ενεργεί εντελώς ανεξάρτητα κατά την εκτέλεση των καθηκόντων της δυνάμει του κανονισμού Ευρωπόλ ⁸²⁷. Για την εξακρίβωση της νομιμότητας της επεξεργασίας δεδομένων, τον αυτοέλεγχο των δραστηριοτήτων της και τη διασφάλιση της ακεραιότητας και ασφάλειας των δεδομένων, η Ευρωπόλ τηρεί καταχωρίσεις ή τεκμηριώσεις των δραστηριοτήτων επεξεργασίας δεδομένων που εκτελεί. Οι εν λόγω καταχωρίσεις περιέχουν πληροφορίες σχετικά με πράξεις επεξεργασίας που πραγματοποιούνται σε συστήματα αυτοματοποιημένης επεξεργασίας όσον αφορά τη συλλογή, τη μεταβολή, την εξέταση, τη γνωστοποίηση, τον συνδυασμό και τη διαγραφή δεδομένων προσωπικού χαρακτήρα ⁸²⁸.

Προσφυγές κατά των αποφάσεων του ΕΕΠΔ μπορούν να ασκηθούν ενώπιον του ΔΕΕ ⁸²⁹. Τα πρόσωπα που έχουν υποστεί ζημία λόγω παράνομης επεξεργασίας δεδομένων δικαιούνται αποζημίωση για τη ζημία που υπέστησαν, είτε από την Ευρωπόλ είτε από το υπεύθυνο κράτος μέλος, μέσω προσφυγής ενώπιον του ΔΕΕ, στην πρώτη περίπτωση, ή του αρμόδιου εθνικού δικαστηρίου, στη δεύτερη περίπτωση ⁸³⁰. Επιπλέον, μία εξειδικευμένη μικτή ομάδα κοινοβουλευτικού ελέγχου (ΜΟΚΕ) η οποία συστήνεται από κοινού από τα εθνικά κοινοβούλια και το Ευρωπαϊκό Κοινοβούλιο μπορεί να ελέγχει τις δραστηριότητες της Ευρωπόλ ⁸³¹. Κάθε πρόσωπο έχει δικαίωμα πρόσβασης σε οποιαδήποτε δεδομένα προσωπικού χαρακτήρα το αφορούν και ενδέχεται να έχει στην κατοχή της η Ευρωπόλ. Επιπλέον, έχει δικαίωμα να ζητήσει τον έλεγχο, τη διόρθωση ή τη διαγραφή των εν λόγω δεδομένων προσωπικού χαρακτήρα. Τα εν λόγω δικαιώματα ενδέχεται να υπόκεινται σε εξαιρέσεις και περιορισμούς.

826 Ό.π., άρθρο 42 παράγραφος 1.

827 Ό.π., άρθρο 42 παράγραφος 1.

828 Ό.π., άρθρο 40.

829 Ό.π., άρθρο 48.

830 Ό.π., άρθρο 50.

831 Ό.π., άρθρο 51.

Eurojust

Η Eurojust, η οποία ιδρύθηκε το 2002, είναι οργανισμός της ΕΕ με έδρα τη Χάγη. Προάγει τη δικαστική συνεργασία σε έρευνες και διώξεις σχετικά με περιπτώσεις σοβαρού εγκλήματος που αφορούν τουλάχιστον δύο κράτη μέλη⁸³². Η Eurojust είναι αρμόδια:

- να προωθεί και να βελτιώνει τον συντονισμό των ερευνών και των διώξεων μεταξύ των αρμόδιων αρχών των διαφόρων κρατών μελών·
- να διευκολύνει την εκτέλεση αιτήσεων και αποφάσεων δικαστικής συνεργασίας.

Τα καθήκοντα της Eurojust επιτελούνται από εθνικά μέλη. Κάθε κράτος μέλος διορίζει έναν δικαστή ή εισαγγελέα στην Eurojust, το καθεστώς του οποίου υπόκειται στο εθνικό δίκαιο και ο οποίος διαθέτει τις απαιτούμενες αρμοδιότητες για την εκτέλεση των αναγκαίων καθηκόντων που αποσκοπούν στην προώθηση και τη βελτίωση της δικαστικής συνεργασίας. Επιπλέον, τα εθνικά μέλη ενεργούν από κοινού ως συλλογικό όργανο για την εκτέλεση ειδικών καθηκόντων της Eurojust.

Η Eurojust δύναται να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα στο μέτρο που κρίνεται αναγκαίο για την επίτευξη των στόχων της. Ωστόσο, τα δεδομένα αυτά περιορίζονται σε συγκεκριμένες πληροφορίες που αφορούν πρόσωπα τα οποία είναι ύποπτα για διάπραξη ή συμμετοχή σε αξιόποινη πράξη ή πρόσωπα τα οποία έχουν καταδικαστεί για αξιόποινη πράξη που εμπίπτει στην αρμοδιότητα της Eurojust. Η Eurojust μπορεί επίσης να επεξεργάζεται ορισμένες πληροφορίες που αφορούν μάρτυρες ή θύματα αξιόποινων πράξεων οι οποίες εμπίπτουν στην αρμοδιότητά της⁸³³. Σε εξαιρετικές περιπτώσεις, η Eurojust μπο-

832 Συμβούλιο της Ευρωπαϊκής Ένωσης (2002), απόφαση 2002/187/ΔΕΥ του Συμβουλίου, της 28ης Φεβρουαρίου 2002, σχετικά με τη σύσταση της Eurojust προκειμένου να ενισχυθεί η καταπολέμηση των σοβαρών μορφών εγκλήματος (ΕΕ L 63 της 6.3.2002, σ. 1)· Συμβούλιο της Ευρωπαϊκής Ένωσης (2003), απόφαση 2003/659/ΔΕΥ του Συμβουλίου, της 18ης Ιουνίου 2003, για την τροποποίηση της απόφασης 2002/187/ΔΕΥ σχετικά με τη σύσταση της Eurojust προκειμένου να ενισχυθεί η καταπολέμηση των σοβαρών μορφών εγκλήματος (ΕΕ L 245 της 29.9.2003, σ. 44)· Συμβούλιο της Ευρωπαϊκής Ένωσης (2009), απόφαση 2009/426/ΔΕΥ του Συμβουλίου, της 16ης Δεκεμβρίου 2008, για την ενίσχυση της Eurojust και την τροποποίηση της απόφασης 2002/187/ΔΕΥ σχετικά με τη σύσταση της Eurojust προκειμένου να ενισχυθεί η καταπολέμηση των σοβαρών μορφών εγκλήματος (ΕΕ L 138 της 4.6.2009, σ. 14) (αποφάσεις Eurojust).

833 Ενοποιημένη έκδοση της απόφασης 2002/187/ΔΕΥ του Συμβουλίου, όπως τροποποιήθηκε με την απόφαση 2003/659/ΔΕΥ του Συμβουλίου και με την απόφαση 2009/426/ΔΕΥ του Συμβουλίου, άρθρο 15 παράγραφος 2.

ρεί να επεξεργάζεται, για περιορισμένο χρονικό διάστημα, ευρύτερα δεδομένα προσωπικού χαρακτήρα τα οποία αφορούν τις περιστάσεις μιας αξιόποινης πράξης, εάν αυτά συνδέονται άμεσα με τη διενεργούμενη έρευνα. Στο πλαίσιο των αρμοδιοτήτων της, η Eurojust μπορεί να συνεργάζεται με άλλα θεσμικά και λοιπά όργανα και οργανισμούς της ΕΕ και να ανταλλάσσει μαζί τους δεδομένα προσωπικού χαρακτήρα. Η Eurojust δύναται επίσης να συνεργάζεται και να ανταλλάσσει δεδομένα προσωπικού χαρακτήρα με τρίτες χώρες και οργανισμούς.

Όσον αφορά την προστασία δεδομένων, η Eurojust πρέπει να εγγυάται επίπεδο προστασίας τουλάχιστον ισοδύναμο με τις αρχές της Εκσυγχρονισμένης Σύμβασης 108 και τις μεταγενέστερες τροποποιήσεις της. Σε περιπτώσεις ανταλλαγής δεδομένων πρέπει να τηρούνται συγκεκριμένοι κανόνες και περιορισμοί, οι οποίοι καθορίζονται βάσει συμφωνίας ή ρύθμισης συνεργασίας κατ' εφαρμογή των αποφάσεων του Συμβουλίου για τη Eurojust και των κανόνων της Eurojust για την προστασία των δεδομένων προσωπικού χαρακτήρα⁸³⁴.

Στους κόλπους της Eurojust έχει συσταθεί ανεξάρτητη κοινή εποπτική αρχή (ΚΕΑ), η οποία είναι επιφορτισμένη με το καθήκον παρακολούθησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από την Eurojust. Τα φυσικά πρόσωπα έχουν δικαίωμα προσφυγής στην κοινή εποπτική αρχή εάν διατηρούν αμφιβολίες ως προς την απάντηση της Eurojust σε αίτημα πρόσβασης, διόρθωσης, κλειδώματος ή διαγραφής δεδομένων προσωπικού χαρακτήρα. Σε περίπτωση αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα από την Eurojust, η Eurojust ευθύνεται, σύμφωνα με το εθνικό δίκαιο του κράτους μέλους στο οποίο βρίσκεται η έδρα της (Κάτω Χώρες), για κάθε ζημία που υπέστη το υποκείμενο των δεδομένων.

Προοπτικές

Τον Ιούλιο του 2013 η Ευρωπαϊκή Επιτροπή υπέβαλε πρόταση κανονισμού για τη μεταρρύθμιση της Eurojust. Η πρόταση αυτή συνοδευόταν από πρόταση για τη σύσταση Ευρωπαϊκής Εισαγγελίας (βλ. κατωτέρω). Σκοπός του κανονισμού είναι ο εξορθολογισμός των καθηκόντων και της δομής ώστε να συνάδουν με τη Συνθήκη της Λισαβόνας. Επιπλέον, με τη μεταρρύθμιση επιδιώκεται ο σαφής διαχωρισμός μεταξύ των επιχειρησιακών καθηκόντων της Eurojust, τα οποία επιτελούνται από το συλλογικό όργανο της Eurojust, και των διοικητικών της καθηκόντων.

834 Κανόνες διαδικασίας του εσωτερικού κανονισμού της Eurojust για την επεξεργασία και την προστασία των δεδομένων προσωπικού χαρακτήρα (ΕΕ C 68 της 19.3.2005, σ. 1).

Με τον τρόπο αυτό, θα δοθεί επίσης στα κράτη μέλη η δυνατότητα να εστιάσουν περισσότερο στα επιχειρησιακά καθήκοντα. Θα συσταθεί νέο εκτελεστικό συμβούλιο, το οποίο θα συνδράμει το συλλογικό όργανο κατά την εκτέλεση διοικητικών καθηκόντων ⁸³⁵.

Ευρωπαϊκή Εισαγγελία

Τα κράτη μέλη έχουν αποκλειστική αρμοδιότητα όσον αφορά τη δίωξη των αξιόποινων πράξεων της απάτης και της μη ορθής εκτέλεσης του προϋπολογισμού της ΕΕ, οι οποίες ενδέχεται να έχουν επίσης διασυνοριακές επιπτώσεις. Η σημασία της διερεύνησης, δίωξης και παραπομπής των δραστών τέτοιων αξιόποινων πράξεων ενώπιον της δικαιοσύνης έχει αυξηθεί, δεδομένης ιδίως της συνεχιζόμενης οικονομικής κρίσης ⁸³⁶. Η Ευρωπαϊκή Επιτροπή εξέδωσε πρόταση κανονισμού σχετικά με τη σύσταση Ευρωπαϊκής Εισαγγελίας ⁸³⁷ με στόχο την καταπολέμηση των ποινικών αδικημάτων που θίγουν τα οικονομικά συμφέροντα της ΕΕ. Η Ευρωπαϊκή Εισαγγελία θα συσταθεί μέσω της διαδικασίας της ενισχυμένης συνεργασίας, η οποία επιτρέπει σε τουλάχιστον εννέα κράτη μέλη να καθιερώσουν ενισχυμένη συνεργασία σε έναν τομέα στον πλαίσιο των δομών της ΕΕ, χωρίς τη συμμετοχή των άλλων χωρών της ΕΕ ⁸³⁸. Το Βέλγιο, η Βουλγαρία, η Γαλλία, η Γερμανία, η Ελλάδα, η Εσθονία, η Ισπανία, η Κροατία, η Κύπρος, η Λετονία, η Λιθουανία, το Λουξεμβούργο, η Πορτογαλία, η Ρουμανία, η Σλοβενία, η Σλοβακία, η Τσεχική Δημοκρατία και η Φινλανδία συμμετέχουν όλες στην ενισχυμένη συνεργασία· η Αυστρία και η Ιταλία έχουν εκφράσει την πρόθεσή τους να συμμετάσχουν ⁸³⁹.

Η Ευρωπαϊκή Εισαγγελία θα είναι αρμόδια να διερευνά και να διώκει περιπτώσεις απάτης σε επίπεδο ΕΕ και άλλα αδικήματα που θίγουν τα οικονομικά συμφέροντα της ΕΕ, με σκοπό τον αποτελεσματικό συντονισμό των ερευνών και των

835 Βλ. την [ιστοσελίδα για την Eurojust](#) στον ιστότοπο της Ευρωπαϊκής Επιτροπής.

836 Βλ. Ευρωπαϊκή Επιτροπή (2013), Πρόταση κανονισμού του Συμβουλίου σχετικά με τη σύσταση της Ευρωπαϊκής Εισαγγελίας, COM(2013) 534 final, Βρυξέλλες, 17 Ιουλίου 2013, σ. 1 και την [ιστοσελίδα για την Ευρωπαϊκή Εισαγγελία](#) στον ιστότοπο της Επιτροπής.

837 Ευρωπαϊκή Επιτροπή (2013), Πρόταση κανονισμού του Συμβουλίου σχετικά με τη σύσταση της Ευρωπαϊκής Εισαγγελίας, COM(2013) 534 final, Βρυξέλλες, 17 Ιουλίου 2013.

838 Συνθήκη για τη λειτουργία της ΕΕ, άρθρο 86 παράγραφος 1 και άρθρο 329 παράγραφος 1.

839 Βλ. Συμβούλιο της Ευρωπαϊκής Ένωσης (2017), «*Είκοσι κράτη μέλη συμφωνούν στις λεπτομέρειες της σύστασης της Ευρωπαϊκής Εισαγγελίας (EPPO)*», δελτίο Τύπου, 8 Ιουνίου 2017.

διώξεων μεταξύ των διαφόρων εθνικών έννομων τάξεων και τη βελτίωση της χρήσης των πόρων και της ανταλλαγής πληροφοριών σε ευρωπαϊκό επίπεδο ⁸⁴⁰.

Επικεφαλής της Ευρωπαϊκής Εισαγγελίας θα είναι Ευρωπαίος Εισαγγελέας, ενώ σε κάθε κράτος μέλος θα έχει την έδρα του τουλάχιστον ένας εντεταλμένος Ευρωπαίος Εισαγγελέας, ο οποίος θα είναι επιφορτισμένος με τη διεκπεραίωση των ερευνών και των διώξεων στο συγκεκριμένο κράτος μέλος.

Στην πρόταση καθορίζονται ισχυρές εγγυήσεις για τη διασφάλιση των δικαιωμάτων των προσώπων που εμπλέκονται στις έρευνες της Ευρωπαϊκής Εισαγγελίας όπως προβλέπονται στο εθνικό δίκαιο, στο δίκαιο της ΕΕ και στον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ. Για μέτρα έρευνας που άπτονται κυρίως των θεμελιωδών δικαιωμάτων απαιτείται προηγούμενη έγκριση από εθνικό δικαστήριο ⁸⁴¹. Οι έρευνες της Ευρωπαϊκής Εισαγγελίας θα υπόκεινται σε δικαστικό έλεγχο από τα εθνικά δικαστήρια ⁸⁴².

Ο κανονισμός για την προστασία δεδομένων από τα όργανα της ΕΕ ⁸⁴³ θα εφαρμόζεται στην επεξεργασία διοικητικών δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από την Ευρωπαϊκή Εισαγγελία. Για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σχετικά με επιχειρησιακά θέματα, η Ευρωπαϊκή Εισαγγελία θα διαθέτει, όπως η Ευρώπη, ένα αυτόνομο καθεστώς προστασίας δεδομένων παρόμοιο με αυτό που διέπει τις δραστηριότητες της Ευρώπης και της Eurojust, δεδομένου ότι η άσκηση των καθηκόντων της Ευρωπαϊκής Εισαγγελίας θα περιλαμβάνει επεξεργασία δεδομένων προσωπικού χαρακτήρα σε συνεργασία με τις αρχές επιβολής του νόμου και δίωξης σε επίπεδο κρατών μελών. Ως εκ τούτου, οι κανόνες προστασίας δεδομένων που εφαρμόζονται στην Ευρωπαϊκή Εισαγγελία είναι σχεδόν πανομοιότυποι με τους κανόνες που προβλέπονται στην οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης. Σύμφωνα με την πρόταση για τη σύσταση της

840 Ευρωπαϊκή Επιτροπή (2013), Πρόταση κανονισμού του Συμβουλίου σχετικά με τη σύσταση της Ευρωπαϊκής Εισαγγελίας, COM(2013) 534 final, Βρυξέλλες, 17 Ιουλίου 2013, σ. 1 και σ. 51. Βλ. επίσης την ιστοσελίδα για την Ευρωπαϊκή Εισαγγελία στον ιστότοπο της Επιτροπής.

841 Ευρωπαϊκή Επιτροπή (2013), Πρόταση κανονισμού του Συμβουλίου σχετικά με τη σύσταση της Ευρωπαϊκής Εισαγγελίας, COM(2013) 534 final, Βρυξέλλες, 17 Ιουλίου 2013, άρθρο 26 παράγραφος 4.

842 Ο.π., άρθρο 36.

843 Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

Ευρωπαϊκής Εισαγγελίας, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνεται με τις αρχές της νομιμότητας και της αντικειμενικότητας, του περιορισμού του σκοπού, της ελαχιστοποίησης των δεδομένων, της ακρίβειας, της ακεραιότητας και της εμπιστευτικότητας. Η Ευρωπαϊκή Εισαγγελία πρέπει, στον βαθμό του εφικτού, να προβαίνει σε σαφή διάκριση μεταξύ των δεδομένων προσωπικού χαρακτήρα διαφορετικών κατηγοριών υποκειμένων δεδομένων, όπως είναι τα πρόσωπα που έχουν καταδικαστεί για ποινικό αδίκημα, τα πρόσωπα που είναι απλώς ύποπτα, τα θύματα και οι μάρτυρες. Επίσης, πρέπει να επιδιώκει να ελέγχει την ποιότητα των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται και να διακρίνει, στο μέτρο του δυνατού, τα δεδομένα προσωπικού χαρακτήρα που βασίζονται σε πραγματικά περιστατικά από τα δεδομένα προσωπικού χαρακτήρα που βασίζονται σε προσωπικές εκτιμήσεις.

Η πρόταση περιλαμβάνει διατάξεις σχετικά με τα δικαιώματα των υποκειμένων των δεδομένων, ειδικότερα τα δικαιώματα ενημέρωσης, πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν, διόρθωσης και διαγραφής των δεδομένων και περιορισμού της επεξεργασίας, ενώ προβλέπει ότι τα εν λόγω δικαιώματα μπορούν επίσης να ασκούνται έμμεσα, μέσω του ΕΕΠΔ. Επίσης ενσωματώνει τις αρχές της ασφάλειας της επεξεργασίας και της λογοδοσίας προβλέποντας την υποχρέωση της Ευρωπαϊκής Εισαγγελίας να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζει επίπεδο ασφάλειας κατάλληλο για τους κινδύνους που απορρέουν από την επεξεργασία, να τηρεί αρχεία όλων των δραστηριοτήτων επεξεργασίας και να προβαίνει πριν από την επεξεργασία σε εκτίμηση των επιπτώσεων στην προστασία των δεδομένων όταν ένα είδος επεξεργασίας (π.χ. επεξεργασία με χρήση νέων τεχνολογιών) είναι πιθανό να θέσει σε μεγάλο κίνδυνο τα δικαιώματα των προσώπων. Τέλος, η πρόταση προβλέπει τον διορισμό υπευθύνου προστασίας δεδομένων από το συλλογικό όργανο, ο οποίος πρέπει να μεριμνά δεόντως για όλα τα θέματα που αφορούν την προστασία δεδομένων προσωπικού χαρακτήρα και να διασφαλίζει τη συμμόρφωση της Ευρωπαϊκής Εισαγγελίας με την εφαρμοστέα νομοθεσία για την προστασία δεδομένων.

8.3.2. Προστασία δεδομένων στα κοινά συστήματα πληροφοριών σε επίπεδο ΕΕ

Πέραν της ανταλλαγής δεδομένων μεταξύ των κρατών μελών και της δημιουργίας εξειδικευμένων αρχών της ΕΕ για την πάταξη του διασυνοριακού εγκλήματος, όπως η Ευρωπόλ, η Eurojust και η Ευρωπαϊκή Εισαγγελία, έχουν

δημιουργηθεί διάφορα κοινά συστήματα πληροφοριών σε επίπεδο ΕΕ για τη διευκόλυνση της συνεργασίας και της ανταλλαγής δεδομένων μεταξύ των αρμόδιων εθνικών και ενωσιακών αρχών για καθορισμένους σκοπούς στους τομείς της προστασίας των συνόρων, της μετανάστευσης και του ασύλου, καθώς και των τελωνείων. Δεδομένου ότι ο χώρος Σένγκεν δημιουργήθηκε αρχικά μέσω διεθνούς συμφωνίας, η οποία είχε εφαρμογή ανεξάρτητα από το δίκαιο της ΕΕ, το Σύστημα Πληροφοριών Σένγκεν (SIS) αναπτύχθηκε από πολυμερείς συμφωνίες και ενσωματώθηκε κατόπιν στο δίκαιο της ΕΕ. Το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS), το Eurodac, το Eurosur και το τελωνειακό σύστημα πληροφοριών (CIS) δημιουργήθηκαν ως μέσα που διέπονται από το δίκαιο της ΕΕ.

Η εποπτεία των συστημάτων αυτών επιμερίζεται μεταξύ των εθνικών εποπτικών αρχών και του ΕΕΠΔ. Για τη διασφάλιση υψηλού επιπέδου προστασίας, οι αρχές αυτές συνεργάζονται στο πλαίσιο συντονιστικών ομάδων εποπτείας (SCG), οι οποίες είναι υπεύθυνες για τα ακόλουθα συστήματα ΤΠ μεγάλης κλίμακας: 1) Eurodac, 2) Σύστημα Πληροφοριών για τις Θεωρήσεις, 3) Σύστημα Πληροφοριών Σένγκεν, 4) Τελωνειακό Σύστημα Πληροφοριών και 5) Σύστημα Πληροφόρησης της Εσωτερικής Αγοράς ⁸⁴⁴. Οι συντονιστικές ομάδες εποπτείας συνεδριάζουν συνήθως δύο φορές ετησίως, υπό την προεδρία εκλεγμένου προέδρου, και εκδίδουν κατευθυντήριες γραμμές, συζητούν διασυνοριακές υποθέσεις ή θεσπίζουν κοινά πλαίσια επιθεωρήσεων.

Ο Ευρωπαϊκός Οργανισμός για τα Συστήματα ΤΠ Μεγάλης Κλίμακας (eu-LISA) ⁸⁴⁵, ο οποίος ιδρύθηκε το 2012, είναι υπεύθυνος για τη λειτουργική διαχείριση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II), του Συστήματος Πληροφοριών για τις Θεωρήσεις (VIS) και του Eurodac. Βασικό καθήκον του eu-LISA είναι να εξασφαλίζει την ουσιαστική, ασφαλή και συνεχή λειτουργία των συστημάτων τεχνολογίας πληροφοριών. Επίσης, είναι υπεύθυνος για τη λήψη των αναγκαίων μέτρων για την ασφάλεια των συστημάτων και την ασφάλεια των δεδομένων.

844 Βλ. την [ιστοσελίδα για τον συντονισμό της εποπτείας](#) στον ιστότοπο του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων.

845 Κανονισμός (ΕΕ) αριθ. 1077/2011 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Οκτωβρίου 2011, σχετικά με την ίδρυση Ευρωπαϊκού Οργανισμού για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης, ΕΕ L 286 της 1.11.2011, σ. 1.

Το Σύστημα Πληροφοριών Σένγκεν

Το 1985 διάφορα κράτη μέλη της τότε Ευρωπαϊκής Κοινότητας προσχώρησαν στη συμφωνία που είχαν συνάψει τα κράτη της Οικονομικής Ένωσης Μπενελούξ, η Γερμανία και η Γαλλία για τη σταδιακή κατάργηση των ελέγχων στα κοινά τους σύνορα (συμφωνία Σένγκεν), με στόχο τη δημιουργία ενός χώρου ελεύθερης κυκλοφορίας των προσώπων, χωρίς συνοριακούς ελέγχους στο έδαφος Σένγκεν⁸⁴⁶. Για να αντισταθμιστεί η απειλή που θα μπορούσε να προκύψει για τη δημόσια ασφάλεια από τα ανοικτά σύνορα, καθιερώθηκαν ενισχυμένοι συνοριακοί έλεγχοι στα εξωτερικά σύνορα του χώρου Σένγκεν, καθώς και στενή συνεργασία μεταξύ των εθνικών αστυνομικών και δικαστικών αρχών.

Ως αποτέλεσμα της προσχώρησης και άλλων κρατών στη συμφωνία Σένγκεν, το σύστημα Σένγκεν ενσωματώθηκε εντέλει στο νομικό πλαίσιο της ΕΕ με τη Συνθήκη του Άμστερνταμ⁸⁴⁷. Η απόφαση αυτή τέθηκε σε εφαρμογή το 1999. Η πιο πρόσφατη έκδοση του Συστήματος Πληροφοριών Σένγκεν, το αποκαλούμενο SIS II, τέθηκε σε λειτουργία στις 9 Απριλίου 2013. Εξυπηρετεί πλέον τα περισσότερα κράτη μέλη της ΕΕ⁸⁴⁸, καθώς και την Ελβετία, την Ισλανδία, το Λιχτενστάιν και τη Νορβηγία⁸⁴⁹. Στο SIS II έχουν επίσης πρόσβαση η Ευρωπόλ και η Eurojust.

Το SIS II απαρτίζεται από ένα κεντρικό σύστημα (C-SIS), ένα εθνικό σύστημα (N-SIS) σε κάθε κράτος μέλος και μια επικοινωνιακή υποδομή που συνδέει το κεντρικό σύστημα με τα εθνικά συστήματα. Το C-SIS περιέχει ορισμένα δεδομένα που καταχωρίζονται από τα κράτη μέλη σχετικά με πρόσωπα και αντικείμενα. Το SIS χρησιμοποιείται από τις εθνικές αρχές συνοριακών ελέγχων, τις αστυνομικές

846 Συμφωνία μεταξύ των κυβερνήσεων του Βασιλείου του Βελγίου, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας, της Γαλλικής Δημοκρατίας, του Μεγάλου Δουκάτου του Λουξεμβούργου και του Βασιλείου των Κάτω Χωρών σχετικά με τη σταδιακή κατάργηση των ελέγχων στα κοινά σύνορα (ΕΕ L 239 της 22.9.2000, σ. 13).

847 Ευρωπαϊκές Κοινότητες (1997), Συνθήκη του Άμστερνταμ που τροποποιεί τη Συνθήκη για την Ευρωπαϊκή Ένωση, τις Συνθήκες περί ιδρύσεως των Ευρωπαϊκών Κοινοτήτων και ορισμένες συναφείς πράξεις (ΕΕ C 340 της 10.11.1997, σ. 1).

848 Η Ιρλανδία, η Κροατία και η Κύπρος βρίσκονται στο στάδιο των προπαρασκευαστικών εργασιών για την ένταξή τους στο SIS II, αλλά δεν έχουν προσχωρήσει ακόμη σε αυτό. Βλ. τις πληροφορίες σχετικά με το Σύστημα Πληροφοριών Σένγκεν που διατίθενται στον ιστότοπο της Γενικής Διεύθυνσης Μετανάστευσης και Εσωτερικών Υποθέσεων της Ευρωπαϊκής Επιτροπής.

849 Κανονισμός (ΕΚ) αριθ. 1987/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Δεκεμβρίου 2006, σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (ΕΕ L 381 της 28.12.2006, σ. 4) (SIS II) και Συμβούλιο της Ευρωπαϊκής Ένωσης (2007), απόφαση 2007/533/ΔΕΥ του Συμβουλίου, της 12ης Ιουνίου 2007, σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) (ΕΕ L 205 της 7.8.2007, σ. 63).

αρχές, τις τελωνειακές αρχές, τις αρχές θεωρήσεων και τις δικαστικές αρχές σε ολόκληρο τον χώρο Σένγκεν. Σε κάθε κράτος μέλος λειτουργεί εθνικό αντίγραφο του C-SIS, τα αποκαλούμενα εθνικά τμήματα του Συστήματος Πληροφοριών Σένγκεν (N-SIS), τα οποία επικαιροποιούνται συνεχώς και επικαιροποιούν με τη σειρά τους το C-SIS. Υπάρχουν διάφορα είδη καταχωρίσεων στο SIS:

- πρόσωπο το οποίο δεν έχει δικαίωμα εισόδου ή διαμονής στην επικράτεια Σένγκεν· ή
- πρόσωπο ή αντικείμενο το οποίο αναζητείται από τις δικαστικές αρχές ή τις αρχές επιβολής του νόμου (π.χ. ευρωπαϊκά εντάλματα σύλληψης, αιτήσεις διακριτικής παρακολούθησης)· ή
- το πρόσωπο το οποίο έχει αναφερθεί ως εξαφανισθέν· ή
- αντικείμενα, όπως τραπεζογραμμάτια, αυτοκίνητα, ημιφορτηγά, πυροβόλα όπλα και έγγραφα ταυτότητας, τα οποία έχουν αναφερθεί ως κλαπέντα ή απολεσθέντα.

Όταν υπάρχει καταχώριση, πρέπει να δρομολογούνται επακόλουθες δραστηριότητες μέσω των γραφείων SIRENE. Το SIS II διαθέτει νέες λειτουργικές δυνατότητες, όπως η δυνατότητα εισαγωγής βιομετρικών δεδομένων, π.χ. δακτυλικά αποτυπώματα και φωτογραφίες, νέων κατηγοριών καταχωρίσεων, π.χ. κλαπέντα πλοία, αεροσκάφη, εμπορευματοκιβώτια ή μέσα πληρωμής, αναβαθμισμένων καταχωρίσεων για πρόσωπα και αντικείμενα, καθώς και αντιγράφων ευρωπαϊκών ενταλμάτων σύλληψης προσώπων τα οποία καταζητούνται με σκοπό τη σύλληψη, την παράδοση ή την έκδοση.

Το SIS II βασίζεται σε δύο πράξεις που αλληλοσυμπληρώνονται: στην απόφαση SIS II ⁸⁵⁰ και στον κανονισμό SIS II ⁸⁵¹. Ο νομοθέτης της ΕΕ χρησιμοποίησε διαφορετική νομική βάση για την έκδοση της απόφασης και του κανονισμού. Η απόφαση διέπει τη χρήση του SIS II για σκοπούς που καλύπτονται από την αστυνομική και δικαστική συνεργασία σε ποινικές υποθέσεις (ο πρώην τρίτος πυλώνας της ΕΕ).

850 Απόφαση 2007/533/ΔΕΥ του Συμβουλίου, της 12ης Ιουνίου 2007, σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) (ΕΕ L 205 της 7.8.2007, σ. 63).

851 Κανονισμός (ΕΚ) αριθ. 1987/2006 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 20ής Δεκεμβρίου 2006, σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) (ΕΕ L 381 της 28.12.2006, σ. 4).

Ο κανονισμός εφαρμόζεται στις διαδικασίες καταχώρισης που εμπίπτουν στις πολιτικές για τις θεωρήσεις, το άσυλο και τη μετανάστευση, καθώς και σε άλλες πολιτικές που συνδέονται με την ελεύθερη κυκλοφορία των προσώπων (ο πρώην πρώτος πυλώνας). Οι διαδικασίες καταχώρισης για κάθε πυλώνα πρέπει να ρυθμίζονται από χωριστές πράξεις, δεδομένου ότι οι δύο νομικές πράξεις εκδόθηκαν πριν από τη Συνθήκη της Λισαβόνας και την κατάργηση της δομής των πυλώνων.

Και οι δύο νομικές πράξεις περιλαμβάνουν κανόνες σχετικά με την προστασία δεδομένων. Η απόφαση SIS II απαγορεύει την επεξεργασία ευαίσθητων δεδομένων⁸⁵². Η επεξεργασία δεδομένων προσωπικού χαρακτήρα καλύπτεται από το πεδίο εφαρμογής της Εκσυγχρονισμένης Σύμβασης 108⁸⁵³. Επιπλέον, τα πρόσωπα έχουν το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και είναι καταχωρισμένα στο SIS II⁸⁵⁴.

Ο κανονισμός SIS II ρυθμίζει τις προϋποθέσεις και τις διαδικασίες για την εισαγωγή και επεξεργασία των καταχωρίσεων σχετικά με τις απαγορεύσεις εισόδου ή διαμονής πολιτών χωρών εκτός ΕΕ. Επίσης, προβλέπει κανόνες για την ανταλλαγή συμπληρωματικών και πρόσθετων πληροφοριών για τους σκοπούς της εισόδου ή της διαμονής σε ένα κράτος μέλος⁸⁵⁵. Ο εν λόγω κανονισμός περιλαμβάνει επίσης κανόνες σχετικά με την προστασία δεδομένων. Δεν επιτρέπεται η επεξεργασία ευαίσθητων κατηγοριών δεδομένων, όπως αναφέρονται στο άρθρο 9 παράγραφος 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων⁸⁵⁶. Ο κανονισμός SIS II περιλαμβάνει επίσης ορισμένα δικαιώματα του υποκειμένου των δεδομένων, τα οποία είναι τα εξής:

- το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που αφορούν το υποκείμενο των δεδομένων⁸⁵⁷.
- το δικαίωμα διόρθωσης πραγματικά ανακριβών δεδομένων⁸⁵⁸.
- το δικαίωμα διαγραφής δεδομένων που αποθηκεύτηκαν παράνομα⁸⁵⁹ και

852 Απόφαση SIS II, άρθρο 56· κανονισμός SIS II, άρθρο 40.

853 Απόφαση SIS II, άρθρο 57.

854 Απόφαση SIS II, άρθρο 58· κανονισμός SIS II, άρθρο 41.

855 Κανονισμός SIS II, άρθρο 2.

856 Ό.π., άρθρο 40.

857 Ό.π., άρθρο 41 παράγραφος 1.

858 Ό.π., άρθρο 41 παράγραφος 5.

859 Ό.π., άρθρο 41 παράγραφος 5.

- το δικαίωμα ενημέρωσης εάν εισαχθεί καταχώριση που αφορά το υποκείμενο των δεδομένων. Η σχετική ενημέρωση παρέχεται γραπτώς συνοδευόμενη από αντίγραφο ή μνεία της εθνικής απόφασης βάσει της οποίας εκδόθηκε η καταχώριση ⁸⁶⁰.

Το δικαίωμα ενημέρωσης δεν παρέχεται εάν 1) τα δεδομένα προσωπικού χαρακτήρα δεν έχουν ληφθεί από το υποκείμενο των δεδομένων και η παροχή της εν λόγω ενημέρωσης είναι αδύνατη ή απαιτεί δυσανάλογη προσπάθεια, 2) το υποκείμενο των δεδομένων έχει ήδη στην κατοχή του τις πληροφορίες ή 3) σύμφωνα με την εθνική νομοθεσία, προβλέπεται περιορισμός με γνώμονα, μεταξύ άλλων, τη διαφύλαξη της εθνικής ασφάλειας ή την πρόληψη αξιόποινων πράξεων ⁸⁶¹.

Τόσο η απόφαση SIS II όσο και ο κανονισμός SIS II προβλέπουν ότι τα δικαιώματα πρόσβασης των προσώπων σε δεδομένα του SIS II μπορούν να ασκούνται σε οποιοδήποτε κράτος μέλος και διέπονται από την εθνική νομοθεσία του εκάστοτε κράτους μέλους ⁸⁶².

Παράδειγμα: Στην υπόθεση *Dalea κατά Γαλλίας* ⁸⁶³, η αίτηση του προσφεύγοντος για χορήγηση θεώρησης προκειμένου να επισκεφθεί τη Γαλλία απορρίφθηκε, διότι οι γαλλικές αρχές είχαν καταχωρίσει στο Σύστημα Πληροφοριών Σένγκεν ότι δεν έπρεπε να του επιτραπεί η είσοδος. Ο προσφεύγων υπέβαλε ανεπιτυχώς αίτηση πρόσβασης και διόρθωσης ή διαγραφής των δεδομένων ενώπιον της γαλλικής επιτροπής προστασίας δεδομένων και, εντέλει, ενώπιον του Συμβουλίου της Επικρατείας. Το ΕΔΔΑ αποφάνθηκε ότι η καταχώριση του προσφεύγοντος στο Σύστημα Πληροφοριών Σένγκεν ήταν σύμφωνη με τον νόμο και επιδίωκε τον θεμιτό σκοπό της προστασίας της εθνικής ασφάλειας. Δεδομένου ότι ο προσφεύγων δεν απέδειξε επακριβώς τι είδους βλάβη είχε υποστεί ζημία λόγω της άρνησης εισόδου στον χώρο Σένγκεν, και δεδομένου ότι είχαν ληφθεί επαρκή μέτρα για την προστασία του έναντι αυθαίρετων αποφάσεων, η επέμβαση στο δικαίωμά σεβασμού της ιδιωτικής ζωής του ήταν αναλογική. Ως εκ τούτου, η αιτίαση του προσφεύγοντος δυνάμει του άρθρου 8 κηρύχθηκε απαράδεκτη.

860 Ό.π., άρθρο 42 παράγραφος 1.

861 Ό.π., άρθρο 42 παράγραφος 2.

862 Κανονισμός SIS II, άρθρο 41 παράγραφος 1 και απόφαση SIS II, άρθρο 58.

863 ΕΔΔΑ, *Dalea κατά Γαλλίας*, προσφυγή αριθ. 964/07, 2 Φεβρουαρίου 2010.

Η αρμόδια εθνική εποπτική αρχή σε κάθε κράτος μέλος εποπτεύει το οικείο N-SIS. Η εθνική εποπτική αρχή πρέπει να μεριμνά ώστε να διενεργείται, τουλάχιστον ανά τετραετία, έλεγχος των λειτουργιών επεξεργασίας δεδομένων που επιτελούνται στο οικείο N-SIS ⁸⁶⁴. Οι εθνικές εποπτικές αρχές και ο ΕΕΠΔ συνεργάζονται και διασφαλίζουν τη συντονισμένη εποπτεία του N-SIS, ενώ ο ΕΕΠΔ είναι υπεύθυνος για την εποπτεία του C-SIS. Για λόγους διαφάνειας, διαβιβάζεται ανά διετία κοινή έκθεση δραστηριοτήτων στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Επιτροπή και στον eu-LISA. Για τη διασφάλιση του συντονισμού της εποπτείας του SIS έχει συσταθεί συντονιστική ομάδα εποπτείας (SCG) του SIS II, η οποία συνεδριάζει δύο φορές ετησίως. Η ομάδα αυτή απαρτίζεται από τον ΕΕΠΔ και εκπροσώπους των εποπτικών αρχών των κρατών μελών που έχουν θέσει σε εφαρμογή το SIS II, καθώς και της Ελβετίας, της Ισλανδίας, του Λιχτενστάιν και της Νορβηγίας, δεδομένου ότι το SIS εφαρμόζεται επίσης στις εν λόγω χώρες διότι είναι μέλη του χώρου Σένγκεν ⁸⁶⁵. Η Ιρλανδία, η Κροατία και η Κύπρος δεν έχουν ενταχθεί ακόμη στο σύστημα SIS και, ως εκ τούτου, συμμετέχουν μόνον ως παρατηρητές στη συντονιστική ομάδα εποπτείας. Στο πλαίσιο της συντονιστικής ομάδας εποπτείας, ο ΕΕΠΔ και οι εθνικές εποπτικές αρχές συνεργάζονται ενεργά, ανταλλάσσοντας πληροφορίες, παρέχοντας αμοιβαία συνδρομή στη διενέργεια ελέγχων και επιθεωρήσεων, καταρτίζοντας εναρμονισμένες προτάσεις για κοινές λύσεις σε πιθανά προβλήματα και προάγοντας την ευαισθητοποίηση του κοινού όσον αφορά τα δικαιώματα τους στην προστασία δεδομένων ⁸⁶⁶. Η συντονιστική ομάδα εποπτείας του SIS II εκδίδει επίσης κατευθυντήριες γραμμές για την παροχή συνδρομής στα υποκείμενα των δεδομένων. Παράδειγμα αποτελεί ο οδηγός για την παροχή βοήθειας στα υποκείμενα των δεδομένων κατά την άσκηση των δικαιωμάτων πρόσβασης ⁸⁶⁷.

864 Κανονισμός SIS II, άρθρο 60 παράγραφος 2.

865 Βλ. την ιστοσελίδα για το Σύστημα Πληροφοριών Σένγκεν στον ιστότοπο του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων.

866 Κανονισμός SIS II, άρθρο 46 και απόφαση SIS II, άρθρο 62.

867 Βλ. Συντονιστική ομάδα εποπτείας (SCG) του SIS II, *The Schengen Information System. A guide for exercising the right of access*, που διατίθεται στον ιστότοπο του ΕΕΠΔ.

Προοπτικές

Το 2016 η Ευρωπαϊκή Επιτροπή προέβη σε αξιολόγηση του SIS ⁸⁶⁸, από την οποία προέκυψε ότι έχουν τεθεί σε εφαρμογή εθνικοί μηχανισμοί οι οποίοι παρέχουν στα πρόσωπα στα οποία αναφέρονται τα δεδομένα τη δυνατότητα να ζητούν πρόσβαση, διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα που τα αφορούν στο SIS II ή την καταβολή αποζημίωσης εξαιτίας εσφαλμένων δεδομένων. Για τη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας του SIS II, η Ευρωπαϊκή Επιτροπή υπέβαλε τρεις προτάσεις κανονισμών:

- Κανονισμός σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του SIS στον τομέα των συνοριακών ελέγχων, ο οποίος θα καταργήσει τον κανονισμό SIS II·
- Κανονισμός σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του SIS στον τομέα της αστυνομικής συνεργασίας και της δικαστικής συνεργασίας σε ποινικές υποθέσεις, ο οποίος θα καταργήσει, μεταξύ άλλων, την απόφαση SIS II· και
- Κανονισμός σχετικά με τη χρήση του SIS για την επιστροφή των παρانونώς διαμενόντων υπηκόων τρίτων χωρών.

Είναι σημαντικό να αναφερθεί ότι οι συγκεκριμένες προτάσεις επιτρέπουν την επεξεργασία άλλων κατηγοριών βιομετρικών δεδομένων –πέραν των φωτογραφιών και των δακτυλικών αποτυπωμάτων, που αποτελούν ήδη μέρος του υφιστάμενου καθεστώτος του SIS II. Στη βάση δεδομένων του SIS II θα αποθηκεύονται επίσης εικόνες προσώπου, αποτυπώματα παλάμης και προφίλ DNA. Επιπλέον, ενώ ο κανονισμός SIS II και η απόφαση SIS II προέβλεπαν τη δυνατότητα αναζήτησης με χρήση δακτυλικών αποτυπωμάτων για την ταυτοποίηση προσώπου, οι προτάσεις καθιστούν την αναζήτηση αυτή υποχρεωτική εάν δεν είναι δυνατή η εξακρίβωση της ταυτότητας του προσώπου με άλλον τρόπο. Εικόνες προσώπου, φωτογραφίες και αποτυπώματα παλάμης θα χρησιμοποιούνται για την αναζήτηση στο σύστημα και την ταυτοποίηση προσώπων, όταν αυτό καταστεί τεχνικά εφικτό. Οι νέοι κανόνες για τα βιομετρικά στοιχεία συνεπάγονται ιδιαίτερους

868 Ευρωπαϊκή Επιτροπή (2016), Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο σχετικά με την αξιολόγηση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) σύμφωνα με το άρθρο 24 παράγραφος 5, το άρθρο 43 παράγραφος 3 και το άρθρο 50 παράγραφος 5 του κανονισμού (ΕΚ) αριθ. 1987/2006 και με το άρθρο 59 παράγραφος 3 και το άρθρο 66 παράγραφος 5 της απόφασης 2007/533/ΔΕΥ, COM(2016) 880 final, Βρυξέλλες, 21 Δεκεμβρίου 2016.

