ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

UNIVERSITY OF PIRAEUS

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΚΑΙΟ & ΟΙΚΟΝΟΜΊΑ

MASTER IN LAW & ECONOMICS

Διπλωματική εργασία:

«Ειδικά ζητήματα του δικαίου των προσωπικών δεδομένων»

Γεωργία Γιαννούση (ΜΔΟ 2207)

(Επιβλέπουσα καθηγήτρια: Αριστέα Σινανιώτη - Μαρούδη)

Πειραιάς, Ιούνιος 2024

Παράρτημα Β: Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΔΙΚΑΙΟ ΚΑΙ ΟΙΚΟΝΟΜΙΑ»

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, «Δίκαιο και Οικονομία» με τίτλο Ειδικά ζητήματα του δικαίου των προσωπικών δεδομένων
έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Μεταπτυχιακού Φοιτητή/τριας Υπογραφή

Ονοματεπώνυμο Γεωργία Γιαννούση

Ημερομηνία 05.06.2024

Στην οικογένεια μου

ΕΥΧΑΡΙΣΤΙΕΣ

Είναι σημαντικό στο σημείο αυτό να ευχαριστήσω εκείνους τους ανθρώπους, που διαδραμάτισαν σημαντικό ρόλο όχι μόνο κατά το στάδιο εκπόνησης της παρούσας μεταπτυχιακής διπλωματικής εργασίας, αλλά γενικότερα σε όλη τη διάρκεια του μεταπτυχιακού προγράμματος.

Αρχικά θα ήθελα να ευχαριστήσω την κα. Αριστέα Σινανιώτη - Μαρούδη τόσο για την ανάθεση του θέματος και την εμπιστοσύνη που μου έδειξε, όσο και για την επίβλεψη και καθοδήγηση της καθ' όλη τη διάρκεια της εκπόνησης της εργασίας.

Επιπλέον θα ήθελα να ευχαριστήσω όλους τους καθηγητές του μεταπτυχιακού προγράμματος για το πολύτιμο αυτό ταξίδι γνώσεως, που προσέφεραν κατά τη διάρκεια των μαθημάτων.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΛΗΨΗ

Το δίκαιο των προσωπικών δεδομένων και η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων, γνωστού και ως GDPR, αποτελεί το αντικείμενο της παρούσης εργασίας.

Στο πρώτο κεφάλαιο παρουσιάζεται ο ΓΚΠΔ, ο οποίος διαδραμάτισε καθοριστικό ρόλο στην αλλαγή της καθημερινότητας όχι μόνο των φυσικών προσώπων, αλλά και των επιχειρήσεων ωθώντας τους στην υιοθέτηση νέων συνηθειών και πρακτικών. Επιπλέον γίνεται αναφορά στο πως το εθνικό μας Σύνταγμα προστατεύει το δικαίωμα στα προσωπικά δεδομένα.

Στο δεύτερο κεφάλαιο της παρούσης δίνεται έμφαση σε ορισμένες ρυθμίσεις του Κανονισμού, οι οποίες παρουσιάζουν έντονο ενδιαφέρον και εισάγουν καινοτομίες σε σχέση με το προηγούμενο καθεστώς, ενώ ταυτόχρονα ενισχύουν την θέση των υποκειμένων των δεδομένων και παρέχουν μεγαλύτερο εύρος προστασίας. Πρόκειται για μία ανάλυση των δικαιωμάτων των υποκειμένων των δεδομένων κάνοντας ειδική μνεία στα δικαιώματα των παιδιών.

Στο τρίτο κεφάλαιο, έπειτα της ανάλυσης των αρχών που διέπουν των Κανονισμό, και ειδικά της αρχής της λογοδοσίας, η παρουσίαση της εθνικής Αρχής Προστασίας Προσωπικών Δεδομένων και το πως κάποιος μπορεί να προσφύγει σε αυτή.

Στο τέταρτο κεφάλαιο βρίσκονται κάποιες πρόσφατες αποφάσεις της εποπτικής αρχής, οι οποίες μας βοηθούν να κατανοήσουμε το πως εφαρμόζεται στην πράξη ο Κανονισμός και φυσικά πόσο αυστηρές είναι οι κυρώσεις που επιβάλλονται από την Αρχή Προστασίας Δεδομένων.

Τέλος στο δεύτερο μέρος της εργασίας γίνεται μία προσπάθεια, ώστε να γίνει αντιληπτή η παρουσία και τα οφέλη της εφαρμογής του σε διάφορους τομείς της ζωής μας, όπως στην εργασία, στον τομέα της υγείας και φυσικά στο διαδίκτυο που τόσο πολύ έχει επηρεάσει την καθημερινότητα μας και αποτελεί αναπόσπαστο μέρος της.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Άρθ.	Άρθρο
ΓΚΠΔ	Γενικός Κανονισμός Προστασίας Δεδομένων
ΔΕΕ	Δικαστήριο της Ευρωπαϊκής Ένωσης
ΕΔΔΑ	Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων
ΕΕ	Ευρωπαϊκή Ένωση
ΕΣΠΔ	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
Κλπ.	Και τα λοιπά
Παρ.	Παράγραφος
Π.χ.	Παραδείγματος χάρη
Ν.	Νόμος
Σ.	Σύνταγμα

ΕΙΣΑΓΩΓΗ

Οι άνθρωποι κατανόησαν από νωρίς την σπουδαιότητα της προστασίας των δικαιωμάτων τους έναντι οποιουδήποτε επιχειρούσε να τα παραβιάσει και να θέσει σε κίνδυνο τις ελευθερίες τους. Μεταξύ των βασικών δικαιωμάτων, που αντελήφθησαν, πως χρήζουν προστασίας, είναι και το δικαίωμα στην ιδιωτική ζωή. Στα φιλελεύθερα συνταγματικά κείμενα του 18ου αιώνα, αλλά και αργότερα στην Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου του Οργανισμού Ηνωμένων Εθνών (1948), καθώς επίσης και στην Ευρωπαϊκή Σύμβαση Δικαιωμάτων του Ανθρώπου, παρατηρείται η ανάγκη για αναγνώριση του δικαιώματος αυτού και οι προσπάθειες για την νομική του προστασία. Μάλιστα εμφανίζεται από τη δεκαετία του 1970 τόσο στην ευρωπαϊκή νομοθεσία, όσο και σε αυτή των Η.Π.Α., το δικαίωμα προστασίας δεδομένων προσωπικού χαρακτήρα ως εξειδίκευση του δικαιώματος στην ιδιωτική ζωή, διότι διαφαινόταν ήδη από εκείνη την χρονική περίοδο πως η εξέλιξη της τεχνολογίας εγκυμονούσε σοβαρούς κινδύνους για παραβίασης της ιδιωτικής ζωής.

Στην συνέχεια ακολούθησαν περαιτέρω νομικές ρυθμίσεις για την προστασία των προσωπικών δεδομένων, όπως για παράδειγμα η Διεθνής Σύμβαση 108[1], έως ότου φτάσουμε στην έκδοση της καθοριστικής για την προστασία των προσωπικών δεδομένων Οδηγίας 95/46/ΕΚ το 1995. Η Οδηγία αυτή αποτέλεσε ένα σταθμό – εθνικά και ευρωπαϊκά- για τη νομοθετική ρύθμιση των δεδομένων προσωπικού χαρακτήρα και η μεταφορά της στην εθνική έννομη τάξη κατέστη εφικτή με το Ν. 2472/1997.

Ποιο όμως ήταν το έρεισμα για την έκδοση της Οδηγίας 95/46/ΕΚ; Το δικαίωμα προστασίας προσωπικών δεδομένων ή δικαίωμα πληροφοριακού αυτοκαθορισμού (informationelles Selbstbestimmungsrecht) αναπτύχθηκε και προσδιορίστηκε κατά περιεχόμενο το 1983 από το Ομοσπονδιακό Συνταγματικό Δικαστήριο της Γερμανίας, στην απόφαση του για την απογραφή (Volkszählungsurteil), ως το δικαίωμα του καθενός να αποφασίζει ο ίδιος ή η ίδια ποιος, τι, από που και για ποιο σκοπό θα γνωρίζει γι' αυτόν. Όμως ο μη απόλυτος χαρακτήρας του ανωτέρω δικαιώματος, είχε ως αποτέλεσμα να οδηγήσει το Ομοσπονδιακό Δικαστήριο της Γερμανίας στην υιοθέτηση της άποψης, πως

[1] Η Σύμβαση αυτή, η οποία ρύθμιζε την προστασία του ατόμου από την αυτοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, τέθηκε σε ισχύ την 1/10/1985, ότε και συγκέντρωσε τις απαιτούμενες υπογραφές και κυρώσεις από εθνικά κράτη. Η χώρα μας την υπέγραψε στις 17/2/1983, κυρώθηκε με τον Ν. 2068/1992 και τέθηκε σε ισχύ από την 1/12/1995.

το άτομο οφείλει να κοινοποιεί πληροφορίες που το αφορούν, ειδικά σε περίπτωση προστασίας υπέρτερων γενικών συμφερόντων και ενώ η κοινοποίηση προβλέπεται ρητά σε συγκεκριμένη ρύθμιση που καθορίζει και τον σκοπό επεξεργασίας.

Οι σκέψεις αυτές επηρέασαν σημαντικά τόσο τον τρόπο θεωρητικής προσέγγισης και ανάλυσης του δικαιώματος των προσωπικών δεδομένων, όσο και τη σχετική νομοθεσία της Ευρωπαϊκής Ένωσης και την νομολογία του ΔΕΕ και ΕΔΔΑ, με αποτέλεσμα να διακρίνουμε τα πρώτα εμφανή αποτυπώματα της απόφασης αυτής στην Οδηγία 95/46/ΕΚ.[2]

Αξιοσημείωτο πως το δικαίωμα στα προσωπικά δεδομένα αναβαθμίστηκε στη συνέχεια με τη Συνθήκη της Λισαβόνας (2007)[3] αλλά και με τον Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης[4], δίνοντας με αυτόν τον τρόπο την ώθηση για τη διακήρυξη των βασικών αρχών προστασίας τους. Επιπλέον κατοχυρώθηκε ο κανόνας νομιμότητας επεξεργασίας των προσωπικών δεδομένων, καθώς και το δικαίωμα πρόσβασης και διόρθωσης. Παράλληλα επιβλήθηκε η εξασφάλιση του ελέγχου της προστασίας των προσωπικών δεδομένων από ανεξάρτητη αρχή.

Παρατηρείται πως σε κάθε στάδιο διαμόρφωσης των κανόνων δικαίου για την ενίσχυση της προστασίας των προσωπικών δεδομένων, το καθεστώς προστασίας γίνεται ολοένα και πιο αυστηρό, ενώ ταυτόχρονα διευρύνονται τα δικαιώματα των υποκειμένων των δεδομένων, παρέχοντας τους μεγαλύτερη ασφάλεια.

[2]Βλ. Γ. Λαζαράκος σε: Σ. Βλαχόπουλος, Θεμελιώδη δικαιώματα, Νομική Βιβλιοθήκη, 2017
[3] Αρ 16 ΣΛΕΕ
[4] Άρ. 8 Χάρτη Θεμελιωδών Δικαιωμάτων του Ανθρώπου.

ΚΕΦΑΛΑΙΟ 1ο

1.1 Το ισχύον νομοθετικό πλαίσιο

Η ραγδαία ανάπτυξη της τεχνολογίας σε συνδυασμό με την παγκοσμιοποιημένη οικονομία δημιούργησαν ένα διασυνδεδεμένο κόσμο, όπου δημόσιες αρχές, νομικά ή φυσικά πρόσωπα χρησιμοποιούν σε μεγάλο βαθμό αδιαλείπτως δεδομένα προσωπικού χαρακτήρα. Η δυνατότητα που παρείχαν οι νέες τεχνολογικές εξελίξεις για συλλογή και διακίνηση τέτοιου όγκου πληροφοριών, οι οποίες δύνανται να εκτίθενται στο διαδίκτυο, *έθεσε ως ζητούμενο να συμβαδίζει το δίκαιο με την τεχνολογία και να μην την ακολουθεί ασθμαίνοντας*[5]. Έτσι είκοσι χρόνια μετά την Οδηγία 95/46/ΕΚ, *ο νομοθέτης της Ένωσης αποφάσισε τη γενναία μεταρρύθμιση του καθεστώτος για τα προσωπικά δεδομένα*[6] και προέβη στην έκδοση του Κανονισμού 2016/679[7]. Μάλιστα κάθε άλλο παρά τυχαία ήταν η επιλογή του νομοθέτη, το νέο κείμενο να έχει τη μορφή ενός Κανονισμού, *που θα τυγχάνει άμεσης και συνακόλουθα ομοιόμορφης και πιο συνεκτικής εφαρμογής από τα κράτη-μέλη, και όχι μίας Οδηγίας, που θα απαιτεί την ενσωμάτωση της από τα κράτη-μέλη με νόμο*[8].

Ο Κανονισμός 679 (Γενικός Κανονισμός για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα «ΓΚΠΔ» ή "GDPR", general data protection regulation)

---

[5]Βλ. Φ.Παναγοπούλου-Κουτνατζή, σε: Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

[6] Γ. Δελλής, Για μία αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016, ΕφημΔΔ 1/2017.2

[7] Κανονισμός 679/2016 (ΕΕ) του Ευρωπαϊκού Συμβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (Γενικός Κανονισμός για την Προστασία Δεδομένων). Τον Κανονισμό αυτό συμπληρώνουν, για ειδικότερα ζητήματα, η 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, καθώς και η 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.

[8] Στην πραγματικότητα ο Κανονισμός αυτός έχει πολλά χαρακτηριστικά Οδηγίας, διότι αναγνωρίζεται η διακριτική ευχέρεια στον εθνικό νομοθέτη για υιοθέτηση συγκεκριμένων επιλογών, π.χ. σχετικά με τη χορήγηση αδειών επεξεργασίας ειδικών κατηγοριών δεδομένων (αρ. 36παρ. 5Κ)

καθορίζει το ρυθμιστικό πλαίσιο των δεδομένων προσωπικού χαρακτήρα, διασαφηνίζοντας την όποια ασάφεια της έως τότε νομοθεσίας. Αποτελείται από 99 άρθρα και η έκταση του είναι πολύ μεγαλύτερη από εκείνη της ισχύσασας Οδηγίας. Η δημιουργία περισσότερων ρυθμίσεων στοχεύει στην βελτιωμένη προστασία των υποκειμένων των δεδομένων μέσω της διεύρυνσης των δικαιωμάτων τους, όπως με το δικαίωμα στη φορητότητα, τη διόρθωση, τη λήθη και την εναντίωση. Παράλληλα ενισχύει τον εποπτικό και ελεγκτικό χαρακτήρα των Αρμόδιων Αρχών Προστασίας Δεδομένων, προσφέροντας ως εργαλείο μια ενιαία νομοθεσία και θεσμοθετώντας υψηλές ποινές και πρόστιμα για τις περιπτώσεις μη συμμόρφωσης. Πιο συγκεκριμένα, οι παραβάσεις του Κανονισμού μπορεί να οδηγήσουν από συστάσεις, όταν αφορούν σε ελάσσονος σημασίας περιστατικά, μέχρι και διοικητικά πρόστιμα που ανέρχονται στα 10-20 εκατ. ευρώ ή σε περίπτωση επιχειρήσεων στο 2%-4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου έτους, ανάλογα με το ποιο είναι υψηλότερο.

Περαιτέρω είναι σημαντικό πως ο ΓΚΠΔ καθιερώνει την υποχρέωση των Υπεύθυνων Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα να παρέχουν διαφανείς και εύκολα προσβάσιμες πληροφορίες στα υποκείμενα των δεδομένων όσον αφορά στην επεξεργασία των δεδομένων τους, ενώ ταυτόχρονα προβλέπει συγκεκριμένα χρονικά περιθώρια ενημέρωσης αφενός της Αρχής Προστασίας, και αφετέρου των υποκειμένων των δεδομένων σε περίπτωση που υπάρξει κάποιο περιστατικό διαρροής αυτών [9].

Η εφαρμογή του εκκίνησε από την 25η Μαΐου 2018, σύμφωνα με τα οριζόμενα στο άρθρο 99 παρ. 2, παρότι θεσπίστηκε το 2016, καθώς είχε προβλεφθεί διετής μεταβατική περίοδος, ώστε να δοθεί στα κράτη μέλη ο απαραίτητος χρόνος για να προετοιμαστούν για το νέο καθεστώς.

Μετά την έναρξη εφαρμογής του Γενικού Κανονισμού για την προστασία των Δεδομένων Προσωπικού Χαρακτήρα της Ευρωπαϊκής Ένωσης, ψηφίστηκε και τέθηκε σε ισχύ, στην εθνική έννομη τάξη, ο Ν.4624/2019[10].Ο εν λόγω νόμος στοχεύει στην αντικατάσταση του νομοθετικού πλαισίου, που ρυθμίζει τη συγκρότηση και λειτουργία της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στη λήψη μέτρων

[9] Α. Σιανιώτη-Μαρούδη, Ασφαλιστικό Δίκαιο, Νομική Βιβλιοθήκη, 2017
[10] Νόμος υπ' αριθμ. 4624, τεύχος Α' 137/29.08.2019.

εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Καν. 2016/679) και στην ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (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.[11]

Ο Ν.4624/2019 αντικατέστησε τον προϊσχύσαντα Ν. 2472/1997 πλήρως. Εξαίρεση αποτελούν ορισμένες διατάξεις, που εξακολουθούν να βρίσκονται σε ισχύ με ρητή πρόβλεψη του νέου νόμου.

Συμπλήρωση και εξειδίκευση του θεσμικού πλαισίου της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών αποτελεί ο Ν. 3471/2006, ο οποίος ενσωματώνει την Οδηγία 2002/58/ΕΚ (Οδηγία e-Privacy), όπως αυτή έχει τροποποιηθεί με την Οδηγία 2009/136/ΕΚ[12].

1.2 Συνταγματική κατοχύρωση (9^{α})

Με την αναθεώρηση του Συντάγματος το 2001 κατοχυρώθηκε για πρώτη φορά ρητά στο Σύνταγμα το δικαίωμα στην προστασία των προσωπικών δεδομένων, αποτελώντας μία επιπλέον προσπάθεια εναρμόνισης, της εθνικής έννομης τάξης, με το δίκαιο της Ε.Ε. σε ό,τι αφορά τα προσωπικά δεδομένα και τον τρόπο προστασίας τους. Συγκεκριμένα το άρθρο 9^{Α} ορίζει ότι : « Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.»