κινδύνους για τα δικαιώματα των ατόμων. Στη γνωμοδότησή του σχετικά με τις προτάσεις της Επιτροπής ⁸⁶⁹, ο ΕΕΠΔ επισήμανε ότι τα βιομετρικά δεδομένα είναι ιδιαίτερα ευαίσθητα και ότι η εισαγωγή τους σε μια τόσο μεγάλης κλίμακας βάση δεδομένων θα πρέπει να βασιστεί σε μια αξιολόγηση της ανάγκης καταχώρισής τους στο SIS, βασισμένη σε αποδεικτικά στοιχεία. Με άλλα λόγια, η ανάγκη επεξεργασίας των νέων στοιχείων θα πρέπει να αποδεικνύεται. Ο ΕΕΠΔ έκρινε επίσης ότι πρέπει να διευκρινιστεί περαιτέρω το είδος των πληροφοριών που μπορούν να περιλαμβάνονται στο προφίλ DNA. Δεδομένου ότι το προφίλ DNA μπορεί να περιλαμβάνει ευαίσθητες πληροφορίες (με πλέον αξιοσημείωτο παράδειγμα τις πληροφορίες που αποκαλύπτουν προβλήματα υγείας), τα προφίλ DNA που αποθηκεύονται στο SIS θα πρέπει να περιλαμβάνουν: «μόνο τις ελάχιστες πληροφορίες που είναι αυστηρά αναγκαίες για την ταυτοποίηση των εξαφανισθέντων προσώπων και να αποκλείουν ρητά πληροφορίες που αφορούν την υγεία και τη φυλετική καταγωγή, καθώς και κάθε άλλη ευαίσθητη πληροφορία» ⁸⁷⁰. Ωστόσο, οι προτάσεις θεσπίζουν πρόσθετες διασφαλίσεις για τον περιορισμό της συλλογής και της περαιτέρω επεξεργασίας δεδομένων στον απολύτως αναγκαίο βαθμό από λειτουργική άποψη και για τον περιορισμό της πρόσβασης στα δεδομένα αυτά μόνο στα πρόσωπα τα οποία πρέπει να τα επεξεργάζονται για επιχειρησιακούς λόγους ⁸⁷¹. Επιπλέον, σύμφωνα με τις προτάσεις, ο eu-LISA εξουσιοδοτείται να εκδίδει ανά τακτά χρονικά διαστήματα εκθέσεις για τα κράτη μέλη όσον αφορά την ποιότητα των δεδομένων, προκειμένου να πραγματοποιείται τακτικός έλεγχος των καταχωρίσεων με σκοπό τη διασφάλιση της ποιότητας των δεδομένων ⁸⁷².

Σύστημα Πληροφοριών για τις Θεωρήσεις

Το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS), το οποίο επίσης διαχειρίζεται ο eu-LISA, αναπτύχθηκε για την υποστήριξη της εφαρμογής της κοινής πολιτικής

869 ΕΕΠΔ (2017), Γνωμοδότηση του ΕΕΠΔ σχετικά με τη νέα νομική βάση του συστήματος πληροφοριών Σένγκεν, Γνωμοδότηση 7/2017, 2 Μαΐου 2017.

870 Ό.π., σημείο 22.

871 Ευρωπαϊκή Επιτροπή (2016), Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν (SIS) στον τομέα της αστυνομικής συνεργασίας και της δικαστικής συνεργασίας σε ποινικές υποθέσεις, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 515/2014 και την κατάργηση του κανονισμού (ΕΚ) αριθ. 1986/2006, της απόφασης 2007/533/ΔΕΥ του Συμβουλίου και της απόφασης 2010/261/ΕΕ της Επιτροπής, COM(2016) 883 final, Βρυξέλλες, 21 Δεκεμβρίου 2016.

872 Ό.π., σ. 15.

θεωρήσεων της ΕΕ ⁸⁷³. Το σύστημα VIS παρέχει στα κράτη Σένγκεν τη δυνατότητα να ανταλλάσσουν δεδομένα σχετικά με αιτούντες θεώρηση μέσω ενός αμιγώς κεντρικού συστήματος το οποίο συνδέει τα προξενία και τις πρεσβείες των κρατών Σένγκεν που βρίσκονται σε τρίτες χώρες με τα εξωτερικά σημεία συνοριακής διέλευσης του συνόλου των κρατών Σένγκεν. Το σύστημα VIS επεξεργάζεται δεδομένα που αφορούν αιτήσεις χορήγησης θεωρήσεων μικρής διάρκειας για λόγους επίσκεψης ή διέλευσης από τον χώρο Σένγκεν. Το VIS παρέχει στις συνοριακές αρχές τη δυνατότητα να εξακριβώνουν, με τη βοήθεια βιομετρικών στοιχείων, κυρίως δακτυλικών αποτυπωμάτων, αν το πρόσωπο το οποίο επιδεικνύει μια θεώρηση είναι ο νόμιμος κάτοχός της, καθώς και να εντοπίζουν πρόσωπα τα οποία δεν διαθέτουν έγγραφα ή διαθέτουν πλαστά έγγραφα.

Ο κανονισμός (ΕΚ) αριθ. 767/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) και την ανταλλαγή δεδομένων μεταξύ κρατών μελών για τις θεωρήσεις μικρής διάρκειας (κανονισμός VIS) ρυθμίζει τις προϋποθέσεις και τις διαδικασίες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα που αφορούν αιτήσεις θεωρήσεων μικρής διάρκειας. Εποπτεύει επίσης τις αποφάσεις που λαμβάνονται σχετικά με αιτήσεις, περιλαμβανομένων αποφάσεων ακύρωσης, ανάκλησης ή παράτασης της θεώρησης ⁸⁷⁴. Ο κανονισμός VIS καλύπτει κυρίως δεδομένα σχετικά με τον αιτούντα, τις θεωρήσεις, τις φωτογραφίες, τα δακτυλικά αποτυπώματά του, συνδέσμους με προηγούμενες αιτήσεις και τους φακέλους αιτήσεων προσώπων που συνοδεύουν τον αιτούντα ή δεδομένα σχετικά με τους προσκαλούντες ⁸⁷⁵. Η πρόσβαση στο σύστημα VIS για την εισαγωγή, τροποποίηση ή διαγραφή δεδομένων περιορίζεται αποκλειστικά στις αρχές θεωρήσεων, ενώ πρόσβαση για αναζήτηση δεδομένων παρέχεται στις αρχές θεωρήσεων και στις αρχές που είναι αρμόδιες για τους

873 Συμβούλιο της Ευρωπαϊκής Ένωσης (2004), απόφαση 2004/512/ΕΚ του Συμβουλίου, της 8ης Ιουνίου 2004, για τη δημιουργία του Συστήματος Πληροφοριών για τις Θεωρήσεις (VIS) (ΕΕ L 213 της 15.6.2004, σ. 5)- κανονισμός (ΕΚ) αριθ. 767/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) και την ανταλλαγή δεδομένων μεταξύ κρατών μελών για τις θεωρήσεις μικρής διάρκειας (ΕΕ L 218 της 13.8.2008, σ. 60) (κανονισμός VIS)- Συμβούλιο της Ευρωπαϊκής Ένωσης (2008), απόφαση 2008/633/ΔΕΥ του Συμβουλίου, της 23ης Ιουνίου 2008, σχετικά με την πρόσβαση στο Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) των εντεταλμένων αρχών των κρατών μελών καθώς και της Ευρωπαϊκής, προς αναζήτηση δεδομένων για την πρόληψη, εξακρίβωση και διερεύνηση τρομοκρατικών πράξεων και άλλων σοβαρών αξιόποινων πράξεων (ΕΕ L 218 της 13.8.2008, σ. 129).

874 Κανονισμός VIS, άρθρο 1.

875 Άρθρο 5 του κανονισμού (ΕΚ) αριθ. 767/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Ιουλίου 2008, για το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) και την ανταλλαγή δεδομένων μεταξύ κρατών μελών για τις θεωρήσεις μικρής διάρκειας (κανονισμός VIS) (ΕΕ L 218 της 13.8.2008, σ. 60).

ελέγχους στα εξωτερικά σημεία συνοριακής διέλευσης και για τους ελέγχους σε θέματα μετανάστευσης και ασύλου.

Υπό ορισμένες προϋποθέσεις, οι αρμόδιες εθνικές αστυνομικές αρχές και η Ευρωπόλ μπορούν να ζητήσουν πρόσβαση σε δεδομένα που εισάγονται στο σύστημα VIS για τους σκοπούς της πρόληψης, της εξακρίβωσης και της διερεύνησης τρομοκρατικών και αξιόποινων πράξεων ⁸⁷⁶. Δεδομένου ότι το VIS έχει σχεδιαστεί ως μέσο για την υποστήριξη της εφαρμογής της κοινής πολιτικής θεωρήσεων, σε περίπτωση μετατροπής του σε εργαλείο επιβολής του νόμου, θα παραβιαζόταν η αρχή του περιορισμού του σκοπού η οποία επιβάλλει, όπως διευκρινίζεται στο **κεφάλαιο 3.2**, την υποχρέωση να πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο για καθορισμένους, ρητούς και νόμιμους σκοπούς, καθώς και να είναι τα δεδομένα κατάλληλα, συναφή και όχι δυσανάλογα σε σχέση με τους σκοπούς για τους οποίους υφίστανται επεξεργασία. Για τον λόγο αυτό, στις αρχές επιβολής του νόμου και στην Ευρωπόλ δεν χορηγείται συστηματική πρόσβαση στη βάση δεδομένων του VIS. Πρόσβαση μπορεί να χορηγείται μόνο κατά περίπτωση και να συνοδεύεται από αυστηρές διασφαλίσεις. Οι προϋποθέσεις και οι διασφαλίσεις όσον αφορά την πρόσβαση και την αναζήτηση δεδομένων στο σύστημα VIS από τις αρχές αυτές έχουν ρυθμιστεί με την απόφαση 2008/633/ΔΕΥ του Συμβουλίου ⁸⁷⁷.

Επιπλέον, ο κανονισμός VIS ορίζει τα δικαιώματα των υποκειμένων των δεδομένων, τα οποία είναι τα εξής:

- Το δικαίωμα να ενημερώνονται από το υπεύθυνο κράτος μέλος σχετικά με την ταυτότητα και τα στοιχεία επαφής του υπεύθυνου επεξεργασίας που είναι αρμόδιος για την επεξεργασία δεδομένων προσωπικού χαρακτήρα εντός του συγκεκριμένου κράτους μέλους, τον σκοπό για τον οποίο θα γίνει επεξεργασία των δεδομένων που τα αφορούν εντός του συστήματος VIS, τις κατηγορίες προσώπων στα οποία μπορούν να διαβιβαστούν τα δεδομένα (αποδέκτες) και τη διάρκεια διατήρησης των δεδομένων. Επιπλέον, οι αιτούντες θεώρηση πρέπει να ενημερώνονται για το γεγονός ότι η συλλογή δεδομένων που τους αφορούν στο πλαίσιο του VIS είναι υποχρεωτική για την εξέταση της αίτησής τους, ενώ τα κράτη μέλη πρέπει επίσης να τους ενημερώνουν σχετικά με το δικαίωμά τους να έχουν πρόσβαση στα δεδομένα τους και να

⁸⁷⁶ Συμβούλιο της Ευρωπαϊκής Ένωσης (2008), απόφαση 2008/633/ΔΕΥ του Συμβουλίου, της 23ης Ιουνίου 2008, σχετικά με την πρόσβαση στο Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS) των εντεταλμένων αρχών των κρατών μελών καθώς και της Ευρωπόλ, προς αναζήτηση δεδομένων για την πρόληψη, εξακρίβωση και διερεύνηση τρομοκρατικών πράξεων και άλλων σοβαρών αξιόποινων πράξεων (ΕΕ L 218 της 13.8.2008, σ. 129).

⁸⁷⁷ Ό.π.

ζητήσουν τη διόρθωση ή τη διαγραφή τους, καθώς και σχετικά με τις διαδικασίες που τους παρέχουν τη δυνατότητα να ασκήσουν αυτά τα δικαιώματα ⁸⁷⁸.

- Το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν, τα οποία έχουν καταχωριστεί στο VIS ⁸⁷⁹.
- Το δικαίωμα διόρθωσης ανακριβών δεδομένων ⁸⁸⁰.
- Το δικαίωμα διαγραφής δεδομένων που δεν έχουν αποθηκευτεί παράνομα ⁸⁸¹.

Για τη διασφάλιση της εποπτείας του VIS, συστάθηκε η συντονιστική ομάδα εποπτείας του VIS, η οποία απαρτίζεται από εκπροσώπους του ΕΕΠΔ και των εθνικών εποπτικών αρχών, που συνεδριάζουν δύο φορές ετησίως. Στην ομάδα συμμετέχουν εκπρόσωποι από 28 κράτη μέλη της ΕΕ, καθώς και από την Ελβετία, την Ισλανδία, το Λιχτενστάιν και τη Νορβηγία.

Eurodac

Το Eurodac είναι αρκτικόλεξο του ευρωπαϊκού συστήματος δακτυλοσκόπησης ⁸⁸². Πρόκειται για κεντρικό σύστημα το οποίο περιέχει δεδομένα δακτυλικών αποτυπωμάτων των υπηκόων τρίτων χωρών και απάτριδων οι οποίοι υποβάλλουν αίτηση χορήγησης ασύλου σε ένα από τα κράτη μέλη της ΕΕ ⁸⁸³. Το σύστημα

878 Κανονισμός VIS, άρθρο 37.

879 Ό.π., άρθρο 38 παράγραφος 1.

880 Ό.π., άρθρο 38 παράγραφος 2.

881 Ό.π., άρθρο 38 παράγραφος 2.

882 Βλ. την [ιστοσελίδα για το Eurodac](#) στον ιστότοπο του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων.

883 Κανονισμός (ΕΚ) αριθ. 2725/2000 του Συμβουλίου, της 11ης Δεκεμβρίου 2000, σχετικά με τη θέσπιση του «Eurodac» για την αντιπαραβολή δακτυλικών αποτυπωμάτων για την αποτελεσματική εφαρμογή της Σύμβασης του Δουβλίνου (ΕΕ L 316 της 15.12.2000, σ. 1)· κανονισμός (ΕΚ) αριθ. 407/2002 του Συμβουλίου, της 28ης Φεβρουαρίου 2002, που θεσπίζει ορισμένους κανόνες εφαρμογής του κανονισμού (ΕΚ) αριθ. 2725/2000 σχετικά με τη θέσπιση του «Eurodac» για την αντιπαραβολή δακτυλικών αποτυπωμάτων για την αποτελεσματική εφαρμογή της Σύμβασης του Δουβλίνου (ΕΕ L 62 της 5.3.2002, σ. 1) (κανονισμοί Eurodac)· κανονισμός (ΕΕ) αριθ. 603/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με τη θέσπιση του «Eurodac» για την αντιπαραβολή δακτυλικών αποτυπωμάτων για την αποτελεσματική εφαρμογή του κανονισμού (ΕΕ) αριθ. 604/2013 για τη θέσπιση των κριτηρίων και μηχανισμών για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης διεθνούς προστασίας που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας ή από απάτριδα και σχετικά με αιτήσεις της αντιπαραβολής με τα δεδομένα Eurodac που υποβάλλουν οι αρχές επιβολής του νόμου των κρατών μελών και η Ευρωπαϊκή Υπηρεσία επιβολής του νόμου και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 1077/2011 σχετικά με την ίδρυση Ευρωπαϊκού Οργανισμού για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης (ΕΕ L 180 της 29.6.2013, σ. 1) (αναδιατύπωση του κανονισμού Eurodac).

λειτουργεί από τον Ιανουάριο του 2003, με την υιοθέτηση του κανονισμού αριθ. 2725/2000 του Συμβουλίου· το 2015 τέθηκε σε ισχύ αναδιατύπωσή του. Πρωταρχικός σκοπός του είναι να διευκολύνει τον προσδιορισμό του κράτους μέλους το οποίο θα πρέπει να είναι υπεύθυνο για την εξέταση μιας αίτησης άσυλου βάσει του κανονισμού (ΕΚ) αριθ. 604/2013. Ο εν λόγω κανονισμός θεσπίζει τα κριτήρια και τους μηχανισμούς για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης διεθνούς προστασίας που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας ή από απάτριδα (κανονισμός Δουβλίνο III)⁸⁸⁴. Τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται στο Eurodac χρησιμεύουν για τη διευκόλυνση της εφαρμογής του κανονισμού Δουβλίνο III⁸⁸⁵.

Στις εθνικές αρχές επιβολής του νόμου και στην Ευρωπόλ επιτρέπεται να πραγματοποιούν αντιπαραβολή μεταξύ των δακτυλικών αποτυπωμάτων που συνδέονται με ποινικές έρευνες και των δακτυλικών αποτυπωμάτων που περιέχονται στο Eurodac, αλλά μόνο για τους σκοπούς της πρόληψης, της εξακρίβωσης ή της διερεύνησης τρομοκρατικών εγκλημάτων ή άλλων σοβαρών αξιόποινων πράξεων. Δεδομένου ότι το Eurodac έχει σχεδιαστεί ως μέσο για την υποστήριξη της εφαρμογής της πολιτικής της ΕΕ για το άσυλο, και όχι ως εργαλείο επιβολής του νόμου, οι αρχές επιβολής του νόμου έχουν πρόσβαση στη βάση δεδομένων μόνο σε συγκεκριμένες περιπτώσεις, υπό συγκεκριμένες συνθήκες και αυστηρές προϋποθέσεις⁸⁸⁶. Για την περαιτέρω χρήση των δεδομένων για σκοπούς επιβολής του νόμου, εφαρμόζεται η οδηγία για την προστασία δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, ενώ τα δεδομένα που χρησιμοποιούνται με κύριο σκοπό τη διευκόλυνση της εφαρμογής του κανονισμού Δουβλίνο III προστατεύονται βάσει του Γενικού Κανονισμού για την Προστασία Δεδομένων. Απαγορεύεται η περαιτέρω διαβίβαση σε τρίτη χώρα, διεθνή οργανισμό ή ιδιωτική οντότητα εγκατεστημένη εντός ή εκτός της ΕΕ δεδομένων προσωπικού χαρακτήρα τα οποία λαμβάνει ένα κράτος μέλος ή η Ευρωπόλ στα πλαίσια της εφαρμογής του αναδιατυπωμένου κανονισμού Eurodac⁸⁸⁷.

884 Κανονισμός (ΕΕ) αριθ. 604/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, για τη θέσπιση των κριτηρίων και μηχανισμών για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης διεθνούς προστασίας που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας ή από απάτριδα (ΕΕ L 180 της 29.6.2013, σ. 31) (κανονισμός Δουβλίνο III).

885 Αναδιατύπωση του κανονισμού Eurodac (ΕΕ L 180 της 29.6.2013, σ. 1), άρθρο 1 παράγραφος 1.

886 Ό.π., άρθρο 1 παράγραφος 2.

887 Ό.π., άρθρο 35.

Το Eurodac αποτελείται από μια κεντρική μονάδα για την αποθήκευση και την αντιπαράβολή δακτυλικών αποτυπωμάτων, την οποία διαχειρίζεται ο eu-LISA, και ένα σύστημα ηλεκτρονικής διαβίβασης δεδομένων μεταξύ των κρατών μελών και της κεντρικής βάσης δεδομένων. Τα κράτη μέλη λαμβάνουν και διαβιβάζουν τα δακτυλικά αποτυπώματα κάθε προσώπου ηλικίας τουλάχιστον 14 ετών το οποίο αιτείται άσυλο στο έδαφός τους και κάθε υπηκόου τρίτης χώρας ή απάτριδος ηλικίας τουλάχιστον 14 ετών που συλλαμβάνεται στο έδαφός τους για παράνομη διέλευση των εξωτερικών συνόρων τους. Τα κράτη μέλη μπορούν επίσης να λαμβάνουν και να διαβιβάζουν τα δακτυλικά αποτυπώματα υπηκόων τρίτων χωρών ή απάτριδων για τους οποίους διαπιστώνεται ότι διαμένουν στο έδαφός τους χωρίς άδεια.

Παρότι κάθε κράτος μέλος μπορεί να πραγματοποιεί αναζήτηση στο Eurodac και να ζητεί την αντιπαράβολή δακτυλικών αποτυπωμάτων, μόνο το κράτος μέλος που έχει συλλέξει και διαβιβάσει τα δακτυλικά αποτυπώματα στην κεντρική μονάδα έχει το δικαίωμα να τροποποιήσει τα δεδομένα, διορθώνοντας, συμπληρώνοντας ή απαλείφοντάς τα ⁸⁸⁸. Ο eu-LISA τηρεί αρχεία κάθε επεξεργασίας δεδομένων με σκοπό την παρακολούθηση της προστασίας δεδομένων και τη διαφύλαξη της ασφάλειας των δεδομένων ⁸⁸⁹. Οι εθνικές εποπτικές αρχές παρέχουν συνδρομή και συμβουλές στα υποκείμενα των δεδομένων σχετικά με την άσκηση των δικαιωμάτων τους ⁸⁹⁰. Η συλλογή και διαβίβαση δεδομένων δακτυλικών αποτυπωμάτων υπόκειται σε δικαστικό έλεγχο από τα εθνικά δικαστήρια ⁸⁹¹. Ο κανονισμός για την προστασία δεδομένων από τα όργανα της ΕΕ ⁸⁹² και η άσκηση εποπτείας από τον ΕΕΠΔ εφαρμόζονται στις δραστηριότητες επεξεργασίας του κεντρικού συστήματος, το οποίο τελεί υπό τη διαχείριση του eu-LISA όσον αφορά το Eurodac ⁸⁹³. Εάν ένα πρόσωπο υποστεί ζημία ως αποτέλεσμα παράνομης επεξεργασίας ή οποιασδήποτε πράξης που δεν συμβιβάζεται με τον κανονισμό Eurodac, το πρόσωπο αυτό δικαιούται να λάβει αποζημίωση από το κράτος μέλος που είναι υπεύθυνο για τη ζημία ⁸⁹⁴. Ωστόσο, είναι σκόπιμο να τονιστεί ότι οι

888 Ό.π., άρθρο 27.

889 Ό.π., άρθρο 28.

890 Ό.π., άρθρο 29.

891 Ό.π., άρθρο 29.

892 Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

893 Αναδιατύπωση του κανονισμού Eurodac (ΕΕ L 180 της 29.6.2013, σ. 1), άρθρο 31.

894 Ό.π., άρθρο 37.

αιτούντες άσυλο αποτελούν μια ιδιαίτερα ευάλωτη ομάδα προσώπων, τα οποία πραγματοποιούν συνήθως μεγάλα και επικίνδυνα ταξίδια. Λόγω του ευάλωτου χαρακτήρα τους και της επισφαλούς κατάστασης στην οποία βρίσκονται συχνά ενόσω εκκρεμεί η εξέταση της αίτησης ασύλου τους, η άσκηση των δικαιωμάτων τους, συμπεριλαμβανομένου του δικαιώματος αποζημίωσης, μπορεί να αποδειχθεί δύσκολη στην πράξη.

Προκειμένου να είναι σε θέση να χρησιμοποιήσουν το Eurodac για σκοπούς επιβολής του νόμου, τα κράτη μέλη πρέπει να ορίσουν τις αρχές που θα έχουν το δικαίωμα να ζητήσουν πρόσβαση, καθώς και τις αρχές που θα επαληθεύουν ότι οι αιτήσεις αντιπαράβολής είναι νόμιμες⁸⁹⁵. Η πρόσβαση των εθνικών αρχών και της Ευρωπόλ στα δεδομένα δακτυλικών αποτυπωμάτων του Eurodac υπόκειται σε πολύ αυστηρές προϋποθέσεις. Η αιτούσα αρχή πρέπει να υποβάλλει αιτιολογημένη ηλεκτρονική αίτηση μόνο κατόπιν αντιπαράβολής των δεδομένων με δεδομένα που περιλαμβάνονται σε άλλα διαθέσιμα συστήματα πληροφοριών, όπως εθνικές βάσεις δεδομένων δακτυλικών αποτυπωμάτων και το σύστημα VIS. Πρέπει να υπάρχει υπέρτερο ζήτημα δημόσιας ασφάλειας, το οποίο καθιστά την αντιπαράβολή αναλογική. Η αντιπαράβολή πρέπει να είναι πραγματικά αναγκαία, να αφορά συγκεκριμένη υπόθεση και να συντρέχουν βάσιμοι λόγοι ώστε να θεωρείται ότι η αντιπαράβολή μπορεί να συμβάλει σημαντικά στην πρόληψη, την εξακρίβωση ή τη διερεύνηση οποιασδήποτε από τις επίμαχες αξιόπινες πράξεις, ιδίως όταν υπάρχει βάσιμη υπόνοια ότι ο ύποπτος, ο δράστης ή το θύμα τρομοκρατικής ή άλλης σοβαρής αξιόπινης πράξης εμπίπτει σε κατηγορία υποκείμενη στη συλλογή δακτυλικών αποτυπωμάτων στο πλαίσιο του συστήματος Eurodac. Η αντιπαράβολή πρέπει να πραγματοποιείται αποκλειστικά και μόνο με δεδομένα δακτυλικών αποτυπωμάτων. Η Ευρωπόλ πρέπει επίσης να λαμβάνει άδεια από το κράτος μέλος το οποίο συνέλεξε τα δεδομένα δακτυλικών αποτυπωμάτων.

Τα δεδομένα προσωπικού χαρακτήρα που αποθηκεύονται στο Eurodac και αφορούν αιτούντες άσυλο διατηρούνται για 10 έτη από την ημερομηνία λήψης των δακτυλικών αποτυπωμάτων, εκτός εάν το υποκείμενο των δεδομένων αποκτήσει την ιθαγένεια κράτους μέλους της ΕΕ. Στην περίπτωση αυτή, τα δεδομένα πρέπει να διαγράφονται αμέσως. Τα δεδομένα που αφορούν αλλοδαπούς υπηκόους οι οποίοι συλλαμβάνονται για παράνομη διέλευση των εξωτερικών συνόρων διατηρούνται για 18 μήνες. Τα δεδομένα αυτά πρέπει να διαγράφονται

⁸⁹⁵ Roots, L. (2015), «The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination», *Baltic Journal of European Studies Tallinn University of Technology*, τόμος 5, αριθ. 2, σ. 108-129.

αμέσως εάν το υποκείμενο των δεδομένων λάβει άδεια διαμονής, εγκαταλείψει το έδαφος της ΕΕ ή αποκτήσει την ιθαγένεια κράτους μέλους. Τα δεδομένα των προσώπων στα οποία χορηγήθηκε άσυλο παραμένουν διαθέσιμα προς αντιπαράβολή στο πλαίσιο της πρόληψης, εξακρίβωσης και διερεύνησης τρομοκρατικών εγκλημάτων και άλλων σοβαρών αξιόποινων πράξεων για τρία έτη.

Πέρα από τα κράτη μέλη της ΕΕ, το σύστημα Eurodac εφαρμόζεται και στην Ισλανδία, τη Νορβηγία, το Λιχτενστάιν και την Ελβετία, βάσει διεθνών συμφωνιών.

Για τη διασφάλιση της εποπτείας του Eurodac έχει συσταθεί συντονιστική ομάδα εποπτείας του Eurodac, η οποία απαρτίζεται από εκπροσώπους του ΕΕΠΔ και των εθνικών εποπτικών αρχών, οι οποίοι συνεδριάζουν δύο φορές ετησίως. Στην ομάδα συμμετέχουν εκπρόσωποι των 28 κρατών μελών της ΕΕ, καθώς και της Ελβετίας, της Ισλανδίας, του Λιχτενστάιν και της Νορβηγίας⁸⁹⁶.

Προοπτικές

Τον Μάιο του 2016 η Επιτροπή εξέδωσε πρόταση νέας αναδιατύπωσης του κανονισμού Eurodac, στο πλαίσιο μεταρρύθμισης με στόχο τη βελτίωση της λειτουργίας του κοινού ευρωπαϊκού συστήματος ασύλου (ΚΕΣΑ)⁸⁹⁷. Η προτεινόμενη αναδιατύπωση είναι σημαντική διότι θα επεκτείνει σε μεγάλο βαθμό το πεδίο εφαρμογής της αρχικής βάσης δεδομένων του Eurodac. Το Eurodac δημιουργήθηκε αρχικά με σκοπό να υποστηριχθεί η εφαρμογή του ΚΕΣΑ, μέσω της παροχής αποδεικτικών στοιχείων δακτυλικών αποτυπωμάτων για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης ασύλου που υποβάλλεται στην ΕΕ. Η προτεινόμενη αναδιατύπωση θα επεκτείνει το πεδίο εφαρμογής της βάσης δεδομένων ώστε να διευκολύνεται η επιστροφή παράνομων μεταναστών⁸⁹⁸. Οι εθνικές αρχές θα είναι σε θέση να πραγματοποιούν

896 Βλ. την [ιστοσελίδα για το Eurodac](#) στον ιστότοπο του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων.

897 Ευρωπαϊκή Επιτροπή, Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση του «Eurodac» για την αντιπαράβολή δακτυλικών αποτυπωμάτων για την αποτελεσματική εφαρμογή του [κανονισμού (ΕΕ) αριθ. 604/2013 για τη θέσπιση των κριτηρίων και μηχανισμών για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης διεθνούς προστασίας που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας ή από απάτριδα], για την ταυτοποίηση παρανόμως διαμενόντων υπηκόων τρίτων χωρών ή απάτριδων και σχετικά με αιτήσεις αντιπαράβολής με τα δεδομένα Eurodac που υποβάλλουν οι αρχές επιβολής του νόμου των κρατών μελών και η Ευρωπόλ για σκοπούς επιβολής του νόμου (αναδιατύπωση), COM(2016) 272 final, 4 Μαΐου 2016.

898 Βλ. την αιτιολογική έκθεση της πρότασης, σ. 3.

αναζήτηση στη βάση δεδομένων για τον σκοπό του εντοπισμού υπηκόων τρίτων χωρών που διαμένουν ή έχουν εισέλθει παράνομα στην ΕΕ, προκειμένου να εξασφαλίζουν αποδεικτικά στοιχεία τα οποία θα διευκολύνουν τα κράτη μέλη στο πλαίσιο της επιστροφής των εν λόγω προσώπων. Επιπλέον, σε αντίθεση με το ισχύον νομικό καθεστώς, το οποίο απαιτεί μόνο τη συλλογή και αποθήκευση δακτυλικών αποτυπωμάτων, η πρόταση προβλέπει επίσης τη συλλογή εικόνων προσώπου⁸⁹⁹ των ατόμων, οι οποίες αποτελούν ένα άλλο είδος βιομετρικών δεδομένων. Με την πρόταση μειώνεται επίσης το κατώτατο όριο ηλικίας των παιδιών από τα οποία μπορούν να ληφθούν βιομετρικά δεδομένα, δηλαδή η ηλικία των έξι ετών⁹⁰⁰ και όχι των 14 ετών, που είναι το κατώτατο όριο ηλικίας βάσει του κανονισμού του 2013. Το διευρυμένο πεδίο εφαρμογής της πρότασης σημαίνει ότι η λήψη βιομετρικών δεδομένων συνιστά επέμβαση στα δικαιώματα προστασίας της ιδιωτικής ζωής και προστασίας των δεδομένων περισσότερων προσώπων τα οποία ενδέχεται να συμπεριλαμβάνονται στη βάση δεδομένων. Για να αντισταθμιστεί η επέμβαση αυτή, τόσο η πρόταση όσο και οι τροποποιήσεις που προτάθηκαν από την επιτροπή LIBE του Ευρωπαϊκού Κοινοβουλίου⁹⁰¹ επιδιώκουν την ενίσχυση των απαιτήσεων προστασίας δεδομένων. Κατά τον χρόνο σύνταξης του παρόντος εγχειριδίου, οι συζητήσεις σχετικά με την πρόταση στο Κοινοβούλιο και το Συμβούλιο βρίσκονταν σε εξέλιξη.

899 Ευρωπαϊκή Επιτροπή, Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση του «Eurodac» για την αντιπαράβολή δακτυλικών αποτυπωμάτων για την αποτελεσματική εφαρμογή του [κανονισμού (ΕΕ) αριθ. 604/2013 για τη θέσπιση των κριτηρίων και μηχανισμών για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης διεθνούς προστασίας που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας ή από απάτριδα], για την ταυτοποίηση παρανόμως διαμενόντων υπηκόων τρίτων χωρών ή απάτριδων και σχετικά με αιτήσεις αντιπαράβολής με τα δεδομένα Eurodac που υποβάλλουν οι αρχές επιβολής του νόμου των κρατών μελών και η Ευρωπαϊκή για σκοπούς επιβολής του νόμου (αναδιατύπωση), COM(2016) 272 final, 4 Μαΐου 2016, άρθρο 2 παράγραφος 1.

900 Ό.π., άρθρο 2 παράγραφος 2.

901 Ευρωπαϊκό Κοινοβούλιο, *Έκθεση σχετικά με την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση του «Eurodac» για την αντιπαράβολή δακτυλικών αποτυπωμάτων για την αποτελεσματική εφαρμογή του [κανονισμού (ΕΕ) αριθ. 604/2013 για τη θέσπιση των κριτηρίων και μηχανισμών για τον προσδιορισμό του κράτους μέλους που είναι υπεύθυνο για την εξέταση αίτησης διεθνούς προστασίας που υποβάλλεται σε κράτος μέλος από υπήκοο τρίτης χώρας ή από απάτριδα]*, για την ταυτοποίηση παρανόμως διαμενόντων υπηκόων τρίτων χωρών ή απάτριδων και σχετικά με αιτήσεις αντιπαράβολής με τα δεδομένα Eurodac που υποβάλλουν οι αρχές επιβολής του νόμου των κρατών μελών και η Ευρωπαϊκή για σκοπούς επιβολής του νόμου (αναδιατύπωση), PE 597.620v03-00, 9 Ιουνίου 2017.

Eurosur

Το ευρωπαϊκό σύστημα επιτήρησης των συνόρων (Eurosur)⁹⁰² έχει σχεδιαστεί με σκοπό την ενίσχυση του ελέγχου των εξωτερικών συνόρων Σένγκεν μέσω του εντοπισμού, της πρόληψης και της καταπολέμησης της παράνομης μετανάστευσης και του διασυνοριακού εγκλήματος. Συμβάλλει στην ενίσχυση της ανταλλαγής πληροφοριών και της επιχειρησιακής συνεργασίας μεταξύ των εθνικών κέντρων συντονισμού και του Frontex, του οργανισμού της ΕΕ ο οποίος είναι αρμόδιος για την ανάπτυξη και την εφαρμογή της νέας αντίληψης περί ολοκληρωμένης διαχείρισης των συνόρων⁹⁰³. Οι γενικοί του στόχοι είναι οι εξής:

- μείωση του αριθμού των παράνομων μεταναστών που εισέρχονται στην ΕΕ χωρίς να εντοπίζονται·
- μείωση του αριθμού των θανάτων παράνομων μεταναστών με τη διάσωση περισσότερων ανθρώπινων ζωών στη θάλασσα·
- ενίσχυση της εσωτερικής ασφάλειας της ΕΕ συνολικά, συμβάλλοντας στην πρόληψη του διασυνοριακού εγκλήματος⁹⁰⁴.

Το Eurosur άρχισε να λειτουργεί στις 2 Δεκεμβρίου 2013 σε όλα τα κράτη μέλη με εξωτερικά σύνορα και την 1η Δεκεμβρίου 2014 στα υπόλοιπα. Ο κανονισμός εφαρμόζεται στην επιτήρηση των εξωτερικών χερσαίων, θαλάσσιων και εναέριων συνόρων των κρατών μελών. Το Eurosur ανταλλάσσει και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα σε πολύ περιορισμένο βαθμό, δεδομένου ότι

902 Κανονισμός (ΕΕ) αριθ. 1052/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 22ας Οκτωβρίου 2013, για τη θέσπιση του Ευρωπαϊκού Συστήματος Επιτήρησης των Συνόρων (Eurosur) (ΕΕ L 295 της 6.11.2013, σ. 11).

903 Κανονισμός (ΕΕ) 2016/1624 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Σεπτεμβρίου 2016, για την Ευρωπαϊκή Συνοριοφυλακή και Ακτοφυλακή και για την τροποποίηση του κανονισμού (ΕΕ) 2016/399 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και την κατάργηση του κανονισμού (ΕΚ) αριθ. 863/2007 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και του κανονισμού (ΕΚ) αριθ. 2007/2004 του Συμβουλίου και της απόφασης 2005/267/ΕΚ του Συμβουλίου (ΕΕ L 251 της 16.9.2016, σ. 1).

904 Βλ. επίσης: Ευρωπαϊκή Επιτροπή (2008), Ανακοίνωση της Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο, στην Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και στην Επιτροπή Περιφερειών: Εξέταση της δημιουργίας ενός ευρωπαϊκού συστήματος επιτήρησης των συνόρων (Eurosur), COM(2008) 68 τελικό, Βρυξέλλες, 13 Φεβρουαρίου 2008· Ευρωπαϊκή Επιτροπή (2011), Εκτίμηση επιπτώσεων που συνοδεύει την πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση του ευρωπαϊκού συστήματος επιτήρησης των συνόρων (Eurosur), έγγραφο εργασίας των υπηρεσιών της Επιτροπής, SEC(2011) 1536 τελικό, Βρυξέλλες, 12 Δεκεμβρίου 2011, σ. 18.

μόνο τα κράτη μέλη και ο Frontex έχουν το δικαίωμα να ανταλλάσσουν αριθμούς αναγνώρισης πλοίων. Το Eufosur ανταλλάσσει επιχειρησιακές πληροφορίες, όπως η θέση περιπολιών και συμβάντων, και, κατά γενικό κανόνα, στις πληροφορίες που ανταλλάσσονται δεν μπορούν να περιλαμβάνονται δεδομένα προσωπικού χαρακτήρα⁹⁰⁵. Στις εξαιρετικές περιπτώσεις στις οποίες πραγματοποιείται ανταλλαγή δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του Eufosur, ο κανονισμός προβλέπει ότι ισχύει πλήρως το γενικό νομικό πλαίσιο της ΕΕ για την προστασία των δεδομένων⁹⁰⁶.

Ως εκ τούτου, το Eufosur διασφαλίζει το δικαίωμα στην προστασία των δεδομένων, αναφέροντας συγκεκριμένα ότι οι ανταλλαγές δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνονται με τα κριτήρια και τις διασφαλίσεις που ορίζονται τόσο στην οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης όσο και στον Γενικό Κανονισμό για την Προστασία Δεδομένων⁹⁰⁷.

Τελωνειακό Σύστημα Πληροφοριών

Ένα ακόμη σημαντικό σύστημα πληροφοριών που έχει θεσπιστεί σε επίπεδο ΕΕ είναι το Τελωνειακό Σύστημα Πληροφοριών (CIS)⁹⁰⁸. Στο πλαίσιο της δημιουργίας της εσωτερικής αγοράς καταργήθηκαν όλοι οι έλεγχοι και οι διατυπώσεις όσον αφορά εμπορεύματα που διακινούνται εντός του εδάφους της ΕΕ, με αποτέλεσμα να προκληθεί αυξημένος κίνδυνος απάτης. Ο κίνδυνος αυτός αντισταθμίστηκε με την εντατικοποίηση της συνεργασίας μεταξύ των τελωνειακών διοικήσεων των κρατών μελών. Σκοπός του CIS είναι να παρέχει συνδρομή στα κράτη μέλη στο πλαίσιο της πρόληψης, διερεύνησης και δίωξης σοβαρών παραβιάσεων της εθνικής και της ενωσιακής τελωνειακής και γεωργικής νομοθεσίας. Το CIS θεσπίστηκε με δύο νομικές πράξεις που εκδόθηκαν επί διαφορετικών νομικών

905 Ευρωπαϊκή Επιτροπή, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29 Νοεμβρίου 2013.

906 Κανονισμός 1052/2013, αιτιολογική σκέψη 13 και άρθρο 13.

907 Ό.π., αιτιολογική σκέψη 13 και άρθρο 13.

908 Συμβούλιο της Ευρωπαϊκής Ένωσης (1995), Πράξη του Συμβουλίου, της 26ης Ιουλίου 1995, για την κατάρτιση της Σύμβασης σχετικά με τη χρήση της πληροφορικής στον τελωνειακό τομέα (ΕΕ C 316 της 27.11.1995, σ. 33), όπως τροποποιήθηκε με την πράξη του Συμβουλίου της Ευρωπαϊκής Ένωσης (2009): κανονισμός (ΕΚ) αριθ. 515/97, της 13ης Μαρτίου 1997, περί της αμοιβαίας συνδρομής μεταξύ των διοικητικών αρχών των κρατών μελών και της συνεργασίας των αρχών αυτών με την Επιτροπή με σκοπό τη διασφάλιση της ορθής εφαρμογής των τελωνειακών και γεωργικών ρυθμίσεων· απόφαση 2009/917/ΔΕΥ του Συμβουλίου, της 30ής Νοεμβρίου 2009, για τη χρήση της πληροφορικής για τελωνειακούς σκοπούς (ΕΕ L 323 της 10.12.2009, σ. 20) (απόφαση CIS).

βάσεων: ο κανονισμός (ΕΚ) αριθ. 515/97 αφορά τη συνεργασία μεταξύ των διαφόρων εθνικών διοικητικών αρχών για την καταπολέμηση της απάτης στο πλαίσιο της τελωνειακής ένωσης και της κοινής γεωργικής πολιτικής, ενώ η απόφαση 2009/917/ΔΕΥ του Συμβουλίου αποσκοπεί στην παροχή συνδρομής στην πρόληψη, διερεύνηση και δίωξη σοβαρών παραβιάσεων της τελωνειακής νομοθεσίας. Αυτό σημαίνει ότι το CIS δεν αφορά μόνο την επιβολή του νόμου.

Οι πληροφορίες που περιέχονται στο CIS περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα τα οποία αφορούν εμπορεύματα, μεταφορικά μέσα, επιχειρήσεις, πρόσωπα, καθώς και κατακρατήσεις, κατασχέσεις ή δημεύσεις αγαθών ή ρευστών διαθεσίμων. Οι κατηγορίες των δεδομένων που μπορούν να υποβληθούν σε επεξεργασία καθορίζονται με σαφήνεια και σε αυτές περιλαμβάνονται τα ονόματα, η ιθαγένεια, το φύλο, ο τόπος και η ημερομηνία γέννησης των ενδιαφερομένων ατόμων, ο λόγος της συμπερίληψης των δεδομένων τους στο σύστημα και ο αριθμός καταχώρισης των μεταφορικών μέσων ⁹⁰⁹. Οι πληροφορίες αυτές μπορούν να χρησιμοποιούνται αποκλειστικά και μόνο για τους σκοπούς της παρατήρησης, της αναφοράς ή της διενέργειας ειδικών ελέγχων ή για τους σκοπούς της διενέργειας στρατηγικών ή επιχειρησιακών αναλύσεων σχετικά με πρόσωπα για τα οποία υπάρχουν υπόνοιες ότι παραβιάζουν τις τελωνειακές διατάξεις.

Πρόσβαση στο CIS παρέχεται σε εθνικές τελωνειακές, φορολογικές, γεωργικές, υγειονομικές και αστυνομικές αρχές, καθώς και στην Ευρωπόλ και τη Eurojust.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνεται με τους ειδικούς κανόνες που προβλέπονται στον κανονισμό (ΕΚ) αριθ. 515/97 και την απόφαση 2009/917/ΔΕΥ του Συμβουλίου, καθώς και με τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων, τον κανονισμό για την προστασία δεδομένων από τα θεσμικά όργανα της ΕΕ, την Εκσυγχρονισμένη Σύμβαση 108 και τη σύσταση για τη χρήση δεδομένων προσωπικού χαρακτήρα στον αστυνομικό τομέα. Ο ΕΠΔ είναι υπεύθυνος για την εποπτεία της συμμόρφωσης του CIS με τον κανονισμό (ΕΚ) αριθ. 45/2001. Συγκαλεί τουλάχιστον μία φορά ετησίως συνάντηση με όλες τις εθνικές εποπτικές αρχές προστασίας δεδομένων που είναι αρμόδιες για θέματα εποπτείας του CIS.

⁹⁰⁹ Βλ. απόφαση CIS, άρθρα 24, 25 και 28.

Διαλειτουργικότητα μεταξύ των συστημάτων πληροφοριών της ΕΕ

Η διαχείριση της μετανάστευσης, η ολοκληρωμένη διαχείριση των εξωτερικών συνόρων της ΕΕ και η καταπολέμηση της τρομοκρατίας και του διασυνοριακού εγκλήματος εγείρουν σημαντικές προκλήσεις και καθίστανται ολοένα και πιο πολύπλοκες στην εποχή της παγκοσμιοποίησης. Τα τελευταία έτη, η ΕΕ εργάζεται για τη διαμόρφωση μιας νέας ολοκληρωμένης προσέγγισης όσον αφορά τη διαφύλαξη και τη διατήρηση της ασφάλειας χωρίς να υπονομεύονται οι αξίες και οι θεμελιώδεις ελευθερίες της ΕΕ. Στο πλαίσιο των προσπάθειών αυτών, η αποτελεσματική ανταλλαγή πληροφοριών μεταξύ των εθνικών αρχών επιβολής του νόμου και μεταξύ των κρατών μελών και των αρμόδιων οργανισμών της ΕΕ συνιστά παράγοντα καθοριστικής σημασίας⁹¹⁰. Καθένα από τα υφιστάμενα συστήματα πληροφοριών της ΕΕ για τη διαχείριση των συνόρων και την εσωτερική ασφάλεια χαρακτηρίζεται από αντίστοιχους στόχους, θεσμική δομή, υποκείμενα δεδομένων και χρήστες. Η ΕΕ καταβάλλει προσπάθειες για την αντιμετώπιση των ελλείψεων στις λειτουργίες της κατακερματισμένης διαχείρισης δεδομένων της ΕΕ μεταξύ των διαφόρων συστημάτων πληροφοριών, όπως το SIS II, το VIS και το Eurodac, μέσω διερεύνησης των δυνατοτήτων διαλειτουργικότητας⁹¹¹. Βασικός στόχος είναι να διασφαλιστεί ότι οι αρμόδιες αστυνομικές, τελωνειακές και δικαστικές αρχές διαθέτουν συστηματικά τις αναγκαίες πληροφορίες για την εκτέλεση των καθηκόντων τους, εξασφαλίζοντας παράλληλα τη διατήρηση

910 Ευρωπαϊκή Επιτροπή (2016), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Πιο Ισχυρά και Έξυπνα Συστήματα Πληροφοριών για τα Σύνορα και την Ασφάλεια, COM(2016) 205 final, Βρυξέλλες, 6 Απριλίου 2016, Ευρωπαϊκή Επιτροπή (2016): ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το Συμβούλιο: Ενίσχυση της ασφάλειας σε έναν κόσμο σε διαρκή κίνηση: βελτιωμένη ανταλλαγή πληροφοριών για την καταπολέμηση της τρομοκρατίας και ισχυρότερα εξωτερικά σύνορα, COM(2016) 602 final, Βρυξέλλες, 14 Σεπτεμβρίου 2016, Ευρωπαϊκή Επιτροπή (2016): πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη χρήση του συστήματος Πληροφοριών Σένγκεν για την επιστροφή των παρانونως διαμενόντων υπηκόων τρίτων χωρών. Βλ. επίσης ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Ευρωπαϊκό Συμβούλιο και το Συμβούλιο: Έβδομη έκθεση προόδου προς την κατεύθυνση μιας αποτελεσματικής και πραγματικής Ένωσης ασφάλειας, COM(2017) 261 final, Βρυξέλλες, 16 Μαΐου 2017.

911 Συμβούλιο της Ευρωπαϊκής Ένωσης (2005), Το πρόγραμμα της Χάγης: ενίσχυση της ελευθερίας, της ασφάλειας και της δικαιοσύνης στην Ευρωπαϊκή Ένωση (ΕΕ C 53 της 3.3.2005, σ. 1), Ευρωπαϊκή Επιτροπή (2010), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Επιοκρότηση της διαχείρισης των πληροφοριών στον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης, COM(2010) 385 τελικό, Ευρωπαϊκή Επιτροπή (2016), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Πιο Ισχυρά και Έξυπνα Συστήματα Πληροφοριών για τα Σύνορα και την Ασφάλεια, COM(2016) 205 final, Βρυξέλλες, 6 Απριλίου 2016, Ευρωπαϊκή Επιτροπή (2016), απόφαση της Επιτροπής, της 17ης Ιουνίου 2016, για τη σύσταση της ομάδας εμπειρογνομόνων υψηλού επιπέδου σχετικά με τα συστήματα πληροφοριών και τη διαλειτουργικότητα (ΕΕ C 257 της 15.7.2016, σ. 3).

ισορροπίας όσον αφορά τα δικαιώματα στην προστασία της ιδιωτικής ζωής και στην προστασία των δεδομένων, καθώς και άλλα θεμελιώδη δικαιώματα.

Διαλειτουργικότητα είναι «η ικανότητα των συστημάτων πληροφοριών να ανταλλάσσουν δεδομένα και να καθιστούν δυνατή την ανταλλαγή πληροφοριών»⁹¹². Η ανταλλαγή αυτή δεν πρέπει να διακυβεύει τους απαραίτητως αυστηρούς κανόνες σχετικά με την πρόσβαση και τη χρήση που κατοχυρώνονται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων, την οδηγία για την προστασία των δεδομένων για τις αστυνομικές αρχές και τις αρχές ποινικής δικαιοσύνης, τον Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ, καθώς και άλλους σχετικούς κανόνες. Τυχόν ολοκληρωμένες λύσεις για τη διαχείριση δεδομένων δεν πρέπει να θίγουν τις αρχές του περιορισμού του σκοπού, της προστασίας των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού⁹¹³.

Πέραν της βελτίωσης των λειτουργικών δυνατοτήτων των τριών βασικών συστημάτων πληροφοριών –SIS II, VIS και Eurodac– η Επιτροπή έχει προτείνει την καθιέρωση ενός τέταρτου κεντρικού συστήματος διαχείρισης των συνόρων, του Συστήματος Εισόδου-Εξόδου (ΣΕΕ)⁹¹⁴, το οποίο προορίζεται για τους υπηκόους τρίτων χωρών και αναμένεται να τεθεί σε εφαρμογή έως το 2020⁹¹⁵. Η Επιτροπή έχει εκδώσει επίσης πρόταση για τη θέσπιση ευρωπαϊκού συστήματος πληροφοριών και αδείας ταξιδιού (ETIAS)⁹¹⁶, ένα σύστημα το οποίο θα συλλέγει πληροφορίες σχετικά με πρόσωπα που ταξιδεύουν στην ΕΕ χωρίς υποχρέωση θεώρησης, ώστε να καταστεί δυνατή η εκ των προτέρων διενέργεια ελέγχων όσον αφορά την παράνομη μετανάστευση και την ασφάλεια.

912 Ευρωπαϊκή Επιτροπή (2016), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Πιο Ισχυρά και Έξυπνα Συστήματα Πληροφοριών για τα Σύνορα και την Ασφάλεια, COM(2016) 205 final, Βρυξέλλες, 6 Απριλίου 2016, σ. 14.

913 Ό.π., σ. 4-5.

914 Ευρωπαϊκή Επιτροπή (2016), Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη θέσπιση συστήματος εισόδου/εξόδου (ΣΕΕ) για την καταχώριση δεδομένων εισόδου και εξόδου και δεδομένων άρνησης εισόδου των υπηκόων τρίτων χωρών που διέρχονται τα εξωτερικά σύνορα των κρατών μελών της Ευρωπαϊκής Ένωσης, και τον καθορισμό των όρων πρόσβασης στο ΣΕΕ για σκοπούς επιβολής του νόμου και σχετικά με την τροποποίηση του κανονισμού (ΕΚ) αριθ. 767/2008 και του κανονισμού (ΕΕ) αριθ. 1077/2011, COM(2016) 194 final, Βρυξέλλες, 6 Απριλίου 2016.

915 Ευρωπαϊκή Επιτροπή (2016), Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο: Πιο Ισχυρά και Έξυπνα Συστήματα Πληροφοριών για τα Σύνορα και την Ασφάλεια, COM(2016) 205 final, Βρυξέλλες, 6 Απριλίου 2016, σ. 5.

916 Ευρωπαϊκή Επιτροπή (2016), Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τη θέσπιση ευρωπαϊκού συστήματος πληροφοριών και αδείας ταξιδιού (ETIAS), καθώς και για την τροποποίηση των Κανονισμών (ΕΕ) αριθ. 515/2014, (ΕΕ) 2016/399, (ΕΕ) 2016/794 και (ΕΕ) 2016/1624, COM(2016) 731 final, 16 Νοεμβρίου 2016.

9

Συγκεκριμένα είδη δεδομένων και οι σχετικοί κανόνες προστασίας δεδομένων που τα διέπουν

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Γενικός Κανονισμός για την Προστασία Δεδομένων Οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες	Ηλεκτρονικές επικοινωνίες	Εκσυγχρονισμένη Σύμβαση 108 Σύσταση για τις υπηρεσίες τηλεπικοινωνιών
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 89	Εργασιακές σχέσεις	Εκσυγχρονισμένη Σύμβαση 108 Σύσταση για τον εργασιακό τομέα ΕΔΔΑ, <i>Copland κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 62617/00, 2007
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 9 παράγραφος 2 στοιχεία η) και θ)	Ιατρικά δεδομένα	Εκσυγχρονισμένη Σύμβαση 108 Σύσταση σχετικά με τα ιατρικά δεδομένα ΕΔΔΑ, <i>Z κατά Φινλανδίας</i> , προσφυγή αριθ. 22009/93, 1997
Κανονισμός για τις κλινικές δοκιμές	Κλινικές δοκιμές	
Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 6 παράγραφος 4, άρθρο 89	Στατιστικές	Εκσυγχρονισμένη Σύμβαση 108 Σύσταση σχετικά με τα στατιστικά δεδομένα
Κανονισμός (ΕΚ) αριθ. 223/2009 σχετικά με τις ευρωπαϊκές στατιστικές ΔΕΕ, C-524/06, <i>Heinz Huber κατά Bundesrepublik Deutschland</i> [τμήμα μείζονος συνθέσεως], 2008	Επίσημες στατιστικές	Εκσυγχρονισμένη Σύμβαση 108 Σύσταση σχετικά με τα στατιστικά δεδομένα

ΕΕ	Ζητήματα που εξετάζονται	Συμβούλιο της Ευρώπης
Οδηγία 2014/65/ΕΕ για τις αγορές χρηματοπιστωτικών μέσων Κανονισμός (ΕΕ) αριθ. 648/2012 για τα εξωχρηματοπιστηριακά παράγωγα, τους κεντρικούς αντισυμβαλλομένους και τα αρχεία καταγραφής συναλλαγών Κανονισμός (ΕΚ) αριθ. 1060/2009 για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας Οδηγία 2007/64/ΕΚ για τις υπηρεσίες πληρωμών στην εσωτερική αγορά	Χρηματοοικονομικά δεδομένα	Εκσυγχρονισμένη Σύμβαση 108 Σύσταση 90(19) σχετικά με την προστασία των προσωπικών δεδομένων που χρησιμοποιούνται για πληρωμές και άλλες συναφείς συναλλαγές ΕΔΔΑ, <i>Michaud κατά Γαλλίας</i>, προσφυγή αριθ. 12323/11, 2012

Σε διάφορες περιπτώσεις έχουν εγκριθεί ειδικές νομικές πράξεις σε ευρωπαϊκό επίπεδο για τη λεπτομερέστερη εφαρμογή των γενικών κανόνων της Εκσυγχρονισμένης Σύμβασης 108 ή του Γενικού Κανονισμού για την Προστασία Δεδομένων σε ειδικές καταστάσεις.

9.1. Ηλεκτρονικές επικοινωνίες

Κύρια σημεία

- Συγκεκριμένοι κανόνες για την προστασία των δεδομένων στον τομέα των τηλεπικοινωνιών, με ιδιαίτερη αναφορά στις τηλεφωνικές υπηρεσίες, περιλαμβάνονται στη σύσταση του Συμβουλίου της Ευρώπης του 1995.
- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα όσον αφορά την παροχή τηλεπικοινωνιακών υπηρεσιών σε επίπεδο ΕΕ ρυθμίζεται με την οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.
- Το απόρρητο των ηλεκτρονικών επικοινωνιών δεν καλύπτει μόνο το περιεχόμενο των επικοινωνιών, αλλά και τα μεταδεδομένα, όπως για παράδειγμα πληροφορίες σχετικά με το ποιος επικοινωνήσε με ποιον, τότε και για πόσο χρόνο, καθώς και τα δεδομένα θέσης, όπως για παράδειγμα από πού έγινε η διαβίβαση των δεδομένων.

Τα δίκτυα επικοινωνιών χαρακτηρίζονται από αυξημένες πιθανότητες αδικαιολόγητων επεμβάσεων στην προσωπική σφαίρα των χρηστών, καθώς τα εν λόγω δίκτυα παρέχουν ισχυρές τεχνικές δυνατότητες υποκλοπής και παρακολούθησης των επικοινωνιών που εκτελούνται μέσω αυτών. Ως εκ τούτου, κρίθηκε αναγκαίο να θεσπιστούν ειδικοί κανονισμοί για την προστασία των δεδομένων,

ώστε να ανταποκρίνονται στους ιδιαίτερους κινδύνους που διατρέχουν οι χρήστες υπηρεσιών επικοινωνιών.

Το 1995 το **Συμβούλιο της Ευρώπης** εξέδωσε σύσταση για την προστασία των δεδομένων στον τομέα των τηλεπικοινωνιών, με ιδιαίτερη αναφορά στις τηλεφωνικές υπηρεσίες ⁹¹⁷. Σύμφωνα με την εν λόγω σύσταση, οι σκοποί της συλλογής και της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στον τομέα των τηλεπικοινωνιών θα πρέπει να περιορίζονται στα εξής: σύνδεση του χρήστη με το δίκτυο, διάθεση της συγκεκριμένης τηλεπικοινωνιακής υπηρεσίας, χρέωση του συνδρομητή, επαλήθευση ταυτότητας, διασφάλιση της βέλτιστης τεχνικής λειτουργίας και ανάπτυξη του δικτύου και των υπηρεσιών.

Ιδιαίτερη προσοχή δόθηκε επίσης στη χρήση των δικτύων επικοινωνιών για την αποστολή μηνυμάτων με σκοπό την απευθείας εμπορική προώθηση. Ο γενικός κανόνας είναι ότι μηνύματα απευθείας εμπορικής προώθησης δεν επιτρέπεται να αποστέλλονται σε κανέναν συνδρομητή ο οποίος έχει δηλώσει ρητά ότι δεν επιθυμεί να λαμβάνει τέτοιου είδους μηνύματα. Οι συσκευές αυτόματης κλήσης για τη μετάδοση προηχογραφημένων διαφημιστικών μηνυμάτων μπορούν να χρησιμοποιούνται μόνον εφόσον ο συνδρομητής έχει παράσχει τη ρητή συγκατάθεσή του. Λεπτομερέστεροι κανόνες στον εν λόγω τομέα προβλέπονται στο εθνικό δίκαιο.

Όσον αφορά το **νομικό πλαίσιο της ΕΕ**, έπειτα από μια πρώτη απόπειρα το 1997, η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες εκδόθηκε το 2002 και τροποποιήθηκε το 2009. Αυτό έγινε με σκοπό τη συμπλήρωση και την ειδική προσαρμογή των διατάξεων της προηγούμενης οδηγίας για την προστασία δεδομένων στον τομέα των τηλεπικοινωνιών ⁹¹⁸.

⁹¹⁷ Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1995), Σύσταση Rec (95)4 σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των τηλεπικοινωνιακών υπηρεσιών, με ιδιαίτερη αναφορά στις τηλεφωνικές υπηρεσίες, 7 Φεβρουαρίου 1995.

⁹¹⁸ Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (ΕΕ L 201 της 31.7.2002, σ. 37) (οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) όπως τροποποιήθηκε από την οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009 για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (ΕΕ L 337 της 18.12.2009, σ. 11).

Το πεδίο εφαρμογής της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες περιορίζεται στις υπηρεσίες επικοινωνιών που παρέχονται σε δημόσια δίκτυα ηλεκτρονικών επικοινωνιών.

Η οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες διακρίνει τρεις κύριες κατηγορίες δεδομένων που παράγονται κατά τη διάρκεια της επικοινωνίας:

- τα δεδομένα τα οποία συνιστούν το περιεχόμενο των μηνυμάτων που αποστέλλονται κατά τη διάρκεια της επικοινωνίας· τα εν λόγω δεδομένα είναι αυστηρώς εμπιστευτικά·
- τα δεδομένα που είναι αναγκαία για τη δημιουργία και τη διατήρηση της επικοινωνίας –γνωστά και ως μεταδεδομένα, τα οποία καλούνται «δεδομένα κίνησης» στην οδηγία– όπως πληροφορίες σχετικά με τους συμμετέχοντες στην επικοινωνία, τον χρόνο και τη διάρκεια της επικοινωνίας·
- μεταξύ των μεταδεδομένων, υπάρχουν δεδομένα που αφορούν ειδικά τη θέση της συσκευής επικοινωνίας, γνωστά και ως δεδομένα θέσης. Τα εν λόγω δεδομένα αφορούν ταυτόχρονα και τη θέση των χρηστών των συσκευών επικοινωνίας και έχουν ιδιαίτερη σημασία για τους χρήστες συσκευών κινητής τηλεφωνίας.

Τα δεδομένα κίνησης μπορούν να χρησιμοποιηθούν από τον πάροχο της υπηρεσίας μόνο για τη χρέωση του συνδρομητή και για την παροχή της υπηρεσίας από τεχνική άποψη. Ωστόσο, με τη συγκατάθεση του υποκειμένου των δεδομένων, τα εν λόγω δεδομένα μπορούν να κοινοποιούνται σε άλλους υπευθύνους επεξεργασίας οι οποίοι παρέχουν υπηρεσίες προστιθέμενης αξίας, όπως π.χ. η παροχή πληροφοριών, ανάλογα με την τοποθεσία του χρήστη, για τον πλησιέστερο σταθμό του μετρό ή το πλησιέστερο φαρμακείο ή το τοπικό δελτίο καιρού για τη συγκεκριμένη τοποθεσία.

Σύμφωνα με το άρθρο 15 της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, άλλη πρόσβαση στα δεδομένα σχετικά με τις επικοινωνίες σε ηλεκτρονικά δίκτυα, πρέπει να πληροί τα κριτήρια της δικαιολογημένης επέμβασης στο δικαίωμα προστασίας των δεδομένων, όπως προβλέπεται στο άρθρο 8 παράγραφος 2 της ΕΣΔΑ και επιβεβαιώνεται από τον Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ στα άρθρα 8 και 52. Αυτή η πρόσβαση θα ήταν δυνατόν να περιλαμβάνει πρόσβαση για τον σκοπό της διερεύνησης εγκλημάτων.

Με τις τροποποιήσεις του 2009 στην οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες⁹¹⁹ θεσπίστηκαν οι ακόλουθες διατάξεις:

- Οι περιορισμοί στην αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας εμπορικής προώθησης επεκτάθηκαν και στις υπηρεσίες σύντομων μηνυμάτων (SMS), στις υπηρεσίες μηνυμάτων πολυμέσων (MMS) και σε άλλα είδη παρεμφερών εφαρμογών· απαγορεύονται τα μηνύματα ηλεκτρονικού ταχυδρομείου για σκοπούς εμπορικής προώθησης χωρίς την προηγούμενη συγκατάθεση του αποδέκτη. Εάν δεν έχει δοθεί η εν λόγω συγκατάθεση, μηνύματα ηλεκτρονικού ταχυδρομείου για σκοπούς εμπορικής προώθησης μπορούν να αποστέλλονται μόνο σε προηγούμενους πελάτες, υπό την προϋπόθεση ότι έχουν δώσει τη διεύθυνση ηλεκτρονικού ταχυδρομείου τους και δεν αντιτάσσονται στην αποστολή των εν λόγω μηνυμάτων.
- Τα κράτη μέλη υποχρεούνται να παρέχουν ένδικα μέσα σε περίπτωση παράβασης της απαγόρευσης σχετικά με τις αυτόκλητες κλήσεις⁹²⁰.
- Η εγκατάσταση cookies, δηλαδή λογισμικού το οποίο παρακολουθεί και καταγράφει τις ενέργειες του χρήστη του υπολογιστή, δεν επιτρέπεται πλέον χωρίς τη συγκατάθεση του χρήστη του υπολογιστή. Το εθνικό δίκαιο θα πρέπει να ρυθμίζει λεπτομερέστερα τον τρόπο με τον οποίο θα πρέπει να δηλώνεται και να λαμβάνεται η συγκατάθεση προκειμένου να παρέχεται επαρκές επίπεδο προστασίας⁹²¹.

Σε περίπτωση παραβίασης των δεδομένων λόγω μη εξουσιοδοτημένης πρόσβασης, απώλειας ή καταστροφής των δεδομένων, πρέπει να ενημερώνεται αμελλητί η αρμόδια εποπτική αρχή. Οι συνδρομητές πρέπει να ενημερώνονται σε

919 Οδηγία 2009/136/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 25ης Νοεμβρίου 2009, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών (ΕΕ L 337 της 18.12.2009, σ. 11).

920 Βλ. την αναθεωρημένη οδηγία, άρθρο 13.

921 Βλ. ό.π., άρθρο 5· βλ. επίσης Ομάδα εργασίας του άρθρου 29 (2012), *Γνώμη 04/2012 σχετικά με την απαλλαγή που ισχύει σε σχέση με τη συναίνεση για τα cookies*, WP 194, Βρυξέλλες, 7 Ιουνίου 2012.

περίπτωση που είναι πιθανό να υποστούν ζημία ως συνέπεια αυτής της παραβί-
ασης δεδομένων ⁹²².

Η οδηγία για τη διατήρηση δεδομένων ⁹²³ υποχρέωνε τους παρόχους υπηρεσιών
επικοινωνιών να διατηρούν μεταδεδομένα. Ωστόσο, η εν λόγω οδηγία ακυρώ-
θηκε από το ΔΕΕ (για περισσότερες λεπτομέρειες, βλ. [ενότητα 8.3](#)).

Προοπτικές

Τον Ιανουάριο του 2017 η Ευρωπαϊκή Επιτροπή εξέδωσε νέα πρόταση κανονισμού
για τον σεβασμό της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, με σκοπό
την αντικατάσταση της παλαιότερης οδηγίας για την προστασία της ιδιωτικής
ζωής στις ηλεκτρονικές επικοινωνίες. Ο στόχος εξακολουθεί να είναι η προστασία
των «θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον
αφορά την παροχή και χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών, ιδίως των
δικαιωμάτων στον σεβασμό της ιδιωτικής ζωής και των επικοινωνιών, καθώς και
η προστασία των φυσικών προσώπων όσον αφορά την επεξεργασία δεδομένων
προσωπικού χαρακτήρα». Παράλληλα, η νέα πρόταση διασφαλίζει την ελεύ-
θερη κυκλοφορία των δεδομένων ηλεκτρονικών επικοινωνιών και των υπηρε-
σιών ηλεκτρονικών επικοινωνιών εντός της Ένωσης ⁹²⁴. Σε αντίθεση με τον Γενικό
Κανονισμό για την Προστασία Δεδομένων, ο οποίος διαλαμβάνει κατά κύριο λόγο
το άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, ο προτεινόμενος
κανονισμός επιδιώκει να ενσωματώσει το άρθρο 7 του Χάρτη στο παράγωγο
δίκαιο της ΕΕ.

Με τον κανονισμό αναμένεται να προσαρμοστούν οι διατάξεις της
προηγούμενης οδηγίας στις νέες τεχνολογίες και στις πραγματικές συνθή-
κες της αγοράς και να διαμορφωθεί ένα ολοκληρωμένο και συνεκτικό πλαίσιο
με τον Γενικό Κανονισμό για την Προστασία Δεδομένων. Υπό αυτή την έννοια,

⁹²² Βλ. επίσης Ομάδα εργασίας του άρθρου 29 (2011), [Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments](#), WP 184, Βρυξέλλες, 5 Απριλίου 2011.

⁹²³ Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαρτίου 2006, για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ (ΕΕ L 105 της 13.4.2006, σ. 54).

⁹²⁴ Πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες και την κατάργηση της οδηγίας 2002/58/ΕΚ (κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες), COM(2017) 10 final, άρθρο 1.

ο κανονισμός για τον σεβασμό της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες θα αποτελεί ειδική νομοθετική πράξη (*lex specialis*) σε σχέση με τον Γενικό Κανονισμό για την Προστασία Δεδομένων, διότι θα προβλέπει κατάλληλα προσαρμοσμένες διατάξεις σχετικά με τα δεδομένα των ηλεκτρονικών επικοινωνιών τα οποία συνιστούν δεδομένα προσωπικού χαρακτήρα. Ο νέος κανονισμός καλύπτει την επεξεργασία των «δεδομένων ηλεκτρονικών επικοινωνιών», συμπεριλαμβανομένου του περιεχομένου ηλεκτρονικών επικοινωνιών και των μεταδιδόμενων που δεν συνιστούν απαραίτητως δεδομένα προσωπικού χαρακτήρα. Το εδαφικό πεδίο εφαρμογής περιορίζεται στην ΕΕ, μεταξύ άλλων σε περίπτωση που τα δεδομένα που λαμβάνονται στην ΕΕ υποβάλλονται σε επεξεργασία εκτός των συνόρων της, και επεκτείνονται στους παρόχους υπηρεσιών που παρέχουν περιεχόμενο, υπηρεσίες ή εφαρμογές μέσω του διαδικτύου. Αυτοί είναι πάροχοι υπηρεσιών οι οποίοι παρέχουν περιεχόμενο χωρίς την άμεση συμμετοχή φορέα εκμετάλλευσης δικτύου ή φορέα παροχής υπηρεσιών στο διαδίκτυο (ISP). Παραδείγματα παρόχων αυτού του είδους αποτελούν το Skype (φωνητικές κλήσεις και βιντεοκλήσεις), το WhatsApp (ανταλλαγή μηνυμάτων), το Google (αναζήτηση), το Spotify (μουσική) ή το Netflix (περιεχόμενο βίντεο). Οι μηχανισμοί επιβολής του Γενικού Κανονισμού για την Προστασία Δεδομένων θα ισχύουν και για τον νέο κανονισμό.

Ο κανονισμός για τον σεβασμό της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες πρόκειται να εκδοθεί πριν από τις 25 Μαΐου 2018, ημερομηνία κατά την οποία ο Γενικός Κανονισμός για την Προστασία Δεδομένων θα είναι εφαρμοστέος και στα 28 κράτη μέλη. Ωστόσο, αυτό προϋποθέτει τη συμφωνία τόσο του Ευρωπαϊκού Κοινοβουλίου όσο και του Συμβουλίου ⁹²⁵.

925 Για περισσότερες πληροφορίες, βλ. Ευρωπαϊκή Επιτροπή (2017), «Η Επιτροπή προτείνει αυστηρούς κανόνες προστασίας της ιδιωτικής ζωής σε όλες τις ηλεκτρονικές επικοινωνίες και επικαιροποιεί τους κανόνες προστασίας δεδομένων τους οποίους εφαρμόζουν τα όργανα της ΕΕ», δελτίο Τύπου, 10 Ιανουαρίου 2017.

9.2. Δεδομένα στο πλαίσιο των εργασιακών σχέσεων

Κύρια σημεία

- Συγκεκριμένοι κανόνες για την προστασία των δεδομένων στο πλαίσιο των εργασιακών σχέσεων περιγράφονται στη σύσταση του Συμβουλίου της Ευρώπης για τα εργασιακά δεδομένα.
- Στον Γενικό Κανονισμό για την Προστασία Δεδομένων γίνεται ειδική αναφορά στις εργασιακές σχέσεις μόνο στο πλαίσιο της επεξεργασίας ευαίσθητων δεδομένων.
- Η εγκυρότητα της συγκατάθεσης, η οποία πρέπει να παρέχεται ελεύθερα, ως νομική βάση για την επεξεργασία δεδομένων των εργαζομένων μπορεί να τεθεί υπό αμφισβήτηση, λαμβανομένης υπόψη της οικονομικής ανισότητας μεταξύ του εργοδότη και των εργαζομένων. Απαιτείται προσεκτική αξιολόγηση των περιστάσεων υπό τις οποίες ζητείται η συγκατάθεση.

Η επεξεργασία δεδομένων στο πλαίσιο της απασχόλησης υπόκειται στη γενική νομοθεσία της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα. Ωστόσο, ένας κανονισμός⁹²⁶ πραγματεύεται ειδικά την προστασία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα ευρωπαϊκά θεσμικά όργανα στο πλαίσιο της απασχόλησης (μεταξύ άλλων). Στον Γενικό Κανονισμό για την Προστασία Δεδομένων γίνεται ειδική μνεία στις εργασιακές σχέσεις στο άρθρο 9 παράγραφος 2, όπου ορίζεται ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται κατά την εκτέλεση των υποχρεώσεων ή την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα της απασχόλησης.

Βάσει του Γενικού Κανονισμού για την Προστασία Δεδομένων, ο εργαζόμενος θα πρέπει να είναι σε θέση να διακρίνει σαφώς τα δεδομένα για τα οποία συγκατατίθεται να υποβληθούν σε επεξεργασία/ να αποθηκευτούν, καθώς και τους σκοπούς για τους οποίους αποθηκεύονται τα δεδομένα που τον αφορούν. Οι εργαζόμενοι θα πρέπει επίσης να ενημερώνονται για τα δικαιώματά τους και για τη χρονική διάρκεια αποθήκευσης των δεδομένων προκειμένου να είναι σε θέση

⁹²⁶ Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 8 της 12.1.2001, σ. 1).

να δώσουν ελεύθερα τη συγκατάθεσή τους. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα η οποία είναι πιθανό να θέτει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ο εργοδότης πρέπει να γνωστοποιεί την εν λόγω παραβίαση στον εργαζόμενο. Το άρθρο 88 του κανονισμού επιτρέπει στα κράτη μέλη να θεσπίζουν ειδικούς κανόνες προκειμένου να διασφαλίζουν την προστασία των δικαιωμάτων και των ελευθεριών έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των εργαζομένων στο πλαίσιο της απασχόλησης.

Παράδειγμα: Στην υπόθεση *Worten*⁹²⁷, τα δεδομένα περιλάμβαναν δελτίο καταγραφής του χρόνου εργασίας που περιείχε τις περιόδους εργασίας ανά ημέρα και τις περιόδους ανάπαυλας, τα οποία συνιστούν δεδομένα προσωπικού χαρακτήρα. Το εθνικό δίκαιο μπορεί να επιβάλλει στον εργοδότη την υποχρέωση να θέτει τα δελτία καταγραφής του χρόνου εργασίας στη διάθεση των εθνικών αρχών που είναι αρμόδιες για την εποπτεία των συνθηκών εργασίας. Με τον τρόπο αυτόν παρέχεται η δυνατότητα άμεσης πρόσβασης στα σχετικά δεδομένα προσωπικού χαρακτήρα. Ωστόσο, η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα είναι αναγκαία ώστε να καθίσταται δυνατή η εποπτεία της νομοθεσίας σχετικά με τις συνθήκες εργασίας από την εθνική αρχή⁹²⁸.

Όσον αφορά το **Συμβούλιο της Ευρώπης**, η σύσταση για τα εργασιακά δεδομένα εκδόθηκε το 1989 και αναθεωρήθηκε το 2015⁹²⁹. Η σύσταση καλύπτει την επεξεργασία δεδομένων προσωπικού χαρακτήρα για τους σκοπούς της απασχόλησης, τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα. Η επεξεργασία πρέπει να τηρεί ορισμένες αρχές και περιορισμούς, όπως η αρχή της διαφάνειας και η διαβούλευση με εκπροσώπους των εργαζομένων πριν από την έναρξη εφαρμογής συστημάτων παρακολούθησης στον χώρο εργασίας. Η σύσταση ορίζει επίσης ότι οι εργοδότες θα πρέπει να θέτουν σε εφαρμογή προληπτικά μέτρα, όπως φίλτρα, αντί να παρακολουθούν τη χρήση του διαδικτύου από τους εργαζομένους.

927 ΔΕΕ, C-342/12, *Worten – Equipamentos para o Lar SA κατά Autoridade para as Condições de Trabalho (ACT)*, 30 Μαΐου 2013, σκέψη 19.

928 Ό.π., σκέψη 43.

929 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2015), Σύσταση Rec (2015)5 προς τα κράτη μέλη σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της απασχόλησης, Απρίλιος 2015.

Μελέτη των συνηθέστερων προβλημάτων όσον αφορά την προστασία των δεδομένων ειδικά στον εργασιακό τομέα περιλαμβάνεται σε έγγραφο εργασίας της Ομάδας εργασίας του άρθρου 29 ⁹³⁰. Η Ομάδα εργασίας ανέλυσε τη σημασία της συγκατάθεσης ως νομικής βάσης για την επεξεργασία δεδομένων στον τομέα της απασχόλησης ⁹³¹. Κατέληξε δε στο συμπέρασμα ότι η οικονομική ανισότητα μεταξύ του εργοδότη που ζητεί τη συγκατάθεση και του εργαζομένου που δίνει τη συγκατάθεση δημιουργεί συχνά αμφιβολίες ως προς το κατά πόσον η συγκατάθεση δόθηκε ελεύθερα ή όχι. Ως εκ τούτου, κατά την εκτίμηση της εγκυρότητας της συγκατάθεσης στο πλαίσιο της απασχόλησης θα πρέπει να εξετάζονται προσεκτικά οι περιστάσεις υπό τις οποίες βασίζεται η συγκατάθεση ως νομική βάση για την επεξεργασία δεδομένων.

Ένα συχνό πρόβλημα όσον αφορά την προστασία δεδομένων στο σύνηθες περιβάλλον εργασίας στη σημερινή εποχή έγκειται στη θεμιτή έκταση της παρακολούθησης των ηλεκτρονικών επικοινωνιών των εργαζομένων εντός του χώρου εργασίας. Προβάλλεται συχνά ο ισχυρισμός ότι το εν λόγω πρόβλημα μπορεί να επιλυθεί εύκολα με την απαγόρευση της χρήσης των μέσων επικοινωνίας στον χώρο εργασίας για ιδιωτικούς σκοπούς. Ωστόσο, μια γενική απαγόρευση αυτού του είδους θα ήταν ενδεχομένως δυσανάλογη και μη ρεαλιστική. Οι αποφάσεις του ΕΔΔΑ στις υποθέσεις *Copland κατά Ηνωμένου Βασιλείου* και *Bărbulescu κατά Ρουμανίας* παρουσιάζουν εν προκειμένω ιδιαίτερο ενδιαφέρον.

Παράδειγμα: Στην υπόθεση *Copland κατά Ηνωμένου Βασιλείου* ⁹³², η χρήση τηλεφώνου, ηλεκτρονικού ταχυδρομείου και διαδικτύου από μια υπάλληλο σχολής τριτοβάθμιας εκπαίδευσης τελούσε υπό μυστική παρακολούθηση προκειμένου να διαπιστωθεί αν έκανε υπέρμετρη χρήση των υποδομών της σχολής για προσωπικούς σκοπούς. Το ΕΔΔΑ έκρινε ότι οι τηλεφωνικές κλήσεις από τον χώρο εργασίας καλύπτονται από τις έννοιες της ιδιωτικής ζωής και αλληλογραφίας. Ως εκ τούτου, οι τηλεφωνικές κλήσεις και τα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από τον χώρο εργασίας, καθώς και οι πληροφορίες που προέρχονται από την παρακολούθηση της προσωπικής χρήσης του διαδικτύου, προστατεύονται από το άρθρο 8 της ΕΣΔΑ. Στην περίπτωση της προσφεύγουσας, δεν

930 Ομάδα εργασίας του άρθρου 29 (2017), *Γνώμη 2/2017 σχετικά με την επεξεργασία δεδομένων στην εργασία*, WP 249, Βρυξέλλες, 8 Ιουνίου 2017.

931 Ομάδα εργασίας του άρθρου 29 (2005), *Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/ΕΚ της 24ης Οκτωβρίου 1995*, WP 114, Βρυξέλλες, 25 Νοεμβρίου 2005.

932 ΕΔΔΑ, *Copland κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 62617/00, 3 Απριλίου 2007.

υπήρχαν διατάξεις οι οποίες να ρυθμίζουν τις συνθήκες υπό τις οποίες οι εργοδότες μπορούν να παρακολουθούν τη χρήση του τηλεφώνου, του ηλεκτρονικού ταχυδρομείου και του διαδικτύου από τους εργαζομένους. Κατά συνέπεια, η εν λόγω επέμβαση δεν ήταν σύμφωνη με τον νόμο. Το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι παραβιάστηκε το άρθρο 8 της ΕΣΔΑ.

Παράδειγμα: Στην υπόθεση *Bărbulescu κατά Ρουμανίας*⁹³³, ο προσφεύγων απολύθηκε επειδή χρησιμοποίησε το διαδίκτυο στον χώρο απασχόλησής του εν ώρα εργασίας, κατά παράβαση των εσωτερικών κανονισμών. Ο εργοδότης του παρακολουθούσε τις επικοινωνίες του. Τα αρχεία, στα οποία καταγράφονται μηνύματα αμιγώς ιδιωτικού χαρακτήρα, προσκομίστηκαν κατά τη διάρκεια των διαδικασιών ενώπιον εθνικών δικαστηρίων. Το ΕΔΔΑ έκρινε ότι έχει εφαρμογή το άρθρο 8 και, ως εκ τούτου, δεν εξέτασε αν οι περιοριστικοί κανονισμοί του εργοδότη παρείχαν στον προσφεύγοντα εύλογη προσδοκία όσον αφορά την προστασία της ιδιωτικής ζωής, αλλά αποφάνθηκε, εν πάση περιπτώσει, ότι οι οδηγίες εκ μέρους εργοδότη δεν μπορούν να εκμηδενίζουν την ιδιωτική κοινωνική ζωή στον χώρο εργασίας.

Επί της ουσίας, πρέπει να αναγνωρίζεται στα συμβαλλόμενα κράτη ευρύ περιθώριο εκτίμησης κατά την αξιολόγηση της ανάγκης θέσπισης νομικού πλαισίου που θα διέπει τις προϋποθέσεις υπό τις οποίες ένας εργοδότης μπορεί να ρυθμίζει τις ηλεκτρονικές ή άλλης μορφής μη επαγγελματικές επικοινωνίες των υπαλλήλων του στον χώρο εργασίας. Μολαταύτα, οι τοπικές αρχές έπρεπε να διασφαλίσουν ότι η θέσπιση, από τον εργοδότη, μέτρων παρακολούθησης της αλληλογραφίας και άλλων επικοινωνιών, ανεξάρτητα από την έκταση και τη διάρκεια των εν λόγω μέτρων, συνοδεύεται από κατάλληλες και επαρκείς εγγυήσεις έναντι της κατάχρησης. Η αναλογικότητα και οι διαδικαστικές εγγυήσεις έναντι της αυθαιρεσίας ήταν καθοριστικής σημασίας και το ΕΔΔΑ προσδιόρισε ορισμένους παράγοντες οι οποίοι ήταν λυσιτελείς υπό τις συγκεκριμένες περιστάσεις. Στους παράγοντες αυτούς συγκαταλέγονταν, για παράδειγμα, η έκταση της παρακολούθησης των υπαλλήλων από τον εργοδότη και ο βαθμός επέμβασης στην ιδιωτική ζωή του υπαλλήλου, οι επιπτώσεις για τον υπάλληλο και η πρόβλεψη ή μη των κατάλληλων εγγυήσεων. Επιπλέον, οι εθνικές αρχές έπρεπε να διασφαλίσουν ότι υπάλληλος

933 ΕΔΔΑ, *Bărbulescu κατά Ρουμανίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 61496/08, 5 Σεπτεμβρίου 2017, σκέψη 121.

του οποίου οι επικοινωνίες είχαν υποβληθεί σε παρακολούθηση είχε δικαίωμα προσφυγής ενώπιον δικαστηρίου με δικαιοδοσία να καθορίσει, τουλάχιστον επί της ουσίας, τον τρόπο τήρησης των περιγραφέντων κριτηρίων και αν τα προσβαλλόμενα μέτρα ήταν νόμιμα.

Στην προκειμένη περίπτωση, το ΕΔΔΑ διαπίστωσε παράβαση του άρθρου 8, επειδή οι τοπικές αρχές δεν είχαν προστατεύσει κατάλληλα το δικαίωμα του προσφεύγοντος στον σεβασμό της ιδιωτικής ζωής και της αλληλογραφίας του και, ως εκ τούτου, δεν είχαν επιτύχει ορθή ισορροπία μεταξύ των διακυβευόμενων συμφερόντων.

Σύμφωνα με τη σύσταση του Συμβουλίου της Ευρώπης για τον εργασιακό τομέα, τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται για τους σκοπούς της απασχόλησης θα πρέπει να λαμβάνονται απευθείας από τον εργαζόμενο.

Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται για την πρόσληψη προσωπικού πρέπει να περιορίζονται στις πληροφορίες που είναι αναγκαίες για την εκτίμηση της καταλληλότητας των υποψηφίων και των δυνατοτήτων εξέλιξης της σταδιοδρομίας τους.

Στη σύσταση γίνεται επίσης ειδική μνεία στις υποκειμενικές κρίσεις σχετικά με την απόδοση στην εργασία ή τις δυνατότητες του κάθε εργαζομένου. Οι υποκειμενικές κρίσεις πρέπει να βασίζονται σε δίκαιη και έντιμη αξιολόγηση και να μην διατυπώνονται με προσβλητικό τρόπο. Η απαίτηση αυτή προκύπτει από την αρχή της θεμιτής επεξεργασίας των δεδομένων και από την αρχή της ακρίβειας των δεδομένων.

Ιδιαίτερη πτυχή του δικαίου για την προστασία των δεδομένων στις σχέσεις εργοδοτών–εργαζομένων συνιστά ο ρόλος των εκπροσώπων των εργαζομένων. Οι εν λόγω εκπρόσωποι μπορούν να λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων μόνο στον βαθμό που απαιτείται ώστε να είναι σε θέση να εκπροσωπούν τα συμφέροντα των εργαζομένων ή εάν τα εν λόγω δεδομένα είναι αναγκαία για την εκπλήρωση ή την εποπτεία των υποχρεώσεων που καθορίζονται στις συλλογικές συμβάσεις.

Η επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα που συλλέγονται για τους σκοπούς της απασχόλησης επιτρέπεται μόνο σε συγκεκριμένες περιπτώσεις και κατ' εφαρμογή των εγγυήσεων που προβλέπονται από το εθνικό δίκαιο. Οι εργοδότες μπορούν να ερωτούν τους εργαζομένους ή τους

υποψήφιους εργαζομένους για την κατάσταση της υγείας τους ή να τους υποβάλλουν σε ιατρικές εξετάσεις μόνον εάν αυτό είναι αναγκαίο. Αυτό μπορεί να είναι: για την εξακρίβωση της καταλληλότητάς τους για τη θέση εργασίας, τη συμμόρφωση προς τις απαιτήσεις της προληπτικής ιατρικής, τη διασφάλιση των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλων εργαζομένων και ατόμων, την έγκριση της χορήγησης κοινωνικών επιδομάτων ή την ανταπόκριση σε δικαστική αίτηση. Δεδομένα υγείας δεν επιτρέπεται να συλλέγονται από άλλες πηγές εκτός του ενδιαφερόμενου εργαζομένου, εκτός εάν έχει δοθεί ρητή και εν πλήρει επιγνώσει συγκατάθεσή του ή εάν αυτό προβλέπεται από το εθνικό δίκαιο.

Σύμφωνα με τη σύσταση για τον εργασιακό τομέα, οι εργαζόμενοι θα πρέπει να ενημερώνονται για τον σκοπό της επεξεργασίας των δεδομένων που τους αφορούν, για το είδος των δεδομένων που συλλέγονται, για τους αποδέκτες στους οποίους διαβιβάζονται τακτικά τα εν λόγω δεδομένα, καθώς και για τον σκοπό και τη νομική βάση των εν λόγω κοινοποιήσεων. Η πρόσβαση σε ηλεκτρονικές επικοινωνίες στον χώρο εργασίας είναι δυνατή μόνο για λόγους ασφαλείας ή για άλλους θεμιτούς λόγους και επιτρέπεται μόνον κατόπιν ενημέρωσης των εργαζομένων ότι ο εργοδότης μπορεί να έχει πρόσβαση σε αυτού του είδους τις επικοινωνίες.