Το δικαίωμα στην προστασία των προσωπικών δεδομένων δεν αποτελεί όμως ένα νέο δικαίωμα, το οποίο δημιούργησε η αναθεώρηση του 2001. Στην πραγματικότητα η

[11] Β.-Α. Κόλλιας, Προβληματικές διατάξεις του ελληνικού νόμου για τα δεδομένα προσωπικού χαρακτήρα. Ο Ν.4624/2019 και η σχέση του με τον Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Αρμ 3-4/2019.265

[12] Βλ. https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpikon_dedomenon

αναθεώρηση επέφερε την τυποποίηση ενός δικαιώματος που έως τότε είχε νομική βάση είτε στο άρθρο 9 παρ. 1 είτε στο άρθρο 5 του Σ, είτε σε συνδυασμό αυτών.[13]

Φορείς του δικαιώματος αυτού, όπως προκύπτει από τη διατύπωση της διάταξης του άρθρου 9Α, είναι όλα τα φυσικά πρόσωπα, όχι δηλαδή μόνο Έλληνες πολίτες, αλλά και οι αλλοδαποί και οι ανιθαγενείς. Οι ανωτέρω προστατεύονται από οποιαδήποτε αθέμιτη επεξεργασία των προσωπικών τους δεδομένων, είτε στην περίπτωση που η επεξεργασία πραγματοποιείται από οιονδήποτε φορέα του δημοσίου, είτε αν η επεξεργασία συντελείται από κάποιον ιδιωτικό φορέα.

ΚΕΦΑΛΑΙΟ 2Ο

2.1 Δεδομένα προσωπικού χαρακτήρα

Τα δεδομένα προσωπικού χαρακτήρα συνιστούν πληροφορίες, που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο.[14] Ένας σαφής και απλός ορισμός των προσωπικών δεδομένων δίνεται στο άρθρο 4 παράγραφος 1 του Κανονισμού , περιγράφοντάς τα ως: «κάθε πληροφορία που σχετίζεται με ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (ή «υποκείμενο δεδομένων») που μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό όπως ένα όνομα, έναν αριθμό αναγνώρισης, δεδομένα τοποθεσίας, ένα διαδικτυακό αναγνωριστικό ή σε έναν ή περισσότερους παράγοντες που αφορούν τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικό πρόσωπο».

Είναι πραγματικά εντυπωσιακό πως μπορεί κάποιος να ανακαλύψει την ταυτότητα ενός ατόμου και να λάβει γνώση ή ακόμη και να δημοσιοποιήσει τόσο σημαντικά στοιχεία αυτού, προκαλώντας του διάφορες ανεπιθύμητες καταστάσεις. Αυτό όμως δεν χρειάζεται να δημιουργεί έντονες ανησυχίες στα άτομα για την ασφάλεια της ιδιωτικότητας τους, γιατί ο ΓΚΠΔ έχει θεσπίσει ένα ισχυρό πλαίσιο προστασίας των δεδομένων. Ο Κανονισμός δίνει τη δυνατότητα, μέσω των ρυθμίσεων, που προβλέπει, ώστε τα υποκείμενα των δεδομένων να ελέγχουν τη συλλογή αυτών των πληροφοριών

[13]Γ. Λαζαράκος σε: Σ. Βλαχόπουλος, Θεμελιώδη δικαιώματα, Νομική Βιβλιοθήκη, 2017
[14] https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_el

και την επεξεργασία τους από τρίτους. Με άλλα λόγια, τα άτομα έχουν δικαιώματα και ελευθερίες και δύνανται να αποφασίζουν αν και σε ποιο βαθμό επιθυμούν να παραχωρήσουν πρόσβαση στις πληροφορίες, που τα αφορούν. Εξάλλου έχουν τη δυνατότητα ανά πάσα στιγμή να ζητήσουν τη διαγράφη των δεδομένων τους.

Ορισμένα προσωπικά δεδομένα είναι ιδιαίτερα σημαντικά για τον ΓΚΠΔ (Καν. ΕΕ 2016/679) και ταξινομούνται στις ακόλουθες κατηγορίες:

- **δεδομένα άμεσης αναγνώρισης**, όπως όνομα και επώνυμο ή βιομετρικά στοιχεία
- **έμμεσα δεδομένα αναγνώρισης**, όπως διευθύνσεις IP, αριθμοί κινητών τηλεφώνων ή σειριακούς κωδικούς·
- **ευαίσθητα δεδομένα**, τα οποία αποκαλύπτουν συγκεκριμένες κατηγορίες πληροφοριών όπως καταγωγή, θρησκευτικές πεποιθήσεις, πολιτικές απόψεις, πληροφορίες για την υγεία, σεξουαλικό προσανατολισμό κ.λπ.
- **δικαστικά δεδομένα**, τα οποία επαληθεύουν την ύπαρξη ορισμένων δικαστικών μέτρων που υπόκεινται σε εγγραφή στο ποινικό μητρώο, όπως οριστικά μέτρα ποινικής καταδίκης και εναλλακτικά μέτρα κράτησης.

Σχετικά με την άμεση ταυτοποίηση των υποκειμένων αξιοσημείωτη είναι η άποψη της ιταλικής προστασίας δεδομένων «Garante», η οποία το 2014 στις «Οδηγίες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, που περιέχονται επίσης σε διοικητικές πράξεις και έγγραφα, που διενεργούνται για λόγους διαφήμισης και διαφάνειας στο διαδίκτυο από δημόσιους φορείς και άλλους υπόχρεους φορείς»[15] διευκρίνισε ότι «η πρακτική που ακολουθείται από ορισμένες διοικήσεις της αντικατάστασης του ονόματος και του επωνύμου του ενδιαφερόμενου μόνο με αρχικά είναι από μόνη της ανεπαρκής για την ανωνυμοποίηση των προσωπικών δεδομένων που περιέχονται στους τίτλους και τα έγγραφα που δημοσιεύονται στο διαδίκτυο» και ότι « Ο κίνδυνος αναγνώρισης του ενδιαφερομένου είναι ακόμη πιο πιθανός όταν, μεταξύ άλλων, παράλληλα με τα αρχικά του ονόματος και του επωνύμου, παραμένουν περαιτέρω

[15] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436

συμφραζόμενες πληροφορίες που ούτως ή άλλως καθιστούν το ενδιαφερόμενο μέρος αναγνωρίσιμο».

2.2 Δικαιώματα των υποκείμενων των δεδομένων

Τα υποκείμενα των δεδομένων έχουν μια σειρά από δικαιώματα που κατοχυρώνονται στο τρίτο κεφάλαιο του ΓΚΠΔ (άρθρα 12-23), το οποίο τιτλοφορείται ως «δικαιώματα του υποκειμένου των δεδομένων» και διακρίνεται σε πέντε τμήματα. Τα δικαιώματα, που προβλέπονται στο παρόν κεφάλαιο, θωρακίζονται με την πρόβλεψη αποτελεσματικών κυρώσεων σε περίπτωση μη συμμόρφωσης του υπεύθυνου επεξεργασίας με τις υποχρεώσεις του ως προς αυτά (άρθρο 83 παρ. 5 στοιχ. γ΄ ΓΚΠΔ)[16].

Το πρώτο τμήμα του εν λόγω κεφαλαίου έχοντας τίτλο *«διαφάνεια και ρυθμίσεις»* περιλαμβάνει το άρθρο 12, το οποίο ρυθμίζει το πλαίσιο εντός του οποίου ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15 έως 22 και του άρθρου 34 σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά. Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα, και αν ενδείκνυται, ηλεκτρονικώς. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται και προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα.[17]

Στο δεύτερο τμήμα του αυτού κεφαλαίου *(«ενημέρωση και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα»)* περιλαμβάνονται τα άρθρα 13 και 14, τα οποία θεμελιώνουν το **δικαίωμα στην πληροφόρηση**. Πιο συγκεκριμένα το άρθρο 13 προβλέπει το δικαίωμα πληροφόρησης στη περίπτωση, κατά την οποία τα προσωπικά δεδομένα συλλέγονται απευθείας από το υποκείμενο των δεδομένων, ενώ στο άρθρο 14 ρυθμίζεται η περίπτωση που τα δεδομένα συλλέγονται από έτερη πηγή.

Στο τμήμα αυτό προβλέπεται και ένα ακόμη δικαίωμα, το οποίο συναντάται στο άρθρο 15 και θεμελειώνει το **δικαίωμα της πρόσβασης** του υποκειμένου των

[16] Ι. Ιγγλεζάκης, Το δίκαιο της ψηφιακής οικονομίας, 2022, σ. 84
[17] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679

δεδομένων. Ειδικότερα το δικαίωμα πρόσβασης επιτρέπει στο υποκείμενο των δεδομένων να λαμβάνει γνώση των δεδομένων του και των πληροφοριών για την επεξεργασία, για να είναι σε θέση να επαληθεύει τη νομιμότητά της. Σημαντικό δε πως το δικαίωμα αυτό δεν χρήζει αιτιολόγησης από το υποκείμενο των δεδομένων.[18]

Έπειτα, στο τρίτο τμήμα του τρίτου κεφαλαίου του Κανονισμού υφίστανται τα δικαιώματα του υποκειμένου που σχετίζονται με τη δυνατότητα διόρθωσης ή διαγραφής των δεδομένων. Αρχικά κατά ρητή επιταγή το άρθρο 16 θεμελιώνει το **δικαίωμα διόρθωσης** και επιτρέπει στο υποκείμενο των δεδομένων να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση την διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα. Επιπρόσθετα παρέχεται η δυνατότητα σε αυτό να απαιτήσει την συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.[19]

Αντίθετα, στο άρθρο 17 του Κανονισμού καθορίζεται το **δικαίωμα διαγραφής** ή άλλως **δικαίωμα της λήθης**, το οποίο επιτρέπει στο υποκείμενο των δεδομένων να απαιτήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα, που το αφορούν και τη μη περαιτέρω διάδοση τους, ιδίως σε σχέση με δεδομένα, τα οποία διατέθηκαν από το συγκεκριμένο πρόσωπο κατά την παιδική του ηλικία, εάν: α) τα δεδομένα δεν είναι πλέον απαραίτητα σε σχέση με το σκοπό της συλλογής ή επεξεργασίας, β) το πρόσωπο στο οποίο αναφέρονται τα δεδομένα αποσύρει τη συγκατάθεσή του στην επεξεργασία τους ή το χρονικό διάστημα αποθήκευσης για το οποίο παρασχέθηκε συγκατάθεση έληξε, γ) το υποκείμενο των δεδομένων αντιτάσσεται στην επεξεργασία κατά τα οριζόμενα στο άρθρο 19 § 1 και δεν υπάρχουν υπέρτεροι λόγοι που να συνηγορούν υπέρ της επεξεργασίας ή το υποκείμενο των δεδομένων αντιτίθεται στην επεξεργασία δεδομένων σύμφωνα με το άρθρο 19 § 2 ή έχουν τύχει παρανόμως επεξεργασίας ή τα δεδομένα πρέπει να διαγραφούν με σκοπό τη συμμόρφωση με μια νομική υποχρέωση του δικαίου της Ένωσης ή του κράτους μέλους ή τα δεδομένα συλλέχθηκαν για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας σε παιδιά σύμφωνα με το άρθρο 8 § 1[20].

[18] https://www.dpa.gr/el/polites/gkpd/dikaiwma_prosvasis_upokeimenou
[19] https://www.dpa.gr/index.php/el/polites/gkpd/dikaiwma_diorthwsis
[20] Ι. Ιγγλεζάκης, Δίκαιο της πληροφορικής - Συμπλήρωμα, 2016, σ. 34 = sakkoulas-online και βλ. Προοίμιο κανονισμού σκέψη 65

Περαιτέρω, στο άρθρο 18 προβλέπεται το **δικαίωμα του περιορισμού της επεξεργασίας των δεδομένων**. Όπως ρητώς ορίζεται στο εν λόγω άρθρο τα φυσικά πρόσωπα, τα υποκείμενα των δεδομένων, δύνανται να ζητήσουν τον περιορισμό της επεξεργασίας των δεδομένων τους. Ειδικότερα το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο να περιορίσει την επεξεργασία. Φυσικά το δικαίωμα αυτό είναι εναλλακτικό του δικαιώματος διαγραφής (άρθρο 16 του ΓΚΠΔ) και του δικαιώματος εναντίωσης (άρθρο 21 του ΓΚΠΔ).

Το **δικαίωμα της εναντίωσης**, το οποίο θεμελιώνεται παρακάτω στο άρθρο 21 του Κανονισμού και βρίσκεται στο τέταρτο τμήμα του εξεταζόμενου κεφαλαίου, συνίσταται στο δικαίωμα που έχει το φυσικό πρόσωπο να αντιτάσσεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έτσι λοιπόν σε περίπτωση που το υποκείμενο των δεδομένων εναντιωθεί στην επεξεργασία των προσωπικών του δεδομένων, ο υπεύθυνος επεξεργασίας οφείλει να σταματήσει την εν λόγω επεξεργασία εκτός και αν καταδείξει επιτακτικούς και νόμιμους λόγους για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων, των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων ή καθίσταται απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.[21]

Σε κάθε περίπτωση, βάσει των όσων ορίζονται στο άρθρο 19 του Κανονισμού, «*ο υπεύθυνος επεξεργασίας ανακοινώνει κάθε διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων που διενεργείται σύμφωνα με το άρθρο 16, το άρθρο 17 παράγραφος 1 και το άρθρο 18 σε κάθε αποδέκτη στον οποίο γνωστοποιήθηκαν τα δεδομένα προσωπικού χαρακτήρα, εκτός εάν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια. Ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων σχετικά με τους εν λόγω αποδέκτες, εφόσον αυτό ζητηθεί από το υποκείμενο των δεδομένων*».[22]

Τέλος στο άρθρο 20 συναντάμε μία καινοτομία του Κανονισμού, η οποία αφορά στο **δικαίωμα φορητότητας** των δεδομένων από έναν πάροχο υπηρεσίας σε έναν άλλο. Το σχετικό δικαίωμα συνίσταται στη δυνατότητα του υποκειμένου των δεδομένων να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα, που το αφορούν και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και

[21] https://www.dpa.gr/index.php/el/polites/gkpd/dikaiwma_enadiosis
[22] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679

αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο, και να τα διαβιβάζει χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας σε άλλον υπεύθυνο επεξεργασίας, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα διενεργείται με αυτοματοποιημένα μέσα. Η διαβίβαση θα γίνεται απευθείας από τον έναν πάροχο στον άλλο και όχι μέσω του υποκειμένου των δεδομένων.[23]

Αξιοσημείωτο δε πως το δικαίωμα στη φορητότητα εισάγεται στο δίκαιο προστασίας δεδομένων προσωπικού χαρακτήρα ως δάνειο από το δίκαιο του ανταγωνισμού σκοπεύοντας στην ελεύθερη διακίνηση των δεδομένων τηρουμένων πάντοτε των προϋποθέσεων ασφάλειας αυτών και σεβασμού των δικαιωμάτων των τρίτων.[24]

2.3 Συγκατάθεση του υποκειμένου

Η συγκατάθεση του υποκειμένου αποτελεί προϋπόθεση μίας σύννομης επεξεργασίας δεδομένων, την οποία μάλιστα ο εκάστοτε υπεύθυνος επεξεργασίας θα πρέπει να είναι σε θέση να αποδείξει. Θέτοντας ο ΓΚΠΔ αυστηρούς κανόνες για την επεξεργασία δεδομένων βάσει συγκατάθεσης, αποσκοπεί στο να διασφαλιστεί, ότι το υποκείμενο των δεδομένων κατανοεί για τι πραγματικά έχει δώσει τη συγκατάθεσή του.[25] Ειδικότερα τα υποκείμενα των δεδομένων θα πρέπει να παρέχουν την συγκατάθεση τους με σαφή θετική ενέργεια, η οποία συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επίγνωσει ένδειξη συμφωνίας του υποκειμένου των δεδομένων υπέρ της επεξεργασίας δεδομένων, που το αφορούν. Αυτό θα μπορούσε να συμβεί για παράδειγμα με γραπτή δήλωση, μεταξύ άλλων, με ηλεκτρονικά μέσα ή με προφορική δήλωση. Επομένως σε καμία περίπτωση η σιωπή ή η αδράνεια δεν θα πρέπει να λαμβάνονται ως συγκατάθεση. Η συγκατάθεση θα πρέπει να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς. Εάν όμως η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει υποχρεωτικά να παρέχεται συγκατάθεση για όλους αυτούς τους σκοπούς.[26]

[23] Φ. Παναγοπούλου-Κουτνατζή, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, 2017, σ. 122
[24] Φ. Παναγοπούλου-Κουτνατζή, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, 2017, σ. 122
[25] https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm#shortcut-10
[26] Προοίμιο Κανονισμού σκέψη 32

Σημαντικό δε πως η συγκατάθεση του υποκειμένου δεν θα πρέπει να 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 την συγκατάθεση του χωρίς να ζημιωθεί.[27]

Επιπρόσθετα για τη νομιμότητα της συγκατάθεσης του υποκειμένου διαδραματίζει σημαντικό ρόλο **η αρχή της διαφάνειας**, η οποία συγκαταλέγεται στις θεμελιώδεις αρχές του Κανονισμού. Σύμφωνα με την αρχή αυτή απαιτείται οποιαδήποτε ενημέρωση, που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση και πλέον κατά περίπτωση απεικόνιση. Αυτό έχει ιδιαίτερη σημασία σε περιπτώσεις στις οποίες η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το υποκείμενο των δεδομένων να γνωρίζει και να κατανοεί εάν, από ποιόν, και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα, που το αφορούν, όπως την περίπτωση της επιγραμμικής διαφήμισης[28]. Ένεκα τούτου ο υπεύθυνος επεξεργασίας θα πρέπει να παρέχει στο υποκείμενο των δεδομένων κάθε περαιτέρω πληροφορία που είναι αναγκαία για τη διασφάλιση της δίκαιης και διαφανούς επεξεργασίας[29].