Οι εργαζόμενοι πρέπει να έχουν δικαίωμα πρόσβασης στα δεδομένα για την απασχόλησή τους, καθώς και δικαίωμα διόρθωσης ή διαγραφής. Εάν τα δεδομένα που υποβάλλονται σε επεξεργασία είναι υποκειμενικές κρίσεις, οι εργαζόμενοι πρέπει επίσης να έχουν δικαίωμα να αμφισβητήσουν τις εν λόγω κρίσεις. Ωστόσο, τα δικαιώματα αυτά μπορεί να περιορίζονται προσωρινά για τον σκοπό της διενέργειας εσωτερικών ερευνών. Όταν απορρίπτεται αίτημα εργαζομένου για πρόσβαση, διόρθωση ή διαγραφή δεδομένων απασχόλησης προσωπικού χαρακτήρα, το εθνικό δίκαιο πρέπει να προβλέπει τις κατάλληλες διαδικασίες προσφυγής κατά της απορριπτικής απόφασης.

9.3. Δεδομένα υγείας

Κύριο σημείο

- Τα ιατρικά δεδομένα είναι ευαίσθητα δεδομένα προσωπικού χαρακτήρα και, ως εκ τούτου, τυγχάνουν ειδικής προστασίας.

Τα δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία του υποκειμένου των δεδομένων χαρακτηρίζονται ως ευαίσθητα δεδομένα σύμφωνα με το άρθρο 9 παράγραφος 1 του Γενικού Κανονισμού για την Προστασία Δεδομένων και το άρθρο 6 της Εκσυγχρονισμένης Σύμβασης 108. Για τον λόγο αυτόν, τα δεδομένα που συνδέονται με την υγεία υπάγονται σε αυστηρότερο καθεστώς επεξεργασίας δεδομένων σε σύγκριση με τα μη ευαίσθητα δεδομένα. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων απαγορεύει την επεξεργασία «δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία» (τα οποία νοούνται ως «όλα τα δεδομένα που αφορούν την κατάσταση της υγείας του υποκειμένου των δεδομένων και τα οποία αποκαλύπτουν πληροφορίες για την προηγούμενη, τρέχουσα ή μελλοντική κατάσταση της σωματικής ή ψυχικής υγείας του υποκειμένου των δεδομένων») ⁹³⁴, καθώς και την επεξεργασία γενετικών και βιομετρικών δεδομένων, εκτός εάν επιτρέπεται βάσει του άρθρου 9 παράγραφος 2. Και τα δύο είδη δεδομένων έχουν προστεθεί στον κατάλογο με τις «ειδικές κατηγορίες δεδομένων» ⁹³⁵.

Παράδειγμα: Στην υπόθεση *Z κατά Φινλανδίας* ⁹³⁶, ο πρώην σύζυγος της προσφεύγουσας, ο οποίος είχε προσβληθεί από τον ιό HIV, είχε διαπράξει σειρά σεξουαλικών αδικημάτων. Στη συνέχεια καταδικάστηκε για ανθρωποκτονία εκ προθέσεως διότι είχε εκθέσει εν γνώσει του τα θύματά του στον κίνδυνο μόλυνσης από τον ιό HIV. Το εθνικό δικαστήριο διέταξε το πλήρες κείμενο της απόφασης και η δικογραφία να παραμείνουν απόρρητα για διάστημα 10 ετών, παρότι η προσφεύγουσα ζητούσε να παραμείνουν απόρρητα για μεγαλύτερο χρονικό διάστημα. Τα αιτήματά

⁹³⁴ Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογική σκέψη 35.

⁹³⁵ Ό.π., άρθρο 2.

⁹³⁶ ΕΔΔΑ, *Z κατά Φινλανδίας*, προσφυγή αριθ. 22009/93, 25 Φεβρουαρίου 1997, σκέψεις 94 και 112· βλ. επίσης ΕΔΔΑ, *M.S. κατά Σουηδίας*, προσφυγή αριθ. 20837/92, 27 Αυγούστου 1997· ΕΔΔΑ, *L.L. κατά Γαλλίας*, προσφυγή αριθ. 7508/02, 10 Οκτωβρίου 2006· ΕΔΔΑ, *I κατά Φινλανδίας*, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008· ΕΔΔΑ, *Κ.Η. κ.λπ. κατά Σλοβακίας*, προσφυγή αριθ. 32881/04, 28 Απριλίου 2009· ΕΔΔΑ, *Szuluk κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 36936/05, 2 Ιουνίου 2009.

της απορρίφθηκαν και σε δεύτερο βαθμό, η δε απόφαση του εφετείου περιείχε το πλήρες όνομα τόσο της προσφεύγουσας όσο και του πρώην συζύγου της. Το ΕΔΔΑ έκρινε ότι η επέμβαση αυτή δεν ήταν αναγκαία σε μια δημοκρατική κοινωνία, διότι η προστασία των ιατρικών δεδομένων είναι θεμελιώδους σημασίας για την απόλαυση του δικαιώματος στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, ιδίως όσον αφορά τις πληροφορίες σχετικά με τη μόλυνση από τον ιό HIV, δεδομένου ότι η εν λόγω ασθένεια επιφέρει στιγματισμό του ασθενούς σε πολλές κοινωνίες. Ως εκ τούτου, το ΕΔΔΑ κατέληξε στο συμπέρασμα ότι η παροχή πρόσβασης στην απόφαση του εφετείου, στην οποία περιγράφονται τα στοιχεία ταυτότητας της προσφεύγουσας και η κατάσταση της υγείας της, αμέσως μετά την παρέλευση 10 ετών από την έκδοση της απόφασης, θα συνιστούσε παραβίαση του άρθρου 8 της ΕΣΔΑ.

Στο πλαίσιο του **δικαίου της ΕΕ**, το άρθρο 9 παράγραφος 2 στοιχείο η) του Γενικού Κανονισμού για την Προστασία Δεδομένων επιτρέπει την επεξεργασία ιατρικών δεδομένων όταν είναι απαραίτητη για σκοπούς προληπτικής ιατρικής, ιατρικής διάγνωσης, παροχής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών υπηρεσιών. Ωστόσο, η επεξεργασία επιτρέπεται μόνον όταν εκτελείται από επαγγελματίες του τομέα της υγείας ο οποίος υπόκειται σε υποχρέωση τήρησης του επαγγελματικού απορρήτου ή από άλλο πρόσωπο το οποίο υπέχει ομοίως αντίστοιχη υποχρέωση.

Στο πλαίσιο του **δικαίου του Συμβουλίου της Ευρώπης**, η σύσταση του Συμβουλίου της Ευρώπης του 1997 σχετικά με τα ιατρικά δεδομένα εφαρμόζει λεπτομερέστερα τις αρχές της Σύμβασης 108 στην επεξεργασία δεδομένων στον ιατρικό τομέα⁹³⁷. Οι προτεινόμενοι κανόνες συνάδουν με τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων όσον αφορά τους νόμιμους σκοπούς της επεξεργασίας ιατρικών δεδομένων, τις αναγκαίες υποχρεώσεις τήρησης του επαγγελματικού απορρήτου που πρέπει να δεσμεύει τα πρόσωπα τα οποία χρησιμοποιούν τα ιατρικά δεδομένα, καθώς και τα δικαιώματα των υποκειμένων των δεδομένων όσον αφορά τη διαφάνεια και την πρόσβαση, τη διόρθωση και τη διαγραφή. Επιπλέον, τα ιατρικά δεδομένα τα οποία υποβάλλονται νόμιμα σε επεξεργασία από επαγγελματίες του τομέα της υγείας δεν επιτρέπεται να διαβιβάζονται στις αρχές επιβολής του νόμου, εκτός εάν παρέχονται «επαρκείς εγγυήσεις για την αποτροπή δημοσιοποίησης η οποία δεν συνάδει με τον σεβασμό

937 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1997), Σύσταση Rec (97)5 προς τα κράτη μέλη της ΕΕ σχετικά με την προστασία των ιατρικών δεδομένων, 13 Φεβρουαρίου 1997. Σημειώνεται ότι η συγκεκριμένη Πρόταση βρίσκεται σε διαδικασία επικαιροποίησης.

[...] της ιδιωτικής ζωής που κατοχυρώνεται στο άρθρο 8 της ΕΣΔΑ»⁹³⁸. Το εθνικό δίκαιο πρέπει επίσης να «διατυπώνεται με επαρκή βαθμό ακρίβειας και να διασφαλίζει κατάλληλη νομική προστασία έναντι της αυθαιρεσίας»⁹³⁹.

Επιπλέον, η σύσταση σχετικά με τα ιατρικά δεδομένα περιέχει ειδικές διατάξεις για τα ιατρικά δεδομένα των εμβρύων και των ανίκανων προς δικαιοπραξία προσώπων, καθώς και για την επεξεργασία γενετικών δεδομένων. Η επιστημονική έρευνα αναγνωρίζεται ρητά ως λόγος διατήρησης των δεδομένων για μεγαλύτερο από το αναγκαίο χρονικό διάστημα, αν και για τον σκοπό αυτόν απαιτείται συνήθως ανωνυμοποίηση. Στο άρθρο 12 της σύστασης σχετικά με τα ιατρικά δεδομένα προτείνονται λεπτομερείς ρυθμίσεις για καταστάσεις στις οποίες οι ερευνητές χρειάζονται προσωπικά δεδομένα, και τα ανωνυμοποιημένα δεδομένα δεν επαρκούν.

Η ψευδωνυμοποίηση μπορεί να αποδειχθεί πρόσφορο μέσο, αφενός, για την κάλυψη των επιστημονικών αναγκών και, αφετέρου, για την προστασία των συμφερόντων των ενδιαφερόμενων ασθενών. Η έννοια της ψευδωνυμοποίησης στο πλαίσιο της προστασίας των δεδομένων επεξηγείται αναλυτικότερα στην [ενότητα 2.1.1](#).

Η σύσταση του Συμβουλίου της Ευρώπης του 2016 σχετικά με τα δεδομένα που προκύπτουν από γενετικούς ελέγχους ισχύει επίσης για την επεξεργασία δεδομένων στον ιατρικό τομέα⁹⁴⁰. Η σύσταση αυτή είναι ιδιαίτερης σημασίας για την ηλεκτρονική υγεία, στο πλαίσιο της οποίας χρησιμοποιούνται ΤΠΕ για τη διευκόλυνση της ιατρικής περίθαλψης. Σχετικό παράδειγμα αποτελεί η αποστολή των αποτελεσμάτων εξέτασης γονικής συγγένειας ενός ασθενούς από έναν φορέα παροχής υγειονομικής περίθαλψης σε άλλον. Σκοπός της εν λόγω σύστασης είναι η προστασία των δικαιωμάτων των προσώπων των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για ασφαλιστικούς σκοπούς, ήτοι για την ασφάλιση έναντι κινδύνων σχετικών με την υγεία, τη σωματική ακεραιότητα, την ηλικία ή τον θάνατο ενός προσώπου. Οι ασφαλιστές πρέπει να αιτιολογούν την επεξεργασία δεδομένων που αφορούν την υγεία, η οποία θα πρέπει να είναι ανάλογη προς τη φύση και τη σημασία του υπό εξέταση κινδύνου.

938 ΕΔΔΑ, *Avilkina κ.λπ. κατά Ρωσίας*, προσφυγή αριθ. 1585/09, 6 Ιουνίου 2013, σκέψη 53. Βλ. επίσης ΕΔΔΑ, *Birjuk κατά Λιθουανίας*, Νο. 23373/03, 25 Νοεμβρίου 2008.

939 ΕΔΔΑ, *L.H. κατά Λετονίας*, προσφυγή αριθ. 52019/07, 29 Απριλίου 2014, σκέψη 59.

940 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2016), Σύσταση Rec (2016) 8 προς τα κράτη μέλη σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία για σκοπούς ασφάλισης, συμπεριλαμβανομένων των δεδομένων που προκύπτουν από γενετικές δοκιμές, 26 Οκτωβρίου 2016.

Η επεξεργασία δεδομένων αυτού του είδους εξαρτάται από τη συγκατάθεση του υποκειμένου των δεδομένων. Οι ασφαλιστές θα πρέπει επίσης να προβλέπουν την παροχή εγγυήσεων για την αποθήκευση δεδομένων που αφορούν την υγεία.

Οι κλινικές δοκιμές –οι οποίες αφορούν την αξιολόγηση της επίδρασης νέων φαρμάκων σε ασθενείς σε τεκμηριωμένα ερευνητικά περιβάλλοντα– έχουν σημαντικές επιπτώσεις ως προς την προστασία των δεδομένων. Οι κλινικές δοκιμές φαρμάκων που προορίζονται για τον άνθρωπο διέπονται από τον κανονισμό (ΕΕ) αριθ. 536/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Απριλίου 2014, για τις κλινικές δοκιμές φαρμάκων που προορίζονται για τον άνθρωπο και για την κατάργηση της οδηγίας 2001/20/ΕΚ (κανονισμός για τις κλινικές δοκιμές)⁹⁴¹. Τα κύρια στοιχεία του κανονισμού για τις κλινικές δοκιμές είναι τα ακόλουθα:

- εναρμονισμένη διαδικασία εφαρμογής μέσω της δικτυακής πύλης της ΕΕ⁹⁴².
- προθεσμίες για την αξιολόγηση της εφαρμογής όσον αφορά τις κλινικές δοκιμές⁹⁴³.
- επιτροπή δεοντολογίας, η οποία εντάσσεται στο πλαίσιο της αξιολόγησης, σύμφωνα με το δίκαιο των κρατών μελών (και το δίκαιο της ΕΕ που ορίζει τα αντίστοιχα χρονικά διαστήματα)⁹⁴⁴ και
- βελτίωση της διαφάνειας των κλινικών δοκιμών και των αποτελεσμάτων τους⁹⁴⁵.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων ορίζει ότι για τον σκοπό της συγκατάθεσης στη συμμετοχή σε δραστηριότητες επιστημονικής έρευνας στο πλαίσιο κλινικών δοκιμών ισχύει ο κανονισμός (ΕΕ) αριθ. 536/2014⁹⁴⁶.

941 Κανονισμός (ΕΕ) αριθ. 536/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Απριλίου 2014 για τις κλινικές δοκιμές φαρμάκων που προορίζονται για τον άνθρωπο και για την κατάργηση της οδηγίας 2001/20/ΕΚ (κανονισμός για τις κλινικές δοκιμές) (ΕΕ L 158 της 27.5.2014, σ. 1).

942 Κανονισμός για τις κλινικές δοκιμές, άρθρο 5 παράγραφος 1.

943 Ο.π., άρθρο 5 παράγραφοι 2 έως 5.

944 Ο.π., άρθρο 2 παράγραφος 2 σημείο 11.

945 Ο.π., άρθρο 9 παράγραφος 1 και αιτιολογική σκέψη 67.

946 Γενικός Κανονισμός για την Προστασία Δεδομένων, αιτιολογικές σκέψεις 156 και 161.

Σε επίπεδο ΕΕ εκκρεμεί μεγάλος αριθμός νομοθετικών και άλλων πρωτοβουλιών σχετικά με τα δεδομένα προσωπικού χαρακτήρα στον τομέα της υγείας⁹⁴⁷.

Ηλεκτρονικά μητρώα υγείας

Το ηλεκτρονικό μητρώο υγείας ορίζεται ως «λεπτομερές ιατρικό μητρώο ή αντίστοιχο αρχείο που αφορά την προηγούμενη και την παρούσα φυσική και διανοητική κατάσταση της υγείας ενός ατόμου, σε ηλεκτρονική μορφή, και το οποίο παρέχει άμεση πρόσβαση στα δεδομένα αυτά για ιατρική περίθαλψη και άλλους στενά συνδεδεμένους σκοπούς»⁹⁴⁸. Τα ηλεκτρονικά μητρώα υγείας είναι οι ηλεκτρονικές μορφές του ιατρικού ιστορικού των ασθενών και ενδέχεται να περιλαμβάνουν κλινικά δεδομένα τα οποία αφορούν τα συγκεκριμένα άτομα, όπως είναι το προηγούμενο ιατρικό τους ιστορικό, τα προβλήματα και οι παθήσεις που έχουν παρουσιάσει κατά το παρελθόν, οι φαρμακευτικές αγωγές και θεραπείες, καθώς και τα αποτελέσματα εξετάσεων και εργαστηριακών ελέγχων, και οι αντίστοιχες εκθέσεις. Δυνατότητα πρόσβασης στους εν λόγω ηλεκτρονικούς φακέλους, οι οποίοι μπορεί να ποικίλλουν από ολόκληρα αρχεία μέχρι απλά αποσπάσματα ή περιλήψεις, μπορεί να έχει ο γενικός ιατρός, ο φαρμακοποιός και άλλοι επαγγελματίες του τομέα της υγείας. Η έννοια της «ηλεκτρονικής υγείας» άπτεται επίσης αυτών των ιατρικών μητρώων.

Παράδειγμα: Ο κ. Α υπέγραψε ασφαλιστήριο συμβόλαιο με την ασφαλιστική εταιρεία Β. Η ασφαλιστική εταιρεία θα λάβει από τον Α ορισμένες πληροφορίες που αφορούν την υγεία του, όπως τρέχοντα προβλήματα υγείας ή ασθένειες. Η ασφαλιστική εταιρεία θα πρέπει να αποθηκεύσει τα δεδομένα προσωπικού χαρακτήρα του Α που αφορούν την υγεία του χωριστά από άλλα δεδομένα. Η ασφαλιστική εταιρεία πρέπει επίσης να αποθηκεύσει τα δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία χωριστά από άλλα δεδομένα προσωπικού χαρακτήρα. Αυτό σημαίνει ότι μόνον ο αρμόδιος υπάλληλος για την υπόθεση του Α θα έχει πρόσβαση στα δεδομένα του Α που αφορούν την υγεία του.

947 ΕΕΠΔ (2013), Γνωμοδότηση του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων επί της ανακοίνωσης της Επιτροπής σχετικά με το «Σχέδιο δράσης 2012-2020 για την ηλ-υγεία – Καινοτομική υγιεινομική περίθαλψη για τον 21ο αιώνα, Βρυξέλλες, 27 Μαρτίου 2013.

948 Σύσταση της Επιτροπής, της 2ας Ιουλίου 2008, περί της διασυνοριακής διαλειτουργικότητας των συστημάτων ηλεκτρονικών μητρώων υγείας, σημείο 3 στοιχείο γ).

Ωστόσο, από τα ηλεκτρονικά μητρώα υγείας προκύπτουν ορισμένα ζητήματα σχετικά με την προστασία των δεδομένων, όπως η προσβασιμότητά τους, η δέουσα αποθήκευση και η πρόσβαση από το υποκείμενο των δεδομένων.

Πέραν των ηλεκτρονικών μητρώων υγείας, στις 10 Απριλίου 2014, η Ευρωπαϊκή Επιτροπή δημοσίευσε Πράσινη Βίβλο για την «κινητή» υγεία («mHealth»), εκτιμώντας ότι η mHealth συνιστά ένα αναδυόμενο και ταχέως αναπτυσσόμενο πεδίο, το οποίο έχει τη δυνατότητα να επηρεάσει τον μετασχηματισμό της υγειονομικής περίθαλψης και να βελτιώσει την ποιότητα και την αποτελεσματικότητά της. Ο όρος καλύπτει την άσκηση της ιατρικής και της δημόσιας υγείας που υποστηρίζεται από κινητές συσκευές, όπως κινητά τηλέφωνα, συσκευές παρακολούθησης ασθενών, προσωπικούς ψηφιακούς βοηθούς (PDA) και άλλες ασύρματες συσκευές, καθώς και εφαρμογές («apps») (για παράδειγμα, εφαρμογές ευζωίας) που μπορούν να συνδεθούν με ιατρικές συσκευές ή αισθητήρες ⁹⁴⁹. Στο εν λόγω έγγραφο περιγράφονται συνοπτικά οι κίνδυνοι τους οποίους θα μπορούσε να συνεπάγεται η ανάπτυξη της mHealth για το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα και προβλέπει ότι, δεδομένου του ευαίσθητου χαρακτήρα των δεδομένων υγείας, η ανάπτυξη της mHealth θα πρέπει να περιέχει συγκεκριμένες και κατάλληλες εγγυήσεις ασφάλειας, όπως κρυπτογράφηση των δεδομένων του ασθενούς και κατάλληλους μηχανισμούς ελέγχου ταυτότητας του ασθενούς για τον περιορισμό των κινδύνων ασφαλείας. Η συμμόρφωση με τους κανόνες προστασίας των προσωπικών δεδομένων, συμπεριλαμβανομένης της υποχρέωσης ενημέρωσης του υποκειμένου των δεδομένων, της ασφάλειας των δεδομένων και της αρχής της νομιμότητας της επεξεργασίας των προσωπικών δεδομένων, είναι ζωτικής σημασίας για την οικοδόμηση εμπιστοσύνης στις λύσεις mHealth ⁹⁵⁰. Για τον σκοπό αυτόν, ο κλάδος κατάρτισε κώδικα δεοντολογίας, βάσει την συμβολή που παρείχε ευρύ φάσμα ενδιαφερόμενων φορέων, συμπεριλαμβανομένων εκπροσώπων με εμπειρογνώσια στους τομείς της προστασίας δεδομένων, της αυτορρύθμισης και της συρρύθμισης, των ΤΠΕ και της υγειονομικής περίθαλψης ⁹⁵¹. Κατά τον χρόνο σύνταξης του παρόντος εγχειριδίου, το σχέδιο του κώδικα δεοντολογίας είχε υποβληθεί για διατύπωση παρατηρήσεων στην Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, εν αναμονή της επίσημης έγκρισής του.

949 Ευρωπαϊκή Επιτροπή (2014), *Πράσινη Βίβλος για την «κινητή» υγεία ("mHealth")*, COM(2014) 219 final, Βρυξέλλες, 10 Απριλίου 2014.

950 Ό.π., σ. 8.

951 *Draft Code of Conduct on privacy for mobile health applications*, 7 Ιουνίου 2016.

9.4. Επεξεργασία δεδομένων για ερευνητικούς και στατιστικούς σκοπούς

Κύρια σημεία

- Τα δεδομένα που συλλέγονται για στατιστικούς σκοπούς και για σκοπούς επιστημονικής ή ιστορικής έρευνας δεν επιτρέπεται να χρησιμοποιούνται για κανέναν άλλον σκοπό.
- Τα δεδομένα που συλλέγονται νόμιμα για οποιονδήποτε σκοπό μπορούν να χρησιμοποιηθούν μεταγενέστερα για στατιστικούς σκοπούς και για σκοπούς επιστημονικής ή ιστορικής έρευνας, υπό την προϋπόθεση ότι παρέχονται επαρκείς εγγυήσεις. Για τον σκοπό αυτόν, οι εν λόγω εγγυήσεις μπορούν να παρέχονται με την ανωνυμοποίηση ή ψευδωνυμοποίηση πριν από τη διαβίβαση των δεδομένων σε τρίτους.

Το **δίκαιο της ΕΕ** επιτρέπει την επεξεργασία δεδομένων για στατιστικούς σκοπούς και για σκοπούς επιστημονικής ή ιστορικής έρευνας, υπό την προϋπόθεση ότι παρέχονται κατάλληλες εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στις εγγυήσεις αυτές μπορεί να περιλαμβάνεται η ψευδωνυμοποίηση⁹⁵². Το δίκαιο της ΕΕ ή το εθνικό δίκαιο μπορεί να προβλέπει ορισμένες παρεκκλίσεις από τα δικαιώματα των υποκειμένων των δεδομένων εάν τα εν λόγω δικαιώματα είναι πιθανό να καταστήσουν αδύνατη ή να παρακωλύσουν σοβαρά την επίτευξη του νόμιμου σκοπού της έρευνας⁹⁵³. Είναι δυνατή η θέσπιση παρεκκλίσεων από το δικαίωμα πρόσβασης του υποκειμένου των δεδομένων, από το δικαίωμα διάρθωσης, από το δικαίωμα περιορισμού της επεξεργασίας και από το δικαίωμα εναντίωσης.

Παρότι τα δεδομένα που συλλέγονται νόμιμα από υπεύθυνο επεξεργασίας για οποιονδήποτε σκοπό μπορούν να χρησιμοποιηθούν περαιτέρω από τον συγκεκριμένο υπεύθυνο επεξεργασίας για δικούς του στατιστικούς σκοπούς ή σκοπούς επιστημονικής ή ιστορικής έρευνας, τα δεδομένα θα πρέπει να ανωνυμοποιούνται ή να υπόκεινται σε μέτρα, όπως η ψευδωνυμοποίηση, ανάλογα με το εκάστοτε πλαίσιο, πριν διαβιβαστούν σε τρίτο για στατιστικούς σκοπούς ή για σκοπούς επιστημονικής ή ιστορικής έρευνας, εκτός εάν το υποκείμενο των δεδομένων έχει παράσχει τη συγκατάθεσή του ή εάν αυτό προβλέπεται ρητά από το εθνικό δίκαιο. Σε αντίθεση με τα ανώνυμα δεδομένα, τα δεδομένα που

952 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 89 παράγραφος 1.

953 Ό.π., άρθρο 89 παράγραφος 2.

υπόκεινται σε ψευδωνυμοποίηση εξακολουθούν να διέπονται από τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων ⁹⁵⁴.

Επομένως, ο κανονισμός επιφυλάσσει στην έρευνα καθεστώς ειδικής αντιμετώπισης όσον αφορά τους γενικούς κανόνες για την προστασία των δεδομένων, ούτως ώστε να αποφεύγονται περιορισμοί στην εξέλιξη της έρευνας και να διασφαλίζεται η συμμόρφωση με τον στόχο της δημιουργίας ενός ευρωπαϊκού χώρου έρευνας, όπως προβλέπεται στο άρθρο 179 της ΣΛΕΕ. Ο κανονισμός προβλέπει τη διασταλτική ερμηνεία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας, συμπεριλαμβανομένης της τεχνολογικής ανάπτυξης και επίδειξης, της βασικής έρευνας, της εφαρμοσμένης έρευνας και της ιδιωτικά χρηματοδοτούμενης έρευνας. Αναγνωρίζει επίσης τη σημασία της συγκέντρωσης δεδομένων σε μητρώα για ερευνητικούς σκοπούς, καθώς και την πιθανή δυσκολία που συνίσταται στο να μην είναι δυνατόν να προσδιορίζεται πλήρως ο σκοπός της επακόλουθης επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για σκοπούς επιστημονικής έρευνας κατά τον χρόνο συλλογής των δεδομένων ⁹⁵⁵. Για τον λόγο αυτόν, ο κανονισμός επιτρέπει την επεξεργασία δεδομένων για τους συγκεκριμένους σκοπούς, χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων, υπό την προϋπόθεση ότι παρέχονται οι σχετικές εγγυήσεις.

Σημαντικό παράδειγμα της χρήσης δεδομένων για στατιστικούς σκοπούς αποτελούν οι επίσημες στατιστικές, οι οποίες καταρτίζονται από τις εθνικές και ενωσιακές στατιστικές υπηρεσίες δυνάμει των εθνικών και ενωσιακών νομοθεσιών για τις επίσημες στατιστικές. Σύμφωνα με τις εν λόγω νομοθεσίες, οι πολίτες και οι επιχειρήσεις υποχρεούνται συνήθως να κοινοποιούν τα δεδομένα στις αρμόδιες στατιστικές αρχές. Οι υπάλληλοι που εργάζονται στις στατιστικές υπηρεσίες δεσμεύονται από ειδικές υποχρεώσεις επαγγελματικού απορρήτου οι οποίες πρέπει να τηρούνται δεόντως, δεδομένου ότι είναι καίριας σημασίας για την εξασφάλιση του απαιτούμενου υψηλού βαθμού εμπιστοσύνης των πολιτών σε περίπτωση που τα δεδομένα πρόκειται να τεθούν στη διάθεση των στατιστικών αρχών ⁹⁵⁶.

Ο κανονισμός (ΕΕ) αριθ. 223/2009 σχετικά με τις ευρωπαϊκές στατιστικές (κανονισμός για τις ευρωπαϊκές στατιστικές) περιέχει βασικούς κανόνες για την προστασία των δεδομένων στο πλαίσιο των επίσημων στατιστικών και μπορεί,

954 Ό.π., αιτιολογική σκέψη 26.

955 Ό.π., αιτιολογικές σκέψεις 33, 157 και 159.

956 Ό.π., άρθρο 90.

συνεπώς, να θεωρηθεί συναφής προς τις διατάξεις σχετικά με τις επίσημες στατιστικές που καταρτίζονται σε εθνικό επίπεδο ⁹⁵⁷. Ο κανονισμός διατηρεί την αρχή σύμφωνα με την οποία η δραστηριότητα κατάρτισης επίσημων στατιστικών προϋποθέτει αρκούντως σαφή νομική βάση ⁹⁵⁸.

Παράδειγμα: Στην υπόθεση *Huber κατά Bundesrepublik Deutschland* ⁹⁵⁹, ένας αυστριακός επιχειρηματίας που μετακόμισε στη Γερμανίας, υπέβαλε προσφυγή ισχυριζόμενος ότι η συλλογή και η αποθήκευση δεδομένων προσωπικού χαρακτήρα αλλοδαπών υπηκόων από τις γερμανικές αρχές σε κεντρικό μητρώο (AZR) και για στατιστικούς σκοπούς συνιστούσε παραβίαση των δικαιωμάτων του σύμφωνα με την Οδηγία για την Προστασία Δεδομένων. Λαμβανομένου υπόψη του σκοπού της οδηγίας 95/46/ΕΚ που συνίσταται στην εξασφάλιση ισοδύναμου επιπέδου προστασίας δεδομένων σε όλα τα κράτη μέλη, το ΔΕΕ αποφάνθηκε ότι, για την κατοχύρωση υψηλού επιπέδου προστασίας στην ΕΕ, η έννοια της αναγκαιότητας, όπως απορρέει από το άρθρο 7 στοιχείο ε), δεν μπορεί να έχει περιεχόμενο που μεταβάλλεται αναλόγως του κράτους μέλους. Επομένως, πρόκειται για αυτοτελή έννοια του ενωσιακού δικαίου η οποία πρέπει να ερμηνευθεί κατά τρόπο που να ανταποκρίνεται πλήρως στον σκοπό της οδηγίας 95/46/ΕΚ. Το ΔΕΕ επισήμανε ότι δεν θα πρέπει να απαιτούνται ονομαστικές πληροφορίες για στατιστικούς σκοπούς και αποφάνθηκε ότι το γερμανικό μητρώο δεν συνάδει με την περί αναγκαιότητας επιταγή του άρθρου 7 στοιχείο ε).

Στο πλαίσιο του **Συμβουλίου της Ευρώπης**, η περαιτέρω επεξεργασία δεδομένων για ιστορικούς, στατιστικούς ή επιστημονικούς σκοπούς είναι δυνατή εάν κρίνεται

957 Κανονισμός (ΕΚ) αριθ. 223/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 11ης Μαρτίου 2009, σχετικά με τις ευρωπαϊκές στατιστικές και την κατάργηση του κανονισμού (ΕΚ, Ευρατόμ) αριθ. 1101/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τη διαβίβαση στη Στατιστική Υπηρεσία των Ευρωπαϊκών Κοινοτήτων πληροφοριών που καλύπτονται από το στατιστικό απόρρητο, του κανονισμού (ΕΚ) αριθ. 322/97 του Συμβουλίου σχετικά με τις κοινοτικές στατιστικές και της απόφασης 89/382/ΕΟΚ, Ευρατόμ του Συμβουλίου για τη σύσταση επιτροπής του στατιστικού προγράμματος των Ευρωπαϊκών Κοινοτήτων (ΕΕ L 87 της 31.3.2009, σ. 164), όπως τροποποιήθηκε με τον κανονισμό (ΕΕ) 2015/759 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 29ης Απριλίου 2015, για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 223/2009 σχετικά με τις ευρωπαϊκές στατιστικές (ΕΕ L 123 της 19.5.2015, σ. 90).

958 Η αρχή αυτή πρέπει να περιγράφεται αναλυτικότερα στον [Κώδικα ορθής πρακτικής της Eurostat](#), ο οποίος παρέχει, σύμφωνα με το άρθρο 11 του κανονισμού για τις ευρωπαϊκές στατιστικές, δεοντολογική καθοδήγηση σχετικά με τον τρόπο κατάρτισης επίσημων στατιστικών, συμπεριλαμβανομένης της συνετής χρήσης των δεδομένων προσωπικού χαρακτήρα.

959 ΔΕΕ, C-524/06, *Heinz Huber κατά Bundesrepublik Deutschland* [τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008· βλ. ιδίως σκέψη 68.

αναγκαία για λόγους δημοσίου συμφέροντος και πρέπει να υπόκειται σε κατάλληλες εγγυήσεις⁹⁶⁰. Τα δικαιώματα των υποκειμένων των δεδομένων είναι επίσης πιθανό να περιορίζονται κατά την επεξεργασία δεδομένων για στατιστικούς σκοπούς, υπό την προϋπόθεση ότι δεν υπάρχει αναγνωρίσιμος κίνδυνος παραβίασης των δικαιωμάτων και των ελευθεριών τους⁹⁶¹.

Η σύσταση σχετικά με τα στατιστικά δεδομένα, η οποία εκδόθηκε το 1997, καλύπτει την άσκηση στατιστικής δραστηριότητας στον δημόσιο και στον ιδιωτικό τομέα⁹⁶².

Τα δεδομένα που συλλέγονται από υπεύθυνο επεξεργασίας για στατιστικούς σκοπούς δεν επιτρέπεται να χρησιμοποιούνται για κανέναν άλλον σκοπό. Τα δεδομένα που συλλέγονται για μη στατιστικούς σκοπούς καθίστανται διαθέσιμα για μεταγενέστερη στατιστική χρήση. Η σύσταση σχετικά με τα στατιστικά δεδομένα επιτρέπει επίσης τη διαβίβαση των δεδομένων σε τρίτους, υπό την προϋπόθεση ότι εξυπηρετεί αποκλειστικά και μόνο στατιστικούς σκοπούς. Στις περιπτώσεις αυτές, τα μέρη θα πρέπει να συμφωνούν και να καταγράφουν την έκταση της νόμιμης περαιτέρω χρήσης για στατιστικούς σκοπούς. Δεδομένου ότι η υποχρέωση αυτή δεν μπορεί να υποκαταστήσει τη συγκατάθεση του υποκειμένου των δεδομένων, εάν απαιτείται, πρέπει να προβλέπονται από το εθνικό δίκαιο κατάλληλες εγγυήσεις ώστε να ελαχιστοποιούνται οι κίνδυνοι κατάχρησης των δεδομένων προσωπικού χαρακτήρα, όπως η υποχρέωση ψευδωνυμοποίησης ή ανωνυμοποίησης των δεδομένων πριν από την κοινοποίηση.

Τα πρόσωπα που ασχολούνται κατ' επάγγελμα με τη στατιστική έρευνα πρέπει να δεσμεύονται από ειδικές υποχρεώσεις τήρησης του επαγγελματικού απορρήτου –όπως συμβαίνει συνήθως και στην περίπτωση των επίσημων στατιστικών– δυνάμει του εθνικού δικαίου. Οι υποχρεώσεις αυτές πρέπει να επεκτείνονται και στα πρόσωπα που λαμβάνουν τις συνεντεύξεις, καθώς και σε άλλους υπευθύνους συλλογής δεδομένων προσωπικού χαρακτήρα, εάν ασχολούνται κατ' επάγγελμα με τη συλλογή δεδομένων από υποκείμενα δεδομένων ή άλλα πρόσωπα.

Εάν η διεξαγωγή στατιστικής έρευνας με τη χρήση δεδομένων προσωπικού χαρακτήρα δεν επιτρέπεται από τη νομοθεσία, είτε θα πρέπει ενδεχομένως τα

960 Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5 παράγραφος 4 (στοιχείο β).

961 Ό.π., άρθρο 11 παράγραφος 2.

962 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1997), Σύσταση Rec (97)18 προς τα κράτη μέλη σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που συλλέγονται και υποβάλλονται σε επεξεργασία για στατιστικούς σκοπούς, 30 Σεπτεμβρίου 1997.

υποκείμενα των δεδομένων να δώσουν τη συγκατάθεσή τους για τη χρήση των δεδομένων τους προκειμένου αυτή να νομιμοποιείται, είτε θα πρέπει ενδεχομένως να τους παρέχεται η δυνατότητα εναντίωσης. Εάν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται για στατιστικούς σκοπούς μέσω της λήψης συνεντεύξεων από πρόσωπα, τα εν λόγω πρόσωπα πρέπει να λαμβάνουν σαφή ενημέρωση σχετικά με το αν η παροχή των εν λόγω δεδομένων είναι υποχρεωτική δυνάμει του εθνικού δικαίου.

Όταν μια στατιστική έρευνα δεν μπορεί να διεξαχθεί με τη χρήση ανώνυμων δεδομένων και απαιτούνται δεδομένα προσωπικού χαρακτήρα, τα δεδομένα που συλλέγονται για τον σκοπό αυτόν πρέπει να ανωνυμοποιούνται το συντομότερο δυνατόν. Τα αποτελέσματα της στατιστικής έρευνας δεν πρέπει να επιτρέπουν, τουλάχιστον, την εξακρίβωση της ταυτότητας των υποκειμένων των δεδομένων, εκτός εάν αυτό δεν ενέχει προδήλως κανέναν κίνδυνο.

Μετά την ολοκλήρωση της στατιστικής ανάλυσης, τα δεδομένα προσωπικού χαρακτήρα που χρησιμοποιήθηκαν θα πρέπει είτε να διαγράφονται είτε να ανωνυμοποιούνται. Στις περιπτώσεις αυτές, στη σύσταση σχετικά με τα στατιστικά δεδομένα υποδεικνύεται ότι τα δεδομένα ταυτοποίησης πρέπει να αποθηκεύονται χωριστά από τα υπόλοιπα δεδομένα προσωπικού χαρακτήρα. Αυτό σημαίνει, για παράδειγμα, ότι είτε το κλειδί κρυπτογράφησης είτε ο κατάλογος που περιέχει τα ταυτοποιητικά συνώνυμα πρέπει να αποθηκεύεται χωριστά από τα υπόλοιπα δεδομένα.

9.5. Χρηματοοικονομικά δεδομένα

Κύρια σημεία

- Παρότι τα χρηματοοικονομικά δεδομένα δεν θεωρούνται ευαίσθητα δεδομένα βάσει της Εκσυγχρονισμένης Σύμβασης 108 ή του Γενικού Κανονισμού για την Προστασία Δεδομένων, για την επεξεργασία τους απαιτούνται ιδιαίτερες εγγυήσεις, ώστε να διασφαλίζεται η ακρίβεια και η ασφάλεια των δεδομένων.
- Τα συστήματα ηλεκτρονικών πληρωμών ειδικότερα πρέπει να διαθέτουν ενσωματωμένη προστασία δεδομένων, δηλαδή τη λεγόμενη προστασία της ιδιωτικής ζωής ή των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού.
- Στον συγκεκριμένο τομέα μπορεί να ανακύπτουν ειδικά προβλήματα προστασίας των δεδομένων, δεδομένου ότι πρέπει να εφαρμόζονται κατάλληλοι μηχανισμοί επαλήθευσης της ταυτότητας.

Παράδειγμα: Στην υπόθεση *Michaud κατά Γαλλίας*⁹⁶³, ο προσφεύγων, γάλλος δικηγόρος, αμφισβήτησε την υποχρέωση που υπέχει δυνάμει της γαλλικής νομοθεσίας να αναφέρει υπόνοιες σχετικά με πιθανή νομιμοποίηση εσόδων από παράνομες δραστηριότητες των πελατών του. Το ΕΔΔΑ επισήμανε ότι η απαίτηση να αναφέρουν οι δικηγόροι στις διοικητικές αρχές πληροφορίες που αφορούν τρίτο πρόσωπο και έχουν περιέλθει σε γνώση τους μέσω των επαγγελματικών επαφών τους συνιστούν επέμβαση στο δικαίωμα σεβασμού της αλληλογραφίας και της ιδιωτικής ζωής των δικηγόρων δυνάμει του άρθρου 8 της ΕΣΔΑ, δεδομένου ότι η έννοια αυτή καλύπτει τις δραστηριότητες επαγγελματικού ή επιχειρηματικού χαρακτήρα. Ωστόσο, η εν λόγω επέμβαση ήταν σύμφωνη με τον νόμο και επιδίωκε νόμιμο σκοπό, δηλαδή την αποτροπή της διασάλευσης της τάξης και των εγκληματικών πράξεων. Δεδομένου ότι οι δικηγόροι υποχρεούνται να αναφέρουν ύποπτες δραστηριότητες αποκλειστικά και μόνο σε εξαιρετικά περιορισμένες περιστάσεις, το ΕΔΔΑ έκρινε ότι η εν λόγω υποχρέωση ήταν αναλογική και κατέληξε στο συμπέρασμα ότι δεν παραβιάστηκε το άρθρο 8.

Παράδειγμα: Στην υπόθεση *Μ.Ν. κ.λπ. κατά Αγίου Μαρίνου*⁹⁶⁴, ο προσφεύγων, ιταλός υπήκοος, σύναψε σύμβαση καταπίστευσης με εταιρεία η οποία αποτελούσε αντικείμενο έρευνας. Αυτό σήμαινε ότι η εταιρεία υποβλήθηκε σε έρευνα και κατάσχεση αντιγράφων (ηλεκτρονικής) τεκμηρίωσης. Ο προσφεύγων υπέβαλε προσφυγή ενώπιον του δικαστηρίου του Αγίου Μαρίνου, ισχυριζόμενος ότι δεν υπήρχε σύνδεση μεταξύ του ίδιου και των εικαζόμενων αξιόποινων πράξεων. Ωστόσο, το δικαστήριο κήρυξε την προσφυγή του απαράδεκτη διότι ο προσφεύγων δεν συνιστούσε «ενδιαφερόμενο μέρος». Το ΕΔΔΑ έκρινε ότι ο προσφεύγων περιήλθε σε ιδιαίτερως μειονεκτική θέση από πλευράς δικαστικής προστασίας σε σύγκριση με το «ενδιαφερόμενο μέρος», πλην όμως τα δεδομένα του εξακολουθούσαν να αποτελούν αντικείμενο των ενεργειών έρευνας και κατάσχεσης. Ως εκ τούτου, το ΕΔΔΑ αποφάνθηκε ότι παραβιάστηκε το άρθρο 8.

963 ΕΔΔΑ, *Michaud κατά Γαλλίας*, προσφυγή αριθ. 12323/11, 6 Δεκεμβρίου 2012. Βλ. επίσης ΕΔΔΑ, *Niemietz κατά Γερμανίας*, προσφυγή αριθ. 13710/88, 16 Δεκεμβρίου 1992, σκέψη 29, και ΕΔΔΑ, *Halford κατά Ηνωμένου Βασιλείου*, προσφυγή αριθ. 20605/92, 25 Ιουνίου 1997, σκέψη 42.

964 ΕΔΔΑ, *Μ.Ν. κ.λπ. κατά Αγίου Μαρίνου*, προσφυγή αριθ. 28005/12, 7 Ιουλίου 2015.

Παράδειγμα: Στην υπόθεση *G.S.B. κατά Ελβετίας*⁹⁶⁵, τα στοιχεία τραπεζικού λογαριασμού του προσφεύγοντος διαβιβάστηκαν στις φορολογικές αρχές των ΗΠΑ δυνάμει της συμφωνίας διοικητικής συνεργασίας μεταξύ της Ελβετίας και των ΗΠΑ. Το ΕΔΔΑ αποφάνθηκε ότι η εν λόγω διαβίβαση δεν συνιστούσε παράβαση του άρθρου 8 της ΕΣΔΑ, διότι η επέμβαση στο δικαίωμα προστασίας της ιδιωτικής ζωής του προσφεύγοντος προβλεπόταν από τον νόμο, επιδίωκε νόμιμο σκοπό και ήταν αναλογική προς το διακυβευόμενο δημόσιο συμφέρον.

Με τη σύσταση R(90)19 του **Συμβουλίου της Ευρώπης** του 1990⁹⁶⁶ έγινε μια απόπειρα εφαρμογής του γενικού νομικού πλαισίου για την προστασία των δεδομένων (όπως ορίζεται στη Σύμβαση 108) στον τομέα των πληρωμών. Με τη σύσταση αυτή αποσαφηνίζεται το πεδίο εφαρμογής της νόμιμης συλλογής και χρήσης δεδομένων στον τομέα των πληρωμών, ιδίως μέσω καρτών πληρωμής. Διατυπώνονται επίσης λεπτομερείς συστάσεις προς τους εθνικούς νομοθέτες σχετικά με κανόνες για την κοινοποίηση δεδομένων πληρωμών σε τρίτους, τα χρονικά όρια διατήρησης των δεδομένων, τη διαφάνεια, την ασφάλεια των δεδομένων και τις διασυννοριακές ροές δεδομένων, καθώς και την εποπτεία και τα μέσα προσφυγής. Το Συμβούλιο της Ευρώπης κατάρτισε επίσης Γνωμοδότηση σχετικά με τη διαβίβαση φορολογικών δεδομένων⁹⁶⁷, στην οποία διατυπώνονται συστάσεις και ζητήματα που πρέπει να λαμβάνονται υπόψη κατά τον χειρισμό της διαβίβασης φορολογικών δεδομένων.