Στην εικόνα που ακολουθεί παρουσιάζονται συνοπτικά, αλλά πλήρως κατανοητά το τι απαιτείται για την συγκατάθεση του ατόμου, αλλά και τι δεν συνιστά την έκφραση συγκατάθεσης εκ μέρους τους:

[27] Προοίμιο κανονισμού σκέψη 42
[28] Προοίμιο κανονισμού σκέψη 58
[29] Προοίμιο Κανονισμού σκέψη 60

30

2.4 Προστασία των δικαιωμάτων του παιδιού

Ο Κανονισμός, όπως αναφέρθηκε και ανωτέρω, πέτυχε την κατοχύρωση πολλαπλών δικαιωμάτων των υποκειμένων των δεδομένων, πετυχαίνοντας ταυτοχρόνως αρκετές καινοτομίες, ενισχύοντας με τον τρόπο αυτό το αίσθημα της ασφάλειας της ιδιωτικότητας. Ένα από τα σημαντικότερα επιτεύγματα του ΓΚΠΔ αποτέλεσε η ενίσχυση της προστασίας των παιδιών. Όπως καθίσταται εύκολα κατανοητό τα παιδιά χρήζουν ιδιαίτερης προστασίας κατά την επεξεργασία προσωπικών τους δεδομένων, κυρίως, για τον λόγο ότι δεν γνωρίζουν τους κινδύνους, που ενδεχομένως, συνεπάγεται η επεξεργασία αυτή.[31]

Η προστιθέμενη αξία του Κανονισμού στον τομέα της προστασίας της παιδικής ηλικίας συνίσταται στην απαίτηση, που προβλέπεται ρητά στο άρθρο 8, της λήψεως ή

[30] lawspot.gr/sites/default/files/images/nea/misc/consent.png?lspt_context=gdpr
[31] Βλ https://www.dpa.gr/el/polites/prostasia

εγκρίσεως της συγκαταθέσεως από τους ασκούντες τη γονική μέριμνα για την επεξεργασία προσωπικών δεδομένων παιδιών ηλικίας έως δεκαέξι ετών.[32]

Έτσι, λοιπόν, τα παιδιά άνω των 16 ετών έχουν δικαίωμα να υποβάλουν έγκυρα τη συγκατάθεσή τους, ενώ για τα παιδιά κάτω των 16 ετών η συγκατάθεση δίνεται από εκείνον, που έχει τη γονική μέριμνα, δηλαδή τον γονέα ή τον κηδεμόνα. Ο υπεύθυνος επεξεργασίας οφείλει να καταβάλει κάθε εύλογη προσπάθεια για την εξακρίβωση της ηλικίας και την επαλήθευση της ταυτότητας αυτού που δίνει τη συγκατάθεση στην περίπτωση που πρόκειται για παιδί κάτω των 16 χρόνων. Ωστόσο τα κράτη μέλη έχουν τη δυνατότητα να προβλέπουν με νόμο μικρότερο όριο ηλικίας για τους εν λόγω σκοπούς, υπό την βασική προϋπόθεση ότι η ηλικία αυτή δεν είναι κάτω από τα 13 έτη.[33]

Μία σημαντική εξαίρεση στο ζήτημα της νομιμότητας της συγκατάθεσης των παιδιών, προβλέπεται στη σκέψη 38, και ορίζει πως δεν τίθεται ως απαραίτητη προϋπόθεση η συγκατάθεση του γονέα ή κηδεμόνα σε συνάρτηση με υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε ένα παιδί. Αν για παράδειγμα, ένα παιδί θέλει να καταγγείλει μία πράξη κακοποιήσεως, όπως καθίσταται εύλογο, δεν θα απαιτείται η λήψη συγκαταθέσεως από τους ασκούντες τη γονική μέριμνα.

Επιπρόσθετα στην σκέψη 58 του Κανονισμού ορίζεται πως «*δεδομένου ότι τα παιδιά χρήζουν ειδικής προστασίας, κάθε ενημέρωση 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.»*. Συνεπώς είναι καθοριστικής σημασίας για την διαπίστωση της σύννομης παραχώρησης συγκατάθεσης εκ μέρους του υποκειμένου η σαφής, ακριβής και κατανοητή διατύπωση, ανεξάρτητα με την ηλικιακή ομάδα, που αυτό ανήκει.

Περαιτέρω η απαγόρευση εκμετάλλευσης της αδυναμίας κατανόησης ή της εν γένει αδύναμης θέσης στην οποία εκ των πραγμάτων τα παιδιά βρίσκονται, προβλέπεται ρητά και στην περίπτωση που καταρτίζεται προφίλ για παιδιά. Από τον Κανονισμό

[32] Βλ. Φ.Παναγοπούλου-Κουτνατζή, σε: Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

[33] https://www.dpa.gr/el/polites/prostasia

προκύπτει πως ο υπεύθυνος επεξεργασίας είναι και στην περίπτωση αυτή υποχρεωμένος να παρέχει σαφείς πληροφορίες αναφορικά με την επεξεργασία των δεδομένων τους.

Εξάλλου απαγορεύεται η κατάρτιση προφίλ για παιδιά για σκοπούς εμπορικής προώθησης. Ο υπεύθυνος επεξεργασίας οφείλει να σέβεται το απόλυτο δικαίωμα του παιδιού να εναντιωθεί σε μια τέτοια ενέργεια του υπευθύνου, που σχετίζεται με την απευθείας εμπορική προώθηση και να τη σταματήσει αμέσως μόλις του ζητηθεί.

Στα πλαίσια της ιδιαίτερης και διευρυμένης προστασίας των παιδιών κατοχυρώνεται ένα πιο ενισχυμένο δικαίωμα διαγραφής (λήθης) για τα παιδιά στη σκέψη 65 του Προοιμίου το οποίο όμως δεν κατοχυρώνεται στο άρθρο 17 του Κανονισμού, σχετικά με το δικαίωμα στη λήθη.[34]

Σε κάθε περίπτωση η προσπάθεια για την προστασία των παιδιών δεν θα πρέπει να εμποδίζει την ελευθέρια του λόγου και το δικαίωμα στην ελεύθερη ανάπτυξη στην προσωπικότητα. Το διαδίκτυο αποτελεί πράγματι έναν αχανή χώρο, όπου ελλοχεύουν αρκετοί κίνδυνοι, αποτελεί όμως ταυτόχρονα μία αστέρευτη πηγή γνώσης και επικοινωνίας, την οποία τα παιδιά ορθά και με σύνεση μπορούν να μάθουν να χρησιμοποιούν.

2.5 Η συγκατάθεση ανήλικου

Μελετώντας κάποιος αφενός τον Κανονισμό (άρθρο 8) και αφετέρου τον Ν. 4624/2019 (άρθρο 21) διαπιστώνει την ύπαρξη διακριτικής ευχέρειας σε ότι αφορά τα ηλικιακά όρια των ανήλικων για την εγκυρότητα της συγκατάθεσης τους. Παρότι ο Κανονισμός απαιτεί για τους κάτω των 16 η συγκατάθεση να δίνεται από τους ασκούντες την γονική μέριμνα, δηλαδή τον γονέα ή τον κηδεμόνα, δίνει τη ίδια στιγμή την ευχέρεια στα κράτη να θεσπίζουν ηλικιακά όρια χαμηλότερα από αυτά που ο ίδιος ο Κανονισμός προβλέπει. **Επομένως προκύπτει εύλογα το ερώτημα για το τι θα συμβεί εάν ορισμένα κράτη διατηρούν το προβλεπόμενο από τον Κανονισμό κατώτερο ηλικιακό όριο των 16 ετών και εάν κάποια άλλα κράτη επιλέξουν διαφορετικά κατώτερα ηλικιακά όρια.**

[34] Βλ. Φ.Παναγοπούλου-Κουτνατζή, σε: Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

Έστω ότι έχουμε την περίπτωση ενός ανηλίκου 15 ετών, προερχόμενου από κράτος μέλος της ΕΕ, το οποίο διατηρεί το κατώτερο ηλικιακό όριο των 16 ετών. Ο ανήλικος αυτός τυγχάνει να επισκεφθεί μία ελληνική ιστοσελίδα και να δώσει την συγκατάθεση του για την επεξεργασία των δεδομένων του. Στη χώρα μας η επεξεργασία δεδομένων προσωπικού χαρακτήρα ανηλίκου είναι σύννομη, εφόσον ο ανήλικος έχει συμπληρώσει το 15ο έτος της ηλικίας του και παρέχει τη συγκατάθεσή του. Για την χώρα προέλευσης του όμως αυτή η συγκατάθεση θα έπρεπε για να είναι σύννομη να δοθεί από τον γονέα ή τον κηδεμόνα του και όχι από τον ίδιο.

Πράγματι, σύμφωνα με τον Έλληνα νομοθέτη στην ηλικία των 15 ετών επέρχεται η «ψηφιακή ενηλικίωση». Ωστόσο αυτό ισχύει για τους προερχόμενους από την Ελλάδα επισκέπτες της εκάστοτε ιστοσελίδας, ενώ για τους εκτός Ελλάδος επισκέπτες, στα κράτη των οποίων δεν υπάρχει νομοθετική ρύθμιση για το ηλικιακό όριο, εφαρμόζεται ο Κανονισμός, ο οποίος ως ενωσιακό δίκαιο υπερέχει έναντι των εθνικών νόμων.

Στην περίπτωση βέβαια που η νομοθεσία του κράτους προέλευσης του επισκέπτη προβλέπει ηλικιακό όριο ίσο ή μικρότερο των 15 ετών, τότε θα ισχύει το όριο των 15 ετών λόγω του Ν. 4624/2019.

Επομένως στη φόρμα συλλογής δεδομένων της ιστοσελίδας θα πρέπει να αναγράφεται το ακόλουθο κείμενο:
«*Έχω διαβάσει τους <u>όρους χρήσης</u> (με σύνδεσμο προς τους όρους χρήσης) του παρόντος διαδικτυακού τόπου και τους αποδέχομαι πλήρως*» και στους όρους χρήσης υποχρεωτικά να αναγράφεται σε μία παράγραφο:
«Ο επισκέπτης (χρήστης της υπηρεσίας) δηλώνει πως είναι κάτοικος Ελλάδας με ηλικία άνω των 15 ετών ή κάτοικος εξωτερικού με ηλικία άνω των 15 ετών και, βάσει της νομοθεσίας της χώρας προέλευσής του, είναι σε θέση να συναινέσει στην επεξεργασία των προσωπικών του δεδομένων».

ΚΕΦΑΛΑΙΟ 3Ο

3.1 Οι αρχές του ΓΚΠΔ

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων βασίζεται σε μια σειρά από αρχές, οι οποίες διασφαλίζουν τη συμμόρφωση με τους προβλεπόμενους κανόνες. Οι αρχές αυτές περιγράφουν τις δεσμεύσεις που πρέπει να τηρούν οι οργανισμοί όταν συλλέγουν, επεξεργάζονται και αποθηκεύουν τα προσωπικά δεδομένα κάποιου ατόμου. Αν και οι αρχές προστασίας δεδομένων, στις οποίες βασίζεται ο Κανονισμός, είναι παρόμοιες με εκείνες της ισχύσασας Οδηγίας για την Προστασία Δεδομένων, ο ενωσιακός νομοθέτης προσπάθησε να τις κάνει πιο λεπτομερείς για να διασφαλιστεί υψηλότερο επίπεδο συμμόρφωσης και να ληφθούν υπόψη οι τεχνολογικές εξελίξεις.

Ειδικότερα ο GDPR ερείδεται σε επτά αρχές, οι οποίες παρέχουν στους οργανισμούς καθοδήγηση σχετικά με τον καλύτερο τρόπο διαχείρισης των προσωπικών τους δεδομένων και τη συμμόρφωση με τους κανονισμούς GDPR. Η μη συμμόρφωση με τις αρχές δύναται να οδηγήσει σε σημαντικές κυρώσεις. Ο ΓΚΠΔ ορίζει ότι οι παραβιάσεις των βασικών αρχών για την επεξεργασία προσωπικών δεδομένων τιμωρούνται με το υψηλότερο επίπεδο πρόστιμου. Αυτό μπορεί να συνεπάγεται ποινή έως και 4% του ετήσιου κύκλου εργασιών μίας επιχείρησης ή 20 εκατ. ευρώ, ανάλογα με το ποιο είναι το υψηλότερο.

3.1.1 Αρχή της νομιμότητας, της αντικειμενικότητας και της διαφάνειας

Η πρώτη αρχή είναι ίσως η πιο σημαντική και υπογραμμίζει την πλήρη διαφάνεια για όλα τα υποκείμενα των δεδομένων στην ΕΕ. Όταν συλλέγονται δεδομένα, οι οργανισμοί πρέπει να δηλώνουν με σαφήνεια γιατί συλλέγονται αυτά και πώς θα χρησιμοποιηθούν. Εάν το υποκείμενο τον δεδομένων ζητήσει περαιτέρω πληροφορίες σχετικά με την επεξεργασία των δεδομένων του, οι επιχειρήσεις υποχρεούνται να τις παρέχουν εγκαίρως. Σε περίπτωση μάλιστα που απαιτείται συγκατάθεση για την επεξεργασία, η ενημέρωση θα πρέπει να συνοδεύει το κείμενο της συγκατάθεσης. Η

συλλογή, η επεξεργασία και η διαβίβαση δεδομένων πρέπει να γίνεται πάντοτε σύμφωνα με το νόμο.

3.1.2Η αρχή (περιορισμού) του σκοπού

Οι οργανισμοί πρέπει να έχουν συγκεκριμένο και νόμιμο λόγο συλλογής και επεξεργασίας προσωπικών δεδομένων. Τα δεδομένα μπορούν να χρησιμοποιηθούν μόνο για τον αναφερόμενο σκοπό και δεν επιτρέπεται η επεξεργασία τους για άλλους σκοπούς εκτός εάν το υποκείμενο των δεδομένων έχει ρητά συναινέσει. Υπάρχει ελαφρώς μεγαλύτερη ευελιξία κατά την επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή για επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς.

Ο Υπεύθυνος επεξεργασίας πρέπει να ενημερώνει το υποκείμενο των δεδομένων εάν χρησιμοποιήσει τα δεδομένα για οποιονδήποτε άλλο σκοπό, πέραν αυτού για τον οποίον το υποκείμενο των δεδομένων παρείχε την συγκατάθεση του και να διασφαλίζει την ύπαρξη νόμιμης βάσης επεξεργασίας. Ωστόσο στην περίπτωση που ένας νέος σκοπός είναι συμβατός με τον σκοπό της επεξεργασίας δε χρειάζεται η επεξεργασία να βασίζεται σε νέα νομική βάση και η επεξεργασία μπορεί να γίνει με την ίδια υπάρχουσα νομική βάση[35].

Για παράδειγμα ένας γιατρός δεν μπορεί να χρησιμοποιήσει τα email των ασθενών του για να διαφημίσει μια καινούρια θεραπεία. Εκτός βέβαια και εάν έχει ήδη ενημερώσει τους ασθενείς για τον σκοπό επεξεργασίας και έχει για παράδειγμα λάβει την προηγούμενη συγκατάθεσή τους.

3.1.3 Η αρχή της ελαχιστοποίησης των δεδομένων “data minimization”

Η αρχή αυτή προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς

[35] Ε. Τρούλη, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων και Ευθύνη για Αποζημίωση, 2023, σ. 55, αρ. 66 = sakkoulas-online

για τους οποίους υποβάλλονται σε επεξεργασία. Αυτό σημαίνει ότι οι οργανισμοί θα πρέπει να αποθηκεύουν μόνο τον ελάχιστο όγκο δεδομένων που είναι απαραίτητος για το σκοπό τους. Δεν δύνανται δηλαδή απλώς να συλλέγουν προσωπικά δεδομένα τυχαία, με την προοπτική ότι θα μπορούσαν να είναι χρήσιμα στο μέλλον. Εάν αποθηκεύουν περισσότερα δεδομένα από όσα χρειάζεται, τότε μάλλον παραβιάζουν την αρχή της ελαχιστοποίησης και θα επέλθει η επιβολή προστίμων.

3.1.4 Η αρχή της ακρίβειας

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ορθά, κατάλληλα και επικαιροποιημένα. Αυτό σημαίνει ότι οι οργανισμοί θα πρέπει να ελέγχουν τακτικά τις πληροφορίες που διατηρούν για τα άτομα και να διαγράφουν ή να τροποποιούν ανακριβή δεδομένα. Εξάλλου παρέχεται στο άτομο η δυνατότητα να ζητήσει, εντός 30 ημερών, τη διαγραφή ή τη διόρθωση εσφαλμένων ή ελλιπών δεδομένων. Η βελτίωση αυτή της πληροφόρησης θα συμβάλει στη βελτίωση της συμμόρφωσης και στην εξασφάλιση ότι οι επιχειρηματικές βάσεις δεδομένων είναι ακριβείς και πλήρως ενημερωμένες.

3.1.5 Η αρχή του περιορισμού της περιόδου αποθήκευσης

Σύμφωνα με το άρθρο 5 στ. ε του ΓΚΠΔ τα δεδομένα « *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 καθίσταται σαφές, πως όταν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον αναγκαία για τον σκοπό για τον οποίο συλλέχθηκαν, θα πρέπει να διαγραφούν ή να καταστραφούν, εκτός εάν υπάρχουν άλλοι λόγοι για τη διατήρηση τους. Ο κανονισμός περί προστασίας προσωπικών δεδομένων δεν ορίζει με ακρίβεια το χρονικό διάστημα, για το οποίο είναι επιτρεπτή η διατήρηση των δεδομένων αυτών μετέπειτα της εκπλήρωσης τους σκοπού συλλογής τους. Ο καθορισμός του χρονικό διαστήματος αποθήκευσης των δεδομένων επαφίεται στον κάθε οργανισμό με βάση τους σκοπούς της

επεξεργασίας. Για να διασφαλιστεί η συμμόρφωση, οι οργανισμοί θα πρέπει να διαθέτουν μια διαδικασία ελέγχου για τον καθαρισμό των βάσεων δεδομένων.

Παρόλο που ο γενικός κανόνας είναι ότι δεν επιτρέπεται να αποθηκεύονται προσωπικά δεδομένα για μελλοντική χρήση, υπάρχουν εξαιρέσεις για σκοπούς αρχειοθέτησης, έρευνας ή στατιστικής. Προϋπόθεση για τις εξαιρέσεις αυτές είναι να εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο παρών κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

3.1.6 Αρχή της ακεραιότητας και της εμπιστευτικότητας

Κατά ρητή επιταγή του Κανονισμού τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπον που «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». Προς κατοχύρωση των ως άνω κατ' άρθρ. 5 §1στ αρχών της εμπιστευτικότητας και ακεραιότητας των δεδομένων επιβάλλεται σύμφωνα με τα άρθρ. 24 §1 (αλλά και 25 §1, 32 κ.ά.) ΓΚΠΔ «να εφαρμόζονται κατάλληλα οργανωτικά και τεχνικά μέτρα, προκειμένου να διασφαλίζεται και να αποδεικνύεται ότι η επεξεργασία των δεδομένων διενεργείται σύμφωνα με τον ΓΚΠΔ»[36]

Η αρχή αυτή τυγχάνει εφαρμογής στα οριζόμενα από τα ακόλουθα άρθρα του Κανονισμού: αρ.28 «Εκτελών την επεξεργασία», αρ.29 «Επεξεργασία υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία», αρ.32 «Αρχεία των δραστηριοτήτων επεξεργασίας», αρ.33 «Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή» και αρ.34 « Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων».