Το ΕΔΔΑ επιτρέπει τη διαβίβαση χρηματοοικονομικών δεδομένων –και ειδικότερα των στοιχείων τραπεζικού λογαριασμού ενός ατόμου– κατ’ εφαρμογή του άρθρου 8 της ΕΣΔΑ, εάν προβλέπεται από τον νόμο, επιδίωκει νόμιμο σκοπό και είναι αναλογική προς το διακυβευόμενο δημόσιο συμφέρον⁹⁶⁸.

Όσον αφορά το **δίκαιο της ΕΕ**, τα συστήματα ηλεκτρονικών πληρωμών που περιλαμβάνουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να συμμορφώνονται με τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων. Ως εκ τούτου, τα συστήματα αυτά πρέπει να διασφαλίζουν την

965 ΕΔΔΑ, *G.S.B. κατά Ελβετίας*, προσφυγή αριθ. 28601/11, 22 Δεκεμβρίου 2015.

966 Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (1990), Σύσταση αριθ. R (90)19 σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται για τις πληρωμές και άλλες συναφείς πράξεις, 13 Σεπτεμβρίου 1990.

967 Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108 (2014), Γνωμοδότηση σχετικά με τον αντίκτυπο που έχουν στην προστασία των δεδομένων οι μηχανισμοί για αυτόματες διακρατικές ανταλλαγές δεδομένων για διοικητικούς και φορολογικούς σκοπούς, 4 Ιουνίου 2014.

968 ΕΔΔΑ, *G.S.B. κατά Ελβετίας*, προσφυγή αριθ. 28601/11, 22 Δεκεμβρίου 2015.

προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού. Η προστασία των δεδομένων ήδη από τον σχεδιασμό επιβάλλει στον υπεύθυνο επεξεργασίας την υποχρέωση εφαρμογής κατάλληλων τεχνικών και οργανωτικών μέτρων για την εφαρμογή των αρχών της προστασίας δεδομένων. Προστασία των δεδομένων εξ ορισμού σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι μόνο τα δεδομένα προσωπικού χαρακτήρα τα οποία κρίνονται αναγκαία για την εξυπηρέτηση συγκεκριμένου σκοπού μπορούν εξ ορισμού να υποβάλλονται σε επεξεργασία (βλ. [ενότητα 4.4](#)). Όσον αφορά τα χρηματοοικονομικά δεδομένα, το ΔΕΕ αποφάνθηκε ότι τα διαβιβαζόμενα φορολογικά δεδομένα ενδέχεται να συνιστούν δεδομένα προσωπικού χαρακτήρα⁹⁶⁹. Η Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων εξέδωσε σχετικές κατευθυντήριες γραμμές για τα κράτη μέλη, στις οποίες περιλαμβάνονται τα κριτήρια για τη διασφάλιση της συμμόρφωσης με τους κανόνες προστασίας δεδομένων κατά την αυτόματη ανταλλαγή δεδομένων προσωπικού χαρακτήρα για φορολογικούς σκοπούς με τη χρήση αυτοματοποιημένων μέσων⁹⁷⁰. Επιπλέον, έχουν θεσπιστεί διάφορες νομοθετικές πράξεις για τη ρύθμιση των χρηματοπιστωτικών αγορών και των δραστηριοτήτων των πιστωτικών ιδρυμάτων και των επιχειρήσεων επενδύσεων⁹⁷¹. Άλλες νομοθετικές πράξεις συμβάλλουν στην καταπολέμηση των πράξεων προσώπων που κατέχουν εμπιστευτικές πληροφορίες και των πράξεων χειραγώγησης της αγοράς⁹⁷². Οι κυριότεροι τομείς οι οποίοι έχουν αντίκτυπο στην προστασία των δεδομένων είναι οι ακόλουθοι:

- η τήρηση αρχείων χρηματοπιστωτικών πράξεων·
- η διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες·

969 ΔΕΕ, C-201/14, *Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ.*, 1 Οκτωβρίου 2015, σκέψη 29.

970 Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων (2015), Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, 14/EN WP 230.

971 Οδηγία 2014/65/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και την τροποποίηση της οδηγίας 2002/92/ΕΚ και της οδηγίας 2011/61/ΕΕ (ΕΕ L 173 της 12.6.2014, σ. 349)· κανονισμός (ΕΕ) αριθ. 600/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 15ης Μαΐου 2014, για τις αγορές χρηματοπιστωτικών μέσων και για την τροποποίηση του κανονισμού (ΕΕ) αριθ. 648/2012 (ΕΕ L 173 της 12.6.2014, σ. 84)· οδηγία 2013/36/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 26ης Ιουνίου 2013, σχετικά με την πρόσβαση στη δραστηριότητα πιστωτικών ιδρυμάτων και την προληπτική εποπτεία πιστωτικών ιδρυμάτων και επιχειρήσεων επενδύσεων, για την τροποποίηση της οδηγίας 2002/87/ΕΚ και για την κατάργηση των οδηγιών 2006/48/ΕΚ και 2006/49/ΕΚ (ΕΕ L 176 της 27.6.2013, σ. 338).

972 Κανονισμός (ΕΕ) αριθ. 596/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Απριλίου 2014, για την κατάχρηση της αγοράς (κανονισμός για την κατάχρηση της αγοράς) και την κατάργηση της οδηγίας 2003/6/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου και των οδηγιών της Επιτροπής 2003/124/ΕΚ, 2003/125/ΕΚ και 2004/72/ΕΚ (ΕΕ L 173 της 12.6.2014, σ. 1).

- η καταγραφή τηλεφωνικών συνδιαλέξεων ή ηλεκτρονικών επικοινωνιών, καθώς και η εξουσία των αρμόδιων αρχών να ζητούν αρχεία τηλεφωνικών επικοινωνιών και δεδομένων κίνησης·
- η δημοσιοποίηση προσωπικών πληροφοριών, συμπεριλαμβανομένης της δημοσίευσης κυρώσεων·
- οι εποπτικές εξουσίες και εξουσίες έρευνας των αρμόδιων αρχών, συμπεριλαμβανομένων των επιτόπιων ελέγχων και της εισόδου σε ιδιωτικούς χώρους για την κατάσχεση εγγράφων·
- οι μηχανισμοί καταγγελίας παραβάσεων, ήτοι προγράμματα για την καταγγελία δυσλειτουργιών· και
- η συνεργασία μεταξύ των αρμόδιων αρχών των κρατών μελών και της Ευρωπαϊκής Αρχής Κινητών Αξιών και Αγορών (ESMA).

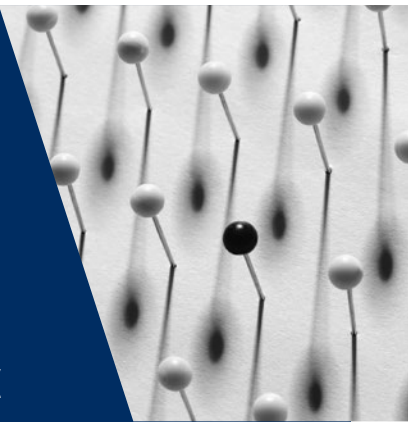
Στους εν λόγω τομείς προκύπτουν και άλλα ζητήματα τα οποία αντιμετωπίζονται με ειδικές διατάξεις, όπως η συλλογή δεδομένων για τη χρηματοοικονομική κατάσταση των υποκειμένων των δεδομένων⁹⁷³ ή οι διασυννοητικές πληρωμές μέσω τραπεζικών εμβασμάτων, που συνεπάγονται αναπόφευκτα ροές δεδομένων προσωπικού χαρακτήρα⁹⁷⁴.

973 Κανονισμός (ΕΚ) αριθ. 1060/2009 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας (ΕΕ L 302 της 17.11.2009, σ. 1), και όπως τροποποιήθηκε τελευταία με την οδηγία 2014/51/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Απριλίου 2014, σχετικά με την τροποποίηση των οδηγιών 2003/71/ΕΚ και 2009/138/ΕΚ, και των κανονισμών (ΕΚ) αριθ. 1060/2009, (ΕΕ) αριθ. 1094/2010 και (ΕΕ) αριθ. 1095/2010, όσον αφορά τις εξουσίες της Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Ασφαλίσεων και Επαγγελματικών Συντάξεων) και της Ευρωπαϊκής Εποπτικής Αρχής (Ευρωπαϊκή Αρχή Κινητών Αξιών και Αγορών) (ΕΕ L 153 της 22.5.2014, σ. 1)· κανονισμός (ΕΕ) αριθ. 462/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 21ης Μαΐου 2013, για την τροποποίηση του κανονισμού (ΕΚ) αριθ. 1060/2009 για τους οργανισμούς αξιολόγησης πιστοληπτικής ικανότητας (ΕΕ L 146 της 31.5.2013, σ. 1).

974 Οδηγία 2007/64/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Νοεμβρίου 2007, για τις υπηρεσίες πληρωμών στην εσωτερική αγορά, την τροποποίηση των οδηγιών 97/7/ΕΚ, 2002/65/ΕΚ, 2005/60/ΕΚ και 2006/48/ΕΚ, και την κατάργηση της οδηγίας 97/5/ΕΚ (ΕΕ L 319 της 5.12.2007, σ. 1), όπως τροποποιήθηκε με την οδηγία 2009/111/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 16ης Σεπτεμβρίου 2009, για την τροποποίηση των οδηγιών 2006/48/ΕΚ, 2006/49/ΕΚ και 2007/64/ΕΚ όσον αφορά τράπεζες συνδεδεμένες με κεντρικούς οργανισμούς, ορισμένα στοιχεία των ιδίων κεφαλαίων, τα μεγάλα χρηματοδοτικά ανοίγματα, τις εποπτικές ρυθμίσεις και τη διαχείριση κρίσεων (ΕΕ L 302 της 17.11.2009, σ. 97).

10

Σύγχρονες προκλήσεις της προστασίας των δεδομένων προσωπικού χαρακτήρα



Η ψηφιακή εποχή, ή η εποχή της τεχνολογίας των πληροφοριών, χαρακτηρίζεται από την ευρέως διαδεδομένη χρήση των ηλεκτρονικών υπολογιστών, του διαδικτύου και των ψηφιακών τεχνολογιών. Συνεπάγεται δε τη συλλογή και την επεξεργασία τεράστιων όγκων δεδομένων, συμπεριλαμβανομένων δεδομένων προσωπικού χαρακτήρα. Η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μια παγκοσμιοποιημένη οικονομία σημαίνει αύξηση του πλήθους των διασυννοριακών ροών δεδομένων. Η εν λόγω επεξεργασία μπορεί να αποφέρει σημαντικά και ορατά οφέλη στην καθημερινή ζωή: οι μηχανές αναζήτησης διευκολύνουν την πρόσβαση σε σημαντικούς όγκους πληροφοριών και γνώσεων, οι υπηρεσίες κοινωνικής δικτύωσης παρέχουν τη δυνατότητα σε άτομα από ολόκληρο τον κόσμο να επικοινωνούν, να εκφράζουν απόψεις και να κινητοποιούν δράσεις υποστήριξης για κοινωνικούς, περιβαλλοντικούς και πολιτικούς σκοπούς, ενώ οι επιχειρήσεις και οι καταναλωτές επωφελούνται από αποτελεσματικές και αποδοτικές τεχνικές εμπορικής προώθησης που τονώνουν την οικονομία. Η τεχνολογία και η επεξεργασία δεδομένων προσωπικού χαρακτήρα συνιστούν επίσης απολύτως απαραίτητα εργαλεία για τις κρατικές αρχές στο πλαίσιο της καταπολέμησης του εγκλήματος και της τρομοκρατίας. Ομοίως, τα μαζικά δεδομένα –η συλλογή, αποθήκευση και ανάλυση μεγάλων όγκων πληροφοριών για τον προσδιορισμό τάσεων και την πρόβλεψη συμπεριφορών– «μπορούν να αποτελέσουν πόρο σημαντικής αξίας για την κοινωνία, βελτιώνοντας την παραγωγικότητα, την αποδοτικότητα του δημόσιου τομέα και την κοινωνική συμμετοχή»⁹⁷⁵.

⁹⁷⁵ Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD(2017)01, Στρασβούργο, 23 Ιανουαρίου 2017.

Παρά τα πολλαπλά οφέλη της, η ψηφιακή εποχή εγείρει επίσης προκλήσεις όσον αφορά τον σεβασμό της ιδιωτικής ζωής και την προστασία των δεδομένων, δεδομένου ότι τεράστιοι όγκοι προσωπικών πληροφοριών συλλέγονται και υποβάλλονται σε επεξεργασία με ολόένα και πιο σύνθετους και αδιαφανείς τρόπους. Η τεχνολογική πρόοδος έχει οδηγήσει στην ανάπτυξη συνόλων μαζικών δεδομένων τα οποία μπορούν να υποβάλλονται εύκολα σε διασταυρωμένο έλεγχο και περαιτέρω ανάλυση για την αναζήτηση τάσεων ή για τη λήψη αποφάσεων βάσει αλγορίθμων, που μπορούν να παράσχουν πρωτοφανείς γνώσεις σχετικά με την ανθρώπινη συμπεριφορά και την ιδιωτική ζωή⁹⁷⁶.

Οι νέες τεχνολογίες αποτελούν ισχυρό εργαλείο και μπορούν να αποβούν εξαιρετικά επικίνδυνες εάν βρεθούν σε λάθος χέρια. Οι κρατικές αρχές οι οποίες αναλαμβάνουν την άσκηση δραστηριοτήτων μαζικής παρακολούθησης με τη χρήση ενδεχομένων των τεχνολογιών αυτών αποτελούν παράδειγμα του σημαντικού αντίκτυπου που μπορούν να έχουν οι εν λόγω τεχνολογίες στα δικαιώματα των ατόμων. Το 2013 οι αποκαλύψεις του Edward Snowden σχετικά με τη διαχείριση προγραμμάτων παρακολούθησης μεγάλης κλίμακας, τόσο του διαδικτύου όσο και τηλεφωνικών συνδιαλέξεων, από υπηρεσίες πληροφοριών σε ορισμένα κράτη πυροδότησαν σοβαρές ανησυχίες ως προς τους κινδύνους τους οποίους συνεπάγονται οι δραστηριότητες παρακολούθησης για την προστασία της ιδιωτικής ζωής, τη δημοκρατική διακυβέρνηση και την ελευθερία της έκφρασης. Η μαζική παρακολούθηση και οι τεχνολογίες που επιτρέπουν την παγκοσμιοποιημένη αποθήκευση και επεξεργασία προσωπικών πληροφοριών, καθώς και τη μαζική πρόσβαση σε δεδομένα, ενδέχεται να προσκρούουν σε αυτή καθαυτή την ουσία του δικαιώματος στον σεβασμό της ιδιωτικής ζωής⁹⁷⁷. Επιπλέον, μπορεί να έχουν αρνητική επίδραση στην πολιτική κουλτούρα και αποτρεπτικό αποτέλεσμα για τη δημοκρατία, τη δημιουργικότητα και την καινοτομία⁹⁷⁸. Απλώς και μόνον ο φόβος ότι το κράτος δύναται να παρακολουθεί και να αναλύει διαρκώς τη συμπεριφορά και τις ενέργειες των πολιτών μπορεί να τους αποθαρρύνει από το να εκφράζουν τις απόψεις τους σε ορισμένα ζητήματα και να συντελεί στη

976 Ευρωπαϊκό Κοινοβούλιο (2017), Ψήφισμα σχετικά με τις επιπτώσεις των μαζικών δεδομένων στα θεμελιώδη δικαιώματα: ιδιωτική ζωή, προστασία δεδομένων, μη διακριτική μεταχείριση, ασφάλεια και επιβολή του νόμου (P8_TA-PROV(2017)0076, Στρασβούργο, 14 Μαρτίου 2017.

977 Βλ. ΟΗΕ, Γενική Συνέλευση, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, A/69/397, 23 Σεπτεμβρίου 2014, παράγραφος 59. Βλ. επίσης ΕΔΔΑ, *Factsheet on Mass surveillance*, Ιούλιος 2017.

978 ΕΕΠΔ (2015), *Αντιμετώπιση της πρόκλησης των μαζικών δεδομένων*, Γνωμοδότηση 7/2015, Βρυξέλλες, 19 Νοεμβρίου 2015.

διαμόρφωση κλίματος καχυποψίας και επιφυλακτικότητας⁹⁷⁹. Οι προκλήσεις αυτές αποτέλεσαν το έναυσμα για διάφορες δημόσιες αρχές, ερευνητικά κέντρα και οργανώσεις της κοινωνίας των πολιτών ώστε να προβούν σε ανάλυση των δυνητικών επιπτώσεων των νέων τεχνολογιών στην κοινωνία. Το 2015 ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων δρομολόγησε διάφορες πρωτοβουλίες με στόχο την εκτίμηση των επιπτώσεων των μαζικών δεδομένων και του διαδικτύου των πραγμάτων στη δεοντολογία. Συγκεκριμένα, συγκρότησε μια συμβουλευτική ομάδα δεοντολογίας με στόχο την προώθηση «μιας ανοιχτής και ενημερωμένης συζήτησης σχετικά με την ψηφιακή δεοντολογία, η οποία παρέχει τη δυνατότητα στην ΕΕ να αξιοποιεί τα οφέλη της τεχνολογίας για την κοινωνία και την οικονομία ενώ ταυτόχρονα ενισχύει τα δικαιώματα και τις ελευθερίες των ατόμων, ιδίως τα δικαιώματα στην προστασία της ιδιωτικής ζωής και των δεδομένων»⁹⁸⁰.

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί επίσης ισχυρό εργαλείο για τις εταιρείες. Επί του παρόντος, μπορεί να αποκαλύψει λεπτομερείς πληροφορίες σχετικά με την υγεία ή την οικονομική κατάσταση ενός προσώπου, πληροφορίες τις οποίες χρησιμοποιούν στη συνέχεια οι εταιρείες προκειμένου να λάβουν σημαντικές αποφάσεις για τα πρόσωπα, όπως τα ασφάλιστρα υγείας που πρέπει να τους επιβληθούν ή η πιστοληπτική τους ικανότητα. Οι τεχνικές επεξεργασίας δεδομένων ενδέχεται επίσης να έχουν αντίκτυπο στις δημοκρατικές διαδικασίες όταν χρησιμοποιούνται από πολιτικούς ή εταιρείες για την άσκηση επιρροής στις εκλογές, για παράδειγμα, μέσω της επικοινωνίας για τους σκοπούς της «μικροστόχευσης» των ψηφοφόρων. Με άλλα λόγια, παρότι η προστασία της ιδιωτικής ζωής γινόταν αρχικά αντιληπτή ως δικαίωμα προστασίας των ατόμων έναντι της αδικαιολόγητης επέμβασης των δημόσιων αρχών, στη σύγχρονη εποχή είναι επίσης πιθανό να απειλείται από τις εξουσίες τις οποίες διαθέτουν φορείς του ιδιωτικού τομέα. Το ζήτημα αυτό εγείρει ερωτήματα σχετικά με τη χρήση της τεχνολογίας και της προγνωστικής ανάλυσης στο πλαίσιο αποφάσεων οι οποίες επηρεάζουν την καθημερινή ζωή των φυσικών προσώπων και ενισχύει την ανάγκη να διασφαλίζεται ότι οποιαδήποτε επεξεργασία δεδομένων προσωπικού χαρακτήρα πληροί τις απαιτήσεις σχετικά με τα θεμελιώδη δικαιώματα.

979 Βλ. ιδίως ΔΕΕ, συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ.* και *Kärntner Landesregierung κ.λπ.* [Τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014, σκέψη 37.

980 ΕΕΠΔ, απόφαση της 3ης Δεκεμβρίου 2015 σχετικά με τη σύσταση εξωτερικής συμβουλευτικής ομάδας για τις δεοντολογικές διατάξεις της προστασίας των δεδομένων («συμβουλευτική ομάδα δεοντολογίας»), 3 Δεκεμβρίου 2015, αιτιολογική σκέψη 5.

Η προστασία των δεδομένων είναι εγγενώς συνυφασμένη με τις τεχνολογικές, κοινωνικές και πολιτικές μεταβολές. Ως εκ τούτου, θα ήταν αδύνατον να καταρτιστεί πλήρης κατάλογος των μελλοντικών προκλήσεων. Στο παρόν κεφάλαιο εξετάζονται επιλεγμένοι τομείς που αφορούν τα μαζικά δεδομένα, τα διαδικτυακά κοινωνικά δίκτυα και την ψηφιακή ενιαία αγορά της ΕΕ. Δεν πρόκειται για εξαντλητική εκτίμηση των εν λόγω τομέων από πλευράς προστασίας των δεδομένων· απεναντίας, επισημαίνεται η πληθώρα των πιθανών αλληλεπιδράσεων μεταξύ των νέων ή αναθεωρημένων ανθρωπίνων δραστηριοτήτων και της προστασίας των δεδομένων.

10.1. Μαζικά δεδομένα, αλγόριθμοι και τεχνητή νοημοσύνη

Κύρια σημεία

- Οι ανατρεπτικές καινοτομίες στον τομέα των ΤΠΕ διαμορφώνουν επί του παρόντος έναν νέο τρόπο ζωής, στο πλαίσιο του οποίου οι κοινωνικές σχέσεις, οι επιχειρήσεις, οι ιδιωτικές και οι δημόσιες υπηρεσίες διασυνδέονται ψηφιακά, δημιουργώντας με αυτόν τον τρόπο ολόένα και μεγαλύτερο όγκο δεδομένων, εκ των οποίων πολλά είναι δεδομένα προσωπικού χαρακτήρα.
- Οι κυβερνήσεις, οι επιχειρήσεις και οι πολίτες δραστηριοποιούνται ολόένα και περισσότερο στο πλαίσιο μιας οικονομίας με γνώμονα τα δεδομένα, όπου τα ίδια τα δεδομένα έχουν αναχθεί πλέον σε πολύτιμους πόρους.
- Η έννοια των μαζικών δεδομένων αφορά τόσο τα δεδομένα αυτά καθαυτά όσο και την ανάλυσή τους.
- Τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία μέσω της ανάλυσης μαζικών δεδομένων εμπίπτουν στο πεδίο εφαρμογής της νομοθεσίας της ΕΕ και του Συμβουλίου της Ευρώπης.
- Οι παρεκκλίσεις από τους κανόνες και τα δικαιώματα στον τομέα της προστασίας των δεδομένων περιορίζονται σε επιλεγμένα δικαιώματα και σε συγκεκριμένες καταστάσεις στις οποίες η άσκηση ενός δικαιώματος θα ήταν αδύνατη ή θα απαιτούσε δυσανάλογες προσπάθειες από τους υπευθύνους επεξεργασίας.
- Κατά γενικό κανόνα, η πλήρως αυτοματοποιημένη λήψη αποφάσεων απαγορεύεται, εκτός από συγκεκριμένες περιπτώσεις.
- Η ενημέρωση και ο έλεγχος από τα άτομα είναι καίριας σημασίας για τη διασφάλιση της άσκησης των δικαιωμάτων.

Στον ολοένα και περισσότερο ψηφιοποιημένο κόσμο όπου ζούμε, κάθε δραστηριότητα αφήνει ένα ψηφιακό ίχνος το οποίο μπορεί να αποτελέσει αντικείμενο συλλογής, επεξεργασίας και αξιολόγησης ή ανάλυσης. Χάρη στις νέες τεχνολογίες πληροφοριών και επικοινωνιών, συλλέγονται και καταγράφονται ολοένα και περισσότερα δεδομένα ⁹⁸¹. Μέχρι πρόσφατα, καμία τεχνολογία δεν παρείχε τη δυνατότητα ανάλυσης ή αξιολόγησης των μαζικών δεδομένων ή εξαγωγής χρήσιμων συμπερασμάτων. Και τούτο διότι τα δεδομένα ήταν απλώς υπερβολικά πολλά για να είναι εφικτή η αξιολόγησή τους, υπερβολικά πολύπλοκα, ταχέως μεταβαλλόμενα και ανεπαρκώς διαρθρωμένα για να είναι εφικτός ο προσδιορισμός τάσεων και συνθηκών.

10.1.1. Ορισμός των μαζικών δεδομένων, των αλγόριθμων και της τεχνητής νοημοσύνης

Μαζικά δεδομένα

Ο όρος «μαζικά δεδομένα» είναι ένας ευρύτατα χρησιμοποιούμενος όρος ο οποίος μπορεί να αναφέρεται σε διάφορες έννοιες, ανάλογα με το εκάστοτε πλαίσιο. Εμπερικλείει συνήθως την έννοια «της αυξανόμενης τεχνολογικής ικανότητας συλλογής, επεξεργασίας και εξαγωγής νέων και προγνωστικών γνώσεων από μεγάλο όγκο και ποικιλομορφία δεδομένων με υψηλή ταχύτητα» ⁹⁸². Επομένως, η έννοια των μαζικών δεδομένων καλύπτει τόσο τα δεδομένα αυτά καθαυτά όσο και την ανάλυση των δεδομένων.

Τα δεδομένα προέρχονται από ευρύ φάσμα **πηγών**, μεταξύ των οποίων άνθρωποι και τα δεδομένα προσωπικού χαρακτήρα που τους αφορούν, μηχανήματα ή αισθητήρες, πληροφορίες σχετικά με το κλίμα, δορυφορικές εικόνες, ψηφιακές φωτογραφίες και βίντεο ή σήματα GPS. Ωστόσο, μεγάλο μέρος των δεδομένων και των πληροφοριών είναι δεδομένα προσωπικού χαρακτήρα και μπορεί να πρόκειται για οποιοδήποτε στοιχείο, από ονόματα, φωτογραφίες,

981 Ευρωπαϊκή Επιτροπή, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα COM(2014) 442 final, Βρυξέλλες, 2 Ιουλίου 2014.

982 Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 Ιανουαρίου 2017, στη σ. 2: Ευρωπαϊκή Επιτροπή, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα COM(2014) 442 final, Βρυξέλλες, 2 Ιουλίου 2014, στη σ. 4: Διεθνής Ένωση Τηλεπικοινωνιών (2015), Recommendation Y.3600. Big Data – Cloud computing based requirements and capabilities.

διευθύνσεις ηλεκτρονικού ταχυδρομείου, τραπεζικά στοιχεία, δεδομένα στίγμα-τος GPS, αναρτήσεις σε ιστότοπους κοινωνικής δικτύωσης, ιατρικές πληροφορίες ή η διεύθυνση IP ενός ηλεκτρονικού υπολογιστή⁹⁸³.

Τα μαζικά δεδομένα αναφέρονται επίσης στην **επεξεργασία**, ανάλυση και αξιολόγηση των όγκων των δεδομένων και των διαθέσιμων πληροφοριών, δηλαδή στην άντληση χρήσιμων πληροφοριών για τους σκοπούς της ανάλυσης μαζικών δεδομένων. Αυτό σημαίνει ότι τα δεδομένα και οι πληροφορίες που συλλέγονται μπορούν να χρησιμοποιηθούν για διαφορετικούς σκοπούς από εκείνους για τους οποίους προορίζονταν αρχικά, π.χ. στατιστικές τάσεις ή περισσότερο εξατομικευμένες υπηρεσίες, όπως η διαφήμιση. Μάλιστα, στις περιπτώσεις στις οποίες υπάρχουν πράγματι νέες τεχνολογίες για τη συλλογή, την επεξεργασία και την αξιολόγηση μαζικών δεδομένων, κάθε είδος πληροφοριών μπορεί να αποτελέσει αντικείμενο συνδυασμού και επαναξιολόγησης: χρηματοπιστωτικές πράξεις, πιστοληπτική ικανότητα, ιατρική περίθαλψη, ιδιωτική κατανάλωση, επαγγελματική δραστηριότητα, εντοπισμός στίγματος και ακολουθούμενες διαδρομές, χρήση του διαδικτύου, ηλεκτρονικές κάρτες και έξυπνα τηλέφωνα (smartphone), βιντεοσκόπηση ή παρακολούθηση επικοινωνιών. Η ανάλυση μαζικών δεδομένων προσδίδει στα δεδομένα μια νέα ποσοτική διάσταση, η οποία μπορεί να αξιολογείται και να χρησιμοποιείται σε πραγματικό χρόνο, με σκοπό, για παράδειγμα, την παροχή εξατομικευμένων υπηρεσιών στους καταναλωτές.

Αλγόριθμοι και τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη αναφέρεται στη νοημοσύνη μηχανών οι οποίες λειτουργούν ως «ευφυείς πράκτορες» («*intelligent agents*»). Ως ευφυείς πράκτορες, ορισμένες συσκευές μπορούν, με την υποστήριξη λογισμικού, να αντιλαμβάνονται το περιβάλλον τους και να προβαίνουν σε ενέργειες σύμφωνα με κατάλληλους αλγορίθμους. Ο όρος «τεχνητή νοημοσύνη» χρησιμοποιείται όταν μια μηχανή μιμείται «γνωστικές» λειτουργίες –όπως η μάθηση και η επίλυση προβλημάτων– που υπό κανονικές συνθήκες θα συνδέονταν με φυσικά πρόσωπα⁹⁸⁴. Για τη μίμηση της διαδικασίας λήψης αποφάσεων, οι σύγχρονες τεχνολογίες και τα λογισμικά χρησιμοποιούν αλγορίθμους, τους οποίους εφαρμόζουν με τη σειρά

983 Ενημερωτικό δελτίο της Ευρωπαϊκής Επιτροπής, Η μεταρρύθμιση της προστασίας δεδομένων της ΕΕ και τα μαζικά δεδομένα· Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 Ιανουαρίου 2017, σ. 2.

984 Stuart Russel και Peter Norvig, *Artificial Intelligence: A Modern Approach* (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, σ. 27, 32-58, 968-972· Stuart Russel και Peter Norvig, *Artificial Intelligence: A Modern Approach* (3rd ed.), 2009, Upper Saddle River, New Jersey: Prentice Hall, σ. 2.

τους οι συσκευές για τη λήψη «αυτοματοποιημένων αποφάσεων». Ένας αλγόριθμος μπορεί να περιγραφεί καλύτερα ως μια διαδικασία βήμα προς βήμα για τον υπολογισμό, την επεξεργασία δεδομένων, την αξιολόγηση και την αυτοματοποιημένη συλλογιστική και λήψη αποφάσεων.

Ομοίως με την ανάλυση μαζικών δεδομένων, η τεχνητή νοημοσύνη, καθώς και η αυτοματοποιημένη λήψη αποφάσεων που παράγει, απαιτεί τη συγκέντρωση και την επεξεργασία μεγάλων όγκων δεδομένων. Τα δεδομένα αυτά μπορεί να προέρχονται από την ίδια τη συσκευή (θερμότητα των φρένων, καύσιμο κ.λπ.) ή από τον περιβάλλοντα χώρο. Η κατάρτιση προφίλ, για παράδειγμα, αποτελεί μια διαδικασία η οποία ενδέχεται να βασίζεται σε αυτοματοποιημένη λήψη αποφάσεων σύμφωνα με προκαθορισμένα πρότυπα ή παράγοντες.

Παράδειγμα: Κατάρτιση προφίλ και στοχευμένη διαφήμιση

Η κατάρτιση προφίλ βάσει μαζικών δεδομένων περιλαμβάνει την αναζήτηση τάσεων οι οποίες αντικατοπτρίζουν τα «χαρακτηριστικά ενός τύπου προσωπικότητας», για παράδειγμα, όταν διαδικτυακές επιχειρήσεις αγορών προτείνουν προϊόντα «που μπορεί επίσης να σας αρέσουν» με βάση τις πληροφορίες που συγκεντρώνονται από τα προϊόντα που έχουν τοποθετηθεί στο καλάθι αγορών ενός πελάτη σε προγενέστερο χρόνο. Όσο περισσότερα είναι τα δεδομένα, τόσο σαφέστερο είναι το μωσαϊκό που διαμορφώνεται. Το έξυπνο τηλέφωνο (smartphone), για παράδειγμα, αποτελεί ένα ισχυρό ερωτηματολόγιο το οποίο συμπληρώνουν τα άτομα με κάθε χρήση, τόσο συνειδητά όσο και ασυνειδητά.

Η σύγχρονη ψυχογραφία –η επιστήμη που μελετά τις προσωπικότητες– χρησιμοποιεί τη μέθοδο OCEAN, βάσει της οποίας καθορίζει τους τύπους χαρακτήρων που εξετάζονται. Τα πέντε χαρακτηριστικά της προσωπικότητας («Big Five») είναι οι πέντε διαστάσεις του χαρακτήρα και περιλαμβάνουν τη δεκτικότητα (Openness) (πόσο ανοικτό είναι ένα πρόσωπο στο καινούργιο), την ευσυνειδησία (Conscientiousness) (κατά πόσον το πρόσωπο παρουσιάζει χαρακτηριστικά τελειομανίας), την εξωστρέφεια (Extraversion) (πόσο κοινωνικό είναι το πρόσωπο), την θελκτικότητα (Agreeableness) (πόσο θελκτικό είναι το πρόσωπο) και τον νευρωτισμό (Neuroticism) (πόσο ευάλωτο είναι το πρόσωπο). Με τις πληροφορίες αυτές καταρτίζεται το προφίλ του υπό εξέταση προσώπου, των αναγκών και των φόβων του, του τρόπου με τον οποίο θα

συμπεριφέρεται κ.λπ. Στη συνέχεια συμπληρώνεται με άλλες πληροφορίες σχετικά με το πρόσωπο, οι οποίες αντλούνται από οποιαδήποτε διαθέσιμη πηγή, από μεσίτες δεδομένων, κοινωνικά δίκτυα (συμπεριλαμβανομένων των δηλώσεων «Μου αρέσει» σε αναρτήσεις και στις φωτογραφίες που αναρτώνται) έως τη μουσική που ακούει το πρόσωπο στο διαδίκτυο ή τα δεδομένα GPS και στίγματος.

Ο όγκος των προφίλ που δημιουργούνται μέσω τεχνικών ανάλυσης μαζικών δεδομένων υποβάλλονται κατόπιν σε σύγκριση προκειμένου να προσδιοριστούν παρόμοιες τάσεις και να ερμηνευθούν οι κατηγορίες προσωπικότητας. Κατά συνέπεια, οι πληροφορίες σχετικά με τη συμπεριφορά και τις αντιλήψεις ορισμένων προσωπικότητας αναστρέφονται. Με την πρόσβαση σε μαζικά δεδομένα και τη χρήση τους, το τεστ προσωπικότητας αντιστρέφεται, καθώς οι πληροφορίες σχετικά με τη συμπεριφορά και τις αντιλήψεις χρησιμοποιούνται πλέον για να περιγράψουν την προσωπικότητα του ατόμου. Χάρη στον συνδυασμό των πληροφοριών σχετικά με τις δηλώσεις «Μου αρέσει» ενός ατόμου στα κοινωνικά δίκτυα, τα δεδομένα παρακολούθησης, τη μουσική που ακούει ή τις ταινίες που παρακολουθεί, μπορεί να διαμορφωθεί σαφής εικόνα της προσωπικότητας του εν λόγω ατόμου, η οποία παρέχει στις επιχειρήσεις τη δυνατότητα να προβάλλουν εξατομικευμένες διαφημίσεις και/ή πληροφορίες σύμφωνα με την «προσωπικότητα» του συγκεκριμένου ατόμου. Το σημαντικότερο όμως είναι ότι οι πληροφορίες αυτές μπορούν να υποβάλλονται σε επεξεργασία σε πραγματικό χρόνο ⁹⁸⁵.

10.1.2. Στάθμιση των οφελών και των κινδύνων των μαζικών δεδομένων

Οι σύγχρονες τεχνικές επεξεργασίας μπορούν να χειρίζονται μεγάλους όγκους δεδομένων, να εισάγουν νέα δεδομένα ταχύτατα, να εξασφαλίζουν σε πραγματικό χρόνο την επεξεργασία των πληροφοριών από πλευράς σύντομου χρόνου απόκρισης (ακόμη και σε περίπτωση πολύπλοκων αιτημάτων), να παρέχουν τη δυνατότητα πολλαπλών και ταυτόχρονων αιτημάτων, ενώ μπορούν επίσης να αναλύουν διαφορετικά είδη πληροφοριών (φωτογραφίες, κείμενα ή αριθμούς).

⁹⁸⁵ Με τη χρήση τεχνικών επεξεργασίας και νέου λογισμικού αξιολογούνται οι πληροφορίες σχετικά με τις προτιμήσεις ενός προσώπου, ελέγχεται ο πραγματικός χρόνος κατά τον οποίο πραγματοποιούνται διαδικτυακές αγορές ή προσθήκες στο καλάθι διαδικτυακών αγορών και μπορούν να προτείνονται «προϊόντα» τα οποία ενδέχεται να ενδιαφέρουν το συγκεκριμένο πρόσωπο βάσει των πληροφοριών που συγκεντρώνονται.

Αυτές οι τεχνολογικές καινοτομίες καθιστούν εφικτή τη διάρθρωση, την επεξεργασία και την αξιολόγηση μαζικών δεδομένων και πληροφοριών σε πραγματικό χρόνο ⁹⁸⁶. Με την εκθετική αύξηση του όγκου των δεδομένων που διατίθενται και αναλύονται, μπορούν πλέον να επιτευχθούν αποτελέσματα τα οποία θα ήταν αδύνατα με ανάλυση μικρότερης κλίμακας. Τα μαζικά δεδομένα έχουν συμβάλει στην ανάπτυξη ενός νέου επιχειρηματικού πεδίου, στο οποίο μπορούν να αναδυθούν νέες υπηρεσίες τόσο για τις επιχειρήσεις όσο και για τους καταναλωτές. Η αξία των δεδομένων προσωπικού χαρακτήρα των πολιτών της ΕΕ έχει τη δυνατότητα να αυξηθεί σε σχεδόν 1 τρις. ευρώ ετησίως έως το 2020 ⁹⁸⁷. Ως εκ τούτου, τα μαζικά δεδομένα μπορούν να προσφέρουν νέες **ευκαιρίες** που απορρέουν από την αξιολόγηση των μαζικών δεδομένων για τη διαμόρφωση νέων κοινωνικών, οικονομικών ή επιστημονικών στοιχείων, τα οποία μπορούν να αποφέρουν οφέλη τόσο στους ιδιώτες όσο και στις επιχειρήσεις και τις κυβερνήσεις ⁹⁸⁸.

Η ανάλυση μαζικών δεδομένων μπορεί να αποκαλύψει σχέσεις μεταξύ διαφόρων πηγών και συνόλων δεδομένων, προσφέροντας έτσι χρήσιμες πληροφορίες σε τομείς όπως η επιστήμη και η ιατρική. Αυτό ισχύει, για παράδειγμα, σε τομείς όπως η υγεία, η επισιτιστική ασφάλεια, τα ευφυή συστήματα μεταφορών, η ενεργειακή απόδοση ή ο πολεοδομικός σχεδιασμός. Η εν λόγω ανάλυση των πληροφοριών σε πραγματικό χρόνο μπορεί να χρησιμοποιηθεί για τη βελτίωση των εφαρμοζόμενων συστημάτων. Στον τομέα της έρευνας μπορούν να αντληθούν νέα στοιχεία χάρη στον συνδυασμό μεγάλων όγκων δεδομένων και στατιστικών εκτιμήσεων, ιδίως σε πεδία στα οποία η αξιολόγηση μεγάλου μέρους

986 Η ανάπτυξη λογισμικού για την επεξεργασία μαζικών δεδομένων εξακολουθεί να βρίσκεται σε πρώιμο στάδιο. Ωστόσο, πρόσφατα αναπτύχθηκαν προγράμματα ανάλυσης, ιδίως για την ανάλυση μαζικών δεδομένων και πληροφοριών σε πραγματικό χρόνο, τα οποία αφορούν δραστηριότητες ατόμων. Η δυνατότητα ανάλυσης και επεξεργασίας μαζικών δεδομένων με διαφανές τρόπο έχει προσφέρει νέα μέσα κατάρτισης προφίλ και στοχευμένης διαφήμισης. Ευρωπαϊκή Επιτροπή, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα COM(2014) 442 final, Βρυξέλλες, 2 Ιουλίου 2014· ενημερωτικό δελτίο της Ευρωπαϊκής Επιτροπής, Η μεταρρύθμιση της προστασίας δεδομένων στην ΕΕ και τα μαζικά δεδομένα, και Συμβούλιο της Ευρώπης, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, 23 Ιανουαρίου 2017, σ. 2.

987 Ενημερωτικό δελτίο της Ευρωπαϊκής Επιτροπής, Η μεταρρύθμιση της προστασίας δεδομένων στην ΕΕ και τα μαζικά δεδομένα.

988 Διεθνής διάσκεψη των επιτρόπων για την προστασία των δεδομένων και την ιδιωτική ζωή (2014), Resolution on Big Data και Ευρωπαϊκή Επιτροπή, Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών Προς μια ακμάζουσα οικονομία βασιζόμενη στα δεδομένα COM(2014) 442 final, Βρυξέλλες, 2 Ιουλίου 2014, σ. 2· ενημερωτικό δελτίο της Ευρωπαϊκής Επιτροπής, Μεταρρύθμιση της προστασίας δεδομένων στην ΕΕ και τα μαζικά δεδομένα και Συμβούλιο της Ευρώπης, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, 23 Ιανουαρίου 2017, σ. 1.

των δεδομένων διενεργείται, μέχρι σήμερα, μόνο με μη αυτοματοποιημένο τρόπο. Μπορούν να αναπτυχθούν νέες θεραπευτικές αγωγές, οι οποίες μπορούν να εξατομικεύονται ανάλογα με τον εκάστοτε ασθενή, βάσει συγκρίσεων με τους όγκους διαθέσιμων πληροφοριών. Οι επιχειρήσεις ευελπιστούν ότι η ανάλυση μαζικών δεδομένων θα τους επιτρέψει να αποκτήσουν ανταγωνιστικό πλεονέκτημα, να διασφαλίσουν πιθανές εξοικονομήσεις και να δημιουργήσουν νέους επιχειρηματικούς τομείς μέσω της άμεσης, εξατομικευμένης εξυπηρέτησης των πελατών τους. Οι κρατικές υπηρεσίες ελπίζουν να επιτύχουν βελτιώσεις στον τομέα της ποινικής δικαιοσύνης. Η στρατηγική της Επιτροπής για την ψηφιακή ενιαία αγορά της Ευρώπης αναγνωρίζει το δυναμικό των τεχνολογιών και των υπηρεσιών που βασίζονται στα δεδομένα, καθώς και των μαζικών δεδομένων, ως καταλύτη για την οικονομική ανάπτυξη, την καινοτομία και την ψηφιοποίηση στην ΕΕ ⁹⁸⁹.

Ωστόσο, τα μαζικά δεδομένα ενέχουν επίσης **κινδύνους**, οι οποίοι συνδέονται κατά γενικό κανόνα με τρία χαρακτηριστικά: τον όγκο, την ταχύτητα και την ποικιλομορφία των δεδομένων που υποβάλλονται σε επεξεργασία. Ο όγκος αναφέρεται στην ποσότητα των δεδομένων που υποβάλλονται σε επεξεργασία, η ποικιλομορφία αφορά τον αριθμό και την πολυμορφία των ειδών δεδομένων, ενώ η ταχύτητα κίνησης αφορά την ταχύτητα επεξεργασίας των δεδομένων. Ειδικά κριτήρια για την προστασία δεδομένων προκύπτουν κυρίως όταν η ανάλυση μαζικών δεδομένων χρησιμοποιείται σε μεγάλα σύνολα δεδομένων προκειμένου να εξαχθούν νέες και προγνωστικές γνώσεις για σκοπούς λήψης αποφάσεων σχετικά με άτομα και/ή ομάδες ⁹⁹⁰. Οι κίνδυνοι για την προστασία των δεδομένων και της ιδιωτικής ζωής που αφορούν τα μαζικά δεδομένα έχουν επισημανθεί σε γνωμοδοτήσεις του ΕΕΠΔ, καθώς και σε γνώμες της Ομάδας εργασίας του άρθρου 29, σε ψηφίσματα του Ευρωπαϊκού Κοινοβουλίου και σε έγγραφα πολιτικής του Συμβουλίου της Ευρώπης ⁹⁹¹.

989 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 14ης Μαρτίου 2017 σχετικά με τις επιπτώσεις των μαζικών δεδομένων στα θεμελιώδη δικαιώματα: ιδιωτική ζωή, προστασία δεδομένων, μη διακριτική μεταχείριση, ασφάλεια και επιβολή του νόμου [2016/2225(INI)].

990 Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, 23 Ιανουαρίου 2017, σ. 2.

991 Βλ. για παράδειγμα, ΕΕΠΔ (2015), *Αντιμετώπιση της πρόκλησης των μαζικών δεδομένων*, Γνωμοδότηση 7/2015, 19 Νοεμβρίου 2015· ΕΕΠΔ (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Γνωμοδότηση 8/2016, 23 Σεπτεμβρίου 2016· Ευρωπαϊκό Κοινοβούλιο (2016), Ψήφισμα σχετικά με τις επιπτώσεις των μαζικών δεδομένων στα θεμελιώδη δικαιώματα: ιδιωτική ζωή, προστασία δεδομένων, μη διακριτική μεταχείριση, ασφάλεια και επιβολή του νόμου, P8_TA(2017)0076, Στρασβούργο, 14 Μαρτίου 2017· Συμβούλιο της Ευρώπης, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, T-PD(2017)01, Στρασβούργο, 23 Ιανουαρίου 2017.

Στους κινδύνους μπορεί να συμπεριλαμβάνεται ο κακός χειρισμός των μαζικών δεδομένων από όσους έχουν πρόσβαση στον όγκο των πληροφοριών μέσω της χειραγώγησης, των διακρίσεων ή της καταπίεσης ατόμων ή συγκεκριμένων ομάδων στην κοινωνία ⁹⁹². Σε περίπτωση που συλλέγονται, υποβάλλονται σε επεξεργασία και αξιολογούνται όγκοι δεδομένων προσωπικού χαρακτήρα ή πληροφορίες σχετικά με τη συμπεριφορά ατόμων, η εκμετάλλευσή τους μπορεί να συνεπάγεται σοβαρές παραβιάσεις θεμελιωδών δικαιωμάτων και ελευθεριών που βαίνουν πέραν του δικαιώματος στην προστασία της ιδιωτικής ζωής. Δεν είναι δυνατόν να προσδιοριστεί με ακρίβεια ο βαθμός στον οποίο μπορεί να θίγονται η προστασία της ιδιωτικής ζωής και τα δεδομένα προσωπικού χαρακτήρα. Το Ευρωπαϊκό Κοινοβούλιο διαπίστωσε ότι δεν υπάρχει μεθοδολογία για τη διενέργεια εμπεριστατωμένης αξιολόγησης όσον αφορά τον αντίκτυπο των μαζικών δεδομένων, ωστόσο υπάρχουν στοιχεία που υποδεικνύουν ότι η ανάλυση μαζικών δεδομένων μπορεί να έχει σημαντικό οριζόντιο αντίκτυπο τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα ⁹⁹³.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων περιλαμβάνει διατάξεις σχετικά με το δικαίωμα των ατόμων να μην υπόκεινται σε αυτοματοποιημένη λήψη αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ ⁹⁹⁴. Το ζήτημα της προστασίας της ιδιωτικής ζωής ανακύπτει σε περίπτωση που η άσκηση του δικαιώματος εναντίωσης προϋποθέτει ανθρώπινη παρέμβαση, μέσω της οποίας επιτρέπεται στα υποκείμενα των δεδομένων να εκφράζουν την άποψή τους και να αμφισβητούν την απόφαση ⁹⁹⁵. Η δυνατότητα αυτή μπορεί να εγείρει προκλήσεις όσον αφορά τη διασφάλιση επαρκούς επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα εάν, για παράδειγμα, δεν είναι δυνατή η ανθρώπινη παρέμβαση ή σε περίπτωση που οι αλγόριθμοι είναι υπερβολικά πολύπλοκοι και ο όγκος των σχετικών δεδομένων είναι υπερβολικά μεγάλος ώστε να παρέχονται στους ενδιαφερομένους αιτιολογήσεις για ορισμένες αποφάσεις και/ή εκ των προτέρων πληροφόρηση που να επιτρέπει τη λήψη της συγκατάθεσής τους. Ένα παράδειγμα της χρήσης τεχνητής νοημοσύνης και αυτοματοποιημένης λήψης αποφάσεων εντοπίζεται στις πρόσφατες εξελίξεις στον τομέα της υποβολής αιτήσεων για τη χορήγηση ενυπόθηκων δανείων ή κατά τη διάρκεια

992 Διεθνής διάσκεψη των επιτρόπων για την προστασία των δεδομένων και την ιδιωτική ζωή (2014), Resolution on Big Data.

993 Ψήφισμα του Ευρωπαϊκού Κοινοβουλίου της 14ης Μαρτίου 2017 σχετικά με τις επιπτώσεις των μαζικών δεδομένων στα θεμελιώδη δικαιώματα: ιδιωτική ζωή, προστασία δεδομένων, μη διακριτική μεταχείριση, ασφάλεια και επιβολή του νόμου [2016/2225(INI)].

994 Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 22.

995 Ό.π., άρθρο 22 παράγραφος 3.

διαδικασιών πρόσληψης. Οι αιτήσεις απορρίπτονται με βάση το γεγονός ότι οι αιτούντες δεν πληρούν προκαθορισμένες παραμέτρους ή παράγοντες.

10.1.3. Ζητήματα προστασίας των δεδομένων

Από πλευράς προστασίας των δεδομένων, τα κύρια ζητήματα αφορούν, αφενός, τον όγκο και την ποικιλομορφία των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και, αφετέρου, την επεξεργασία και τα αποτελέσματά της. Η εισαγωγή πολύπλοκων αλγορίθμων και λογισμικού για τον μετασχηματισμό των μαζικών δεδομένων σε πόρο για τους σκοπούς της λήψης αποφάσεων έχει αντίκτυπο ιδίως στα άτομα και στις ομάδες, κυρίως σε περιπτώσεις κατάρτισης προφίλ ή επισήμανσης, και εγείρει εντέλει πολλά ζητήματα σχετικά με την προστασία των δεδομένων ⁹⁹⁶.

Η εξακρίβωση της ταυτότητας των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία και η ευθύνη τους

Τα μαζικά δεδομένα και η τεχνητή νοημοσύνη εγείρουν ερωτήματα σε σχέση με την εξακρίβωση της ταυτότητας των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία, καθώς και σε σχέση με την ευθύνη τους: όταν συλλέγεται και υποβάλλεται σε επεξεργασία ένας τόσο μεγάλος όγκος δεδομένων, ποιος είναι ο κύριος των εν λόγω δεδομένων; Όταν τα δεδομένα υποβάλλονται σε επεξεργασία από μηχανήματα και λογισμικό τεχνητής νοημοσύνης, ποιος είναι ο υπεύθυνος επεξεργασίας; Ποιες είναι οι ακριβείς αρμοδιότητες κάθε συμμετέχοντος στο πλαίσιο της επεξεργασίας; Και για ποιους σκοπούς μπορούν να χρησιμοποιούνται μαζικά δεδομένα;

Το ζήτημα της ευθύνης στο πλαίσιο της τεχνητής νοημοσύνης αποτελεί ακόμη σημαντικότερη πρόκληση όταν ένα μέσο τεχνητής νοημοσύνης λαμβάνει απόφαση η οποία βασίζεται στην επεξεργασία δεδομένων που έχει αναπτύξει το ίδιο το μέσο. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων παρέχει νομικό πλαίσιο για την ευθύνη του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία δεδομένων. Η παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα συνεπάγεται ευθύνη τόσο για τον υπεύθυνο επεξεργασίας όσο και για τον εκτελούντα την επεξεργασία ⁹⁹⁷. Η τεχνητή νοημοσύνη και η αυτο-

⁹⁹⁶ Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, 23 Ιανουαρίου 2017, σ. 2.

⁹⁹⁷ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 77 έως 79 και άρθρο 82.

ματοποιημένη λήψη αποφάσεων εγείρει ερωτήματα σχετικά με το ποιος είναι υπεύθυνος για παραβάσεις οι οποίες έχουν αντίκτυπο στην προστασία της ιδιωτικής ζωής των υποκειμένων των δεδομένων, σε περίπτωση που δεν μπορούν να αποδοθούν με ακρίβεια η πολυπλοκότητα και ο όγκος των επεξεργασμένων δεδομένων. Όταν η τεχνητή νοημοσύνη και οι αλγόριθμοι θεωρούνται προϊόντα, στην περίπτωση αυτή τίθενται ζητήματα μεταξύ της προσωπικής ευθύνης, η οποία ρυθμίζεται βάσει του Γενικού Κανονισμού για την Προστασία Δεδομένων, και της ευθύνης λόγω ελαττωματικών προϊόντων, η οποία δεν ρυθμίζεται από τον συγκεκριμένο κανονισμό⁹⁹⁸. Προς τούτο, θα απαιτούνταν κανόνες σχετικά με την ευθύνη, ούτως ώστε να καλυφθεί το κενό μεταξύ της προσωπικής ευθύνης και της ευθύνης λόγω ελαττωματικών προϊόντων, για παράδειγμα, στον τομέα της ρομποτικής και της τεχνητής νοημοσύνης, συμπεριλαμβανομένης της αυτοματοποιημένης λήψης αποφάσεων⁹⁹⁹.

Αντίκτυπος στις αρχές προστασίας των δεδομένων

Η φύση, η ανάλυση και η χρήση μαζικών δεδομένων, όπως περιγράφονται ανωτέρω, εγείρουν προκλήσεις όσον αφορά την εφαρμογή ορισμένων παραδοσιακών, θεμελιωδών αρχών του ευρωπαϊκού δικαίου για την προστασία των δεδομένων¹⁰⁰⁰. Οι εν λόγω προκλήσεις αφορούν κυρίως τις αρχές της νομιμότητας, της ελαχιστοποίησης των δεδομένων, του περιορισμού του σκοπού και της διαφάνειας.

Σύμφωνα με την αρχή της ελαχιστοποίησης των δεδομένων, τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκή και συναφή και να περιορίζονται στα αναγκαία για τους σκοπούς της επεξεργασίας τους. Ωστόσο, το επιχειρηματικό μοντέλο των μαζικών δεδομένων ενδέχεται να είναι το άκρο αντίθετο της ελαχιστοποίησης των δεδομένων, διότι απαιτεί ολόένα και περισσότερα δεδομένα, και μάλιστα συχνά για απροσδιόριστους σκοπούς.

998 Ευρωπαϊκό Κοινοβούλιο, *European Civil Law Rules in Robotics*, Γενική Διεύθυνση Εσωτερικών Πολιτικών (Οκτώβριος 2016), σ. 14.

999 Ομιλία του Roberto Viola στο πλαίσιο του σεμιναρίου για τα μέσα ενημέρωσης που πραγματοποιήθηκε στο Ευρωπαϊκό Κοινοβούλιο σχετικά με το ευρωπαϊκό δίκαιο για τη ρομποτική. (ΟΜΙΛΙΑ 16/02/2017) *Ανακοίνωση* του Ευρωπαϊκού Κοινοβουλίου σχετικά με το αίτημα προς την Επιτροπή για υποβολή πρότασης σχετικά με τη θέσπιση κανόνων για την αστική ευθύνη στους τομείς της ρομποτικής και της τεχνητής νοημοσύνης.

1000 Συμβούλιο της Ευρώπης, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, T-PD(2017)01, Στρασβούργο, 23 Ιανουαρίου 2017.

Το ίδιο ισχύει και για την αρχή του περιορισμού του σκοπού, σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία για καθορισμένους σκοπούς και δεν μπορούν να χρησιμοποιούνται για σκοπούς οι οποίοι δεν συνάδουν με τον αρχικό σκοπό της συλλογής των δεδομένων, εκτός εάν η εν λόγω επεξεργασία βασίζεται σε νόμιμους λόγους, όπως είναι, ενδεικτικά, η συγκατάθεση του υποκειμένου των δεδομένων (βλ. [ενότητα 4.1.1](#)).

Τέλος, τα μαζικά δεδομένα εγείρουν επίσης προκλήσεις όσον αφορά την αρχή της ακρίβειας των δεδομένων, διότι οι εφαρμογές μαζικών δεδομένων χαρακτηρίζονται από την τάση να συλλέγουν δεδομένα από πολλές και διαφορετικές πηγές, χωρίς να παρέχεται η δυνατότητα ελέγχου και/ή διατήρησης της ακρίβειας των δεδομένων που συλλέγονται ¹⁰⁰¹.

Ειδικοί κανόνες και δικαιώματα

Εξακολουθεί να ισχύει ο γενικός κανόνας σύμφωνα με τον οποίο τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία μέσω της ανάλυσης μαζικών δεδομένων εμπίπτουν στο πεδίο εφαρμογής της νομοθεσίας για την προστασία των δεδομένων. Ειδικοί κανόνες ή παρεκκλίσεις για συγκεκριμένες περιπτώσεις σε σχέση με την επεξεργασία πολύπλοκων δεδομένων βάσει αλγορίθμων έχουν παρ' όλα αυτά συμπεριληφθεί στο **δίκαιο της ΕΕ** και του Συμβουλίου της Ευρώπης.

Στο δίκαιο του Συμβουλίου της Ευρώπης η Εκσυγχρονισμένη Σύμβαση 108 παρέχει νέα δικαιώματα στο υποκείμενο των δεδομένων προκειμένου να πραγματοποιείται πιο αποτελεσματικά ο έλεγχος στα προσωπικά του δεδομένα στην εποχή των μαζικών δεδομένων. Είναι ακριβώς, για παράδειγμα, η περίπτωση του άρθρου 9 παρ. 1 (α), (γ) και (δ) της Εκσυγχρονισμένης Σύμβασης 108 σχετικά με το δικαίωμα του υποκειμένου των δεδομένων να μην υπόκειται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία των δεδομένων του χωρίς να ληφθούν υπόψη οι απόψεις του το δικαίωμα ενημέρωσης, κατόπιν αίτησης, σχετικά με το σκεπτικό της επεξεργασίας δεδομένων όπου τα αποτελέσματα αυτής της επεξεργασίας εφαρμόζονται στο υποκείμενο των δεδομένων, καθώς και το δικαίωμα εναντίωσης. Άλλες διατάξεις της Εκσυγχρονισμένης Σύμβασης 108, ιδίως όσον αφορά τη διαφάνεια και τις πρόσθετες υποχρεώσεις, αποτελούν συμπληρωματικά στοιχεία του μηχανισμού προστασίας που θεσπίστηκε

¹⁰⁰¹ ΕΕΠΔ (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Γνωμοδότηση 8/2016, 23 Σεπτεμβρίου 2016, σ. 8.

με την Εκσυγχρονησμένη Σύμβαση 108 για την αντιμετώπιση των ψηφιακών προκλήσεων.

Πέραν των περιπτώσεων που απαριθμούνται στο άρθρο 23 του ΓΚΠΔ, πρέπει να εξασφαλίζεται **διαφάνεια** για κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα. Το στοιχείο αυτό είναι ιδιαίτερα σημαντικό στο πλαίσιο των υπηρεσιών διαδικτύου και άλλων πολύπλοκων ειδών αυτοματοποιημένης επεξεργασίας, όπως η χρήση αλγορίθμων για τη λήψη αποφάσεων. Εν προκειμένω, τα χαρακτηριστικά των συστημάτων επεξεργασίας δεδομένων πρέπει να παρέχουν στα υποκείμενα των δεδομένων τη δυνατότητα να κατανοούν πραγματικά τι συμβαίνει με τα δεδομένα τους. Προκειμένου να εξασφαλίζεται δίκαιη και διαφανής επεξεργασία, ο Γενικός Κανονισμός για την Προστασία Δεδομένων επιβάλλει στον υπεύθυνο επεξεργασίας την υποχρέωση να παρέχει στο υποκείμενο των δεδομένων σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται στο πλαίσιο της αυτοματοποιημένης λήψης αποφάσεων, περιλαμβανομένης της κατάρτισης προφίλ ¹⁰⁰². Στη σύστασή της σχετικά με την προστασία και την προώθηση του δικαιώματος στην ελευθερία της έκφρασης και του δικαιώματος στην ιδιωτική ζωή, όσον αφορά την ουδετερότητα των δικτύων, η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης πρότεινε οι φορείς παροχής υπηρεσιών διαδικτύου να «παρέχουν στους χρήστες σαφείς, πλήρεις και δημόσια διαθέσιμες πληροφορίες όσον αφορά τυχόν πρακτικές διαχείρισης της κίνησης οι οποίες ενδέχεται να επηρεάζουν την πρόσβαση των χρηστών σε περιεχόμενο, εφαρμογές ή υπηρεσίες, καθώς και τη διανομή τους» ¹⁰⁰³. Οι εκθέσεις σχετικά με τις πρακτικές διαχείρισης της κίνησης, οι οποίες καταρτίζονται από τις αρμόδιες αρχές σε όλα τα κράτη μέλη, θα πρέπει να εκπονούνται κατά τρόπο ανοικτό και διαφανή και θα πρέπει να διατίθενται δωρεάν στο κοινό ¹⁰⁰⁴.

Οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να **ενημερώνουν** τα υποκείμενα των δεδομένων –ανεξάρτητα από το αν τα δεδομένα συλλέχθηκαν από αυτά ή όχι– όχι μόνο για συγκεκριμένες πληροφορίες σχετικά με τα δεδομένα που συλλέγονται και την προβλεπόμενη επεξεργασία τους (βλ. [ενότητα 6.1.1](#)), αλλά και για την ύπαρξη, κατά περίπτωση, διαδικασιών αυτοματοποιημένης λήψης αποφάσεων, παρέχοντάς τους «σημαντικές πληροφορίες σχετικά με τη λογική που

¹⁰⁰² Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο στ).

¹⁰⁰³ Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών (2016), Σύσταση CM/Rec (2016) 1 της Επιτροπής Υπουργών προς τα κράτη μέλη σχετικά με την προστασία και την προώθηση του δικαιώματος στην ελευθερία έκφρασης και του δικαιώματος στην ιδιωτική ζωή όσον αφορά την ουδετερότητα των δικτύων, 13 Ιανουαρίου 2016, σημείο 5.1.

¹⁰⁰⁴ Ο.π., σημείο 5.2.

ακολουθείται»¹⁰⁰⁵, τους στόχους και τις δυνητικές επιπτώσεις των εν λόγω διαδικασιών. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων διευκρινίζει επίσης (μόνο στις περιπτώσεις στις οποίες τα δεδομένα προσωπικού χαρακτήρα δεν έχουν συλλεγεί από το υποκείμενο των δεδομένων) ότι ο υπεύθυνος επεξεργασίας δεν υποχρεούται να παρέχει πληροφορίες αυτού του είδους στο υποκείμενο των δεδομένων εάν «η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια»¹⁰⁰⁶. Ωστόσο, όπως τονίζεται από την Ομάδα εργασίας του άρθρου 29 στις κατευθυντήριες γραμμές της με τίτλο *Κατευθυντήριες γραμμές για την αυτοματοποιημένη λήψη αποφάσεων και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού 2016/679*, η πολυπλοκότητα της επεξεργασίας δεν θα πρέπει, αυτή καθαυτή, να απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωσή του να παρέχει στο υποκείμενο των δεδομένων σαφείς επεξηγήσεις σχετικά με τους στόχους και την ανάλυση που χρησιμοποιούνται στο πλαίσιο της επεξεργασίας δεδομένων¹⁰⁰⁷.

Τα δικαιώματα των υποκειμένων των δεδομένων όσον αφορά την **πρόσβαση**, τη **διόρθωση** και τη **διαγραφή** των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, καθώς και το δικαίωμά τους όσον αφορά τον **περιορισμό** της επεξεργασίας, δεν περιλαμβάνουν παρόμοια εξαίρεση. Ωστόσο, η υποχρέωση του υπευθύνου επεξεργασίας δεδομένων να γνωστοποιεί στο υποκείμενο των δεδομένων οποιαδήποτε διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν (βλ. **ενότητα 6.1.4**) είναι επίσης δυνατό να αρθεί όταν η εν λόγω γνωστοποίηση «αποδεικνύεται αδύνατη ή θα συνεπαγόταν δυσανάλογη προσπάθεια»¹⁰⁰⁸.

Τα υποκείμενα των δεδομένων έχουν επίσης δικαίωμα **εναντίωσης**, όπως ορίζεται στο άρθρο 21 του ΓΚΠΔ (βλ. **ενότητα 6.1.6**), σε κάθε επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, συμπεριλαμβανομένων των περιπτώσεων ανάλυσης μαζικών δεδομένων. Παρότι οι υπεύθυνοι επεξεργασίας δεδομένων δύνανται να απαλλάσσονται από τη συγκεκριμένη υποχρέωση εάν είναι σε θέση να αποδείξουν την ύπαρξη επιτακτικών έννομων συμφερόντων, δεν έχουν δικαίωμα αντίστοιχης απαλλαγής στο πλαίσιο της επεξεργασίας για σκοπούς απευθείας εμπορικής προώθησης.

¹⁰⁰⁵ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 13 παράγραφος 2 στοιχείο στ) και άρθρο 14 παράγραφος 2 στοιχείο ζ).

¹⁰⁰⁶ Ο.π., άρθρο 14 παράγραφος 5 στοιχείο β).

¹⁰⁰⁷ Ομάδα εργασίας του άρθρου 29, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 Οκτωβρίου 2017, σ. 14.

¹⁰⁰⁸ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 19.

Οι υπεύθυνοι επεξεργασίας μπορούν επίσης να επικαλούνται ειδικές παρεκκλίσεις όσον αφορά τα εν λόγω δικαιώματα κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς¹⁰⁰⁹.

Όσον αφορά **την κατάρτιση προφίλ και την αυτοματοποιημένη λήψη αποφάσεων**, ο ΓΚΠΔ έχει θεσπίσει ειδικούς κανόνες: το άρθρο 22 παράγραφος 1 ορίζει ότι το υποκείμενο των δεδομένων «έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, η οποία παράγει έννομα αποτελέσματα που το αφορούν». Όπως υπογραμμίζεται στις Κατευθυντήριες γραμμές της Ομάδας εργασίας του άρθρου 29, το συγκεκριμένο άρθρο προβλέπει γενική απαγόρευση της πλήρως αυτοματοποιημένης λήψης αποφάσεων¹⁰¹⁰. Οι υπεύθυνοι επεξεργασίας δεδομένων δύνανται να απαλλάσσονται από την εν λόγω απαγόρευση μόνο σε τρεις συγκεκριμένες περιπτώσεις: όταν η απόφαση: 1) είναι αναγκαία για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, 2) επιτρέπεται από το δίκαιο της ΕΕ ή το δίκαιο κράτους μέλους ή 3) βασίζεται σε ρητή συγκατάθεση¹⁰¹¹.

Έλεγχος εκ μέρους των ατόμων

Λόγω της πολυπλοκότητας της ανάλυσης μαζικών δεδομένων, καθώς και της έλλειψης διαφάνειας γύρω από αυτή, είναι πιθανό να απαιτείται η επανεξέταση του σκεπτικού που διέπει τον έλεγχο των ατόμων επί των δεδομένων προσωπικού χαρακτήρα. Ο έλεγχος αυτός θα πρέπει να προσαρμόζεται κατάλληλα στο δεδομένο κοινωνικό και τεχνολογικό πλαίσιο, λαμβανομένης υπόψη της έλλειψης γνώσεων από την πλευρά των ατόμων. Ως εκ τούτου, η προστασία των δεδομένων σε σχέση με τα μαζικά δεδομένα θα πρέπει να διέπεται από ένα ευρύτερο σκεπτικό ελέγχου επί της χρήσης των δεδομένων, σύμφωνα με το οποίο ο έλεγχος εκ μέρους των ατόμων εξελίσσεται σε μια πιο πολύπλοκη διαδικασία πολλών εκτιμήσεων των επιπτώσεων των κινδύνων που συνδέονται με τη χρήση των δεδομένων¹⁰¹².

¹⁰⁰⁹ Ο.π., άρθρο 89 παράγραφοι 2 και 3.

¹⁰¹⁰ Ομάδα εργασίας του άρθρου 29, *Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 Οκτωβρίου 2017, σ. 9.

¹⁰¹¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 22 παράγραφος 2.

¹⁰¹² Συμβούλιο της Ευρώπης, Συμβουλευτική Επιτροπή της Σύμβασης 108, *Κατευθυντήριες Γραμμές για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σε έναν κόσμο μαζικών δεδομένων*, T-PD(2017)01, Στρασβούργο, 23 Ιανουαρίου 2017.

Το πόσο ικανοποιητική είναι η εφαρμογή μαζικών δεδομένων εξαρτάται από τον βαθμό στον οποίο μπορεί να προβλέψει τις επιθυμίες ή τη συμπεριφορά των ατόμων (ή των καταναλωτών) που υποβάλλονται σε δοκιμή. Τα υφιστάμενα προγνωστικά μοντέλα που βασίζονται στην ανάλυση μαζικών δεδομένων βελτιστοποιούνται σε διαρκή βάση. Στις πρόσφατες εξελίξεις δεν περιλαμβάνεται μόνο η χρήση δεδομένων για την κατηγοριοποίηση των προσωπικοτήτων (δηλαδή της συμπεριφοράς και των αντιλήψεων), αλλά και η ανάλυση της συμπεριφοράς μέσω της ανάλυσης τάσεων της φωνής και της έντασης με την οποία πληκτρολογούνται τα μηνύματα ή της θερμοκρασίας του σώματος. Όλες αυτές οι πληροφορίες μπορούν να χρησιμοποιούνται σε πραγματικό χρόνο βάσει των γνώσεων που αντλούνται από τις αξιολογήσεις μαζικών δεδομένων, επί παραδείγματι, για την αξιολόγηση της πιστοληπτικής ικανότητας κατά τη διάρκεια μιας συνάντησης με εκπρόσωπο τραπεζικού ιδρύματος. Η εν λόγω αξιολόγηση δεν διενεργείται με βάση τις δυνατότητες του ατόμου που υποβάλλει την αίτηση χορήγησης πίστωσης, αλλά, απεναντίας, με βάση τα συμπεριφορικά χαρακτηριστικά που αντλούνται από την ανάλυση και την αξιολόγηση των πληροφοριών μαζικών δεδομένων, δηλαδή εξετάζοντας κατά πόσον ο υποψήφιος μιλά με δυνατή ή κολακευτική φωνή, τη γλώσσα του σώματος που χρησιμοποιεί ή τη θερμοκρασία του σώματός του.

Η κατάρτιση προφίλ και η στοχευμένη διαφήμιση πιθανόν να μην συνιστά απαραίτητα πρόβλημα εάν τα άτομα **γνωρίζουν** ότι είναι αποδέκτες εξατομικευμένων διαφημίσεων. Η κατάρτιση προφίλ μετατρέπεται σε πρόβλημα όταν χρησιμοποιείται για τη χειραγώγηση των ατόμων, δηλαδή με σκοπό την αναζήτηση ορισμένων προσωπικοτήτων ή ομάδων ανθρώπων για σκοπούς πολιτικών εκστρατειών. Για παράδειγμα, είναι πιθανή η προσέγγιση ομάδων αναποφάσιστων ψηφοφόρων μέσω πολιτικών μηνυμάτων τα οποία είναι κατάλληλα προσαρμοσμένα στην «προσωπικότητα» και στις αντιλήψεις τους. Άλλο πρόβλημα θα μπορούσε να αποτελεί η χρήση της εν λόγω κατάρτισης προφίλ για την άρνηση της πρόσβασης ορισμένων ατόμων σε αγαθά και υπηρεσίες. Η ψευδωνυμοποίηση αποτελεί μία από τις εγγυήσεις που μπορούν να παρέχουν προστασία έναντι της κατάχρησης μαζικών δεδομένων και προσωπικών πληροφοριών (βλ. [ενότητα 2.1.1](#))¹⁰¹³. Εάν τα δεδομένα προσωπικού χαρακτήρα έχουν πράγματι ανωνυμοποιηθεί, δηλαδή δεν υπάρχουν πληροφορίες που να αφήνουν ίχνη τα οποία τα συνδέουν με το υποκείμενο των δεδομένων, οι περιπτώσεις αυτές δεν εμπίπτουν στο πεδίο εφαρμογής του Γενικού Κανονισμού για την Προστασία Δεδομένων. Η συγκατάθεση των υποκειμένων των δεδομένων και των φυσικών

1013 Ό.π., σ. 2.

προσώπων στο πλαίσιο της επεξεργασίας μαζικών δεδομένων συνιστά επίσης πρόκληση για τη νομοθεσία σχετικά με την προστασία των δεδομένων. Συμπεριλαμβάνεται η συγκατάθεση των υποκειμένων με σκοπό να γίνουν αποδέκτες εξατομικευμένης διαφήμισης και κατάρτισης προφίλ, η οποία μπορεί να δικαιολογείται για τους σκοπούς της «εμπειρίας του πελάτη», καθώς και η συγκατάθεσή τους για τη χρήση όγκων δεδομένων προσωπικού χαρακτήρα με σκοπό τη βελτιστοποίηση και την ανάπτυξη εργαλείων ανάλυσης που βασίζονται στις πληροφορίες. Η επίγνωση, ή η απουσία επίγνωσης, της επεξεργασίας μαζικών δεδομένων εγείρει διάφορα ερωτήματα όσον αφορά τα μέσα με τα οποία τα υποκείμενα των δεδομένων μπορούν να ασκούν τα δικαιώματά τους, λαμβανομένου υπόψη ότι η επεξεργασία μαζικών δεδομένων μπορεί να βασίζεται τόσο σε ψευδωνυμοποιημένες όσο και σε ανωνυμοποιημένες πληροφορίες που υποκινούνται σε αλγόριθμους. Μολονότι τα ψευδωνυμοποιημένα δεδομένα εμπίπτουν στις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων, ο κανονισμός δεν ισχύει για τα ανωνυμοποιημένα δεδομένα. Ο έλεγχος των ατόμων επί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, καθώς και η επίγνωση της εν λόγω επεξεργασίας, είναι καίριας σημασίας στο πλαίσιο της ανάλυσης μαζικών δεδομένων: χωρίς τον έλεγχο αυτόν, δεν θα έχουν σαφή εικόνα του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, γεγονός που δεν θα τους επιτρέπει να ασκούν τα δικαιώματά τους με αποτελεσματικό τρόπο.

10.2. Οι Ιστοί 2.0 και 3.0: κοινωνικά δίκτυα και διαδίκτυο των πραγμάτων

Κύρια σημεία

- Οι υπηρεσίες κοινωνικής δικτύωσης είναι διαδικτυακές πλατφόρμες επικοινωνίας, οι οποίες επιτρέπουν στα άτομα να προσχωρούν –ή να δημιουργούν– δίκτυα χρηστών με παρόμοιες ιδέες.
- Το διαδίκτυο των πραγμάτων είναι η σύνδεση αντικειμένων στο διαδίκτυο, καθώς και η διασύνδεση αντικειμένων μεταξύ τους.
- Η συγκατάθεση των υποκειμένων των δεδομένων αποτελεί τη συνηθέστερη νομική βάση για τη νόμιμη επεξεργασία δεδομένων από τους υπευθύνους επεξεργασίας στα κοινωνικά δίκτυα.

- Κατά γενικό κανόνα, οι χρήστες κοινωνικών δικτύων προστατεύονται από την «εξαίρεση λόγω οικιακής δραστηριότητας»· ωστόσο, παρέχεται η δυνατότητα άρσης της παρέκκλισης αυτής σε συγκεκριμένα πλαίσια.
- Οι πάροχοι κοινωνικών δικτύων δεν προστατεύονται από την «εξαίρεση λόγω οικιακής δραστηριότητας».
- Η προστασία της ιδιωτικής ζωής ήδη από τον σχεδιασμό και εξ ορισμού είναι καίριας σημασίας για τη διαφύλαξη της ασφάλειας των δεδομένων στον συγκεκριμένο τομέα.

10.2.1. Ορισμός των Ιστών 2.0 και 3.0

Υπηρεσίες κοινωνικής δικτύωσης

Αρχικά, το διαδίκτυο είχε σχεδιαστεί ως δίκτυο για τη διασύνδεση ηλεκτρονικών υπολογιστών και για τη διαβίβαση μηνυμάτων με περιορισμένες δυνατότητες ανταλλαγής δεδομένων, με τη χρήση ιστότοπων οι οποίοι παρείχαν στα άτομα απλώς και μόνο τη δυνατότητα παθητικής προβολής του περιεχομένου τους ¹⁰¹⁴. Στην εποχή του Ιστού 2.0, το διαδίκτυο έχει μετασχηματιστεί σε ένα φόρουμ στο οποίο οι χρήστες αλληλεπιδρούν, συνεργάζονται και παράγουν πληροφοριακά στοιχεία. Η σημερινή εποχή χαρακτηρίζεται από την εντυπωσιακή επιτυχία και την ευρέως διαδεδομένη χρήση των υπηρεσιών κοινωνικής δικτύωσης, οι οποίες αποτελούν πλέον σημαντικό μέρος της καθημερινότητας εκατομμυρίων ανθρώπων.

Οι υπηρεσίες κοινωνικής δικτύωσης μπορούν σε γενικές γραμμές να οριστούν ως «διαδικτυακές πλατφόρμες επικοινωνίας, οι οποίες επιτρέπουν στα άτομα να προσχωρούν –ή να δημιουργούν– δίκτυα χρηστών με παρόμοιες ιδέες» ¹⁰¹⁵. Για να προσχωρήσουν –ή να δημιουργήσουν– δίκτυο, τα άτομα καλούνται να υποβάλουν δεδομένα προσωπικού χαρακτήρα και να δημιουργήσουν το προφίλ τους. Οι υπηρεσίες κοινωνικής δικτύωσης παρέχουν στους χρήστες τη δυνατότητα να παράγουν ψηφιακό «περιεχόμενο», το οποίο περιλαμβάνει από φωτογραφίες και βίντεο μέχρι συνδέσμους προς εφημερίδες και προσωπικές δημοσιεύσεις για την έκφραση των απόψεών τους. Μέσω αυτών των διαδικτυακών πλατφορμών επικοινωνίας, οι χρήστες μπορούν να αλληλεπιδρούν και να επικοινωνούν με πολλούς άλλους χρήστες. Σημαντικό είναι το γεγονός ότι, στην πλειονότητα

¹⁰¹⁴ Ευρωπαϊκή Επιτροπή (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

¹⁰¹⁵ Ομάδα εργασίας του άρθρου 29 (2009), *Γνώμη 5/2009 σχετικά με τις επιγραμμικές υπηρεσίες κοινωνικής δικτύωσης*, WP 163, 12 Ιουνίου 2009, σ. 4.

τους, οι δημοφιλείς υπηρεσίες κοινωνικής δικτύωσης δεν απαιτούν την καταβολή τελών εγγραφής. Αντί να επιβάλλουν στους χρήστες την καταβολή τέλους για την προσχώρησή τους στο δίκτυο, οι πάροχοι υπηρεσιών κοινωνικής δικτύωσης παράγουν το μεγαλύτερο μέρος των εσόδων τους από τη στοχευμένη διαφήμιση. Οι διαφημιστές μπορούν να επωφελούνται σε πολύ μεγάλο βαθμό από τις προσωπικές πληροφορίες που αποκαλύπτονται καθημερινά στους εν λόγω ιστότοπους. Το γεγονός ότι έχουν στη διάθεσή τους πληροφορίες σχετικά με την ηλικία, το φύλο, την τοποθεσία και τα ενδιαφέροντα ενός χρήστη, τους παρέχει τη δυνατότητα να απευθύνουν τις διαφημίσεις τους στους «κατάλληλους» ανθρώπους.

Η Επιτροπή Υπουργών του Συμβουλίου της Ευρώπης υιοθέτησε σύσταση σχετικά με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά τις υπηρεσίες κοινωνικής δικτύωσης ¹⁰¹⁶, ένα συγκεκριμένο τμήμα της οποίας αφορά στην προστασία των δεδομένων και η οποία συμπληρώθηκε το 2018 από άλλη σύσταση σχετικά με τους ρόλους και τις ευθύνες των διαμεσολαβητών διαδικτύου ¹⁰¹⁷.

Παράδειγμα: Η Nora είναι πολύ χαρούμενη επειδή δέχτηκε πρόταση γάμου από τον σύντροφό της. Θέλει να μοιραστεί τα ευχάριστα νέα με τους φίλους της και την οικογένειά της και αποφασίζει να αναρτήσει μια συγκινητική δημοσίευση σε ένα κοινωνικό δίκτυο για να εκφράσει τη χαρά της και να αλλάξει την κατάσταση της σχέσης της σε «αρραβωνιασμένη». Τις επόμενες ημέρες, όταν συνδέεται στον λογαριασμό της, η Nora βλέπει διαφημίσεις σχετικά με νυφικά και ανθοπωλεία. Για ποιον λόγο συμβαίνει αυτό;

Κατά τη δημιουργία διαφήμισης στο Facebook, οι εταιρείες νυφικών και τα ανθοπωλεία επέλεξαν ορισμένες παραμέτρους ώστε να είναι σε θέση να απευθύνονται σε άτομα όπως η Nora. Όταν το προφίλ της Nora φέρει ένδειξη ότι είναι γυναίκα, αρραβωνιασμένη, η οποία κατοικεί στο Παρίσι, κοντά στην περιοχή στην οποία βρίσκονται οι εταιρείες νυφικών και τα ανθοπωλεία που έχουν αναρτήσει τις διαφημίσεις, η Nora βλέπει αμέσως τις διαφημίσεις.

¹⁰¹⁶ Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών, Σύσταση Rec (2012) 4 προς τα κράτη μέλη σχετικά με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά τις υπηρεσίες κοινωνικής δικτύωσης, 4 Απριλίου 2012.

¹⁰¹⁷ Συμβούλιο της Ευρώπης, Επιτροπή Υπουργών, Σύσταση Rec (2018) 2 προς τα κράτη μέλη σχετικά με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά τις υπηρεσίες κοινωνικής δικτύωσης, 7 Μαρτίου 2018.

Το διαδίκτυο των πραγμάτων

Το διαδίκτυο των πραγμάτων αποτελεί το επόμενο βήμα στην εξέλιξη του διαδικτύου: την εποχή του Ιστού 3.0. Με το διαδίκτυο των πραγμάτων, οι συσκευές μπορούν να συνδέονται και να αλληλεπιδρούν με άλλες συσκευές μέσω του διαδικτύου. Αυτό παρέχει τη δυνατότητα διασύνδεσης μεταξύ αντικειμένων και ανθρώπων μέσω δικτύων επικοινωνίας, ώστε να είναι δυνατή η αναφορά της κατάστασής τους και/ή της κατάστασης του περιβάλλοντος χώρου ¹⁰¹⁸. Το διαδίκτυο των πραγμάτων και οι συνδεδεμένες συσκευές αποτελούν ήδη πραγματικότητα και αναμένεται να αναπτυχθούν σημαντικά κατά τα προσεχή έτη, με τη δημιουργία και περαιτέρω εξέλιξη των έξυπνων συσκευών που θα οδηγήσουν στη δημιουργία έξυπνων πόλεων, έξυπνων κατοικιών και έξυπνων επιχειρήσεων.

Παράδειγμα: Το διαδίκτυο των πραγμάτων μπορεί να αποδειχθεί ιδιαίτερα ωφέλιμο για τον τομέα της υγειονομικής περίθαλψης. Διάφορες εταιρείες έχουν δημιουργήσει ήδη συσκευές, αισθητήρες και εφαρμογές που επιτρέπουν την παρακολούθηση της υγείας του ασθενούς. Μέσω της χρήσης φορετού κομβίου σήματος κινδύνου και της τοποθέτησης άλλων ασύρματων αισθητήρων σε ολόκληρο το σπίτι, καθίσταται δυνατή η παρακολούθηση των καθημερινών εργασιών των ηλικιωμένων που ζουν μόνοι τους και η εκπομπή σημάτων κινδύνου σε περίπτωση ανίχνευσης σοβαρών διαταραχών του καθημερινού τους προγράμματος. Οι αισθητήρες ανίχνευσης πτώσης, για παράδειγμα, χρησιμοποιούνται ευρύτατα από ηλικιωμένους. Οι αισθητήρες αυτοί μπορούν να ανιχνεύουν πτώσεις με ακρίβεια και να ειδοποιούν τον γιατρό και/ή την οικογένεια του ατόμου για την πτώση του.

Παράδειγμα: Η Βαρκελώνη αποτελεί ένα από τα πλέον γνωστά παραδείγματα έξυπνης πόλης. Από το 2012 η πόλη εφαρμόζει τη χρήση καινοτόμων τεχνολογιών, με σκοπό τη δημιουργία ενός έξυπνου συστήματος δημόσιων συγκοινωνιών, διαχείρισης των αποβλήτων, στάθμευσης και οδοφωτισμού. Για τη βελτίωση της διαχείρισης των αποβλήτων, λόγου χάρη, η πόλη χρησιμοποιεί έξυπνους κάδους απορριμμάτων. Οι κάδοι αυτοί παρέχουν τη δυνατότητα παρακολούθησης της στάθμης των αποβλήτων για τη βελτιστοποίηση των δρομολογίων

¹⁰¹⁸ Ευρωπαϊκή Επιτροπή, Έγγραφο εργασίας των υπηρεσιών της Επιτροπής, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19 Απριλίου 2016.

αποκομιδής. Όταν οι κάδοι είναι σχεδόν πλήρεις, εκπέμπουν σήματα μέσω του δικτύου κινητών επικοινωνιών, τα οποία αποστέλλονται στην εφαρμογή λογισμικού την οποία χρησιμοποιεί η εταιρεία διαχείρισης των αποβλήτων. Με τον τρόπο αυτόν, η εταιρεία μπορεί να σχεδιάζει τη βέλτιστη διαδρομή για την αποκομιδή των απορριμμάτων, δίνοντας προτεραιότητα και/ή οργανώνοντας την αποκομιδή των απορριμμάτων μόνον από τους κάδους που πράγματι πρέπει να αδειάσουν.

10.2.2. Στάθμιση των οφελών και των κινδύνων

Η τεράστια εξάπλωση και επιτυχία των υπηρεσιών κοινωνικής δικτύωσης κατά την τελευταία δεκαετία υποδηλώνει ότι οι υπηρεσίες αυτές αποφέρουν **σημαντικά οφέλη**. Για παράδειγμα, η στοχευμένη διαφήμιση (όπως περιγράφεται στο επιλεγμένο χαρακτηριστικό παράδειγμα) αποτελεί ιδιαίτερος καινοτόμο τρόπο με τον οποίο οι εταιρείες μπορούν να προσεγγίσουν το κοινό, προσφέροντάς του μια πιο εξειδικευμένη αγορά. Μπορεί επίσης να είναι προς το συμφέρον των καταναλωτών να γίνονται αποδέκτες διαφημίσεων οι οποίες είναι περισσότερο χρήσιμες και ενδιαφέρουσες για αυτούς. Το σημαντικότερο, ωστόσο, είναι ότι οι υπηρεσίες κοινωνικής δικτύωσης και τα μέσα κοινωνικής δικτύωσης μπορούν να έχουν θετικό αντίκτυπο στην κοινωνία και στην υλοποίηση αλλαγών. Παρέχουν στους χρήστες τη δυνατότητα να επικοινωνούν, να αλληλεπιδρούν, να συγκροτούν ομάδες και να διοργανώνουν εκδηλώσεις σχετικά με ζητήματα που τους επηρεάζουν.

Ομοίως, το διαδίκτυο των πραγμάτων αναμένεται να αποφέρει σημαντικά οφέλη στην οικονομία και εντάσσεται στο πλαίσιο της στρατηγικής της ΕΕ για την ανάπτυξη ψηφιακής ενιαίας αγοράς. Στο εσωτερικό της ΕΕ, εκτιμάται ότι το 2020 ο αριθμός των συνδέσεων του διαδικτύου των πραγμάτων θα αυξηθεί σε έξι δισεκατομμύρια συνδέσεις. Εκτιμάται ότι αυτή η επέκταση της συνδεσιμότητας θα αποφέρει σημαντικά οικονομικά οφέλη μέσω της ανάπτυξης καινοτόμων υπηρεσιών και εφαρμογών, της βελτίωσης της υγειονομικής περίθαλψης, της καλύτερης κατανόησης των αναγκών των καταναλωτών και της αύξησης της αποδοτικότητας.