[36] Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, Νομική Βιβλιοθήκη, 2020

3.1.7 Η αρχή της λογοδοσίας

Η αρχή της λογοδοσίας συνιστά όχι μόνο μία από τις σημαντικότερες καινοτομίες, αλλά ουσιαστικά αποτελεί τον ακρογωνιαίο λίθο του Γενικού Κανονισμού για την Προστασία των Δεδομένων. Σύμφωνα με τον ΓΚΠΔ, επιχειρήσεις και οργανισμοί οφείλουν να συμμορφώνονται με όλες τις αρχές προστασίας δεδομένων καθώς και να αποδεικνύουν τη συμμόρφωση αυτή. Ο ΓΚΠΔ παρέχει στις επιχειρήσεις και τους οργανισμούς μια σειρά εργαλείων για να τους βοηθά να αποδεικνύουν τη λογοδοσία, ορισμένα εκ των οποίων πρέπει να τίθενται σε εφαρμογή υποχρεωτικά.

Για παράδειγμα, σε ορισμένες περιπτώσεις μπορεί να καθίσταται υποχρεωτικός ο διορισμός υπεύθυνου προστασίας δεδομένων. Επίσης υποχρεωτική μπορεί να είναι η διεξαγωγή εκτιμήσεων αντίκτυπου σχετικά με την προστασία δεδομένων. Οι υπεύθυνοι επεξεργασίας δεδομένων έχουν την ευχέρεια να επιλέξουν να χρησιμοποιήσουν άλλα εργαλεία, όπως για παράδειγμα κώδικες δεοντολογίας και μηχανισμούς πιστοποίησης, για την απόδειξη της συμμόρφωσης με τις αρχές προστασίας δεδομένων.[37]

Μάλιστα ο υπεύθυνος επεξεργασίας βαρύνεται με το επιπρόσθετο καθήκον να αποδεικνύει από μόνος του και ανά πάσα στιγμή τη συμμόρφωση του με τις αρχές του άρθρου 5 παρ. 1 ΓΚΠΔ. Κάθε άλλο παρά τυχαίο συνιστά το γεγονός ότι ο Κανονισμός εντάσσει τη λογοδοσία στη ρύθμιση των αρχών που διέπουν την επεξεργασία, προσδίδοντας σε αυτήν, τη λειτουργία ενός μηχανισμού τήρησής τους, αντιστρέφοντας κατ' ουσίαν το «βάρος της απόδειξης» ως προς την νομιμότητα της επεξεργασίας, μεταθέτοντας τη στον υπεύθυνο επεξεργασίας, ώστε να υποστηρίζεται βάσιμα ότι εκείνος φέρει το βάρος της επίκλησης και απόδειξης τής νομιμότητας τής επεξεργασίας.[38] Τυχόν μεταφορά του βάρους της απόδειξης της συμμόρφωσης στα υποκείμενα των δεδομένων, όπως και η αδυναμία απόδειξης της συμμόρφωσης στους παραπάνω κανόνες, συνιστούν παραβίαση της αρχής της λογοδοσίας.[39]

---

[37] https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/how-can-i-demonstrate-my-organisation-compliant-gdpr_el

[38]. Λ. Μήτρου, Η αρχή τής Λογοδοσίας σε Υποχρεώσεις του υπευθύνου επεξεργασίας [Γ. Γιαννοπουλος, Λ. Μήτρου, Γ. Τσολίας], Συλλογίκος Τόμος Λ. Κοτσαλή – Κ. Μενουδάκου «Ο ΓΚΠΔ, Νομική διάσταση και πρακτική εφαρμογή », εκδ. Νομική Βιβλιοθήκη, 2018, σελ. 172 επ.

[39] Σ. Μαυρίδης, Το δικαίωμα στην προστασία δεδομένων προσωπικού χαρακτήρα κατά την οικοδόμηση μιας ευρωπαϊκής οικονομίας δεδομένων, 2024, σ. 65

Εκ των ανωτέρω προκύπτει πως αποτελεί υποχρέωση του υπευθύνου επεξεργασίας, αρχικά να λαμβάνει από μόνος του τα αναγκαία μέτρα προκείμενου να συμμορφώνεται προς τις απαιτήσεις του Κανονισμού. Ενδεικτικά μέτρα οργάνωσης και επίδειξης της συμμόρφωσης, προβλεπόμενα από τον Κανονισμό, τα οποία ο υπεύθυνος επεξεργασίας οφείλει να εισάγει με κατάλληλες πολιτικές είναι η διενέργεια εκτίμησης αντικτύπου αφετέρου, η τήρηση αρχείου επεξεργασίας και η τήρηση των υποχρεώσεων κοινοποίησης της παραβίασης των δεδομένων.[40]

Επιπλέον επιφορτίζεται με την υποχρέωση να αποδεικνύει ανά πάσα στιγμή την ανωτέρω συμμόρφωση του, χωρίς μάλιστα να απαιτείται η Αρχή, στο πλαίσιο άσκησης των ερευνητικών/ελεγκτικών εξουσιών τής, να υποβάλλει επιμέρους εξειδικευμένα ερωτήματα και αιτήματα προς διαπίστωση τής συμμόρφωσης[41].

3.2 Υπεύθυνος Προστασίας Δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων εισάγει τον ρόλο του Υπεύθυνου Προστασίας Δεδομένων (DPO), του κύριου υπεύθυνου για τη διασφάλιση της συμμόρφωσης, της διαχείρισης, της επεξεργασίας και της προστασίας των προσωπικών δεδομένων τρίτων με τους κανόνες προστασίας δεδομένων. Ο Υπεύθυνος Προστασίας Δεδομένων συνιστά, σύμφωνα την ομάδα του άρθρου 29 στις Κατευθυντήριες γραμμές WP 243 rev.01 σχετικά με τους υπεύθυνους προστασίας δεδομένων, ακρογωνιαίο λίθο της λογοδοσίας και η ύπαρξη του δύναται να αποτελέσει ανταγωνιστικό πλεονέκτημα για τις επιχειρήσεις.[42]

Εκτός από τον διευκολυντικό ρόλο, που έχουν σε επίπεδο συμμόρφωσης μέσω της εφαρμογής εργαλείων λογοδοσίας (όπως διευκόλυνση διενέργειας εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων και διενέργεια ή διευκόλυνση διενέργειας ελέγχων), οι υπεύθυνοι προστασίας δεδομένων ενεργούν και ως μεσολαβητές

[40] Γ. Πλιαβέσης, Η Προστασία των Προσωπικών Δεδομένων στη σχέση Τράπεζας – Πελάτη, Νομική Βιβλιοθήκη, 2019
[41] ΑΠΔΠΧ 30/2020, 23/2021, 36/2021, 61/2021, 42/2022, 66/2022, 67/2022
[42] http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617_appendix_core_issues_plenary_en.pdf

μεταξύ των διαφόρων ενδιαφερομένων (π.χ., εποπτικές αρχές, υποκείμενα των δεδομένων και επιχειρησιακές μονάδες του ίδιου οργανισμού).

Ο Κανονισμός απαιτεί από τους οργανισμούς να προσλαμβάνουν έναν εξειδικευμένο επαγγελματία για τη διαχείριση προσωπικών πληροφοριών τρίτων και την επίβλεψη της γενικής συμμόρφωσης με τον Κανονισμό ΕΕ 2016/679. Ο διορισμός του υπεύθυνου προστασίας δεδομένων είναι σε μερικές περιστάσεις υποχρεωτικός για τους υπευθύνους ή εκτελούντες την επεξεργασία («υποχρεωτικός διορισμός»). Παρόλα αυτά, συνίσταται σε κάθε περίσταση («εθελοντικός διορισμός»).[43]

Σύμφωνα με το άρθρο 37 παράγραφος 1 του ΓΚΠΔ, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός σε τρεις συγκεκριμένες περιπτώσεις[44] : α) όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα[45] β) 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· γ) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Ο Υπεύθυνος Προστασίας Δεδομένων κατά ρητή επιταγή του άρθρου 37 παρ. 5 του Κανονισμού διορίζεται κυρίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων. Οι αρμοδιότητες του περιγράφονται λεπτομερώς στο άρθρο 39 του Κανονισμού και απαιτείται να εκτελεί τα καθήκοντά του ανεξάρτητα. Τούτο συνεπάγεται ότι κατά την άσκηση των καθηκόντων του δεν λαμβάνει εντολές για τον τρόπο άσκησης τους, δεν απολύεται, ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασίας, επειδή επιτέλεσε τα καθήκοντα του.[46]

Για λόγους αποφυγής σύγκρουσης συμφερόντων ο Υπεύθυνος Προστασίας Δεδομένων δεν μπορεί να κατέχει θέση ή αρμοδιότητες που απαιτούν από αυτόν να

[43] Α. Σκουτέλη, Κλινικές δοκιμές φαρμάκων, 2021, § 14, σ. 405, αρ. 1316 = sakkoulas-online
[44] Σημειώνεται ότι, σύμφωνα με το άρθρο 37 παράγραφος 4, το δίκαιο της Ένωσης ή των κρατών μελών είναι δυνατό να επιβάλλει τον ορισμό υπευθύνου προστασίας δεδομένων και σε άλλες περιπτώσεις.
[45] Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα. Βλ. άρθρο 32 της οδηγίας (ΕΕ) 2016/680.
[46] Άρθρο 38παρ. 3 ΓΚΠΔ

ορίσει τους σκοπούς και τις μεθόδους επεξεργασίας προσωπικών δεδομένων. Ο καθορισμός των σκοπών και των μεθόδων επεξεργασίας προσωπικών δεδομένων αποτελεί ευθύνη του υπεύθυνου επεξεργασίας. Μπορεί να προκύψει σύγκρουση συμφερόντων εάν, για παράδειγμα, ένας υπεύθυνος ασφάλειας πληροφοριών ή ανώτερος διευθυντής οριστεί ως Υπεύθυνος Προστασίας Δεδομένων.

Στο πλαίσιο των καθηκόντων παρακολούθησης της συμμόρφωσης, οι υπεύθυνοι προστασίας δεδομένων μπορούν συγκεκριμένα:

- να συλλέγουν πληροφορίες με σκοπό τον προσδιορισμό δραστηριοτήτων επεξεργασίας,
- να αναλύουν και να ελέγχουν τη συμμόρφωση των δραστηριοτήτων επεξεργασίας,
- να ενημερώνουν τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, να τους παρέχουν συμβουλές και να εκδίδουν συστάσεις υπόψη τους.

Το γεγονός ότι επιφορτίζεται με το καθήκον της παρακολούθησης της συμμόρφωσης δεν συνεπάγεται ότι ο υπεύθυνος προστασίας δεδομένων φέρει προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης. Ο ΓΚΠΔ καθιστά σαφές ότι υπεύθυνος επεξεργασίας οφείλει να «*εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό*»[47] και όχι ο υπεύθυνος προστασίας δεδομένων. Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων είναι εταιρική ευθύνη του υπευθύνου επεξεργασίας, και όχι του υπευθύνου προστασίας δεδομένων.

Είναι σημαντικό τα στοιχεία του Υπεύθυνου Προστασίας Δεδομένων να δημοσιοποιούνται, ώστε να καθίσταται εφικτή η επικοινωνία των υποκειμένων των δεδομένων με αυτόν. Πέραν τούτου υφίσταται η υποχρέωση, κατά ρητή επιταγή του Κανονισμού, να ανακοινώνονται στην εποπτική αρχή, με μέριμνα του υπεύθυνου επεξεργασίας και του εκτελούντα την επεξεργασία, τα στοιχεία που αφορούν τον ορισμό του Υπεύθυνου Προστασίας Δεδομένων.

[47] Άρθρο 24 παρ. 1 ΓΚΠΔ

Η ανακοίνωση αυτή γίνεται ηλεκτρονικά μέσω της διαδικτυακής πύλης της Αρχής[48]. Η ίδια διαδικασία ακολουθείται και στις περιπτώσεις αντικατάστασης ή διαγραφής/κατάργησης του DPO.

3.3 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα[49] αποτελεί μία συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή, η οποία ερείδεται στο άρθρο 9^{A} του Συντάγματος. Ιδρύθηκε με τον νόμο 2472/1997, ο οποίος είχε ενσωματώσει στο ελληνικό δίκαιο την ευρωπαϊκή Οδηγία 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Στη συνέχεια με τον Κανονισμό[50] 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, ο οποίος τέθηκε σε εφαρμογή στις 25/5/2018 σε όλες τις χώρες της ΕΕ, η Οδηγία 95/45/ΕΚ καταργήθηκε.

Από τις 29/8/2019 έχει τεθεί σε ισχύ ο νόμος 4624/2019[51] , στον οποίο τα άρθρα 9 έως και 20 αναφέρονται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, που έχει χαρακτήρα εποπτικής αρχής. Βέβαια πλέον ο νόμος 2472/1997 έχει καταργηθεί σχεδόν στο σύνολο του. Εξαίρεση αποτελούν ορισμένες διατάξεις που αναφέρονται ρητά στο άρθρο 84 του νόμου 4624/2019. Επιπλέον ο νόμος 4624/2019 περιλαμβάνει και την ενσωμάτωση στην ελληνική έννομη τάξη της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της $27^{ης}$ 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.

[48] https://www.dpa.gr/el/foreis/dpo_upef/orismos_DPO
[49] https://www.dpa.gr/el/arxi/profile
[50] (Γενικός Κανονισμός Προστασίας Δεδομένων - ΓΚΠΔ)
[51] («Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της $27^{ης}$ Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της $27^{ης}$ Απριλίου 2016 και άλλες διατάξεις»)

Περαιτέρω σχετικά με την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η Αρχή εφαρμόζει τον νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την ευρωπαϊκή Οδηγία 2002/58/ΕΚ.

3.4 Προσφυγή ενώπιον της ΑΠΔΠΧ

Ο Κανονισμός προσφέρει τη δυνατότητα στα υποκείμενα των δεδομένων προσωπικού χαρακτήρα, εάν τυχόν παραβιαστούν τα προσωπικά τους δεδομένα, να προβούν στην υποβολή καταγγελίας σε εποπτική αρχή, ιδίως στο κράτος μέλος της διαμονής τους ή του τόπου εργασίας τους ή του τόπου της εικαζόμενης παράβασης. Έπειτα η εν λόγω εποπτική αρχή οφείλει να ενημερώνει τον καταγγέλοντα όσον αφορά την πρόοδο της καταγγελίας, αλλά και την έκβαση αυτής[52]. Ακόμη στον Κανονισμό υπάρχει σαφής πρόβλεψη δικαιώματος των φυσικών και νομικών προσώπων σε ένδικα μέσα κατά νομικά δεσμευτικών αποφάσεων εποπτικής αρχής εναντίον τους[53]. Μάλιστα ορίζεται ρητά το δικαίωμα του κάθε υποκειμένου των δεδομένων σε πραγματική δικαστική προσφυγή κατά υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία όταν θεωρεί ότι έχει γίνει παραβίαση των δικαιωμάτων του, όπως αυτά ορίζονται στον Κανονισμό, κατά τη διάρκεια της επεξεργασίας των προσωπικών του δεδομένων[54].

Σε περιπτώσεις παραβίασης του Κανονισμού οι εποπτικές αρχές δύνανται να επιβάλουν διοικητικά πρόστιμα. Η επιβολή τους θα πρέπει να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, αναλογική και αποτρεπτική. Εξάλλου τα διοικητικά πρόστιμα, ανάλογα με τις περιστάσεις κάθε μεμονωμένης περίπτωσης, επιβάλλονται επιπρόσθετα ή αντί των μέτρων που αναφέρονται στο άρθρο 58 παράγραφος 2 στοιχεία α) έως η) και στο άρθρο 58 παράγραφος 2 στοιχείο ι). Βέβαια κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται δεόντως υπόψη κάποιες προϋποθέσεις. Αυτές παρέχουν την διακριτική ευχέρεια στην αρχή στην επιλογή του ύψους του προστίμου που θα επιβληθεί.

[52] Άρθρο 77 ΓΚΠΔ
[53] Άρθρο 78 ΓΚΠΔ
[54] Άρθρο 79 ΓΚΠΔ

Τα κράτη μέλη θεσπίζουν τους κανόνες σχετικά με τις άλλες κυρώσεις που επιβάλλονται για παραβάσεις του παρόντος κανονισμού, ιδίως για τις παραβάσεις που δεν αποτελούν αντικείμενο διοικητικών προστίμων δυνάμει του άρθρου 83, και λαμβάνουν όλα τα αναγκαία μέτρα για να διασφαλιστεί ότι εφαρμόζονται. Οι εν λόγω κυρώσεις είναι αποτελεσματικές, αναλογικές και αποτρεπτικές.

Κεφάλαιο 4ο

Αποφάσεις ΑΠΔΧΠ

Τα τελευταία χρόνια και ιδίως μετά την εφαρμογή του Κανονισμού η προστασία των προσωπικών δεδομένων βρίσκεται συνεχώς στο προσκήνιο. Όπως είδαμε ο ΓΚΠΔ έχει δημιουργήσει ένα ασφαλέστερο επίπεδο προστασίας για τα δικαιώματα των υποκειμένων και φυσικά η εποπτική αρχή συμβάλει στην επίτευξη αλλά και στη διατήρηση της προστασίας αυτής.

Είναι σημαντικό συνεπώς να δει κανείς το πραγματικό έργο της ΑΠΔΠΧ και πως αυτή αντιμετωπίζει περιπτώσεις παραβιάσεων. Για τον λόγο αυτό στο παρόν κεφάλαιο θα παρουσιαστούν κάποιες αποφάσεις τις Αρχής, αλλά και οι κυρώσεις που εκείνη επέβαλε ενόψει παραβιάσεων του Κανονισμού.

4.1 35/2023 ΑΠΔΠΧ[55]

Με την απόφαση 35/2023 η Αρχή, αφού εξέτασε καταγγελία κατόχου πιστωτικής κάρτας, επέβαλλε πρόστιμο συνολικού ύψους 60.000 ευρώ σε Τράπεζα για την παράνομη χορήγηση προσωπικών δεδομένων στη σύζυγο του καταγγέλλοντος, καθώς τα στοιχεία συναλλαγών μέσω της κάρτας του, χορηγήθηκαν από υπάλληλο της Τράπεζας στη σύζυγό του χωρίς σχετική εξουσιοδότηση. Το μεγαλύτερο μέρος του προστίμου όμως επιβλήθηκε για τον εσφαλμένο χειρισμό και την παράβαση της υποχρέωσης γνωστοποίησης του περιστατικού παραβίασης.

[55] https://www.dpa.gr/sites/default/files/2023-12/35_2023%20anonym.pdf

Πρόκειται για παραβιάσεις των βασικών αρχών, που διέπουν την επεξεργασία δεδομένων και συγκεκριμένα παράβαση της αρχής της νομιμότητας, αντικειμενικότητας και διαφάνειας της επεξεργασίας (άρθρο 5 παρ. 1 α' ΓΚΠΔ) και της αρχής της εμπιστευτικότητας των δεδομένων (άρθρο 5 παρ. 1 στ' ΓΚΠΔ) εκ μέρους της Τράπεζας. Η καταγγελλόμενη εκτός αυτού δεν ανέλαβε άμεσα ενεργό δράση προς διερεύνηση του περιστατικού, ως όφειλε ως υπεύθυνος επεξεργασίας, ώστε να αποκτήσει τον απαιτούμενο βαθμό βεβαιότητας και να τηρήσει τις εκ του άρθρου 33 ΓΚΠΔ υποχρεώσεις της, θεωρώντας ότι τα στοιχεία που είχε στη διάθεσή της δεν ήταν επαρκή, παρότι ο καταγγέλλων προσκόμισε και καινούργια στοιχεία.