Από την άλλη πλευρά, δεδομένου του τεράστιου όγκου προσωπικών πληροφοριών που παράγονται από τους χρήστες των μέσων κοινωνικής δικτύωσης και υποβάλλονται κατόπιν σε επεξεργασία από τους φορείς εκμετάλλευσης των υπηρεσιών, η επέκταση των υπηρεσιών κοινωνικής δικτύωσης συνοδεύεται από **εντεινόμενη ανησυχία** ως προς τους τρόπους με τους οποίους μπορεί

να διασφαλιστεί η προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα. Οι υπηρεσίες κοινωνικής δικτύωσης είναι πιθανό να συνιστούν απειλή για το δικαίωμα στην ιδιωτική ζωή και το δικαίωμα στην ελευθερία της έκφρασης. Η απειλή αυτή μπορεί να περιλαμβάνει τα εξής: «απουσία νομικών και διαδικαστικών εγγυήσεων για την πλαισίωση των διαδικασιών που μπορούν να οδηγήσουν στον αποκλεισμό χρηστών· ανεπαρκές επίπεδο προστασίας για τα παιδιά και τους νέους έναντι επιβλαβούς περιεχομένου ή συμπεριφοράς· έλλειψη σεβασμού για τα δικαιώματα τρίτων· απουσία προεπιλεγμένων ρυθμίσεων που ευνοούν την προστασία της ιδιωτικής ζωής· έλλειψη διαφάνειας όσον αφορά τους σκοπούς για τους οποίους συλλέγονται και υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα»¹⁰¹⁹. Στο πλαίσιο του ευρωπαϊκού δικαίου για την προστασία των δεδομένων έχουν καταβληθεί προσπάθειες για την αντιμετώπιση των προκλήσεων όσον αφορά την προστασία της ιδιωτικής ζωής/των δεδομένων, οι οποίες προκλήσεις προκύπτουν από τη χρήση των μέσων κοινωνικής δικτύωσης. Αρχές όπως η συγκατάθεση και η προστασία της ιδιωτικής ζωής/των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού, καθώς και τα δικαιώματα των φυσικών προσώπων, είναι υψίστης σημασίας στο πλαίσιο των μέσων και των υπηρεσιών κοινωνικής δικτύωσης.

Στο πλαίσιο του διαδικτύου των πραγμάτων, ο τεράστιος όγκος δεδομένων προσωπικού χαρακτήρα που παράγονται από τις διάφορες διασυνδεδεμένες συσκευές συνεπάγεται επίσης κινδύνους για την προστασία της ιδιωτικής ζωής και των δεδομένων. Παρότι η διαφάνεια αποτελεί σημαντική αρχή του ευρωπαϊκού δικαίου για την προστασία των δεδομένων, λόγω της πληθώρας συνδεδεμένων συσκευών, δεν είναι πάντοτε σαφές ποιος είναι σε θέση να συγκεντρώνει τα δεδομένα που συλλέγονται από τις συσκευές του διαδικτύου των πραγμάτων, να έχει πρόσβαση σε αυτά και να τα χρησιμοποιεί¹⁰²⁰. Δυνάμει, ωστόσο, του δικαίου της ΕΕ και του Συμβουλίου της Ευρώπης, η αρχή της διαφάνειας θεσπίζει την υποχρέωση των υπευθύνων επεξεργασίας να τηρούν ενήμερα τα υποκείμενα των δεδομένων για τον τρόπο χρήσης των δεδομένων τους, χρησιμοποιώντας σαφή και απλή γλώσσα. Οι κίνδυνοι, οι κανόνες, οι εγγυήσεις και τα δικαιώματα στο πλαίσιο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα των υποκειμένων των δεδομένων πρέπει να αποσαφηνίζονται στα ενδιαφερόμενα πρόσωπα. Οι συνδεδεμένες συσκευές του διαδικτύου των πραγμάτων, καθώς και οι πολλαπλές πράξεις επεξεργασίας και τα σχετικά δεδομένα, θα μπορούσαν

1019 Συμβούλιο της Ευρώπης, Σύσταση Rec (2012) 4 προς τα κράτη μέλη σχετικά με την προστασία των ανθρωπίνων δικαιωμάτων όσον αφορά τις υπηρεσίες κοινωνικής δικτύωσης, 4 Απριλίου 2012.

1020 Ευρωπαϊός Επόπτης Προστασίας Δεδομένων (2017), *Understanding the Internet of Things*.

επίσης να συνιστούν πρόκληση όσον αφορά την απαίτηση σαφούς και εν πλήρει επιγνώσει συγκατάθεσης, σε περίπτωση που η επεξεργασία αυτού του είδους βασίζεται στη συγκατάθεση. Τα άτομα συχνά δεν κατανοούν την τεχνική λειτουργία της εν λόγω επεξεργασίας και, κατ' επέκταση, ούτε τις επιπτώσεις της συγκατάθεσής τους.

Ένα άλλο θέμα μεζονος ανησυχίας αποτελεί η ασφάλεια, δεδομένου ότι οι συνδεδεμένες συσκευές είναι ιδιαίτερα ευάλωτες σε κινδύνους ασφαλείας. Οι συνδεδεμένες συσκευές παρουσιάζουν διάφορα επίπεδα ασφαλείας. Λαμβανομένου υπόψη ότι η λειτουργία τους βαίνει πέραν των ορίων της τυποποιημένης υποδομής ΤΠ, ενδέχεται να μην διαθέτουν τη δέουσα υπολογιστική ισχύ και δυνατότητα αποθήκευσης ώστε να μπορούν να υποστηρίξουν τη χρήση λογισμικού ασφαλείας ή την εφαρμογή τεχνικών όπως η κρυπτογράφηση, η ψευδωνυμοποίηση ή η ανωνυμοποίηση για την προστασία των προσωπικών πληροφοριών των χρηστών.

Παράδειγμα: Στη Γερμανία, οι ρυθμιστικές αρχές αποφάσισαν να απαγορεύσουν ένα παιχνίδι το οποίο συνδέεται στο διαδίκτυο μετά τη διατύπωση έντονων ανησυχιών ως προς τον αντίκτυπο του εν λόγω παιχνιδιού στον σεβασμό της ιδιωτικής ζωής των παιδιών. Οι ρυθμιστικές αρχές έκριναν ότι μια κούκλα που συνδεόταν με το διαδίκτυο και ονομαζόταν Cayla αποτελούσε πράγματι κρυφή συσκευή παρακολούθησης. Η κούκλα λειτουργούσε με την αποστολή των ηχητικών ερωτήσεων που έθετε το παιδί στην κούκλα σε μια εφαρμογή ψηφιακής συσκευής, η οποία τις απομαγνητοφωνούσε και εκτελούσε αναζήτηση στο διαδίκτυο για τις αντίστοιχες απαντήσεις. Στη συνέχεια, η εφαρμογή διαβίβαζε την απάντηση στην κούκλα, η οποία την μετέτρεπε σε ηχητικό μήνυμα προς το παιδί. Μέσω της κούκλας αυτής, οι επικοινωνίες του παιδιού, καθώς και των ενηλίκων στον περιβάλλοντα χώρο, μπορούσαν να καταγράφονται και να διαβιβάζονται στην εφαρμογή. Εάν οι κατασκευαστές της κούκλας δεν λάμβαναν κατάλληλα μέτρα ασφαλείας, η κούκλα θα μπορούσε να χρησιμοποιηθεί από οποιονδήποτε για την υποκλοπή των συνομιλιών.

10.2.3. Ζητήματα προστασίας των δεδομένων

Συγκατάθεση

Στην Ευρώπη, η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι νόμιμη μόνον εάν επιτρέπεται βάσει του ευρωπαϊκού δικαίου για την προστασία των δεδομένων. Όσον αφορά τους παρόχους υπηρεσιών κοινωνικής δικτύωσης, η συγκατάθεση των υποκειμένων των δεδομένων παρέχει κατά γενικό κανόνα νόμιμη βάση για την επεξεργασία των δεδομένων. Η συγκατάθεση πρέπει να δίνεται ελεύθερα και να είναι συγκεκριμένη, εν πλήρει επιγνώσει και αδιαμφισβήτητη (βλ. [ενότητα 4.1.1](#))¹⁰²¹. «Δίνεται ελεύθερα» σημαίνει κατ' ουσίαν ότι τα υποκείμενα των δεδομένων πρέπει να έχουν τη δυνατότητα πραγματικής και ουσιαστικής επιλογής. Η συγκατάθεση είναι «συγκεκριμένη» και «εν πλήρει επιγνώσει» όταν είναι κατανοητή και αναφέρεται με σαφήνεια και ακρίβεια στην πλήρη έκταση, στους σκοπούς και στις επιπτώσεις της επεξεργασίας των δεδομένων. Στο πλαίσιο των μέσων κοινωνικής δικτύωσης, το κατά πόσον η συγκατάθεση δίνεται ελεύθερα, είναι συγκεκριμένη και εν πλήρει επιγνώσει για όλα τα είδη επεξεργασίας που διενεργούνται από τον φορέα εκμετάλλευσης των υπηρεσιών κοινωνικής δικτύωσης, καθώς και από τρίτους, μπορεί να τεθεί υπό αμφισβήτηση.

Παράδειγμα: Για να προσχωρήσουν και να έχουν πρόσβαση σε υπηρεσίες κοινωνικής δικτύωσης, τα άτομα πρέπει συνήθως να συμφωνούν ότι αποδέχονται διάφορα είδη επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν, συχνά δε χωρίς να τους παρέχονται οι απαιτούμενες διευκρινίσεις ή εναλλακτικές επιλογές. Παράδειγμα εν προκειμένω θα μπορούσε να αποτελεί η περίπτωση στην οποία, προκειμένου να εγγραφεί κανείς σε υπηρεσία κοινωνικής δικτύωσης, ζητείται η συγκατάθεσή του για να γίνει αποδέκτης συμπεριφορικής διαφήμισης. Όπως επισημαίνει η Ομάδα εργασίας του άρθρου 29 στη γνώμη της σχετικά με τον ορισμό της συγκατάθεσης, «με δεδομένη τη σημασία που έχουν αποκτήσει ορισμένα κοινωνικά δίκτυα, ορισμένες κατηγορίες χρηστών (όπως οι έφηβοι) θα αποδεχθούν την παραλαβή συμπεριφορικής διαφήμισης προκειμένου να αποφύγουν τον κίνδυνο εν μέρει αποκλεισμού τους από τις κοινωνικές διαδράσεις. Ο χρήστης θα

¹⁰²¹ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρα 4 και 7· Εκσυγχρονισμένη Σύμβαση 108, άρθρο 5.

πρέπει να είναι σε θέση να δώσει ελεύθερη και ρητή συγκατάθεση για την παραλαβή συμπεριφορικής διαφήμισης, ανεξάρτητα από την πρόσβασή του στην υπηρεσία κοινωνικής δικτύωσης»¹⁰²².

Δυνάμει του Γενικού Κανονισμού για την Προστασία Δεδομένων, τα δεδομένα προσωπικού χαρακτήρα παιδιών ηλικίας κάτω των 16 ετών δεν μπορούν, καταρχήν, να υποβάλλονται σε επεξεργασία με βάση τη συγκατάθεσή τους¹⁰²³. Εάν απαιτείται συγκατάθεση για την επεξεργασία, αυτή πρέπει να παρέχεται από τον γονέα ή τον κηδεμόνα του παιδιού. Τα παιδιά χρήζουν ειδικής προστασίας λόγω του γεγονότος ότι ενδέχεται να έχουν μικρότερο βαθμό επίγνωσης των κινδύνων και των επιπτώσεων που ενέχει η επεξεργασία δεδομένων. Το στοιχείο αυτό είναι ιδιαίτερης σημασίας στο πλαίσιο των μέσων κοινωνικής δικτύωσης, διότι τα παιδιά είναι περισσότερο ευάλωτα σε ορισμένες από τις αρνητικές επιπτώσεις τις οποίες μπορεί να συνεπάγεται η χρήση των εν λόγω μέσων, όπως ο κυβερνοεκφοβισμός, η επίμονη παρακολούθηση μέσω διαδικτύου ή η υποκλοπή ταυτότητας.

Ασφάλεια και προστασία της ιδιωτικής ζωής / των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα είναι άρρηκτα συνδεδεμένη με κινδύνους κατά της ασφάλειας, λόγω της μόνιμης πιθανότητας παραβίασης της ασφάλειας που συνεπάγεται την εκ παραδρομής ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη πρόσβαση ή κοινολόγηση των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Βάσει του ευρωπαϊκού δικαίου για την προστασία των δεδομένων, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία υποχρεούνται να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποφυγή μη εξουσιοδοτημένης παρέμβασης στις πράξεις επεξεργασίας δεδομένων. Οι πάροχοι υπηρεσιών κοινωνικής δικτύωσης οι οποίοι εμπίπτουν στο πεδίο εφαρμογής των ευρωπαϊκών κανόνων προστασίας των δεδομένων πρέπει επίσης να τηρούν και αυτή την υποχρέωση.

¹⁰²² Ομάδα εργασίας του άρθρου 29 (2011), *Γνώμη 15/2011 σχετικά με τον ορισμό της συγκατάθεσης*, WP 187, 13 Ιουλίου 2011, σ. 18.

¹⁰²³ Βλ. Γενικό Κανονισμό για την Προστασία Δεδομένων, άρθρο 8. Τα κράτη μέλη δύνανται να προβλέπουν διά νόμου μικρότερη ηλικία, υπό την προϋπόθεση ότι η εν λόγω μικρότερη ηλικία δεν είναι κάτω από τα 13 έτη.

Οι αρχές προστασίας της ιδιωτικής ζωής/των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού επιβάλλουν στους υπευθύνους επεξεργασίας την υποχρέωση να διατηρούν την ασφάλεια κατά τον σχεδιασμό των προϊόντων τους και να εφαρμόζουν αυτομάτως κατάλληλες ρυθμίσεις για την προστασία της ιδιωτικής ζωής και των δεδομένων. Αυτό σημαίνει ότι όταν ένα πρόσωπο αποφασίζει να προσχωρήσει σε κάποιο κοινωνικό δίκτυο, ο πάροχος της υπηρεσίας μπορεί να μην καταστήσει αυτομάτως διαθέσιμες στον νέο χρήστη της υπηρεσίας όλες τις πληροφορίες που θέτει στη διάθεση όλων των χρηστών του. Κατά την προσχώρηση στην υπηρεσία, οι προεπιλεγμένες ρυθμίσεις για την προστασία της ιδιωτικής ζωής και των δεδομένων θα πρέπει να είναι τέτοιου είδους ώστε οι πληροφορίες να είναι διαθέσιμες μόνο στις επιλεγμένες επαφές του ατόμου. Η επέκταση της πρόσβασης σε άλλα άτομα πέραν της λίστας αυτής θα πρέπει να επιτρέπεται μόνον αφού ο χρήστης έχει προβεί σε ενέργειες για τη χειροκίνητη αλλαγή των προεπιλεγμένων ρυθμίσεων για την προστασία της ιδιωτικής ζωής και των δεδομένων. Αυτό ενδέχεται να έχει επίσης αντίκτυπο σε περιπτώσεις παραβίασης δεδομένων παρά την εφαρμογή μέτρων ασφαλείας. Στις περιπτώσεις αυτές, οι πάροχοι υπηρεσιών πρέπει να ενημερώνουν τους θιγόμενους χρήστες αν ή εν λόγω παραβίαση είναι πιθανό να συνεπάγεται υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων ¹⁰²⁴.

Η προστασία της ιδιωτικής ζωής/των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού είναι ιδιαίτερης σημασίας στο πλαίσιο των υπηρεσιών κοινωνικής δικτύωσης διότι, πέραν των κινδύνων μη εξουσιοδοτημένης πρόσβασης που ενέχουν τα περισσότερα είδη επεξεργασίας, η κοινοποίηση προσωπικών πληροφοριών στα μέσα κοινωνικής δικτύωσης συνεπάγεται πρόσθετους κινδύνους κατά της ασφάλειας. Οι κίνδυνοι αυτοί οφείλονται συχνά στο γεγονός ότι τα άτομα δεν κατανοούν *ποιοι* μπορούν να έχουν πρόσβαση στις πληροφορίες τους ούτε πώς μπορούν να χρησιμοποιηθούν από αυτούς. Με την ευρέως διαδεδομένη χρήση των μέσων κοινωνικής δικτύωσης, ο αριθμός των κρουσμάτων και των θυμάτων υποκλοπής ταυτότητας έχει αυξηθεί.

Παράδειγμα: Η υποκλοπή ταυτότητας είναι ένα φαινόμενο κατά το οποίο ένα πρόσωπο λαμβάνει πληροφορίες, δεδομένα ή έγγραφα που ανήκουν σε κάποιο άλλο πρόσωπο (το θύμα) και στη συνέχεια χρησιμοποιεί τα στοιχεία αυτά παριστάνοντας ότι είναι το θύμα προκειμένου να αποκτήσει αγαθά και υπηρεσίες στο όνομα του θύματος. Ας εξετάσουμε, για

¹⁰²⁴Ό.π., άρθρο 34.

παράδειγμα, την περίπτωση του Paul, ο οποίος διατηρεί λογαριασμό στον ιστότοπο ενός μέσου κοινωνικής δικτύωσης. Ο Paul είναι εκπαιδευτικός και ενεργό μέλος της κοινότητάς του, ιδιαιτέρως εξωστρεφής και δεν ανησυχεί ιδιαίτερα για τις ρυθμίσεις προστασίας της ιδιωτικής ζωής και των δεδομένων του λογαριασμού του στο συγκεκριμένο μέσο κοινωνικής δικτύωσης. Διαθέτει μακρά λίστα επαφών, η οποία περιλαμβάνει ενίοτε άτομα τα οποία δεν γνωρίζει απαραιτήτως προσωπικά. Δεδομένου ότι εργάζεται σε μεγάλο σχολείο, και έχει γίνει αρκετά δημοφιλής επειδή προπονεί την ποδοσφαιρική ομάδα του σχολείου, θεωρεί ότι τα άτομα αυτά είναι πιθανότατα γονείς ή φίλοι του σχολείου. Η διεύθυνση ηλεκτρονικού ταχυδρομείου του Paul και η ημερομηνία γενεθλίων του εμφανίζονται στον λογαριασμό του στο μέσο κοινωνικής δικτύωσης. Επιπλέον, ο Paul δημοσιεύει φωτογραφίες του σκύλου του Toby, τις οποίες συνοδεύει με λεζάντες, όπως «Εγώ και ο Toby στο πρωινό μας τρέξιμο». Ο Paul δεν έχει συνειδητοποιήσει ότι μία από τις δημοφιλέστερες ερωτήσεις ασφαλείας για την προστασία του λογαριασμού ηλεκτρονικού ταχυδρομείου ή κινητού τηλεφώνου του είναι η ερώτηση «Πώς ονομάζεται το κατοικίδιό σας;». Χρησιμοποιώντας τις διαθέσιμες πληροφορίες στο προφίλ του μέσου κοινωνικής δικτύωσης του Paul, ο Nick επιτυγχάνει με ευκολία τη δικτυοπαράβιαση των λογαριασμών του Paul.

Δικαιώματα των φυσικών προσώπων

Οι πάροχοι υπηρεσιών κοινωνικής δικτύωσης πρέπει να σέβονται τα δικαιώματα των φυσικών προσώπων (βλ. [ενότητα 6.1](#)), συμπεριλαμβανομένου του δικαιώματος πληροφόρησής τους σχετικά με τους σκοπούς της επεξεργασίας και τον τρόπο με τον οποίο τα δεδομένα προσωπικού χαρακτήρα μπορούν να χρησιμοποιηθούν για σκοπούς απευθείας εμπορικής προώθησης. Πρέπει επίσης να παρέχεται στα φυσικά πρόσωπα το δικαίωμα να έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που έχουν δημιουργηθεί στην πλατφόρμα κοινωνικής δικτύωσης και να ζητούν τη διαγραφή τους. Ακόμη και σε περίπτωση που τα πρόσωπα έχουν δώσει τη συγκατάθεσή τους για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και έχουν αναφορτώσει πληροφορίες στο διαδίκτυο, θα πρέπει να είναι σε θέση να ασκούν το δικαίωμα «στη λήθη», εάν δεν επιθυμούν πλέον να λαμβάνουν τις υπηρεσίες του κοινωνικού δικτύου. Το δικαίωμα στη φορητότητα των δεδομένων παρέχει περαιτέρω στους χρήστες τη δυνατότητα να λαμβάνουν αντίγραφο των δεδομένων προσωπικού χαρακτήρα τα οποία παρέχουν στον πάροχο υπηρεσιών κοινωνικής δικτύωσης, σε δομημένο, κοινώς

χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και να διαβιβάζουν τα δεδομένα τους από έναν πάροχο υπηρεσιών κοινωνικής δικτύωσης σε άλλον ¹⁰²⁵.

Υπεύθυνοι επεξεργασίας

Ένα δύσκολο ζήτημα το οποίο ανακύπτει συχνά στο πλαίσιο των μέσων κοινωνικής δικτύωσης αφορά το ερώτημα σχετικά με το ποιος είναι ο υπεύθυνος επεξεργασίας, δηλαδή ποιο είναι το πρόσωπο το οποίο έχει την υποχρέωση και την ευθύνη συμμόρφωσης προς τους κανόνες προστασίας των δεδομένων. Σύμφωνα με το ευρωπαϊκό δίκαιο για την προστασία των δεδομένων, οι πάροχοι υπηρεσιών κοινωνικής δικτύωσης θεωρούνται υπεύθυνοι επεξεργασίας. Αυτό είναι προφανές εάν ληφθεί υπόψη ο ευρύς ορισμός του «υπευθύνου επεξεργασίας» και το γεγονός ότι οι εν λόγω πάροχοι υπηρεσιών καθορίζουν τον σκοπό και τα μέσα για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που κοινοποιούν τα άτομα. Σύμφωνα με το δίκαιο της ΕΕ, εάν προσφέρουν υπηρεσίες σε υποκείμενα των δεδομένων εντός της ΕΕ, οι υπεύθυνοι επεξεργασίας υποχρεούνται να συμμορφώνονται προς τις διατάξεις του Γενικού Κανονισμού για την Προστασία Δεδομένων, ακόμη και αν δεν είναι εγκατεστημένοι στην ΕΕ.

Μπορούν, παρ' όλα αυτά, οι χρήστες υπηρεσιών κοινωνικής δικτύωσης να θεωρούνται επίσης υπεύθυνοι επεξεργασίας; Σε περίπτωση που η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται από φυσικά πρόσωπα «στο πλαίσιο αποκλειστικά προσωπικής ή οικιακής δραστηριότητας», δεν εφαρμόζονται οι κανόνες προστασίας των δεδομένων. Στο πλαίσιο του ευρωπαϊκού δικαίου για την προστασία των δεδομένων, η περίπτωση αυτή είναι γνωστή ως «εξαίρεση λόγω οικιακής δραστηριότητας». Σε ορισμένες περιπτώσεις, ωστόσο, ο χρήστης μιας υπηρεσίας κοινωνικής δικτύωσης μπορεί να μην καλύπτεται από την εξαίρεση λόγω οικιακής δραστηριότητας.

Οι χρήστες κοινοποιούν οικειοθελώς τις προσωπικές πληροφορίες τους στο διαδίκτυο. Ωστόσο, οι πληροφορίες που κοινοποιούνται στο διαδίκτυο περιλαμβάνουν συχνά προσωπικές πληροφορίες άλλων ατόμων.

¹⁰²⁵ Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 21.

Παράδειγμα: Ο Paul διατηρεί λογαριασμό σε μια ιδιαιτέρως δημοφιλή πλατφόρμα κοινωνικής δικτύωσης. Ο Paul προσπαθεί να γίνει ηθοποιός και χρησιμοποιεί τον λογαριασμό του για να δημοσιεύει φωτογραφίες, βίντεο και αναρτήσεις που περιγράφουν το πάθος του για την τέχνη. Η δημοτικότητα είναι σημαντική για το μέλλον του· για τον λόγο αυτόν, αποφάσισε ότι το προφίλ του δεν θα έπρεπε να είναι διαθέσιμο μόνο στη λίστα των στενών επαφών του, αλλά και σε όλους τους χρήστες του διαδικτύου, ανεξάρτητα από το αν είναι μέλη του δικτύου ή όχι. Μπορεί ο Paul να δημοσιεύει φωτογραφίες και βίντεο του ίδιου μαζί με τη φίλη του τη Sarah χωρίς τη συγκατάθεσή της; Ως εκπαιδευτικός πρωτοβάθμιας εκπαίδευσης, η Sarah προσπαθεί να διαφυλάσσει την ιδιωτική της ζωή από τον εργοδότη της, τους μαθητές της και τους γονείς τους. Ας υποθέσουμε ότι η Sarah, η οποία δεν χρησιμοποιεί κοινωνικά δίκτυα, πληροφορείται από τον κοινό τους φίλο Nick ότι έχει αναρτηθεί στο διαδίκτυο μια φωτογραφία της με τον Paul σε ένα πάρτι. Στην προκειμένη περίπτωση, η επεξεργασία των δεδομένων του Paul δεν εμπίπτει στο πεδίο εφαρμογής του δικαίου της ΕΕ, διότι καλύπτεται από την «εξαίρεση λόγω οικιακής δραστηριότητας».

Ωστόσο, εξακολουθεί να είναι καίριας σημασίας για τους χρήστες να γνωρίζουν και να λαμβάνουν υπόψη ότι η αναφόρτωση πληροφοριών σχετικά με τρίτα άτομα χωρίς τη συγκατάθεσή τους ενδέχεται να συνιστά παραβίαση των δικαιωμάτων προστασίας της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα των εν λόγω ατόμων. Ακόμη και στις περιπτώσεις στις οποίες ισχύει η εξαίρεση λόγω οικιακής δραστηριότητας –π.χ. εάν ο χρήστης διατηρεί προφίλ το οποίο δημοσιοποιείται μόνο σε μια λίστα επαφών που επιλέγει ο ίδιος– η δημοσίευση προσωπικών πληροφοριών σχετικά με τρίτους είναι πιθανό να εξακολουθεί να καθιστά υπεύθυνο τον χρήστη. Μολονότι οι κανόνες προστασίας των δεδομένων δεν ισχύουν σε περίπτωση που εφαρμόζεται η εξαίρεση λόγω οικιακής δραστηριότητας, ευθύνη μπορεί να προκύψει λόγω της εφαρμογής άλλων εθνικών κανόνων, όπως η δυσφήμιση ή η προσβολή της προσωπικότητας. Τέλος, μόνον οι χρήστες υπηρεσιών κοινωνικής δικτύωσης προστατεύονται από τις εξαιρέσεις λόγω οικιακής δραστηριότητας: οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία που παρέχουν τα μέσα για την εν λόγω ιδιωτική επεξεργασία εμπίπτουν στο πεδίο εφαρμογής του δικαίου της ΕΕ για την προστασία των δεδομένων¹⁰²⁶.

¹⁰²⁶ Ο.π., αιτιολογική σκέψη 18.

Με τη μεταρρύθμιση της οδηγίας για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, οι κανόνες σχετικά με την προστασία των δεδομένων, την προστασία της ιδιωτικής ζωής και την ασφάλεια που ισχύουν για τους παρόχους υπηρεσιών τηλεπικοινωνιών δυνάμει του υφιστάμενου νομικού πλαισίου θα ίσχυαν επίσης για τις υπηρεσίες επικοινωνιών μεταξύ μηχανών και τις υπηρεσίες ηλεκτρονικών επικοινωνιών, συμπεριλαμβανομένων, για παράδειγμα, των επιφυών υπηρεσιών.



Επιπρόσθετη βιβλιογραφία

Κεφάλαιο 1

Araceli Mangas, M. (επιμ.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Μπιλμπάο, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Βιέννη, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. 'Four fundamental rights: finding the balance', *International Data Privacy Law*, τόμος 6, αριθ. 3, σ. 195-209.

EDRi, *An introduction to data protection*, Βρυξέλλες.

Frowein, J. και Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Βερολίνο, N. P. Engel Verlag.

González Fuster, G. και Gellert, G. (2012), 'The fundamental right of data protection in the European Union: in search of an uncharted right', *International Review of Law, Computers and Technology*, τόμος 26 (1), σ. 73-82.

Grabenwarter, C. και Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Μόναχο, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. και Nouwt, S. (επιμ.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. και Bates, E. (2009), *Law of the European Convention on Human Rights*, Οξφόρδη, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), 'EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation'.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, Μόναχο, C. H. Beck.

Kokott, J. και Sobotta, C. (2013), 'The distinction between privacy and data protection in the case law of the CJEU and the ECtHR', *International Data Privacy Law*, τόμος 3, αριθ. 4, σ. 222-228.

Kranenborg, H. (2015), 'Google and the Right to be Forgotten', *European Data Protection Law Review*, τόμος 1, αριθ. 1, σ. 70-79.

Lynskey, O. (2014), 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order', *International and Comparative Law Quarterly*, τόμος 63, αριθ. 3, σ. 569-597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Οξφόρδη, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Μπάντεν-Μπάντεν, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Οξφόρδη, Oxford University Press.

Nowak, M., Januszewski, K. και Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Αμβέρσα, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. και Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Βρυξέλλες, Emile Bruylant.

Simitis, S. (1997), 'Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?', *Neue Juristische Wochenschrift*, αριθ. 5, σ. 281-288.

Warren, S. και Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review*, τόμος 4, αριθ. 5, σ. 193-220.

White, R. και Ovey, C. (2010), *The European Convention on Human Rights*, Οξφόρδη, Oxford University Press.

Κεφάλαιο 2

Acquisty, A. και Gross R. (2009), 'Predicting Social Security numbers from public data', *Proceedings of the National Academy of Science*, 7 Ιουλίου 2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Οξφόρδη, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., και Blondel V. D. (2013), 'Unique in the Crowd: the Privacy Bounds of Human Mobility', *Nature Scientific Reports*, τόμος 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Μαδρίτη, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Παρίσι, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Μπάντεν-Μπάντεν, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. και Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Λονδίνο, Sweet & Maxwell.

Ohm, P. (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization', *UCLA Law Review*, τόμος 57, αριθ. 6, σ. 1701-1777.

Samarati, P. και Sweeney, L. (1998), 'Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression', Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), 'K-Anonymity: A Model for Protecting Privacy', *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, τόμος 10, αριθ. 5, σ. 557-570.

Tinnefeld, M., Buchner, B. και Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Μόναχο, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

Κεφάλαια 3 έως 6

Brühann, U. (2012), 'Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr' στο: Grabitz, E., Hilf, M. και Nettesheim, M. (επιμ.), *Das Recht der Europäischen Union*, Band IV, A. 30, Μόναχο, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Κάδιθ, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Σααρμπρίκεν, Éditions universitaires européennes.

Curren, L. και Kaye, J. (2010), 'Revoking consent: a 'blind spot' in data protection law?', *Computer Law & Security Review*, τόμος 26, αριθ. 3, σ. 273-283.

Dammann, U. και Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Μπάντεν-Μπάντεν, Nomos.

De Hert, P. και Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, τόμος 22, αριθ. 6, σ. 1-5.

De Hert, P. και Papakonstantinou, V. (2012), 'The proposed data protection regulation replacing Directive 95/46/EC: A sound system for the protection of individuals', *Computer Law & Security Review*, τόμος 28, αριθ. 2, σ. 130-142.

Feretti, Federico (2012), 'A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously', *European Review of Private Law*, τόμος 20, αριθ. 2, σ. 473-506.

FRA (Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Λουξεμβούργο, Υπηρεσία Επίσημων Εκδόσεων της Ευρωπαϊκής Ένωσης, (Υπηρεσία Εκδόσεων).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Βιέννη, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Λουξεμβούργο, Υπηρεσία Εκδόσεων.

Irish Health Information and Quality Authority (2010), [Guidance on Privacy Impact Assessment in Health and Social Care](#).

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. και Saxby, S. (2011), '30 years on – The review of the Council of Europe Data Protection Convention 108', *Computer Law & Security Review*, τόμος 27, αριθ. 3, σ. 223-231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Μπάντεν-Μπάντεν, Nomos.

United Kingdom Information Commissioner's Office, [Privacy Impact Assessment](#).

Κεφάλαιο 7

Gutwirth, S., Pouillet, Y., De Hert, P., De Terwangne, C. και Nouwt, S. (2009), *Reinventing data protection?*, Βερολίνο, Springer.

Kuner, C. (2007), *European data protection law*, Οξφόρδη, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Οξφόρδη, Oxford University Press.

Ευρωπαίος Επόπτης Προστασίας Δεδομένων (2014), *Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies*.

Ομάδα εργασίας του άρθρου 29 (2005), *Έγγραφο εργασίας για την κοινή ερμηνεία του άρθρου 26 παρ. 1 της οδηγίας 95/46/EK της 24ης Οκτωβρίου 1995*.

Κεφάλαιο 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Λονδίνο, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Βερολίνο, Springer.

De Hert, P. και Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, τόμος 22, αριθ. 6, σ. 1-5.

Drewer, D. και Ellermann, J. (2012), 'Europol's data protection framework as an asset in the fight against cybercrime', *ERA Forum*, τόμος 13, αριθ. 3, σ. 381-395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Χάγη, Eurojust.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Βερολίνο, Springer.

Gutwirth, S., Poulet, Y. και De Hert, P. (2010), *Data protection in a profiled world*, Ντόρντρεχτ, Springer.

Gutwirth, S., Poulet, Y., De Hert, P. και Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Ντόρντρεχτ, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, τόμος 36, αριθ. 5, σ. 722-776.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of External Relations, CLEER Working Papers 2013/2.

Ευρωπαϊκή (2012), *Data Protection at Europol*, Λουξεμβούργο, Υπηρεσία Εκδόσεων.

Κεφάλαιο 9

Büllesbach, A., Gijrath, S., Poulet, Y. και Hacon, R. (2010), *Concise European IT law*, Άμστερνταμ, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. και Poulet, Y. (2012), *European data protection: In good health?*, Ντόρντρεχτ, Springer.

Gutwirth, S., Poulet, Y. και De Hert, P. (2010), *Data protection in a profiled world*, Ντόρντρεχτ, Springer.

Gutwirth, S., Poulet, Y., De Hert, P. και Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Ντόρντρεχτ, Springer.

Konstadinides, T. (2011), 'Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem', *European Law Review*, τόμος 36, αριθ. 5, σ. 722-776.

Rosemary, J. και Hamilton, A. (2012), *Data protection law and practice*, Λονδίνο, Sweet & Maxwell.

Κεφάλαιο 10

El Emam, K. και Álvarez, C. (2015), 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques', *International Data Privacy Law*, τόμος 5, αριθ. 1, σ. 73-87.

Mayer-Schönberger, V και Cate, F. (2013), 'Notice and consent in a world of Big Data', *International Data Privacy Law*, τόμος 3, αριθ. 2, σ. 67-73.

Rubinstein, I. (2013), 'Big Data: The End of Privacy or a New Beginning?', *International Data Privacy Law*, τόμος 3, αριθ. 2, σ. 74-87.

Νομολογία

Επιλεγμένη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου

Πρόσβαση στα δεδομένα προσωπικού χαρακτήρα

Gaskin κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 10454/83, 7 Ιουλίου 1989
Godelli κατά Ιταλίας, προσφυγή αριθ. 33783/09, 25 Σεπτεμβρίου 2012
Κ.Η. κ.λπ. κατά Σλοβακίας, προσφυγή αριθ. 32881/04, 28 Απριλίου 2009
Leander κατά Σουηδίας, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987
Μ.Κ. κατά Γαλλίας, προσφυγή αριθ. 19522/09, 18 Απριλίου 2013
Odièvre κατά Γαλλίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 42326/98, 13 Φεβρουαρίου 2003

Στάθμιση της προστασίας των δεδομένων με την ελευθερία της έκφρασης και το δικαίωμα ενημέρωσης

Axel Springer AG κατά Γερμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 39954/08, 7 Φεβρουαρίου 2012
Bohlen κατά Γερμανίας, προσφυγή αριθ. 53495/09, 19 Φεβρουαρίου 2015
Coudec και Hachette Filipacchi Associés κατά Γαλλίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 40454/07, 10 Νοεμβρίου 2015
Magyar Helsinki Bizottság κατά Ουγγαρίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 18030/11, 8 Νοεμβρίου 2016
Müller κ.λπ. κατά Ελβετίας, προσφυγή αριθ. 10737/84, 24 Μαΐου 1988
Vereinigung bildender Künstler κατά Αυστρίας, προσφυγή αριθ. 68354/01, 25 Ιανουαρίου 2007

Von Hannover κατά Γερμανίας (αριθ. 2) [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 40660/08 και 60641/08, 7 Φεβρουαρίου 2012

Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας, προσφυγή αριθ. 931/13, 27 Ιουνίου 2017

Στάθμιση της προστασίας των δεδομένων με τη θρησκευτική ελευθερία
Sinan Işık κατά Τουρκίας, προσφυγή αριθ. 21924/05, 2 Φεβρουαρίου 2010

Προκλήσεις όσον αφορά την προστασία δεδομένων στο διαδίκτυο
K.U. κατά Φινλανδίας, προσφυγή αριθ. 2872/02, 2 Δεκεμβρίου 2008

Συγκατάθεση του υποκειμένου των δεδομένων

Elberte κατά Λετονίας, προσφυγή αριθ. 61243/08, 13 Ιανουαρίου 2015

Sinan Işık κατά Τουρκίας, προσφυγή αριθ. 21924/05, 2 Φεβρουαρίου 2010

Υ κατά Τουρκίας, προσφυγή αριθ. 648/10, 17 Φεβρουαρίου 2015

Αλληλογραφία

Amann κατά Ελβετίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000

Association for European Integration and Human Rights και Ekimdzhiev κατά Βουλγαρίας, προσφυγή αριθ. 62540/00, 28 Ιουνίου 2007

Bernh Larsen Holding AS κ.λπ. κατά Νορβηγίας, προσφυγή αριθ. 24117/08, 14 Μαρτίου 2013

Cemalettin Canli κατά Τουρκίας, προσφυγή αριθ. 22427/04, 18 Νοεμβρίου 2008

D.L. κατά Βουλγαρίας, προσφυγή αριθ. 7472/14, 19 Μαΐου 2016

Dalea κατά Γαλλίας, προσφυγή αριθ. 964/07, 2 Φεβρουαρίου 2010

Gaskin κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 10454/83, 7 Ιουλίου 1989

Haralambie κατά Ρουμανίας, προσφυγή αριθ. 21737/03, 27 Οκτωβρίου 2009

Khelili κατά Ελβετίας, προσφυγή αριθ. 16188/07, 18 Οκτωβρίου 2011

Leander κατά Σουηδίας, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987

Malone κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 8691/79, 2 Αυγούστου 1984

Rotaru κατά Ρουμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000

S. και Marger κατά Ηνωμένου Βασιλείου [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008

Shimonovlos κατά Ρωσίας, προσφυγή αριθ. 30194/09, 21 Ιουνίου 2011

Silver κ.λπ. κατά Ηνωμένου Βασιλείου, προσφυγές αριθ. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Μαρτίου 1983

The Sunday Times κατά *Ηνωμένου Βασιλείου*, προσφυγή αριθ. 6538/74, 26 Απριλίου 1979

Βάσεις δεδομένων ποινικού μητρώου

Aycaguer κατά *Γαλλίας*, προσφυγή αριθ. 8806/12, 22 Ιουνίου 2017
B.B. κατά *Γαλλίας*, προσφυγή αριθ. 5335/06, 17 Δεκεμβρίου 2009
Brunet κατά *Γαλλίας*, προσφυγή αριθ. 21010/10, 18 Σεπτεμβρίου 2014
M.K. κατά *Γαλλίας*, προσφυγή αριθ. 19522/09, 18 Απριλίου 2013
M.M. κατά *Ηνωμένου Βασιλείου*, προσφυγή αριθ. 24029/07, 13 Νοεμβρίου 2012

Ασφάλεια δεδομένων

Haaland κατά *Ρουμανίας*, προσφυγή αριθ. 21737/03, 27 Οκτωβρίου 2009
K.H. κ.λπ. κατά *Σλοβακίας*, προσφυγή αριθ. 32881/04, 28 Απριλίου 2009

Βάσεις δεδομένων DNA

S. και Marger κατά *Ηνωμένου Βασιλείου* [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008

Δεδομένα GPS

Uzun κατά *Γερμανίας*, προσφυγή αριθ. 35623/05, 2 Σεπτεμβρίου 2010

Δεδομένα που αφορούν την υγεία

Avilkina κ.λπ. κατά *Ρωσίας*, προσφυγή αριθ. 1585/09, 6 Ιουνίου 2013
Birjuk κατά *Λιθουανίας*, προσφυγή αριθ. 23373/03, 25 Νοεμβρίου 2008
I κατά *Φινλανδίας*, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008
L.H. κατά *Λετονίας*, προσφυγή αριθ. 52019/07, 29 Απριλίου 2014
L.L. κατά *Γαλλίας*, προσφυγή αριθ. 7508/02, 10 Οκτωβρίου 2006
M.S. κατά *Σουηδίας*, προσφυγή αριθ. 20837/92, 27 Αυγούστου 1997
Szuluk κατά *Ηνωμένου Βασιλείου*, προσφυγή αριθ. 36936/05, 2 Ιουνίου 2009
Υ κατά *Τουρκίας*, προσφυγή αριθ. 648/10, 17 Φεβρουαρίου 2015
Z κατά *Φινλανδίας*, προσφυγή αριθ. 22009/93, 25 Φεβρουαρίου 1997

Ταυτότητα

Ciubotaru κατά *Μολδαβίας*, προσφυγή αριθ. 27138/04, 27 Απριλίου 2010
Godelli κατά *Ιταλίας*, προσφυγή αριθ. 33783/09, 25 Σεπτεμβρίου 2012
Odièvre κατά *Γαλλίας* [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 42326/98, 13 Φεβρουαρίου 2003

Πληροφορίες που αφορούν επαγγελματικές δραστηριότητες

G.S.B. κατά Ελβετίας, προσφυγή αριθ. 28601/11, 22 Δεκεμβρίου 2015
M.N. κ.λπ. κατά Αγίου Μαρίνου, προσφυγή αριθ. 28005/12, 7 Ιουλίου 2015
Michaud κατά Γαλλίας, προσφυγή αριθ. 12323/11, 6 Δεκεμβρίου 2012
Niemietz κατά Γερμανίας, προσφυγή αριθ. 13710/88, 16 Δεκεμβρίου 1992

Υποκλοπές

Ataman κατά Ελβετίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000
Brito Ferrinho Bexiga Villa-Nova κατά Πορτογαλίας, προσφυγή αριθ. 69436/10, 1 Δεκεμβρίου 2015
Corland κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 62617/00, 3 Απριλίου 2007
Halford κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 20605/92, 25 Ιουνίου 1997
Iordachi κ.λπ. κατά Μολδαβίας, προσφυγή αριθ. 25198/02, 10 Φεβρουαρίου 2009
Korpi κατά Ελβετίας, προσφυγή αριθ. 23224/94, 25 Μαρτίου 1998
Liberty κ.λπ. κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 58243/00, 1 Ιουλίου 2008
Malone κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 8691/79, 2 Αυγούστου 1984
Mustafa Sezgin Tanrikulu κατά Τουρκίας, προσφυγή αριθ. 27473/06, 18 Ιουλίου 2017
Pruteanu κατά Ρουμανίας, προσφυγή αριθ. 30181/05, 3 Φεβρουαρίου 2015
Szuluk κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 36936/05, 2 Ιουνίου 2009

Υποχρεώσεις φορέων επιφορτισμένων με ειδικά καθήκοντα

B.B. κατά Γαλλίας, προσφυγή αριθ. 5335/06, 17 Δεκεμβρίου 2009
I κατά Φινλανδίας, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008
Mosley κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 48009/08, 10 Μαΐου 2011

Δεδομένα προσωπικού χαρακτήρα

Ataman κατά Ελβετίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000
Bernh Larsen Holding AS κ.λπ. κατά Νορβηγίας, προσφυγή αριθ. 24117/08, 14 Μαρτίου 2013
Uzun κατά Γερμανίας, προσφυγή αριθ. 35623/05, 2010

Φωτογραφίες

Sciaccia κατά Ιταλίας, προσφυγή αριθ. 50774/99, 11 Ιανουαρίου 2005
Von Hannover κατά Γερμανίας, προσφυγή αριθ. 59320/00, 24 Ιουνίου 2004

Δικαίωμα στη λήθη

Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας, προσφυγή αριθ. 931/13, 27 Ιουνίου 2017

Segerstedt-Wiberg κ.λπ. κατά Σουηδίας, προσφυγή αριθ. 62332/00, 6 Ιουνίου 2006

Δικαίωμα εναντίωσης

Leander κατά Σουηδίας, προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987

M.S. κατά Σουηδίας, προσφυγή αριθ. 20837/92, 27 Αυγούστου 1997

Mosley κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 48009/08, 10 Μαΐου 2011