Ειδικότερα αν και η καταγγελλόμενη είχε ενδείξεις για την πιθανή τέλεση περιστατικού παραβίασης, αρχικά δεν το διερεύνησε μεταθέτοντας την ευθύνη για τον εντοπισμό της πηγής της διαρροής στο υποκείμενο των δεδομένων, στη συνέχεια καθυστέρησε σημαντικά να το χειριστεί ως περιστατικό παραβίασης λόγω έλλειψης συνεννόησης μεταξύ των αρμοδίων Μονάδων της, ακολούθως υποτίμησε τις συνέπειές του για το υποκείμενο και εκτίμησε εσφαλμένα ότι δεν οφείλει να το γνωστοποιήσει στην Αρχή.

Χρειάστηκε να διενεργηθεί εσωτερικός έλεγχος προκειμένου η καταγγελλόμενη να αναγνωρίσει την ύπαρξη διαρροής δεδομένων και να αποδώσει ευθύνες. Όμως δεν γνωστοποίησε ως όφειλε το περιστατικό στην Αρχή και δεν έλαβε μέτρα για τον μετριασμό των συνεπειών του, αλλά και την αποφυγή κάποιου παρόμοιου περιστατικού στο μέλλον. Σημειώνεται επίσης ότι η Τράπεζα δεν εκδήλωσε οποιοδήποτε ενδιαφέρον ή μια έστω τυπική απολογία για την ηθική βλάβη που υπέστη ο καταγγέλλων εξαιτίας του περιστατικού.

Για τους ανωτέρω λόγους η εποπτική αρχή επέβαλλε διοικητικό πρόστιμο ύψους δέκα χιλιάδων (10.000€) ευρώ, για τη διαπιστωθείσα παράβαση των αρχών της νομιμότητας της επεξεργασίας και της εμπιστευτικότητας των δεδομένων κατ' άρθρο 5 παρ. 1 α) και στ) ΓΚΠΔ και , διοικητικό πρόστιμο ύψους πενήντα χιλιάδων (50.000€) ευρώ, για τη διαπιστωθείσα παράβαση της υποχρέωσης χειρισμού και γνωστοποίησης περιστατικού παραβίασης βάσει του άρθρου 33 ΓΚΠΔ.

4.2 6/2024 ΑΠΔΠΧ[56]

Εκτός από την επιβολή χρηματικών προστίμων η Αρχή δύναται σε κάποιες περιπτώσεις να επιπλήττει τους καταγγελλόμενους, όταν αυτοί παραβιάζουν τις διατάξεις του Κανονισμού. Υπάρχει θα λέγαμε μία αναλογία μεταξύ της διαπιστωμένης παράβασης και των κυρώσεων που επιβάλλει η εποπτική αρχή. Σε καμία περίπτωση η Αρχή δεν λειτουργεί ως τιμωρός για τους παραβάτες, αλλά ως αποτρεπτικός παράγοντας για την τέλεση παραβάσεων.

Λόγω αυτού και λαμβάνοντας υπόψιν της ότι διαθέτει κατά το άρθρο 58 παρ. 2 του ΓΚΠΔ διορθωτικές εξουσίες επιβάλλει πάντοτε μέτρα ανάλογα, αποτρεπτικά και αποτελεσματικά σε κάθε περιστατικό. Ακόμη και για την επιβολή διοικητικού χρηματικού προστίμου υπάρχουν κριτήρια στα οποία οφείλει να στηριχθεί για την επιμέτρηση του.

Στην απόφαση 6/2024 η Αρχή επέβαλε στην καταγγελλομένη εταιρεία διοικητικό πρόστιμο ύψους 2.000 ευρώ, για τη διαπιστωθείσα παράβαση των αρχών της νομιμότητας της επεξεργασίας και της απηύθυνε επίπληξη για την ελλιπή ενημέρωση.

Αναλυτικότερα, στην εν λόγω περίπτωση, ο καταγγέλλων, πρώην εργαζόμενος της καταγγελλόμενης εταιρείας, ανέφερε στην καταγγελία, που έκανε ενώπιον της ΑΠΔΠΧ, παράνομη επεξεργασία προσωπικών του δεδομένων μέσω του συστήματος γεωεντοπισμού που λειτουργούσε σε όχημα το οποίο του είχε παραχωρηθεί. Σύμφωνα με τα πραγματικά περιστατικά κατά τη διάρκεια της κανονικής του άδειας τον κάλεσαν στο τηλέφωνο από την καταγγελλόμενη και εκείνος δεν ανταποκρίθηκε στις κλήσεις.

Έτσι λοιπόν ο διευθυντής πωλήσεων της καταγγελλόμενης έκανε χρήση των δεδομένων του εγκατεστημένου συστήματος γεωεντοπισμού στο εταιρικό αυτοκίνητο και εμφανίστηκε στο σούπερ μάρκετ όπου ο καταγγέλλων είχε πάει για ψώνια. Σχετικά με την εγκατάσταση και την ενημέρωση του πρώην εργαζομένου για τον σύστημα αυτό επισημαίνεται πως αυτή είχε λάβει χώρα δύο εβδομάδες πριν συμβεί το περιστατικό.

Η εταιρεία απάντησε στα καταγγελλόμενα, πως παρότι η χρήση του συστήματος γεωεντοπισμού δεν επιτρεπόταν εκτός του ωραρίου εργασίας, προέβη σε χρήση του λόγω ανησυχίας για την υγεία του εργαζομένου, αφού εκείνος δεν ανταποκρινόταν στις

[56] https://www.dpa.gr/sites/default/files/2024-02/6_2024%20anonym.pdf

τηλεφωνικές της κλήσεις. Επιπλέον υποστηρίχθηκε από πλευράς της ότι δεν υπήρχε η τεχνική δυνατότητα να απενεργοποιηθεί το εγκατεστημένο σύστημα μετά τη λήξη του ωραρίου εργασίας. Φυσικά μετά το συμβάν αυτόν και για την αποτροπή παρόμοιων μελλοντικών περιστατικών προχώρησε στη λήψη των ακόλουθων μέτρων :

1. Αφαιρέθηκαν τα υφιστάμενα συστήματα γεωεντοπισμού έτσι ώστε να τοποθετηθούν νέα, τα οποία θα επιτρέπουν την απενεργοποίησή τους από τους χρήστες τους.
2. Ορίστηκε ως υπεύθυνος χειριστής των συστημάτων γεωεντοπισμού ο διαχειριστής-νόμιμος εκπρόσωπος της εταιρίας, με δεδομένο ότι η καταγγελλόμενη πράξη στην οποία προέβη ο προστηθείς κατά του καταγγέλλοντος έγινε εν αγνοία της καταγγελλόμενης και χωρίς καμία προηγούμενη συμβουλή.
3. Επικαιροποιήθηκαν οι οδηγίες χρήσης του συστήματος γεωεντοπισμού από τους χρήστες του και
4. Συντάχθηκαν νέα έγγραφα γνωστοποίησης της εγκατάστασης και λειτουργίας του συστήματος προς τους χρήστες, όπου ενημερώνονται για α) τους σκοπούς για τους οποίους εγκαταστάθηκαν κα λειτουργούν και αφορούν β) το χρόνο διακράτησης των δεδομένων που συλλέγονται ανά ημέρα μέσω των ανωτέρω συστημάτων γεωεντοπισμού και γ) τα δικαιώματα των χρηστών.

Η Αρχή εκτιμώντας τα στοιχεία της καταγγελίας για τη χρήση του συστήματος γεωεντοποισμού διαπίστωσε ότι έγιναν οι εξής παραβάσεις :

α) παράνομη επεξεργασία των προσωπικών δεδομένων του καταγγέλλοντος, λόγω της χρήσης των δεδομένων εντοπισμού του οχήματός του εκτός ωρών εργασίας και για τον σκοπό του εντοπισμού του καταγγέλλοντος

β) ελλιπή ενημέρωση του καταγγέλλοντος, κατά παράβαση των άρθρων 5 παρ. 1 εδ. α και των άρθρων 12 και 13 και 5 παρ. 2 εδ. β του ΓΚΠΔ, σχετικά με τη λειτουργία του συστήματος που είχε εγκατασταθεί στο όχημα που του παραχωρήθηκε, ανεξαρτήτως του ότι δεν είχε το δικαίωμα να το χρησιμοποιεί εκτός ωρών εργασίας, γεγονός που παραδέχτηκε η καταγγελλόμενη και προέβη σε διορθωτικές ενέργειες.

Μάλιστα σημαντικό ρόλο για την διαμόρφωση της απόφαση της αρχής διαδραμάτισε ότι το περιστατικό φαίνεται να είναι μεμονωμένο, καθώς δεν έχει επιβληθεί

από την Αρχή κύρωση στην καταγγελλόμενη για παρόμοια παράβαση στο παρελθόν. Επιπλέον ότι η παράβαση της νομιμότητας της επεξεργασίας εμπίπτει στη διάταξη της παρ. 5 του άρθρου 83 ΓΚΠΔ και αφενός επηρέασε άμεσα ένα υποκείμενο δεδομένων, αφετέρου όμως οφείλεται σε μεμονωμένη ενέργεια υπαλλήλου.

Τελικά επιβλήθηκε στην καταγγελλόμενη εταιρεία ως υπεύθυνο επεξεργασίας, με βάση το άρθρο 58 παρ. 2 εδ. θ) του ΓΚΠΔ, διοικητικό πρόστιμο ύψους δύο χιλιάδων (2.000€) ευρώ, για τη διαπιστωθείσα παράβαση των αρχών της νομιμότητας της επεξεργασίας κατ' άρθρο 5 παρ. 1 α) του ΓΚΠΔ και της απευθύνθηκε με βάση το άρθρο κατ' άρθρο 58 παρ. 2 στοιχ. β΄ ΓΚΠΔ, επίπληξη για την ελλιπή ενημέρωση κατά παράβαση των άρθρων 5 παρ. 1 εδ. α και των άρθρων 12 και 13 και 5 παρ. 2 εδ. β του ΓΚΠΔ.

Συμπερασματικά και συγκρίνοντας τις δύο αυτές αποφάσεις της Αρχής μπορεί να διακρίνει κανείς την πρόθεση, αλλά και την προσπάθεια της για συμμόρφωση των παραβατών. Αποτελεί καθοριστικό παράγοντα για την λήψη των αποφάσεων της η βαρύτητα της παράβασης, το εάν αυτή γίνεται επανειλημμένα, αλλά φυσικά και τα διορθωτικά μέτρα που προτίθεται να λάβει ο παραβάτης για την αποτροπή μελλοντικών παρόμοιων περιστατικών.

Στη μία εξεταζόμενη απόφαση η καταγγελλόμενη όχι μόνο δεν έλαβε διορθωτικά μέτρα, αλλά ούτε και ενδιαφέρθηκε για το υποκείμενο των δεδομένων. Εκ διαμέτρου αντίθετα έδρασε η καταγγελλόμενη στη δεύτερη περίπτωση η οποία κινητοποιήθηκε αμέσως λαμβάνοντας κάποια μέτρα και προχωρώντας σε προσήκουσες ενέργειες.

Ειδικότερα ζητήματα

Κεφάλαιο 5ο

5.1

Κατά την περιήγηση μας στο διαδίκτυο και την επίσκεψη οποιασδήποτε ιστοσελίδας, θα έχουμε παρατηρήσει πως εμφανίζεται ένα πλαίσιο κειμένου το οποίο μας δίνει την επιλογή να αποδεχτούμε ή να απορρίψουμε τα λεγόμενα «cookies». Τι είναι όμως τα cookies και πως αυτά δύνανται να παραβιάσουν τον Κανονισμό για τα Προσωπικά Δεδομένα;

Σύμφωνα με τον ορισμό που παρέχει η ΑΠΔΠΧ «Τα cookies είναι μικρά αρχεία κειμένου με πληροφορίες, τα οποία αποθηκεύονται από τον διακομιστή (server) ενός ιστότοπου στην τερματική συσκευή (υπολογιστής, κινητό τηλέφωνο κλπ.) ενός επισκέπτη/χρήστη κατά την πλοήγηση σε αυτόν. Ο ιστότοπος ανακτά τις εν λόγω πληροφορίες σε κάθε επίσκεψη προκειμένου να προσφέρει σχετικές με αυτές υπηρεσίες. Χαρακτηριστικό παράδειγμα τέτοιων πληροφοριών είναι οι προτιμήσεις του χρήστη σε μια ιστοσελίδα, όπως αυτές δηλώνονται από τις επιλογές που κάνει σε αυτή (π.χ. επιλογή συγκεκριμένων «κουμπιών», αναζητήσεων, κ.λπ.).»[57]

5.1.1 Κατηγορίες Cookies

Επειδή τα cookies αποθηκεύουν δεδομένα στον σκληρό δίσκο των ηλεκτρονικών μας συσκευών και επιτρέπουν στους επισκέπτες ενός ιστότοπου να αναγνωρίζονται ανά πάσα στιγμή, τα μικρά αρχεία κειμένου δεν είναι πάντα δημοφιλή στους χρήστες, παρότι τα cookies κάνουν πολύ πιο άνετη την περιήγηση στο Διαδίκτυο. Ωστόσο υπάρχουν πολλοί διαφορετικοί τύποι πληροφοριών κειμένου που ονομάζονται cookies και μπορούν να ομαδοποιηθούν με βάση τη διάρκεια ζωής τους (όπως cookie περιόδου λειτουργίας

[57] https://www.dpa.gr/el/cookies/plirofories/whatis_cookies

και cookies επίμονης παρακολούθησης) ή με βάση τον τομέα στον οποίο ανήκουν (όπως cookie πρώτου και τρίτου μέρους). [58]

Τα cookies περιόδου λειτουργίας (Session Cookies) αποθηκεύονται μόνο για τη διάρκεια μιας περιόδου λειτουργίας χρήστη. Για παράδειγμα, διασφαλίζουν ότι ο επισκέπτης δεν χρειάζεται να συνδέεται ξανά συνεχώς όταν περιηγείται σε μια σελίδα που προστατεύεται με κωδικό πρόσβασης.

Αντίθετα τα cookies επίμονης παρακολούθησης, τα οποία διαδραματίζουν κεντρικό ρόλο στο διαδικτυακό μάρκετινγκ, αποθηκεύονται στο πρόγραμμα περιήγησης του χρήστη για να ενεργοποιηθεί η παρακολούθηση διασταυρούμενων περιόδων σύνδεσης. Πρόκειται δηλαδή για μόνιμα cookies. Σε αυτά γίνεται διάκριση μεταξύ cookie πρώτου και τρίτου μέρους. Τα cookies πρώτου μέρους εκδίδονται από τον διακομιστή στον οποίο βρίσκεται ο ιστότοπος που επισκεπτόμαστε ενώ τα cookie τρίτου μέρους αναπαράγονται από διακομιστή τρίτου μέρους, για παράδειγμα μέσω ενός εμφανιζόμενου διαφημιστικού μέσου ή μέσω ενός εικονοστοιχείου επαναστόχευσης "τρίτου μέρους" .

Εάν ένας χρήστης μεταβεί σε έναν ιστότοπο που περιέχει διαφημίσεις, ένα διαφημιστικό μέσο, όπως για παράδειγμα ένα banner προβολής, μπορεί χωρίς να γίνει αντιληπτό να τοποθετήσει ένα cookie παρακολούθησης στον επισκέπτη. Αυτό ονομάζεται cookie τρίτου μέρους επειδή οι πληροφορίες κειμένου δεν προέρχονται απευθείας από τον ιστότοπο που επισκεπτόμαστε, αλλά από το διαφημιστικό μέσο. Αυτά στοχεύουν στην ανάλυση της συμπεριφοράς των κλικ, προκειμένου για παράδειγμα να είναι δυνατή η προβολή διαφημίσεων βάσει ενδιαφέροντος.[59]

Περαιτέρω τα cookies διακρίνονται στα Supercookies και Evercookies. Τα Supercookies είναι ειδικά cookie παρακολούθησης που εισάγονται στην κεφαλίδα http από τον πάροχο υπηρεσιών Διαδικτύου. Τοποθετούνται εκεί ώστε να συλλέγουν πληροφορίες σχετικά με το ιστορικό περιήγησης και τη συμπεριφορά κλικ του χρήστη. Τα Evercookies είναι συνδυασμοί παραδοσιακών cookies και supercookies. Με αυτόν τον τρόπο, ο κλάδος της διαφήμισης προσπαθεί να παρακάμψει τα αντίμετρα από χρήστες που θέλουν να προστατευτούν από την παρακολούθηση. Αυτό είναι δυνατό, για παράδειγμα, με ένα πρόγραμμα αποκλεισμού διαφημίσεων. Όμως είναι δύσκολο να

[58] https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html#Frage_1

αφαιρεθούν, γιατί τα Evercookies αποθηκεύονται σε τουλάχιστον οκτώ διαφορετικές τοποθεσίες. Ακόμα δηλαδή κι αν επιτευχθεί η αφαίρεση σε επτά από αυτές τις τοποθεσίες, τα υπόλοιπα cookie θα επαναφέρουν όλα τα στοιχεία του Evercookie.

5.1.2 Νομοθετικό πλαίσιο

Το νομοθετικό καθεστώς των cookies ρυθμίζεται από την Οδηγία ePrivacy[60], η οποία μάλιστα έχει τεθεί σε ισχύ από το 2002 και έχει ενταχθεί στην ελληνική έννομη τάξη με τον Ν. 3471/2006, όπως έχει τροποποιηθεί με την Οδηγία 2009/136/ΕΚ, η οποία αποτελεί συμπλήρωση και εξειδίκευση του θεσμικού πλαισίου της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.[61]

Βέβαια υπάρχει αναφορά σχετικά με τα cookies και στον ΓΚΠΔ, η οποία είναι μία και μοναδική και συναντάται στην αιτιολογική σκέψη 30: « *Τα φυσικά πρόσωπα μπορεί να συνδέονται με επιγραμμικά αναγνωριστικά στοιχεία ταυτότητας, τα οποία παρέχονται από τις συσκευές, τις εφαρμογές, τα εργαλεία και τα πρωτόκολλά τους, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου,* ***αναγνωριστικά cookies*** *ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων.*

Αυτά μπορεί να αφήνουν ίχνη τα οποία, ιδίως όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους.»

Προκύπτει επομένως, από την ανωτέρω σκέψη, πως τα cookies, στο βαθμό που χρησιμοποιούνται για την αναγνώριση χρηστών, χαρακτηρίζονται ως προσωπικά δεδομένα και για τον λόγο αυτό υπόκεινται στον ΓΚΠΔ. Μπορεί ο Κανονισμός να αναγνωρίζει στην πιθανότητα να υπάρξει επεξεργασία προσωπικών δεδομένων από τη

[60] η 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», γνωστή με την ονομασία «ePrivacy Directive» (Οδηγία ePrivacy), η οποία ενσωματώθηκε στην ελληνική έννομη τάξη με τον Ν. 3471/2006.
[61] https://www.dpa.gr/el/enimerwtiko/nomothesia/proswpikon_dedomenon

χρήση των cookies, χωρίς ωστόσο να ρυθμίζει λεπτομερώς το νομοθετικό πλαίσιο που τα διέπει.

Η επίτευξη της συμμόρφωσης με τα cookies, σύμφωνα με τον ΓΚΠΔ και την Οδηγία περί απορρήτου ηλεκτρονικών επικοινωνιών, απαιτεί αφενός τη λήψη συγκατάθεσης των χρηστών, πριν χρησιμοποιηθούν οποιαδήποτε cookie, εκτός από τα αυστηρά απαραίτητα cookies, και αφετέρου τη παροχή ακριβών και συγκεκριμένων πληροφοριών σχετικά με τα δεδομένα που παρακολουθεί το κάθε cookie και τον σκοπό τους σε απλή, σαφή και κατανοητή γλώσσα.

Στη συνέχεια απαραίτητη κρίνεται η λήψη εγγράφου και αποθήκευση συγκατάθεσης από τους χρήστες, ενώ θα πρέπει ακόμη κι αν οι χρήστες αρνούνται να επιτρέψουν τη χρήση ορισμένων cookies να είναι για αυτούς εφικτή η πρόσβαση στον εκάστοτε ιστότοπο. Παράλληλα θα πρέπει να διασφαλίζεται η εύκολη απόσυρση της συγκατάθεσή των χρηστών οποιαδήποτε στιγμή. Όσο εύκολο δηλαδή είναι για τους χρήστες να δώσουν την συγκατάθεση τους, τόσο εύκολο θα πρέπει να είναι και να την ανακαλέσουν, εάν το θελήσουν.

Παρόλα αυτά ήδη από το 2017 έχει εκφραστεί η ανάγκη για αντικατάσταση της Οδηγίας από τον Κανονισμό ePrivacy, ο οποίος θα περιλαμβάνει αναθεωρημένους κανόνες σχετικά με την προστασία της ιδιωτικής ζωής και του απορρήτου κατά τη χρήση υπηρεσιών ηλεκτρονικών επικοινωνιών.[62] Το 2021 τα κράτη μέλη της Ένωσης συμφώνησαν επί της διαπραγματευτικής εντολής για τους αναθεωρημένους κανόνες. Στο πλαίσιο της εντολής του Συμβουλίου αποφασίστηκε, ότι ο Κανονισμός θα καλύπτει το περιεχόμενο των ηλεκτρονικών επικοινωνιών που μεταδίδεται μέσω διαθέσιμων στο κοινό υπηρεσιών και δικτύων, καθώς και τα μεταδεδομένα[63] που σχετίζονται με την επικοινωνία. Επιπλέον οι κανόνες θα τυγχάνουν εφαρμογής όταν οι τελικοί χρήστες βρίσκονται στην ΕΕ. Αυτό καλύπτει επίσης περιπτώσεις στις οποίες η επεξεργασία λαμβάνει χώρα εκτός της ΕΕ ή ο πάροχος υπηρεσιών είναι εγκατεστημένος ή βρίσκεται εκτός της ΕΕ.[64]

[62] https://www.lawspot.gr/nomika-nea/kanonismos-eprivacy-egkrithike-i-thesi-toy-symvoylioy-tis-ee-gia-toys-kanones-gia-tin

[63] Τα μεταδεδομένα περιλαμβάνουν, για παράδειγμα, πληροφορίες σχετικά με τη θέση και τον χρόνο και τον αποδέκτη της επικοινωνίας. Θεωρούνται δυνητικά εξίσου ευαίσθητα με το περιεχόμενο.

[64] https://www.consilium.europa.eu/el/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

5.1.3 Ενημέρωση χρήστη και συγκατάθεση

Σύμφωνα με το άρθρο 4 παρ. 5 του ν.3471/2006 η αποθήκευση ή η απόκτηση πρόσβασης σε αποθηκευμένες πληροφορίες στον τερματικό εξοπλισμό χρήστη επιτρέπεται μόνο αν ο συγκεκριμένος χρήστης έχει δώσει τη συγκατάθεσή του μετά από σαφή και εκτενή ενημέρωση.

Κριτήριο για το κατά πόσο η ενημέρωση του χρήστη είναι σαφής και εκτενής αποτελεί το άρθρο 12 παρ. 1 του ΓΚΠΔ, σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας, ο οποίος στην συγκεκριμένη περίπτωση είναι η εκάστοτε ιστοσελίδα, λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων, δηλαδή εν προκειμένω τον χρήστη της ιστοσελίδας, κάθε πληροφορία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη σε παιδιά. Στο άρθρο 13 του Κανονισμού αναφέρονται τα στοιχεία εκείνα που θεωρούνται απαραίτητα και πρέπει να δίνονται στον χρήστη, όπως για παράδειγμα η ταυτότητα και τα στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας και, κατά περίπτωση, του εκπροσώπου του υπευθύνου επεξεργασίας.

Σύμφωνα με την ΑΠΔΠΧ « *Η ενημέρωση του συνδρομητή ή χρήστη πρέπει να γίνεται με τον προσφορότερο κάθε φορά τρόπο, ώστε να εξασφαλίζεται η επαρκής πληροφόρηση πριν από την αποθήκευση ή απόκτηση πρόσβασης στον τερματικό εξοπλισμό του.*

Η ενημέρωση πρέπει να αναρτάται σε εμφανές σημείο στην ιστοσελίδα και να είναι ειδική για κάθε περίπτωση. Μέσω του αναδυόμενου παραθύρου, πρέπει να παρέχεται στον επισκέπτη της ιστοσελίδας όχι μια γενική ενημέρωση για τη χρήση cookies, αλλά και ενημέρωση για τους σκοπούς των cookies που χρησιμοποιούνται.»[65]

Έτσι ο χρήστης είναι σε θέση να παρέχει τη συγκατάθεση του με δύο τρόπους. Αρχικά δύναται να δηλώσει την συγκατάθεση του μέσω της ιστοσελίδας του παρόχου

65 https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/electronikesepikoinwnies/cookies/enimerwsh_kai_sugatathesi_cookies

υπηρεσίας του διαδικτύου με χρήση κατάλληλων μηχανισμών (π.χ. με αναδυόμενα παράθυρα). Η αποδοχή των «cookies» μπορεί να γίνεται μία φορά για όλα τα cookies που εγκαθίστανται από τον ίδιο πάροχο υπηρεσίας της κοινωνίας της πληροφορίας. Διαφορετικά, όπως αναφέρεται στον ν. 3471/2006, η συγκατάθεση μπορεί να δίδεται και μέσω κατάλληλων ρυθμίσεων στον φυλλομετρητή ιστού ή μέσω άλλης εφαρμογής μόνο εφόσον ζητείται η συγκατάθεση του χρήστη για κάθε cookie, ενώ δεν νοείται ως συγκατάθεση η εκ των προτέρων αποδοχή της λήψης cookies μέσω προεπιλεγμένων ρυθμίσεων του φυλλομετρητή.

Σημειωτέον δε πως υπάρχουν περιστάσεις υπό τις οποίες τα cookies εξαιρούνται από την απαίτηση συναίνεσης μετά από ενημέρωση. Κατά τη γνώμη του Article 29 Data Protection Working Party[66] υφίστανται δύο κριτήρια εξαίρεσης που θεσπίζονται σύμφωνα με το άρθρο 5.3 της Οδηγίας για τα cookies: εάν το cookie (α) χρησιμοποιείται «*με αποκλειστικό σκοπό τη μετάδοση μιας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών* » ή (β) καθίσταται «*αυστηρά απαραίτητο προκειμένου ο πάροχος μιας υπηρεσίας της κοινωνίας της πληροφορίας που ζητείται ρητά από τον συνδρομητή ή τον χρήστη να παρέχει την υπηρεσία*». Εν ολίγοις η συγκατάθεση του χρήστη δεν απαιτείται, σε περιπτώσεις που τα cookies που χρησιμοποιούνται, θεωρούνται από τεχνικής απόψεως απαραίτητα για την πραγματοποίηση της σύνδεσης στον ιστότοπο ή για την παροχή της υπηρεσίας διαδικτύου.[67]

5.2 Σκοτεινά μοτίβα και ΓΚΠΔ

Εξ ορισμού, ο όρος "σκοτεινά μοτίβα" (dark patterns) περιγράφει τον σκόπιμα παραπλανητικό σχεδιασμό της διεπαφής χρήστη ενός ιστότοπου . Τα σκοτεινά μοτίβα στοχεύουν να επηρεάσουν τη συμπεριφορά των χρηστών και όχι μονό μπορούν να εμποδίσουν την ικανότητά τους να προστατεύουν αποτελεσματικά τα προσωπικά τους

[66] Αυτή η ομάδα εργασίας συστάθηκε βάσει του άρθρου 29 της οδηγίας 95/46/ΕΚ. Είναι ένα ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία των δεδομένων και την ιδιωτική ζωή. Τα καθήκοντά του περιγράφονται στο άρθρο 30 της οδηγίας 95/46/ΕΚ και στο άρθρο 15 της οδηγίας 2002/58/ΕΚ.

[67] Opinion 04/2012 on cookie consent expemption, Article 29 Data Protection Working Party βλ. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

δεδομένα αλλά και να τους οδηγήσουν στο να μην κάνουν συνειδητές επιλογές[68]. Με τη βοήθεια σκοτεινών μοτίβων, οι επισκέπτες ενός ιστότοπου δύνανται να ελέγχονται συνειδητά και να εξαπατώνται. Ως εκ τούτου, τα σκοτεινά μοτίβα αναφέρονται επίσης ως παραπλανητικά μοτίβα (deceptive patterns).

Τα σκοτεινά μοτίβα είναι, κατά μία έννοια, η σκοτεινή πλευρά του σχεδιασμού ιστοτόπων . Ήταν τελικά ο σχεδιαστής ιστοσελίδων Harry Brignull (PhD Cognitive Science) ο οποίος κατάφερε να συνοψίσει αυτές τις μεθόδους με τον όρο "Dark Patterns[69]" τον Αύγουστο του 2010.

Ειδικότερα τα όρισε ως: «Μια διεπαφή χρήστη που έχει δημιουργηθεί προσεκτικά για να ξεγελάσει τους χρήστες ώστε να κάνουν πράγματα, που δεν επιθυμούν στην πραγματικότητα, όπως το να αγοράσουν κάτι ή να πραγματοποιήσουν κάποια εγγραφή ή συνδρομή»

Ο Brignull εξηγεί περαιτέρω ότι όταν σκεφτόμαστε τον «κακό σχεδιασμό» μίας ιστοσελίδας, θα πρέπει σκεφτόμαστε ότι ο δημιουργός της είναι ατημέλητος ή τεμπέλης αλλά χωρίς κακή πρόθεση. Τα σκοτεινά μοτίβα, από την άλλη, δεν είναι λάθη. Αντιθέτως είναι προσεκτικά κατασκευασμένα με μια σταθερή κατανόηση της ανθρώπινης ψυχολογίας και δεν έχουν στο μυαλό τους το ενδιαφέρον του χρήστη, αλλά το πως θα των ωθήσουν να προβεί σε ενέργειες που δεν επιθυμεί στην πραγματικότητα.

5.2.1 Τύποι σκοτεινών μοτίβων[70]:

- **Αποτροπή σύγκρισης τιμών (Comparison prevention)**: Ο χρήστης δυσκολεύεται να συγκρίνει προϊόντα επειδή τα χαρακτηριστικά και οι τιμές συνδυάζονται με πολύπλοκο τρόπο ή επειδή είναι δύσκολο να βρεθούν βασικές πληροφορίες.
- **Ντροπή επιβεβαίωσης (Confirmshaming)**: Ο χρήστης χειραγωγείται συναισθηματικά για να κάνει κάτι που διαφορετικά δεν θα είχε κάνει.

[68] Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them βλ. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en
[69] Dark Patterns (homepage), at http://darkpatterns.org.
[70] https://www.deceptive.design/types

- **Συγκαλυμμένες διαφημίσεις (Disguised ads)**: Ο χρήστης πιστεύει λανθασμένα ότι κάνει κλικ σε ένα στοιχείο διεπαφής ή σε εγγενές περιεχόμενο, αλλά στην πραγματικότητα είναι μια συγκεκαλυμμένη διαφήμιση.
- **Ψεύτικη έλλειψη (Fake scarcity)**: Ο χρήστης πιέζεται να ολοκληρώσει μια ενέργεια επειδή παρουσιάζεται με ψεύτικη ένδειξη περιορισμένης προσφοράς ή δημοτικότητας.
- **Ψεύτικη κοινωνική απόδειξη (Fake social proof)**: Ο χρήστης παραπλανάται και πιστεύει ότι ένα προϊόν είναι πιο δημοφιλές ή αξιόπιστο από ό,τι στην πραγματικότητα, επειδή του εμφανίστηκαν ψεύτικες κριτικές, μαρτυρίες ή μηνύματα δραστηριότητας.
- **Ψεύτικη επείγουσα ανάγκη (Fake urgency):** Ο χρήστης πιέζεται να ολοκληρώσει μια ενέργεια επειδή παρουσιάζεται με ψεύτικο χρονικό περιορισμό.
- **Αναγκαστική δράση (Forced action):** Ο χρήστης θέλει να κάνει κάτι, αλλά απαιτείται να κάνει κάτι άλλο ανεπιθύμητο σε αντάλλαγμα.
- **Δύσκολο να ακυρωθεί (Hard to cancel):** Ο χρήστης θεωρεί ότι είναι εύκολο να εγγραφεί ή να εγγραφεί, αλλά όταν θέλει να ακυρώσει το βρίσκει πολύ δύσκολο.
- **Κρυφό Κόστος (Hidden Costs):** Ο χρήστης παρασύρεται με μια χαμηλή διαφημιζόμενη τιμή. Αφού επενδύσουν χρόνο και προσπάθεια, ανακαλύπτουν απροσδόκητες χρεώσεις και χρεώσεις όταν φτάνουν στο ταμείο.
- **Κρυφή συνδρομή (Hidden subscription):** Ο χρήστης είναι εν αγνοία του εγγεγραμμένος σε ένα επαναλαμβανόμενο πρόγραμμα συνδρομής ή πληρωμής χωρίς σαφή αποκάλυψη ή τη ρητή συγκατάθεσή του.
- **Γκρίνια (Nagging):** Ο χρήστης προσπαθεί να κάνει κάτι, αλλά διακόπτεται επίμονα από αιτήματα να κάνει κάτι άλλο που μπορεί να μην είναι προς το συμφέρον του.
- **Παρεμπόδιση (Obstruction):** Ο χρήστης αντιμετωπίζει εμπόδια, γεγονός που τον καθιστά δύσκολο να ολοκληρώσει την εργασία του ή να έχει πρόσβαση σε πληροφορίες.

- **Προεπιλογή (Preselection):** Ο χρήστης εμφανίζεται με μια προεπιλεγμένη επιλογή που έχει ήδη επιλεγεί για αυτόν, προκειμένου να επηρεάσει τη λήψη των αποφάσεών του.
- **Βάζω κρυφά στο καλάθι (Sneaking):**Ο χρήστης παρασύρεται σε μια συναλλαγή με ψευδείς προσχήματα, επειδή οι σχετικές πληροφορίες αποκρύπτονται ή καθυστερούν να παρουσιαστούν σε αυτόν.
- **Παιχνίδι λέξεων (Trick wording):** Ο χρήστης παραπλανάται για να προβεί σε κάποια ενέργεια, λόγω της παρουσίασης μπερδεμένης ή παραπλανητικής γλώσσας.
- **Οπτική παρεμβολή (Visual interference):** Ο χρήστης αναμένει να δει πληροφορίες που παρουσιάζονται με σαφή και προβλέψιμο τρόπο στη σελίδα, αλλά είναι κρυμμένες, συγκαλυμμένες ή συγκαλυμμένες.

Η χρήση σκοτεινών μοτίβων δεν συνιστά από μόνη της παραβίαση των κανονισμών προστασίας δεδομένων. Ωστόσο, η παραπλάνηση των χρηστών προκειμένου να ληφθεί η συγκατάθεσή τους για την επεξεργασία δεδομένων φαίνεται να είναι ιδιαίτερα προβληματική.[71]

5.2.2 Πώς ρυθμίζει ο GDPR τα Dark Patterns;

Τον Φεβρουάριο του 2023, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB)[72] δημοσίευσε οδηγίες για τα σκοτεινά μοτίβα. Όπως αναφέρεται στις κατευθυντήριες γραμμές EDPB στο άρθρο 5 του Κανονισμού υφίστανται οι αρχές προστασίας δεδομένων που ρυθμίζουν τη συμμόρφωση των διεπαφών των επιγραμμικών πλατφορμών. Ειδικότερα η αρχή της δίκαιης επεξεργασίας που ορίζεται στο άρθρο 5 παράγραφος 1 στοιχείο α του ΓΚΠΔ αποτελεί σημείο εκκίνησης για την αξιολόγηση του κατά πόσον ένα πρότυπο σχεδιασμού συνιστά πράγματι "παραπλανητικό πρότυπο σχεδιασμού".

Επιπλέον στην αξιολόγηση αυτή συμβάλει η αρχή της διαφάνειας, η οποία θεμελιώνεται στο άρθρο 12 του Κανονισμού, η αρχή της ελαχιστοποίησης των

[71] (Roman Meier, Dark Patterns, 13.04.2022, https://datenschutz.law/news/dark-patterns, abgerufen am 30.01.2024)
[72] https://edpb.europa.eu/edpb_en

δεδομένων (ή της αναλογικότητας) και της λογοδοσίας δυνάμει του άρθρου 5 παράγραφος 1 και 2 του Κανονισμού. Εξάλλου ιδιαίτερης σημασίας είναι ο περιορισμός του σκοπού δυνάμει του άρθρου 5 παράγραφος 1 στοιχείο β, ο οποίος επιβάλλει να γίνεται η συλλογή των δεδομένων για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται αυτά σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς.