Rotaru κατά Ρουμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000

Sinan Isik κατά Τουρκίας, προσφυγή αριθ. 21924/05, 2 Φεβρουαρίου 2010

Ευαίσθητες κατηγορίες δεδομένων

Brunet κατά Γαλλίας, προσφυγή αριθ. 21010/10, 18 Σεπτεμβρίου 2014

I κατά Φινλανδίας, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008

Michaud κατά Γαλλίας, προσφυγή αριθ. 12323/11, 6 Δεκεμβρίου 2012

S. και Margre κατά Ηνωμένου Βασιλείου [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008

Εποπτεία και επιβολή (ρόλος των διαφόρων φορέων, συμπεριλαμβανομένων των εποπτικών αρχών)

I κατά Φινλανδίας, προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008

K.U. κατά Φινλανδίας, προσφυγή αριθ. 2872/02, 2 Δεκεμβρίου 2008

Von Hannover κατά Γερμανίας, προσφυγή αριθ. 59320/00, 24 Ιουνίου 2004

Von Hannover κατά Γερμανίας (αριθ. 2) [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 40660/08 και 60641/08, 7 Φεβρουαρίου 2012

Μέθοδοι παρακολούθησης

Allan κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 48539/99, 5 Νοεμβρίου 2002

Association for European Integration and Human Rights και Ekimdzhiiev κατά Βουλγαρίας, προσφυγή αριθ. 62540/00, 28 Ιουνίου 2007

Bărbulescu κατά Ρουμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 61496/08, 5 Σεπτεμβρίου 2017

D.L. κατά Βουλγαρίας, προσφυγή αριθ. 7472/14, 19 Μαΐου 2016

Dragojević κατά Κροατίας, προσφυγή αριθ. 68955/11, 15 Ιανουαρίου 2015

Karabegović κατά Τουρκίας, προσφυγή αριθ. 30083/10, 7 Ιουνίου 2016

Klass κ.λπ. κατά Γερμανίας, προσφυγή αριθ. 5029/71, 6 Σεπτεμβρίου 1978

Roman Zakharov κατά Ρωσίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 47143/06, 4 Δεκεμβρίου 2015

Rotaru κατά Ρουμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000

Szabó και Vissy κατά Ουγγαρίας, προσφυγή αριθ. 37138/14, 12 Ιανουαρίου 2016

Taylor-Sabori κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 47114/99, 22 Οκτωβρίου 2002

Uzun κατά Γερμανίας, προσφυγή αριθ. 35623/05, 2 Σεπτεμβρίου 2010

Versini-Campinchi και Crasnianski κατά Γαλλίας, προσφυγή αριθ. 49176/11, 16 Ιουνίου 2016

Vetter κατά Γαλλίας, προσφυγή αριθ. 59842/00, 31 Μαΐου 2005

Vukota-Bojić κατά Ελβετίας, προσφυγή αριθ. 61838/10, 18 Οκτωβρίου 2016

Βιντεοεπιτήρηση

Körke κατά Γερμανίας, προσφυγή αριθ. 420/07, 5 Οκτωβρίου 2010

Peck κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 44647/98, 28 Ιανουαρίου 2003

Δείγματα φωνής

P.G. και J.H. κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 44787/98, 25 Σεπτεμβρίου 2001

Wisse κατά Γαλλίας, προσφυγή αριθ. 71611/01, 20 Δεκεμβρίου 2005

Επιλεγμένη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης

Νομολογία σχετική με την Οδηγία για την Προστασία Δεδομένων

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde κατά Rīgas pašvaldības SIA «Rīgas satiksme»*, 4 Μαΐου 2017

[Αρχή της νόμιμης επεξεργασίας: έννομο συμφέρον που επιδιώκει τρίτος]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*, 9 Μαρτίου 2017

[Δικαίωμα διαγραφής δεδομένων προσωπικού χαρακτήρα· δικαίωμα εναντίωσης στην επεξεργασία]

Συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, *Tele2 Sverige AB κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson κ.λπ.* [Τμήμα μείζονος συνθέσεως], 21 Δεκεμβρίου 2016

[Απόρρητο των ηλεκτρονικών επικοινωνιών· πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών· υποχρέωση γενικής και χωρίς διάκριση διατηρήσεως των δεδομένων κινήσεως και των δεδομένων θέσεως· απουσία προηγούμενου ελέγχου από δικαστήριο ή ανεξάρτητη διοικητική αρχή· Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης· συμβατότητα με το δίκαιο της ΕΕ]

C-582/14, *Patrick Breyer κατά Bundesrepublik Deutschland*, 19 Οκτωβρίου 2016

[Έννοια των «δεδομένων προσωπικού χαρακτήρα»· διευθύνσεις πρωτοκόλλου του διαδικτύου· αποθήκευση δεδομένων από φορέα παροχής υπηρεσιών τηλεμέσων· εθνική κανονιστική ρύθμιση η οποία δεν επιτρέπει τη συνεκτίμηση του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας]

C-362/14, *Maximillian Schrems κατά Data Protection Commissioner* [Τμήμα μείζονος συνθέσεως], 6 Οκτωβρίου 2015

[Αρχή της νόμιμης επεξεργασίας· θεμελιώδη δικαιώματα· ακυρότητα της απόφασης περί επάρκειας του συστήματος ασφαλούς λιμένα· εξουσίες των ανεξάρτητων εποπτικών αρχών]

C-230/14, *Weltimmo s. r. o. κατά Nemzeti Adatvédelmi és Információsztárság Hatóság*, 1 Οκτωβρίου 2015

[Εξουσίες των εθνικών εποπτικών αρχών]

C-201/14, *Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ.*, 1 Οκτωβρίου 2015

[Δικαίωμα ενημέρωσης σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα]

C-212/13, *František Ryneš κατά Úřad pro ochranu osobních údajů*, 11 Δεκεμβρίου 2014

[Έννοια της «επεξεργασίας δεδομένων» και του «υπευθύνου επεξεργασίας»]

C-473/12, *Institut professionnel des agents immobiliers (IPI) κατά Geoffrey Englebert κ.λπ.*, 7 Νοεμβρίου 2013

[Δικαίωμα ενημέρωσης σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα]

T-462/12 R, *Pilkington Group Ltd κατά Ευρωπαϊκής Επιτροπής*, διάταξη του Προέδρου του Γενικού Δικαστηρίου, 11 Μαρτίου 2013

C-342/12, *Worten – Equipamentos para o Lar SA κατά Autoridade para as Condições de Trabalho (ACT)*, 30 Μαΐου 2013

[Έννοια των «δεδομένων προσωπικού χαρακτήρα»· δελτίο καταγραφής του χρόνου εργασίας· αρχές που αφορούν την ποιότητα των δεδομένων και τη νομιμοποίηση της επεξεργασίας δεδομένων· πρόσβαση της αρμόδιας για την εποπτεία των συνθηκών εργασίας εθνικής αρχής· υποχρέωση του εργοδότη να θέτει στη διάθεση της εν λόγω αρχής το δελτίο καταγραφής του χρόνου εργασίας κατά τρόπον ώστε να καθίσταται δυνατή η άμεση εξέτασή του]

Συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, *Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014.

[Παράβαση του πρωτογενούς δικαίου της ΕΕ από την οδηγία για τη διατήρηση δεδομένων νόμιμη επεξεργασία· περιορισμός του σκοπού και της αποθήκευσης]

C-288/12, *Ευρωπαϊκή Επιτροπή κατά Ουγγαρίας* [τμήμα μείζονος συνθέσεως], 8 Απριλίου 2014

[Νομιμότητα του τερματισμού της θητείας του εθνικού επόπτη προστασίας δεδομένων]

Συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, *YS κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S*, 17 Ιουλίου 2014

[Περιεχόμενο του δικαιώματος προσβάσεως του προσώπου το οποίο αφορούν τα δεδομένα· προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· έννοια του όρου «δεδομένα προσωπικού χαρακτήρα»· δεδομένα που αφορούν αιτούντα άδεια παραμονής και νομική ανάλυση περιλαμβανόμενη σε προπαρασκευαστικό της αποφάσεως διοικητικό έγγραφο· Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης]

C-131/12, *Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [τμήμα μείζονος συνθέσεως], 13 Μαΐου 2014

[Υποχρεώσεις των παρόχων μηχανών αναζήτησης να μην εμφανίζουν δεδομένα προσωπικού χαρακτήρα στα αποτελέσματα αναζήτησης, κατόπιν αιτήματος του υποκειμένου των δεδομένων· δυνατότητα εφαρμογής της Οδηγίας για την Προστασία Δεδομένων· έννοια της «επεξεργασίας δεδομένων»· έννοια των «υπευθύνων επεξεργασίας»· στάθμιση της προστασίας των δεδομένων με την ελευθερία της έκφρασης το δικαίωμα στη λήθη]

C-614/10, *Ευρωπαϊκή Επιτροπή κατά Δημοκρατίας της Αυστρίας* [τμήμα μείζονος συνθέσεως], 16 Οκτωβρίου 2012

[Ανεξαρτησία εθνικής εποπτικής αρχής]

Συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado*, 24 Νοεμβρίου 2011

[Ορθή εφαρμογή του άρθρου 7 στοιχείο στ) της Οδηγίας για την Προστασία Δεδομένων –«έννομα συμφέροντα τρίτων»– στο εθνικό δίκαιο]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) κατά Netlog NV*, 16 Φεβρουαρίου 2012

[Υποχρέωση των παρόχων κοινωνικών δικτύων να μην επιτρέπουν την παράνομη χρήση μουσικών και οπτικοακουστικών έργων από τους χρήστες των δικτύων]

C-70/10, *Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Νοεμβρίου 2011

[Κοινωνία της πληροφορίας· δικαίωμα του δημιουργού· διαδικτυο· προγράμματα «peer-to-peer»· φορείς παροχής υπηρεσιών προσβάσεως στο διαδικτυο· εφαρμογή

συστήματος χρήσεως φίλτρου για επικοινωνίες μέσω διαδικτύου προκειμένου να αποκλειστεί η ανταλλαγή αρχείων η οποία συνιστά προσβολή του δικαιώματος του δημιουργού· έλλειψη γενικής υποχρέωσης ελέγχου των διακινούμενων πληροφοριών]

C-543/09, *Deutsche Telekom AG κατά Bundesrepublik Deutschland*, 5 Μαΐου 2011
[Αναγκαιότητα εκ νέου συγκατάθεσης]

Συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, *Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen* [τμήμα μείζονος συνθέσεως],
9 Νοεμβρίου 2010

[Έννοια των «δεδομένων προσωπικού χαρακτήρα»· αναλογικότητα της εκ του νόμου υποχρέωσης δημοσιοποίησης δεδομένων προσωπικού χαρακτήρα σχετικά με τους δικαιούχους ορισμένων γεωργικών ταμείων της ΕΕ]

C-553/07, *College van burgemeester en wethouders van Rotterdam κατά E. E. Rijkeboer*, 7 Μαΐου 2009
[Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων]

C-518/07, *Ευρωπαϊκή Επιτροπή κατά Ομοσπονδιακής Δημοκρατίας της Γερμανίας*
[τμήμα μείζονος συνθέσεως], 9 Μαρτίου 2010
[Ανεξαρτησία εθνικής εποπτικής αρχής]

C-73/07, *Tietosuojavaltuutettu κατά Satakunnan Markkinapörssi Oy και Satamedia Oy*
[τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008
[Έννοια των «δημοσιογραφικών δραστηριοτήτων» κατά το άρθρο 9 της Οδηγίας για την Προστασία των Δεδομένων]

C-524/06, *Heinz Huber κατά Bundesrepublik Deutschland* [τμήμα μείζονος συνθέσεως], 16 Δεκεμβρίου 2008
[Νομιμότητα της διατήρησης δεδομένων σχετικά με αλλοδαπούς σε στατιστικό μητρώο]

C-275/06, *Productores de Música de España (Promusicae) κατά Telefónica de España SAU* [τμήμα μείζονος συνθέσεως], 29 Ιανουαρίου 2008
[Έννοια των «δεδομένων προσωπικού χαρακτήρα»· υποχρέωση των φορέων παροχής προσβάσεως στο διαδίκτυο να γνωστοποιούν την ταυτότητα των χρηστών του προγράμματος ανταλλαγής αρχείων KaZaA σε ένωση προστασίας της διανοητικής ιδιοκτησίας]

C-101/01, *Ποινική δίκη κατά Bodil Lindqvist*, 6 Νοεμβρίου 2003

[Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα]

Συνεκδικασθείσες υποθέσεις C-465/00, C-138/01 και C-139/01, *Rechnungshof κατά Österreichischer Rundfunk κ.λπ. και Christa Neukomm και Joseph Lauer mann κατά Österreichischer Rundfunk*, 20 Μαΐου 2003

[Αναλογικότητα της εκ του νόμου υποχρέωσης δημοσίευσης δεδομένων προσωπικού χαρακτήρα σχετικά με τους μισθούς των υπαλλήλων ορισμένων κατηγοριών οργανισμών που σχετίζονται με τον δημόσιο τομέα]

C-434/16, *Peter Nowak κατά Data Protection Commissioner*, προτάσεις της γενικής εισαγγελέα Kokott της 20ής Ιουλίου 2017

[Έννοια των δεδομένων προσωπικού χαρακτήρα· πρόσβαση υποψηφίου, που μετείχε σε εξέταση, στο γραπτό του· διορθώσεις του εξεταστή]

C-291/12, *Michael Schwarz κατά Stadt Bochum*, 17 Οκτωβρίου 2013

[Προδικαστική παραπομπή· χώρος ελευθερίας, ασφάλειας και δικαιοσύνης· διαβατήριο με βιομετρικά στοιχεία· δακτυλικά αποτυπώματα· νομική βάση· αναλογικότητα]

Νομολογία σχετική με την οδηγία 2016/681

Γνωμοδότηση 1/15 του Δικαστηρίου [τμήμα μείζονος συνθέσεως], της 26ης Ιουλίου 2017

[Νομική βάση· σχέδιο συμφωνίας μεταξύ του Καναδά και της Ευρωπαϊκής ένωσης σχετικά με τη διαβίβαση και επεξεργασία δεδομένων από τις καταστάσεις ονομάτων επιβατών· συμβατότητα του σχεδίου συμφωνίας με το άρθρο 16 της ΣΛΕΕ και τα άρθρα 7 και 8 και το άρθρο 52 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης]

Νομολογία σχετική με τον κανονισμό για την προστασία δεδομένων από τα όργανα της ΕΕ

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) κατά Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων (EFSA), Ευρωπαϊκής Επιτροπής*, 16 Ιουλίου 2015

[Πρόσβαση σε έγγραφα]

C-28/08 P, *Ευρωπαϊκή Επιτροπή κατά The Bavarian Lager Co. Ltd.* [Τμήμα μείζονος συνθέσεως], 29 Ιουνίου 2010

[Πρόσβαση σε έγγραφα]

Νομολογία σχετική με την οδηγία 2002/58/ΕΚ

C-536/15, *Tele2 (Netherlands) BV κ.λπ. κατά Autoriteit Consument en Markt (ACM)*, 15 Μαρτίου 2017

[Αρχή της απαγορεύσεως των διακρίσεων· διάθεση προσωπικών δεδομένων των συνδρομητών, στο πλαίσιο της παροχής διαθέσιμων στο κοινό υπηρεσιών πληροφοριών καταλόγου και καταλόγων συνδρομητών· συγκατάθεση του συνδρομητή· διαφορετική μεταχείριση ανάλογα με το κράτος μέλος εντός του οποίου παρέχονται οι διαθέσιμες στο κοινό τηλεφωνικές υπηρεσίες πληροφοριών καταλόγου και οι κατάλογοι συνδρομητών]

Συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, *Tele2 Sverige AB κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson κ.λπ.* [Τμήμα μείζονος συνθέσεως], 21 Δεκεμβρίου 2016

[Εμπιστευτικότητα των ηλεκτρονικών επικοινωνιών· πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών· υποχρέωση γενικής και χωρίς διάκριση διατηρήσεως των δεδομένων κινήσεως και των δεδομένων θέσεως· απουσία προηγούμενου ελέγχου από δικαστήριο ή ανεξάρτητη διοικητική αρχή· Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης· συμβατότητα με το δίκαιο της ΕΕ]

C-70/10, *Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 Νοεμβρίου 2011

[Κοινωνία της πληροφορίας· δικαίωμα του δημιουργού· διαδίκτυο· προγράμματα «peer-to-peer»· φορείς παροχής υπηρεσιών προσβάσεως στο διαδίκτυο· εφαρμογή συστήματος χρήσεως φίλτρου για επικοινωνίες μέσω διαδικτύου προκειμένου να αποκλειστεί η ανταλλαγή αρχείων η οποία συνιστά προσβολή του δικαιώματος του δημιουργού· έλλειψη γενικής υποχρέωσης ελέγχου των διακινούμενων πληροφοριών]

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB κατά Perfect Communication Sweden AB*, 19 Απριλίου 2012

[Δικαίωμα του δημιουργού και συγγενικά δικαιώματα· επεξεργασία δεδομένων μέσω διαδικτύου· προσβολή αποκλειστικού δικαιώματος ακουστικά βιβλία των οποίων η πρόσβαση κατέστη δυνατή από διακομιστή FTP μέσω διαδικτύου με διεύθυνση IP χορηγηθείσα από τον φορέα παροχής υπηρεσιών διαδικτύου· διαταγή προς τον φορέα παροχής υπηρεσιών διαδικτύου να κοινοποιήσει το όνομα και τη διεύθυνση του χρήστη της διευθύνσεως IP]

Ευρετήριο

Νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης

- Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) και Federación de Comercio Electrónico y Marketing Directo (FECEMD) κατά Administración del Estado*, συνεκδικασθείσες υποθέσεις C-468/10 και C-469/10, 24 Νοεμβρίου 2011 36, 66, 176, 179, 197, 198, 199
- Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) κατά Netlog NV*, C-360/10, 16 Φεβρουαρίου 2012 96
- Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB κατά Perfect Communication Sweden AB*, C-461/10, 19 Απριλίου 2012 96
- Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce κατά Salvatore Manni*, C-398/15, 9 Μαρτίου 2017 19, 99, 104, 126, 254, 255, 283, 288
- ClientEarth, Pesticide Action Network Europe (PAN Europe) κατά Ευρωπαϊκής Αρχής για την Ασφάλεια των Τροφίμων (EFSA), Ευρωπαϊκής Επιτροπής*, C-615/13 P, 16 Ιουλίου 2015 19, 83, 271
- College van burgemeester en wethouders van Rotterdam κατά E. E. Rijkeboer*, C-553/07, 7 Μαΐου 2009 148, 163, 254, 273
- Deutsche Telekom AG κατά Bundesrepublik Deutschland*, C-543/09, 5 Μαΐου 2011 105, 175, 186

<i>Digital Rights Ireland Ltd κατά Minister for Communications, Marine and Natural Resources κ.λπ. και Kärntner Landesregierung κ.λπ.</i> [τμήμα μείζονος συνθέσεως], συνεκδικασθείσες υποθέσεις C-293/12 και C-594/12, 8 Απριλίου 2014	24, 56, 58, 77, 147, 148, 161, 166, 303, 305, 342, 373, 375, 441
<i>František Ryneš κατά Úřad pro ochranu osobních údajů</i> , C-212/13, 11 Δεκεμβρίου 2014	104, 118, 125, 133
<i>Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González</i> [τμήμα μείζονος συνθέσεως], C-131/12, 13 Μαΐου 2014	19, 70, 72, 98, 104, 127, 134, 135, 254, 280, 281, 282, 288
<i>Heinz Huber κατά Bundesrepublik Deutschland</i> [τμήμα μείζονος συνθέσεως], C-524/06, 16 Δεκεμβρίου 2008	175, 179, 192, 193, 194, 411, 432
<i>Institut professionnel des agents immobiliers (IPI) κατά Geoffrey Englebert κ.λπ.</i> , C-473/12, 7 Νοεμβρίου 2013	253, 260
<i>International Transport Workers' Federation, Finnish Seamen's Union κατά Viking Line ABP, OÜ Viking Line Eesti</i> [τμήμα μείζονος συνθέσεως], C-438/05, 11 Δεκεμβρίου 2007	306
<i>Maximilian Schrems κατά Data Protection Commissioner</i> [τμήμα μείζονος συνθέσεως], C-362/14, 6 Οκτωβρίου 2015	54, 235, 238, 239, 245, 256, 300, 303, 313, 319, 320, 321, 322, 327, 329
<i>Michael Schwarz κατά Stadt Bochum</i> , C-291/12, 17 Οκτωβρίου 2013	61, 63
<i>Pasquale Foglia κατά Mariella Novello</i> (αριθ. 2), C-244/80, 16 Δεκεμβρίου 1981	306
<i>Patrick Breyer κατά Bundesrepublik Deutschland</i> , C-582/14, 19 Οκτωβρίου 2016	103, 117
<i>Peter Nowak κατά Data Protection Commissioner</i> , C-434/16, προτάσεις της γενικής εισαγγελέα Kokott, 20 Ιουλίου 2017	104, 254
<i>Pilkington Group Ltd κατά Ευρωπαϊκής Επιτροπής</i> , T-462/12 R, διάταξη του Προέδρου του Γενικού Δικαστηρίου, 11 Μαρτίου 2013	87
<i>Productores de Música de España (Promusicae) κατά Telefónica de España SAU</i> [τμήμα μείζονος συνθέσεως], C-275/06, 29 Ιανουαρίου 2008	19, 66, 94, 97, 103, 114

<i>Rechnungshof κατά Österreichischer Rundfunk κ.λπ. και Christa Neukomm και Joseph Lauermann κατά Österreichischer Rundfunk, συνεκδικασθείσες υποθέσεις C-465/00, C-138/01 και C-139/01, 20 Μαΐου 2003</i>	80, 179
<i>Scarlet Extended SA κατά Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, 24 Νοεμβρίου 2011</i>	103, 114, 117
<i>Smaranda Bara κ.λπ. κατά Casa Națională de Asigurări de Sănătate κ.λπ., C-201/14, 1 Οκτωβρίου 2015</i>	115, 147, 155, 253, 261, 437
<i>Tele2 (Netherlands) BV κ.λπ. κατά Autoriteit Consument en Markt (ACM), C-536/15, 15 Μαρτίου 2017</i>	105, 175, 186, 187
<i>Tele2 Sverige AB κατά Post- och telestyrelsen και Secretary of State for the Home Department κατά Tom Watson κ.λπ. [τμήμα μείζονος συνθέσεως], συνεκδικασθείσες υποθέσεις C-203/15 και C-698/15, 21 Δεκεμβρίου 2016</i>	59, 77, 342, 375
<i>Tietosuoja-valtuutettu κατά Satakunnan Markkinapörssi Oy και Satamedia Oy [τμήμα μείζονος συνθέσεως], C-73/07, 16 Δεκεμβρίου 2008</i>	19, 68
<i>Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde κατά Rīgas pašvaldības SIA «Rīgas satiksme», C-13/16, 4 Μαΐου 2017</i>	176, 196
<i>Volker und Markus Schecke GbR και Hartmut Eifert κατά Land Hessen [τμήμα μείζονος συνθέσεως], συνεκδικασθείσες υποθέσεις C-92/09 και C-93/09, 9 Νοεμβρίου 2010</i>	18, 23, 45, 58, 79, 103, 109, 111
<i>Weltimmo s. r. o. κατά Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1 Οκτωβρίου 2015</i>	245
<i>Worten – Equipamentos para o Lar SA κατά Autoridade para as Condições de Trabalho (ACT), C-342/12, 30 Μαΐου 2013</i>	419
<i>YS κατά Minister voor Immigratie, Integratie en Asiel και Minister voor Immigratie, Integratie en Asiel κατά M και S, συνεκδικασθείσες υποθέσεις C-141/12 και C-372/12, 17 Ιουλίου 2014</i>	103, 111, 115, 254, 271
<i>Γνωμοδότηση 1/15 του Δικαστηρίου [τμήμα μείζονος συνθέσεως], 26 Ιουλίου 2017</i>	54, 335

Ευρωπαϊκή Επιτροπή κατά The Bavarian Lager Co. Ltd. [τμήμα μείζονος συνθέσεως], C-28/08 P, 29 Ιουνίου 2010..... 19, 81, 256, 302

Ευρωπαϊκή Επιτροπή κατά Δημοκρατίας της Αυστρίας [τμήμα μείζονος συνθέσεως], C-614/10, 16 Οκτωβρίου 2012 235, 242

Ευρωπαϊκή Επιτροπή κατά Ομοσπονδιακής Δημοκρατίας της Γερμανίας [τμήμα μείζονος συνθέσεως], C-518/07, 9 Μαρτίου 2010 235, 241

Ευρωπαϊκή Επιτροπή κατά Ουγγαρίας [τμήμα μείζονος συνθέσεως], C-288/12, 8 Απριλίου 2014.....235, 242

Ποινική δίκη κατά Bodil Lindqvist, C-101/01, 6 Νοεμβρίου 2003..... 104, 123, 127, 133, 214

Νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου

Allan κατά Ηνωμένου Βασιλείου, προσφυγή αριθ. 48539/99, 5 Νοεμβρίου 2002.....341, 348

Ατμην κατά Ελβετίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 27798/95, 16 Φεβρουαρίου 2000 46, 103, 110, 113

Association for European Integration and Human Rights και Ekimdzhiev κατά Βουλγαρίας, προσφυγή αριθ. 62540/00, 28 Ιουνίου 2007 47

Avilkina κ.λπ. κατά Ρωσίας, προσφυγή αριθ. 1585/09, 6 Ιουνίου 2013 (μη οριστική απόφαση)..... 426

Axel Springer AG κατά Γερμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 39954/08, 7 Φεβρουαρίου 2012..... 19, 72

Aycaguer κατά Γαλλίας, προσφυγή αριθ. 8806/12, 22 Ιουνίου 2017 346

B.B. κατά Γαλλίας, προσφυγή αριθ. 5335/06, 17 Δεκεμβρίου 2009 341, 342, 346

Bărbulescu κατά Ρουμανίας [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 61496/08, 5 Σεπτεμβρίου 2017 111, 421

Bernh Larsen Holding AS κ.λπ. κατά Νορβηγίας, προσφυγή αριθ. 24117/08, 14 Μαρτίου 2013..... 103, 108

Biriuk κατά Λιθουανίας, προσφυγή αριθ. 23373/03, 25 Νοεμβρίου 2008.....75, 256, 426

Bohlen κατά Γερμανίας, προσφυγή αριθ. 53495/09, 19 Φεβρουαρίου 2015... 19, 75

Brito Ferrinho Bexiga Villa-Nova κατά Πορτογαλίας, προσφυγή αριθ. 69436/10, 1 Δεκεμβρίου 2015 87

Brunet κατά Γαλλίας, προσφυγή αριθ. 21010/10, 18 Σεπτεμβρίου 2014 277

<i>Cemalettin Canli κατά Τουρκίας</i> , προσφυγή αριθ. 22427/04, 18 Νοεμβρίου 2008	254, 276
<i>Čiubotaru κατά Μολδαβίας</i> , προσφυγή αριθ. 27138/04, 27 Απριλίου 2010	254, 275
<i>Copland κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 62617/00, 3 Απριλίου 2007	28, 411, 420
<i>Couderc και Hachette Filipacchi Associés κατά Γαλλίας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 40454/07, 10 Νοεμβρίου 2015	73
<i>D.L. κατά Βουλγαρίας</i> , προσφυγή αριθ. 7472/14, 19 Μαΐου 2016.....	345
<i>Dalea κατά Γαλλίας</i> , προσφυγή αριθ. 964/07, 2 Φεβρουαρίου 2010	276, 342, 393
<i>Dragojević κατά Κροατίας</i> , προσφυγή αριθ. 68955/11, 15 Ιανουαρίου 2015	345
<i>Elberte κατά Λετονίας</i> , προσφυγή αριθ. 61243/08, 2015	105
<i>G.S.B. κατά Ελβετίας</i> , προσφυγή αριθ. 28601/11, 22 Δεκεμβρίου 2015.....	436, 436
<i>Gaskin κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 10454/83, 7 Ιουλίου 1989.....	271
<i>Godelli κατά Ιταλίας</i> , προσφυγή αριθ. 33783/09, 25 Σεπτεμβρίου 2012.....	271
<i>Halford κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 20605/92, 25 Ιουνίου 1997	435
<i>Haralambie κατά Ρουμανίας</i> , προσφυγή αριθ. 21737/03, 27 Οκτωβρίου 2009.....	147, 153
<i>I κατά Φινλανδίας</i> , προσφυγή αριθ. 20511/03, 17 Ιουλίου 2008	29, 176, 211, 424
<i>Iordachi κ.λπ. κατά Μολδαβίας</i> , προσφυγή αριθ. 25198/02, 10 Φεβρουαρίου 2009	46
<i>K.H. κ.λπ. κατά Σλοβακίας</i> , προσφυγή αριθ. 32881/04, 28 Απριλίου 2009.....	147, 151, 271, 424
<i>K.U. κατά Φινλανδίας</i> , προσφυγή αριθ. 2872/02, 2 Δεκεμβρίου 2008.....	29, 256, 306
<i>Karabegoğlu κατά Τουρκίας</i> , προσφυγή αριθ. 30083/10, 7 Ιουνίου 2016.....	299, 351
<i>Khelili κατά Ελβετίας</i> , προσφυγή αριθ. 16188/07, 18 Οκτωβρίου 2011	50
<i>Klass κ.λπ. κατά Γερμανίας</i> , προσφυγή αριθ. 5029/71, 6 Σεπτεμβρίου 1978.....	27, 28, 341, 344

<i>Körke κατά Γερμανίας</i> , προσφυγή αριθ. 420/07, 5 Οκτωβρίου 2010	119, 307
<i>Korpr κατά Ελβετίας</i> , προσφυγή αριθ. 23224/94, 25 Μαρτίου 1998	46
<i>L.H. κατά Λετονίας</i> , προσφυγή αριθ. 52019/07, 29 Απριλίου 2014	426
<i>L.L. κατά Γαλλίας</i> , προσφυγή αριθ. 7508/02, 10 Οκτωβρίου 2006	424
<i>Leander κατά Σουηδίας</i> , προσφυγή αριθ. 9248/81, 26 Μαρτίου 1987	49, 52, 254, 271, 287, 346
<i>Liberty κ.λπ. κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 58243/00, 1 Ιουλίου 2008	108
<i>M.K. κατά Γαλλίας</i> , προσφυγή αριθ. 19522/09, 18 Απριλίου 2013	277, 346
<i>M.M. κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 24029/07, 13 Νοεμβρίου 2012	165, 346
<i>M.N. κ.λπ. κατά Αγίου Μαρίνου</i> , προσφυγή αριθ. 28005/12, 7 Ιουλίου 2015	115, 435
<i>M.S. κατά Σουηδίας</i> , προσφυγή αριθ. 20837/92, 27 Αυγούστου 1997	287, 424
<i>Magyar Helsinki Bizottság κατά Ουγγαρίας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 18030/11, 8 Νοεμβρίου 2016	19, 84
<i>Malone κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 8691/79, 2 Αυγούστου 1984	28, 46, 341
<i>Michaud κατά Γαλλίας</i> , προσφυγή αριθ. 12323/11, 6 Δεκεμβρίου 2012	412, 435
<i>Mosley κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 48009/08, 10 Μαΐου 2011	19, 74, 287
<i>Müller κ.λπ. κατά Ελβετίας</i> , προσφυγή αριθ. 10737/84, 24 Μαΐου 1988	92
<i>Mustafa Sezgin Tanrikulu κατά Τουρκίας</i> , προσφυγή αριθ. 27473/06, 18 Ιουλίου 2017	28, 299
<i>Niemietz κατά Γερμανίας</i> , προσφυγή αριθ. 13710/88, 16 Δεκεμβρίου 1992	111, 435
<i>Odièvre κατά Γαλλίας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 42326/98, 13 Φεβρουαρίου 2003	271
<i>P.G. και J.H. κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 44787/98, 25 Σεπτεμβρίου 2001	119
<i>Peck κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 44647/98, 28 Ιανουαρίου 2003	48, 119

<i>Pruteanu κατά Ρουμανίας</i> , προσφυγή αριθ. 30181/05, 3 Φεβρουαρίου 2015	19, 87
<i>Roman Zakharov κατά Ρωσίας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 47143/06, 4 Δεκεμβρίου 2015	28, 348
<i>Rotaru κατά Ρουμανίας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 28341/95, 4 Μαΐου 2000	27, 47, 111, 276, 344
<i>S. και Marger κατά Ηνωμένου Βασιλείου</i> [τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 30562/04 και 30566/04, 4 Δεκεμβρίου 2008	18, 45, 51, 148, 165, 341, 342, 346
<i>Satakunnan Markkinapörssi Oy και Satamedia Oy κατά Φινλανδίας</i> [τμήμα ευρείας συνθέσεως], προσφυγή αριθ. 931/13, 27 Ιουνίου 2017	21, 69
<i>Siacca κατά Ιταλίας</i> , προσφυγή αριθ. 50774/99, 11 Ιανουαρίου 2005	118
<i>Segerstedt-Wiberg κ.λπ. κατά Σουηδίας</i> , προσφυγή αριθ. 62332/00, 6 Ιουνίου 2006	254, 277
<i>Shimonovos κατά Ρωσίας</i> , προσφυγή αριθ. 30194/09, 21 Ιουνίου 2011	47
<i>Silver κ.λπ. κατά Ηνωμένου Βασιλείου</i> , προσφυγές αριθ. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 Μαρτίου 1983	46
<i>Sinan Isik κατά Τουρκίας</i> , προσφυγή αριθ. 21924/05, 2 Φεβρουαρίου 2010	90
<i>Szabo και Vissy κατά Ουγγαρίας</i> , προσφυγή αριθ. 37138/14, 12 Ιανουαρίου 2016	27, 28, 341, 344, 348
<i>Szuluk κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 36936/05, 2 Ιουνίου 2009	424
<i>Taylor-Sabori κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 47114/99, 22 Οκτωβρίου 2002	47
<i>The Sunday Times κατά Ηνωμένου Βασιλείου</i> , προσφυγή αριθ. 6538/74, 26 Απριλίου 1979	46
<i>Uzun κατά Γερμανίας</i> , προσφυγή αριθ. 35623/05, 2 Σεπτεμβρίου 2010	28, 103
<i>Vereinigung bildender Künstler κατά Αυστρίας</i> , προσφυγή αριθ. 68354/01, 25 Ιανουαρίου 2007	19, 93
<i>Versini-Campinchi και Crasnianski κατά Γαλλίας</i> , προσφυγή αριθ. 49176/11, 16 Ιουνίου 2016	350
<i>Vetter κατά Γαλλίας</i> , προσφυγή αριθ. 59842/00, 31 Μαΐου 2005	47, 341
<i>Von Hannover κατά Γερμανίας</i> , προσφυγή αριθ. 59320/00, 24 Ιουνίου 2004	118

<i>Von Hannover κατά Γερμανίας (αριθ. 2)</i> [Τμήμα ευρείας συνθέσεως], προσφυγές αριθ. 40660/08 και 60641/08, 7 Φεβρουαρίου 2012	66
<i>Vukota-Bojić κατά Ελβετίας</i> , προσφυγή αριθ. 61838/10, 18 Οκτωβρίου 2016	48
<i>Wisse κατά Γαλλίας</i> , προσφυγή αριθ. 71611/01, 20 Δεκεμβρίου 2005	119
<i>Υ κατά Τουρκίας</i> , προσφυγή αριθ. 648/10, 17 Φεβρουαρίου 2015	176, 200
<i>Ζ κατά Φινλανδίας</i> , προσφυγή αριθ. 22009/93, 25 Φεβρουαρίου 1997	30, 411, 424

Νομολογία Εθνικών Δικαστηρίων

Γερμανία, Ομοσπονδιακό Συνταγματικό Δικαστήριο (<i>Bundesverfassungsgericht</i>), 1 BvR 209/83, 1 BvR 484/83, 1 BvR 420/83, 1 BvR 362/83, 1 BvR 269/83, 1 BvR 440/83 (<i>Volkszählungsurteil</i>), 15 Δεκεμβρίου 1983	21
Γερμανία, Ομοσπονδιακό Συνταγματικό Δικαστήριο (<i>Bundesverfassungsgericht</i>), 1 BvR 256/08, 2 Μαρτίου 2010	373
Ρουμανία, Ομοσπονδιακό Συνταγματικό Δικαστήριο (<i>Curtea Constituțională a României</i>), αριθ. 1258, 8 Οκτωβρίου 2009	373
Τσεχική Δημοκρατία, Συνταγματικό Δικαστήριο (<i>Ústavní soud České republiky</i>), 94/2011 Coll., 22 Μαρτίου 2011	373

Στο διαδίκτυο διατίθενται πολλές πληροφορίες σχετικά με τον Οργανισμό Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (FRA). Η πρόσβαση στις εν λόγω πληροφορίες είναι δυνατή μέσω του ιστότοπου του FRA, στη διεύθυνση fra.europa.eu.

Περαιτέρω πληροφορίες σχετικά με τη νομολογία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου διατίθενται στον ιστότοπο του Δικαστηρίου: echr.coe.int. Μέσω της πύλης αναζήτησης HUDOC εξασφαλίζεται πρόσβαση σε δικαστικές αποφάσεις στα αγγλικά και/ή στα γαλλικά, σε μεταφράσεις σε επιπλέον γλώσσες, σε νομικές περιλήψεις, δελτία Τύπου και άλλες πληροφορίες σχετικά με τις εργασίες του Δικαστηρίου (<http://hudoc.echr.coe.int/>).

Πώς θα προμηθευθείτε εκδόσεις του Συμβουλίου της Ευρώπης

Η Επιτροπή Εκδόσεων του Συμβουλίου της Ευρώπης καταρτίζει έργα σε όλους τους τομείς ενασχόλησης του Οργανισμού, συμπεριλαμβανομένων των ανθρωπίνων δικαιωμάτων, της νομικής επιστήμης, της υγείας, της δεοντολογίας, των κοινωνικών υποθέσεων, του περιβάλλοντος, της εκπαίδευσης, του πολιτισμού, του αθλητισμού, της νεολαίας και της αρχιτεκτονικής κληρονομιάς. Παραγγελίες βιβλίων και ηλεκτρονικών εκδόσεων από τον εκτενή κατάλογο μπορούν να πραγματοποιηθούν μέσω διαδικτύου (<http://book.coe.int/>).

Ένα εικονικό αναγνωστήριο επιτρέπει σε χρήστες να ανατρέχουν σε αποσπάσματα των βασικών έργων που έχουν μόλις δημοσιευτεί ή του πλήρους κειμένου ορισμένων επίσημων εγγράφων δωρεάν.

Πληροφορίες σχετικά με τις συμβάσεις του Συμβουλίου της Ευρώπης, καθώς και το πλήρες κείμενό τους, διατίθενται στον ιστότοπο του Γραφείου Συνθηκών: <http://conventions.coe.int/>

Επικοινωνήστε με την ΕΕ

Αυτοπροσώπως

Σε όλη την Ευρωπαϊκή Ένωση υπάρχουν εκατοντάδες κέντρα πληροφόρησης Europe Direct. Μπορείτε να βρείτε τη διεύθυνση του πλησιέστερου σε σας κέντρου στον ιστότοπο Europa: https://europa.eu/european-union/contact_el

Τηλεφωνικά ή μέσω ηλεκτρονικού ταχυδρομείου

Η Europe Direct είναι μια υπηρεσία που απαντά στις ερωτήσεις σας για την Ευρωπαϊκή Ένωση. Μπορείτε να επικοινωνήσετε με αυτήν την υπηρεσία:

- καλώντας ατελώς τον αριθμό 00 800 6 7 8 9 10 11 (ορισμένα δίκτυα τηλεφωνίας ενδέχεται να χρεώνουν τις κλήσεις αυτές),
- καλώντας τον αριθμό +32 22999696 ή
- μέσω ηλεκτρονικού ταχυδρομείου από τον ιστότοπο Europa: https://europa.eu/european-union/contact_el

Βρείτε πληροφορίες σχετικά με την ΕΕ

Στο διαδίκτυο

Πληροφορίες για την Ευρωπαϊκή Ένωση σε όλες τις επίσημες γλώσσες της ΕΕ είναι διαθέσιμες στον ιστότοπο Europa: https://europa.eu/european-union/index_el

Στις εκδόσεις της ΕΕ

Μπορείτε να καταφορτώσετε ή να παραγγείλετε δωρεάν και επί πληρωμή εκδόσεις της ΕΕ στην ακόλουθη διεύθυνση: <https://publications.europa.eu/el/publications>. Μπορείτε να ζητήσετε πολλαπλά αντίγραφα δωρεάν εκδόσεων επικοινωνώντας με την υπηρεσία Europe Direct ή με το τοπικό σας κέντρο πληροφόρησης (βλ. https://europa.eu/european-union/contact_el).

Στη νομοθεσία της ΕΕ και σε σχετικά έγγραφα

Για πρόσβαση σε νομικές πληροφορίες της ΕΕ, συμπεριλαμβανομένου του συνόλου της ενωσιακής νομοθεσίας από το 1951 σε όλες τις επίσημες γλώσσες, μεταβείτε στον ιστότοπο EUR-Lex, στην ακόλουθη διεύθυνση: <http://eur-lex.europa.eu>

Στα δημόσια δεδομένα από την ΕΕ

Η Πύλη Δημόσιων Δεδομένων της Ευρωπαϊκής Ένωσης (<http://data.europa.eu/euodp/el>) παρέχει πρόσβαση σε σύνολα δεδομένων από την ΕΕ. Τα δεδομένα μπορούν να καταφορτωθούν και να επαναχρησιμοποιηθούν δωρεάν, τόσο για εμπορικούς όσο και για μη εμπορικούς σκοπούς.

Η ραγδαία ανάπτυξη της τεχνολογίας των πληροφοριών έχει επιτείνει την ανάγκη για ισχυρή προστασία των δεδομένων προσωπικού χαρακτήρα. Το δικαίωμα στην εν λόγω προστασία διασφαλίζεται μέσω νομικών πράξεων τόσο της Ευρωπαϊκής Ένωσης (ΕΕ), όσο και του Συμβουλίου της Ευρώπης. Η διασφάλιση του σημαντικού αυτού δικαιώματος συνεπάγεται νέες και σημαντικές προκλήσεις, καθώς οι τεχνολογικές εξελίξεις επεκτείνουν τα όρια πεδίων όπως η παρακολούθηση, η υποκλοπή επικοινωνιών και η αποθήκευση δεδομένων. Το παρόν εγχειρίδιο έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να βοηθήσει τους επαγγελματίες του νομικού κλάδου που δεν είναι ειδικευμένοι στον τομέα της προστασίας δεδομένων να εξοικειωθούν με το αναδυόμενο αυτό πεδίο του δικαίου. Στο εγχειρίδιο αυτό παρέχεται επισκόπηση των ισχυόντων νομικών πλαισίων της ΕΕ και του Συμβουλίου της Ευρώπης. Επεξηγείται επίσης η βασική νομολογία, ενώ συνοψίζονται οι κυριότερες αποφάσεις τόσο του Δικαστηρίου της Ευρωπαϊκής Ένωσης, όσο και του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου. Επιπλέον, παρουσιάζονται υποθετικά σενάρια που χρησιμεύουν ως πρακτικά παραδείγματα για τα διάφορα ζητήματα που ανακύπτουν σε αυτόν τον εξελισσόμενο τομέα.

FRA – ΟΡΓΑΝΙΣΜΟΣ ΘΕΜΕΛΙΩΔΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ

Schwarzenbergplatz 11 – 1040 Βιέννη – Αυστρία

Τηλ. +43 158030-0 – Φαξ +43 158030-699

fra.europa.eu

facebook.com/fundamentalrights

linkedin.com/company/eu-fundamental-rights-agency

twitter.com/EURightsAgency

ΕΥΡΩΠΑΪΚΟ ΔΙΚΑΣΤΗΡΙΟ ΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ ΤΟΥ ΑΝΘΡΩΠΟΥ ΣΥΜΒΟΥΛΙΟ ΤΗΣ ΕΥΡΩΠΗΣ

67075 Strasbourg Cedex – Γαλλία

Τηλ. +33 (0) 388412018 – Φαξ +33 (0) 388412730

echr.coe.int – publishing@echr.coe.int

ΕΥΡΩΠΑΙΟΣ ΕΠΟΠΤΗΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Rue Wiertz 60 – 1047 Βρυξέλλες – Βέλγιο

Τηλ. +32 22831900

www.edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

ISBN 978-92-871-9831-0 (ΣτΕ)

ISBN 978-92-9474-295-7 (FRA)



Υπηρεσία Εκδόσεων
της Ευρωπαϊκής Ένωσης