Σε άλλες περιπτώσεις, η νομική αξιολόγηση ερείδεται επίσης σε όρους συναίνεσης κατά το άρθρο 4 παράγραφος 11 και το άρθρο 7 του Κανονισμού ή σε άλλες ειδικές υποχρεώσεις, όπως εκείνες που προβλέπονται στο άρθρο 12 του ΓΚΠΔ. Βέβαια, απαιτείται συμπληρωματικά να ληφθεί υπόψη το τρίτο κεφάλαιο του ΓΚΠΔ στο πλαίσιο των δικαιωμάτων των υποκειμένων των δεδομένων.

Τέλος, οι απαιτήσεις προστασίας των δεδομένων από το σχεδιασμό και από την προεπιλογή βάσει του άρθρου 25 του ΓΚΠΔ είναι καθοριστικής σημασίας, καθώς η εφαρμογή τους πριν από την έναρξη σχεδιασμού διεπαφής θα βοηθούσε τους κατόχους ιστοσελίδων να αποφεύγουν παραπλανητικά μοτίβα.

5.2.3 Dark patterns vs Nudging

Το λεγόμενο "nudging", από το "to nudge" (= απαλά ώθηση), είναι αρχικά ένας όρος από την οικονομία της συμπεριφοράς, που επινοήθηκε από τον οικονομολόγο Richard Thaler και τον νομικό επιστήμονα Cass Sunstein. Μαζί έγραψαν την τυπική εργασία 2Standardwerk2[73] για αυτό το θέμα το 2008, η οποία ισχύει ακόμα και σήμερα.

Η διαφορά μεταξύ του nudging και του dark patterns είναι κυρίως ο βαθμός χειραγώγησης, η πίεση με την οποία προωθείται μια συγκεκριμένη ενέργεια στους χρήστες και η πρόθεση ή το αποτέλεσμα. Η μετάβαση ανάμεσα σε επιτρεπτό (θετικό) nudging και απαγορευμένο nudging, το σκοτεινό πρότυπο, εξετάζεται κατά περίπτωση. Ωστόσο, κατά κανόνα, η επιτρεπόμενη ώθηση έχει ως στόχο να βοηθήσει τους χρήστες να λάβουν αποφάσεις που ανταποκρίνονται στις δικές τους μεσοπρόθεσμες ή μακροπρόθεσμες προτιμήσεις ή τουλάχιστον προωθούν τους στόχους της κοινωνίας. Αντίθετα τα σκοτεινά μοτίβα παραβλέπουν ή τουλάχιστον αγνοούν τους στόχους των

[73] Thaler, R. H., & Sunstein C. R. (2019). Nudge. Wie man kluge Entscheidungen anstößt. Berlin: Ullstein

υποκειμένων. Για παράδειγμα, επηρεάζουν τις αποφάσεις για τη διαχείριση συναίνεσης μόνο σύμφωνα με τα συμφέροντα των διαχειριστών ιστοσελίδων.[74]

Ενώ τα σκοτεινά μοτίβα είναι έντονα απορριπτέα, η χρήση των Nudging είναι από πρακτικής απόψεως δυνατή και εξακολουθεί να συμμορφώνεται με το νόμο. Σύμφωνα με μία έρευνα που διεξήχθη τον Νοέμβριο του 2019 στην Αγγλία [75] παρατηρήθηκε πως οι ειδοποιήσεις συγκατάθεσης, σε ποσοστό 57,4%, χρησιμοποιούν το σχεδιασμό της διεπαφής για να κατευθύνουν τους επισκέπτες του ιστότοπου προς την αποδοχή επιλογών που δεν είναι φιλικές προς την ιδιωτική ζωή. Οι τυπικές τεχνικές περιλαμβάνουν την υπογράμμιση χρώματος του κουμπιού για να αποδεχθούν οι χρήστες προεπιλεγμένες ρυθμίσεις που παραβιάζουν τα προσωπικά τους δεδομένα, την απόκρυψη επιπρόσθετων ρυθμίσεων πίσω από σύνδεσμους που είναι δύσκολο να δει κανείς και την προεπιλογή πλαισίων ελέγχου που ενεργοποιούν τη συλλογή δεδομένων.

«*Εάν ένας χρήστης δεν έχει πλέον πραγματική ελευθερία επιλογής μεταξύ συναίνεσης και απόρριψης ως αποτέλεσμα τέτοιων μέτρων ώθησης, το όριο του επιτρεπόμενου έχει ξεπεραστεί*», λέει η Barbara Thiel, Κρατική Επίτροπος Προστασίας Δεδομένων για την Πολιτεία της Κάτω Σαξονίας[76]. Τούτη η άποψη διατυπώθηκε μετά από εξέταση cookies και υπηρεσιών τρίτων σε ιστότοπους της Κάτω Σαξονίας, όπου και διαπιστώθηκε πως ορισμένοι ιστότοποι «ανάγκασαν» τους χρήστες να συναινέσουν χρησιμοποιώντας το λεγόμενο Nudging. Στόχος ήταν να επηρεαστεί ανεπαίσθητα η συμπεριφορά των χρηστών μέσω λεπτών παρεμβάσεων. Σε ιστότοπους, αυτό συμβαίνει συχνά επειδή η επιλογή "Συμφωνώ" στο banner των cookies είναι πιο εμφανής ως προς το χρώμα σε σύγκριση με την επιλογή "Απόρριψη" ή η διαδικασία απόρριψης περιπλέκεται άσκοπα από μεγαλύτερες διαδρομές κλικ.

Σε καμία περίπτωση, τα nudging στοιχεία στο banner δεν πρέπει να θεωρηθεί ότι εμπίπτουν στην περιοχή της εξαπάτησης ή της χειραγώγησης. Αυτό μπορεί να έχει όχι μόνο σοβαρές νομικές συνέπειες για τις ιστοσελίδες που τα υιοθετούν, αλλά και να

[74] Martini, die Phänomenologie und Antworten der Rechtsordnung (2020) Σελ. 51: https://rsw.beck.de/docs/librariesprovider132/default-document-library/zfdr_heft_2021-01.pdf
[75] (Un)informed Consent: Studying GDPR Consent Notices in the Field: https://dl.acm.org/doi/pdf/10.1145/3319535.3354212
[76] https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/prufung-zu-cookies-und-drittdiensten-auf-nieder-sachsischen-webseiten-194909.html

δημιουργήσει μια αρνητική εικόνα για την εταιρεία και την επωνυμία, αν οι πελάτες αυτής αισθανθούν ότι εξαπατήθηκαν.

Κεφάλαιο 6ο
Διεθνείς μεταφορές δεδομένων

Οι ροές προσωπικών δεδομένων προς και από την Ευρωπαϊκή Ένωση είναι όχι μόνο απαραίτητες, αλλά και αναγκαίες για το διεθνές εμπόριο και τη διεθνή συνεργασία. Η διασυνοριακή μεταφορά δεδομένων έχει γίνει μέρος της καθημερινής λειτουργίας ευρωπαϊκών εταιρειών όλων των μεγεθών, σε όλους τους τομείς.[77]

Ωστόσο, η διαβίβαση τέτοιων δεδομένων προσωπικού χαρακτήρα από την ΕΕ σε υπευθύνους επεξεργασίας και εκτελούντες την επεξεργασία που βρίσκονται εκτός της ΕΕ σε τρίτες χώρες, δεν θα πρέπει επ ουδενί λόγω να υπονομεύει το επίπεδο προστασίας των ενδιαφερομένων ατόμων, καθώς ως τρίτη χώρα νοείται οποιαδήποτε χώρα εκτός του Ευρωπαϊκού Οικονομικού Χώρου («ΕΟΧ»). Για τον λόγο αυτό, οι διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς θα πρέπει να γίνονται πάντοτε με πλήρη συμμόρφωση με το Κεφάλαιο V του Γενικού Κανονισμού Προστασίας Δεδομένων.

6.1 Απόφαση επάρκειας

Οι αποφάσεις επάρκειας έθεσαν τα θεμέλια για στενότερη συνεργασία και περαιτέρω κανονιστική σύγκλιση μεταξύ της ΕΕ και των ομοειδών εταίρων. Με τη θέσπιση της ελεύθερης κυκλοφορίας των δεδομένων προσωπικού χαρακτήρα, οι αποφάσεις αυτές άνοιξαν εμπορικούς δίαυλους για τους φορείς της ΕΕ συμπληρώνοντας και ενισχύοντας τα οφέλη των εμπορικών συμφωνιών, καθώς και τη διευκόλυνση της συνεργασίας με ξένους εταίρους σε ένα ευρύ φάσμα κανονιστικών τομέων.

[77] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC

Κατά ρητή επιταγή του άρθρου 45 του Κανονισμού *«Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί εφόσον η Επιτροπή έχει* ***αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας*** *από την τρίτη χώρα, από έδαφος ή από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα ή από τον εν λόγω διεθνή οργανισμό. Για μια τέτοια διαβίβαση δεν απαιτείται ειδική άδεια.»*

Για να ληφθεί, λοιπόν, μία τέτοια απόφαση απαραίτητη είναι η ύπαρξη πρότασης εκ μέρους της Ευρωπαϊκής Επιτροπής και μετά την γνώμη του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, να εγκριθεί η πρόταση αυτή από εκπροσώπους χωρών της ΕΕ. Έπειτα η απόφαση επάρκειας υιοθετείται από την Ευρωπαϊκή Επιτροπή.

Προκειμένου να εκτιμηθεί η επάρκεια του επιπέδου προστασίας η Επιτροπή λαμβάνει υπόψιν της μεταξύ άλλων, τόσο το επίπεδο του κράτους δικαίου, όσο και το σεβασμό των ανθρωπίνων δικαιωμάτων και των θεμελιωδών ελευθεριών. Επίσης σημαντικό κριτήριο αποτελεί η σχετική νομοθεσία, η ύπαρξη και η αποτελεσματική λειτουργία ανεξάρτητων εποπτικών αρχών, συμπεριλαμβανομένων βεβαίως των επαρκών εξουσιών επιβολής στα ζητήματα προστασίας των υποκείμενων των δεδομένων. Τέλος λαμβάνονται υπόψιν οι διεθνείς δεσμεύσεις που τυχόν έχει αναλάβει η υπό κρίση τρίτη χώρα ή ο διεθνής οργανισμός ή άλλες υποχρεώσεις που δύνανται να απορρέουν από νομικά δεσμευτικές συμβάσεις.

Εφόσον μια μεταφορά δεδομένων καλύπτεται από απόφαση επάρκειας, δεν απαιτούνται επιπρόσθετα προστατευτικά μέτρα. Μέχρι στιγμής υπάρχουν αποφάσεις επάρκειας, για τις ακόλουθες χώρες: το Ισραήλ, την Αργεντινή, την Ιαπωνία και τον Καναδά (μόνο σε σχέση με τον ιδιωτικό τομέα), τη Νέα Ζηλανδία, την Ελβετία, την Ουρουγουάη, το Ηνωμένο Βασίλειο, τις ΗΠΑ (μόνο σε σχέση με εταιρείες και οργανισμούς των ΗΠΑ που συμμετέχουν στο Πλαίσιο Προστασίας Προσωπικών Δεδομένων ΕΕ-ΗΠΑ (ΕΕ-ΗΠΑ DPF). Συγκεκριμένα καθίστανται επιτρεπτές από τον Κανονισμό διαβιβάσεις τόσο σε τρίτες χώρες, όσο και σε έδαφος ή συγκεκριμένο τομέα εντός αυτής της τρίτης χώρας, με αποτέλεσμα να δύναται να αποτελέσει κριτήριο για την

απόφαση επάρκειας μία «τομεακή» νομοθεσία, όπως για παράδειγμα, για τη υγεία ή τον χρηματοπιστωτικό τομέα.[78]

Φυσικά η Επιτροπή, για να εξασφαλίσει την ασφάλεια των διαβιβάσεων δεδομένων και να ενισχύσει εάν απαιτείται την προστασία των υποκειμένων των δεδομένων, δεν επαναπαύεται μετά τη λήψη αποφάσεων επάρκειας, αλλά κατά διαστήματα επανεξετάζει τις αποφάσεις επάρκειας και γνωστοποιεί στο Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο τα όποια ευρήματα της.

6.2 Η απόφαση επάρκειας της Ιαπωνίας

Τον Ιανουάριο του 2019 η Ευρωπαϊκή Επιτροπή εξέδωσε απόφαση επάρκειας σε σχέση με διαβιβάσεις προσωπικών δεδομένων από την ΕΕ σε επιχειρήσεις στην Ιαπωνία. Η απόφαση επάρκειας σηματοδότησε την μη περαιτέρω λήψη μέτρων και τήρηση τυπικών συμβατικών ρητρών της ΕΕ κατά τη μεταφορά προσωπικών δεδομένων από αυτή σε επιχειρήσεις στην Ιαπωνία. Η Ευρωπαϊκή Επιτροπή θεώρησε όμως ότι η απόφαση αυτή θα πρέπει να επανεξεταστεί εντός δύο ετών από την έναρξη ισχύος της.

Πράγματι τον Απρίλιο του 2023, η Ευρωπαϊκή Επιτροπή ολοκλήρωσε την πρώτη επανεξέταση της απόφασης επάρκειας της Ιαπωνίας. Ειδικότερα, η Ευρωπαϊκή Επιτροπή παρατήρησε αυξημένη σύγκλιση μεταξύ των πλαισίων προστασίας δεδομένων στην ΕΕ και την Ιαπωνία και χαιρέτισε τη δημιουργία σημείων επαφής για τα άτομα της ΕΕ σχετικά με την επεξεργασία δεδομένων στην Ιαπωνία, καθώς και την επέκταση των διασφαλίσεων στον ακαδημαϊκό και στον δημόσιο τομέα. Επιπροσθέτως η Ευρωπαϊκή Επιτροπή διατύπωσε την άποψη ότι οι μελλοντικές αναθεωρήσεις της απόφασης επάρκειας θα πρέπει να πραγματοποιούνται κάθε τέσσερα χρόνια και όχι κάθε δύο χρόνια υπό το φως της θετικής φύσης της πρώτης επανεξέτασης. Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων συμφώνησε με την αξιολόγηση της Ευρωπαϊκής Επιτροπής[79].

[78] Κ. Λωσταράκου σε: Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

[79] https://edpb.europa.eu/news/news/2023/edpb-informs-stakeholders-about-implications-dpf-and-adopts-statement-first-review_en

6.3 Κατάλληλες εγγυήσεις

Ελλείψει απόφασης επάρκειας βάσει του άρθρου 45 παράγραφος 3 του Κανονισμού, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δύναται να προβεί σε διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό μόνο υπό την προϋπόθεση, ότι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχει παράσχει κατάλληλες εγγυήσεις και εφόσον ισχύουν εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων.[80]

Στον Γενικό Κανονισμό Προστασίας Δεδομένων προβλέπονται οι κατάλληλες εγγυήσεις, οι οποίες δεν απαιτούν την έκδοση ειδικής άδειας από την εποπτική αρχή, προκειμένου να επιτραπεί η διαβίβαση δεομένων σε Τρίτη χώρα.

Αναλυτικότερα οι εγγυήσεις αυτές συνίστανται στη χρήση:

i. Τυποποιημένων ρητρών προστασίας δεδομένων θεσπιζομένων από την Επιτροπή,

ii. Τυποποιημένων ρητρών προστασίας δεδομένων θεσπιζομένων από την εποπτική αρχή,

iii. Δεσμευτικών εταιρικών κανόνων (Binding Corporate Rules),

iv. Εγκεκριμένου κώδικα δεοντολογίας (άρθρο 40 ΓΚΠΔ),

v. Εγκεκριμένου μηχανισμού πιστοποίησης (άρθρο 42 ΓΚΠΔ),

vi. Νομικά δεσμευτικού και εκτελεστού μέσου μεταξύ δημοσίων αρχών.

6.4 Τυπικές ρήτρες προστασίας δεδομένων

Οι τυπικές ρήτρες προστασίας δεδομένων, τις οποίες εκδίδει η Ευρωπαϊκή Επιτροπή, μπορούν να αξιοποιηθούν ως βάση για διαβιβάσεις δεδομένων σε τρίτες χώρες

[80] Άρθρο 46 του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, 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

και διεθνείς οργανισμούς χωρίς περαιτέρω έγκριση από τις εποπτικές αρχές, εάν ενσωματωθούν στις υποκείμενες συμβάσεις ουσιαστικά αμετάβλητες.

Η Ευρωπαϊκή Επιτροπή εξέδωσε τον Ιούνιο του 2021 τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου[81]. Στο πλαίσιο της διαδικασίας, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων εξέδωσαν κοινή γνώμη[82] . Οι νέες ρήτρες εναρμονίζονται με τις απαιτήσεις του ΓΚΠΔ και αποσκοπούν στην εξασφάλιση ενός υψηλού επιπέδου προστασίας των προσωπικών δεδομένων, λαμβάνοντας υπόψη τις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στη σύγχρονη ψηφιακή εποχή.[83]

Οι εποπτικές αρχές έχουν την δυνατότητα να συντάξουν τις δικές τους τυπικές ρήτρες προστασίας δεδομένων, υπό την προϋπόθεση του συντονισμού τους με τις άλλες ευρωπαϊκές εποπτικές αρχές και την επακόλουθη έγκριση τους από την Ευρωπαϊκή Επιτροπή.

6.5 Δεσμευτικοί εσωτερικοί κανονισμοί προστασίας δεδομένων (Δεσμευτικοί εταιρικοί κανόνες – BCR)

Τα BCR είναι νομικά δεσμευτικοί και εφαρμοστέοι εσωτερικοί κανόνες και πολιτικές για τη μεταφορά δεδομένων εντός εταιρειών πολυεθνικών ομίλων και λειτουργούν με τρόπο, που παρουσιάζει αρκετές ομοιότητες, με έναν εσωτερικό κώδικα δεοντολογίας. Επιτρέπουν σε πολυεθνικές εταιρείες να μεταφέρουν προσωπικά δεδομένα διεθνώς εντός του ίδιου εταιρικού ομίλου σε χώρες που δεν παρέχουν επαρκές επίπεδο προστασίας για τα προσωπικά δεδομένα, όπως απαιτείται βάσει του GDPR.

Το BCR απαιτείται να είναι νομικά δεσμευτικό για όλα τα μέλη του ομίλου εταιρειών και να παρέχει εκτελεστά δικαιώματα στα υποκείμενα των δεδομένων. Οι εταιρείες, από την μεριά τους, υποχρεούνται να υποβάλλουν δεσμευτικούς εταιρικούς

[81] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj
[82] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en
[83] https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres

κανόνες προς έγκριση στην αρμόδια αρχή προστασίας δεδομένων στην ΕΕ. Τα BCR πρέπει να εγκρίνονται από την αρμόδια εποπτική αρχή, σύμφωνα με τον κανονισμό συνεκτικότητας που προβλέπεται στο άρθρο 63του Κανονισμού.

Τέλος η αρμόδια αρχή κοινοποιεί το σχέδιο απόφασής της στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, το οποίο θα εκδώσει τη γνώμη του για τους δεσμευτικούς εταιρικούς κανόνες.[84]

6.6 Εγκεκριμένος Κώδικας Δεοντολογίας ή εγκεκριμένος μηχανισμός πιστοποίησης

Σύμφωνα με τον ΓΚΠΔ, τόσο οι ειδικοί για τον κλάδο κώδικες δεοντολογίας όσο και οι μηχανισμοί πιστοποίησης μπορούν να αποτελέσουν τη βάση για τις διεθνείς διαβιβάσεις δεδομένων εάν έχουν εγκριθεί από την αρμόδια εποπτική αρχή ή έχουν εκδοθεί από τον φορέα πιστοποίησης ή την εποπτική αρχή. Ωστόσο, αυτές οι πράξεις πρέπει να συνοδεύονται από νομικά δεσμευτικές και εκτελεστές υποχρεώσεις του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία στην τρίτη χώρα, ιδίως όσον αφορά τα δικαιώματα των θιγόμενων.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων έχει αναπτύξει κατευθυντήριες γραμμές για το νομικό πλαίσιο και τα διαδικαστικά ζητήματα, για να διασφαλίσει τη συνεπή εφαρμογή αυτών των νέων μέσων μεταφοράς.

6.7 Ειδικές εγγυήσεις για τις δημόσιες αρχές

Ο ΓΚΠΔ δεν ορίζει ξεκάθαρα τι συνιστά «δημόσια αρχή ή δημόσιο φορέα». Το ΕΣΠΔ θεωρεί ότι η εν λόγω έννοια είναι αρκετά ευρεία, ώστε να καλύπτει τόσο τους δημόσιους φορείς σε τρίτες χώρες όσο και τους διεθνείς οργανισμούς. Ως εκ τούτου, οι δημόσιοι φορείς περιλαμβάνουν κρατικές αρχές σε διάφορα επίπεδα (π.χ. εθνικές, περιφερειακές και τοπικές αρχές), αλλά μπορούν επίσης να περιλαμβάνουν και άλλους

[84] commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

οργανισμούς δημοσίου δικαίου (π.χ. εκτελεστικούς οργανισμούς, πανεπιστήμια, νοσοκομεία κ.λπ.). Σύμφωνα με το ΓΚΠΔ, ως «διεθνής οργανισμός» νοείται ο οργανισμός και οι υπαγόμενοι σε αυτόν φορείς που διέπονται από το δημόσιο διεθνές δίκαιο ή οποιοσδήποτε άλλος φορέας που έχει ιδρυθεί δυνάμει ή επί τη βάσει συμφωνίας μεταξύ δύο ή περισσότερων χωρών.[85]

Οι αρχές και οι δημόσιοι φορείς μπορούν να μεταφέρουν δεδομένα με δύο τρόπους, είτε μέσω μιας νομικά δεσμευτικής και εκτελεστής πράξης μεταξύ δημόσιων αρχών ή φορέων(άρθρο 46 παράγραφος 2 στοιχείο α), είτε δυνάμει των διατάξεων που αναφέρονται στο άρθρο 46 παράγραφος 3 στοιχείο β του ΓΚΠΔ, να ενσωματωθούν σε διοικητικές ρυθμίσεις μεταξύ δημόσιων αρχών ή φορέων που περιλαμβάνουν εκτελεστά και αποτελεσματικά δικαιώματα στο υποκείμενο των δεδομένων.

Τα μέσα αυτά δύνανται να λάβουν τη μορφή μίας διμερούς ή πολυμερούς συμφωνίας. Η αρχή προστασίας δεδομένων αξιολογεί τις διοικητικές ρυθμίσεις κατά περίπτωση, δεδομένου ότι απαιτούν την άδεια της εποπτικής αρχής και πάντοτε διεκπεραιώνονται σύμφωνα με τον μηχανισμό συνοχής που προβλέπεται στο άρθρο 63 του Κανονισμού.

Το διαβιβάζον μέρος οφείλει σε κάθε περίπτωση να αξιολογήσει εάν η τρίτη χώρα εγγυάται ουσιαστικά ισοδύναμο επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα, που διαβιβάζονται, με αυτό που διασφαλίζεται εντός της Ένωσης. Σκοπός της αξιολόγησης αυτής είναι να καθοριστεί εάν οι διασφαλίσεις που αναφέρονται στη διεθνή συμφωνία ή τη διοικητική ρύθμιση μπορούν να εφαρμοστούν στην πράξη.

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) έχει εκδώσει γενικές οδηγίες για τις διασφαλίσεις που πρέπει να ενσωματωθούν σε διεθνείς συμφωνίες ή διοικητικές ρυθμίσεις μεταξύ δημόσιων φορέων.

[85] Κατευθυντήριες γραμμές 2/2020 σχετικά με το άρθρο 46 παράγραφος 2 στοιχείο α) και το άρθρο 46 παράγραφος 3 στοιχείο β) του κανονισμού 2016/679 για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και δημόσιων αρχών και φορέων εκτός ΕΟΧ

6.8 Εξαιρέσεις

Οι παρεκκλίσεις βάσει του άρθρου 49 ΓΚΠΔ αποτελούν εξαιρέσεις από τη γενική αρχή ότι τα δεδομένα προσωπικού χαρακτήρα μπορούν να διαβιβάζονται σε τρίτες χώρες, μόνο εάν προβλέπεται επαρκές επίπεδο προστασίας στην τρίτη χώρα ή εάν έχουν τεθεί σε ισχύ κατάλληλες εγγυήσεις.

Σύμφωνα με το άρθρο 49 ΓΚΠΔ διαβιβάσεις δεδομένων σε τρίτη χώρα λαμβάνουν χώρα μόνον εφόσον:

α) το υποκείμενο των δεδομένων συγκατατέθηκε ρητώς στην προτεινόμενη διαβίβαση, αφού ενημερώθηκε για τους πιθανούς κινδύνους που εγκυμονούν τέτοιες διαβιβάσεις για το υποκείμενο των δεδομένων λόγω απουσίας απόφασης επάρκειας και κατάλληλων εγγυήσεων,

β) η διαβίβαση είναι απαραίτητη για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας ή για την εφαρμογή προσυμβατικών μέτρων τα οποία λαμβάνονται κατόπιν αιτήματος του υποκειμένου των δεδομένων,

γ) η διαβίβαση είναι απαραίτητη για τη σύναψη ή την εκτέλεση σύμβασης η οποία συνήφθη προς όφελος του υποκειμένου των δεδομένων μεταξύ του υπευθύνου επεξεργασίας και άλλου φυσικού ή νομικού προσώπου,

δ) η διαβίβαση είναι απαραίτητη για σημαντικούς λόγους δημόσιου συμφέροντος,

ε) η διαβίβαση είναι απαραίτητη για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων,

στ) η διαβίβαση είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλων προσώπων, εφόσον το υποκείμενο των δεδομένων δεν έχει τη φυσική ή νομική ικανότητα να παράσχει τη συγκατάθεσή του,

ζ) η διαβίβαση πραγματοποιείται από μητρώο το οποίο σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους προορίζεται για την παροχή πληροφοριών στο κοινό και είναι ανοικτό για αναζήτηση πληροφοριών είτε στο ευρύ κοινό είτε σε οποιοδήποτε πρόσωπο μπορεί να επικαλεστεί έννομο συμφέρον, αλλά μόνο εφόσον πληρούνται στην

εκάστοτε περίπτωση οι προϋποθέσεις που προβλέπονται στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους για την αναζήτηση πληροφοριών.

Κεφάλαιο 7ο

ΓΚΠΔ και εργασιακές σχέσεις

Ο Κανονισμός προστατεύει το άτομο από την επεξεργασία των προσωπικών του δεδομένων σε κάθε έκφανση της ζωής του, συμπεριλαμβανομένου και του πεδίου των εργασιακών του σχέσεων. Μπορεί να μην προβλέπονται από τον ΓΚΠΔ ξεχωριστοί κανόνες, που να ρυθμίζουν ενδελεχώς τον τομέα της εργασίας, ωστόσο υφίστανται ορισμένες οδηγίες από την ΑΠΔΠΧ αλλά και την Ομάδα εργασίας του άρθρου 29, οι οποίες καλύπτουν τα ζητήματα προστασίας δεδομένων στον εργασιακό χώρο.

Πιο συγκεκριμένα ο Κανονισμός είτε προβαίνει απευθείας σε ειδική μνεία για τις εργασιακές σχέσεις, όπως για την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων (άρθρο 9), είτε εξουσιοδοτεί τα κράτη μέλη να προβλέπουν με ειδικές διατάξεις την προσαρμογή. Ειδικά δε για τις σχέσεις εργασίας συναντάται στο άρθρο 88 ρητή εκτεταμένη εξουσιοδότηση.[86] Οι ειδικοί κανόνες που δύνανται να προβλέπουν τα κράτη μέλη αφορούν όλα τα στάδια της απασχόλησης, δηλαδή την πρόσληψη, την σύμβαση εργασίας αλλά και την απόλυση.

Σημαντικό δε στο σημείο αυτό είναι πως ο Κανονισμός στις προβλεπόμενες ρυθμίσεις του δεν προβαίνει σε διακρίσεις ή διαφοροποιήσεις ανάλογα με το μέγεθος της επιχείρησης, αντίθετα με το εργατικό δίκαιο στο οποίο τέτοιες διαφοροποιήσεις συναντώνται συχνά. Αυτό φυσικά δημιουργεί ορισμένα προβλήματα ιδίως στις μικρότερες επιχειρήσεις, οι οποίες αδυνατούν να αναλάβουν το κόστος προσφυγής σε κατάλληλα καταρτισμένους επαγγελματίες, προκειμένου να τους βοηθήσουν να επιτύχουν την πλήρη και ορθή συμμόρφωση με τις επιταγές του Κανονισμού. Εξαίρεση αποτελούν τα άρθρα 30 και 40 του ΓΚΠΔ στα οποία λαμβάνεται υπόψιν το μέγεθος της εκάστοτε επιχείρησης για τον τρόπο εφαρμογής των εν λόγω ρυθμίσεων.

[86] Δ. Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το Γενικό Κανονισμό Προστασίας Δεδομένων, 2019, σ. 55

7.1 Συλλογή και επεξεργασία δεδομένων των εργαζομένων

Η συλλογή και επεξεργασία δεδομένων ενός εργαζομένου, για να είναι σύννομη προϋποθέτει την πλήρη εναρμόνιση με τις αρχές που διέπουν τον Κανονισμό, όπως για παράδειγμα την αρχή της αναλογικότητας, του σκοπού και του χρονικού περιορισμού της περιόδου αποθήκευσης. Ένεκα τούτου μπορεί να λεχθεί ότι η συλλογή και επεξεργασία προσωπικών δεδομένων του εργαζομένου επιτρέπεται μόνον όταν αυτή γίνεται για σκοπούς της σχέσης απασχόλησης και περιορίζεται στα δεδομένα εκείνα που είναι αναγκαία εν όψει του ειδικότερου κάθε φορά σκοπού συλλογής και επεξεργασίας[87]. Φυσικά η συλλογή και επεξεργασία θα πρέπει να επηρεάζει όσο το δυνατόν λιγότερο τη προσωπική ζωή του εργαζομένου και σε περίπτωση ύπαρξης ηπιότερων μέτρων επίτευξης του σκοπού, αυτά πρέπει να προτιμώνται.

Τα παραπάνω ισχύουν για όλα τα στάδια της εργασιακής σχέσης, αλλά και κατά την διαδικασία που προηγείται της πρόληψης, κατά την οποία εργασιακή εξάρτηση δεν υφίσταται. Ειδικότερα η συλλογή και επεξεργασία δεδομένων των υποψήφιων εργαζομένων θα πρέπει να περιορίζεται στα δεδομένα εκείνα που επιτρέπουν στον εργοδότη να αντιληφθεί την καταλληλότητα του εκάστοτε υποψήφιου για κάποια θέση εργασίας. Από τη στιγμή όμως που θα εκκινήσει η εργασιακή σχέση τότε *η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων πρέπει να πραγματοποιείται με θεμιτά μέσα και με τρόπο ώστε να διασφαλίζεται ο σεβασμός της προσωπικότητας και της ανθρώπινης αξιοπρέπειας των εργαζομένων στο χώρο της εργασίας και γενικότερα στο πλαίσιο των εργασιακών σχέσεων. Μάλιστα η συλλογή και επεξεργασία προσωπικών δεδομένων των εργαζομένων επιτρέπεται αποκλειστικά για σκοπούς που συνδέονται άμεσα με τη σχέση απασχόλησης και εφόσον είναι αναγκαία για την εκπλήρωση των εκατέρωθεν υποχρεώσεων που θεμελιώνονται σε αυτή τη σχέση, είτε αυτές πηγάζουν από το νόμο είτε από σύμβαση.* [88]

Συνάγεται επομένως το δικαίωμα του εργοδότη να πληροφορηθεί όχι μόνο για την οικονομική κατάσταση του εργαζομένου ή για την υγεία του, αλλά και να λάβει πληροφορίες που αφορούν «ευαίσθητα» προσωπικά δεδομένα των εργαζομένων, όπως για παράδειγμα το εάν αυτοί συνδικαλίζονται, εφόσον βέβαια αυτό είναι κρίσιμο για τον

[87] Δ. Ζερδελής, Εργατικό Δίκαιο, 5η έκδ., 2022, § 21, σ. 1127, αρ. 123 = sakkoulas-online

[88] 353/2009 ΑΠ

καθορισμό της εφαρμοστέας συλλογικής σύμβασης και της παρακράτησης υπέρ του σωματείου των συνδικαλιστικών εισφορών[89].

Σε κάθε περίπτωση ο εργοδότης είναι υποχρεωμένος να ενημερώσει τον εργαζόμενο αφενός για τους σκοπούς και τη νομική βάση επεξεργασίας και αφετέρου για τα δικαιώματα του[90]. Πρόκειται για μία θεμελιώδη υποχρέωση, καθώς η συγκατάθεση του υποκειμένου και εν προκειμένω του εργαζομένου είναι απαιτούμενο της σύννομης επεξεργασίας. Ωστόσο έχει διαπιστωθεί ανεπάρκεια της συγκατάθεσης ως αυτοτελούς νομικής βάσης για την επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων , εξαιτίας του στοιχείου της εξάρτησης από τον εργοδότη τους[91].

Όπως υποστηρίζει το ΕΣΠΔ μεταξύ εργοδότη και εργαζομένου υπάρχει ένεκα της σχέσης εξάρτησης που τους συνδέει μία ανισορροπία δυνάμεων, η οποία καθιστά απίθανο να είναι ο εργαζόμενος σε θέση να παράσχει ελεύθερα την συγκατάθεση του για επεξεργασία των δεδομένων του. Τούτο συνάγεται λόγω του φόβου ή και του κινδύνου των δυσμενών συνεπειών που θα επιφέρει η ενδεχόμενη άρνηση του για επεξεργασία των δεδομένων του.

Οι ανωτέρω σκέψεις οδήγησαν το ΕΣΠΔ στην άποψη πως η συγκατάθεση του εργαζομένου καταρχήν δεν συνιστά πρόσφορη νομική βάση για την επεξεργασία προσωπικών δεδομένων από τον εργοδότη. Εξαίρεση φυσικά αποτελεί η περίπτωση που δίνεται η επιλογή της άρνησης παροχής συγκατάθεσης στον εργαζόμενο χωρίς να υφίσταται ο κίνδυνος για επιβολή κυρώσεων.[92]

Σε όλα αυτά όμως θα πρέπει να μην ξεχνάμε τις δυνατότητες που προσφέρει η χρήση της τεχνολογίας. Με μία περιήγηση στο διαδίκτυο και τα μέσα κοινωνικής δικτύωσης ο εργοδότης μπορεί να συλλέξει πληροφορίες είτε για έναν υποψήφιο εργαζόμενο, είτε για κάποιον που ήδη απαρτίζει το εργατικό δυναμικό της επιχείρησης του. Δεδομένα άλλωστε ο εργοδότης συλλέγει για τους εργαζόμενους του και μέσω του συστήματος βιντεοεπιτήρησης, που μπορεί να έχει εγκαταστήσει στην επιχείρηση του ή την παρακολούθηση των ηλεκτρονικών τους υπολογιστών, μέσω ειδικών εφαρμογών.

---

[89] Δ. Ζερδελής, Εργατικό Δίκαιο, 5η έκδ., 2022, § 21, σ. 1127, αρ. 123 = sakkoulas-online

[90] ΑΠΔΠΧ 26/2019 βλ. https://www.dpa.gr/sites/default/files/2020-05/26_2019anonym.pdf

[91] Ζωγραφόπουλος Δ. σε Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

[92] Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679, βλ. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_el.pdf

7.2 Νομική προστασία των εργαζομένων

Σε περίπτωση που τα προσωπικά δεδομένα του εργαζομένου παραβιάζονται, τότε εκείνος έχει το δικαίωμα να αρνηθεί την παροχή εργασίας έως ότου αρθεί η παραβίαση. Η ένσταση της επίσχεσης θεωρείται η πιο κατάλληλη νομική επιλογή του εργαζομένου, δεδομένου ότι η παροχή της εργασίας δεν καθίσταται αδύνατη με υπαιτιότητα του εργοδότη, ώστε να εφαρμοστεί η ΑΚ 381 παρ. 1, ενώ δεν υπάρχει στενή ανταλλακτική σχέση με την παροχή της εργασίας, ώστε να ανατρέξουμε στην ΑΚ 374. Επίσης, η παραβίαση των προσωπικών δεδομένων δεν ισοδυναμεί με άρνηση του εργοδότη να συμπράξει στην παροχή της εργασίας, ώστε να εφαρμοστεί η ΑΚ 351[93].

Κεφάλαιο 8ο
Ο ΓΚΠΔ στον τομέα της υγείας

Σύμφωνα με την ΑΠΔΠΧ ως δεδομένα υγείας ορίζονται *«τα δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με την παρελθούσα, τρέχουσα ή μελλοντική σωματική και ψυχική υγεία ενός προσώπου (άρθρο 4 στοιχ. 15 ΓΚΠΔ)»*[94]. Ειδικότερα πρόκειται για πληροφορίες που αφορούν στη λήψη φαρμάκων, τη χρήση ναρκωτικών ή σχετίζονται με την ψυχική υγεία, χωρίς να γίνεται διαφοροποίηση μεταξύ σοβαρών ή απλών συμβάντων υγείας (π.χ. μεταξύ μίας απλής εκδοράς του δέρματος και μίας σοβαρής ψυχικής παθήσεως)[95].

Αξιοσημείωτο είναι πως το ιατρικό απόρρητο αποτελεί μία ευρύτερη έννοια από τα δεδομένα υγείας, καθώς αυτό αφορά οποιοδήποτε στοιχείο υποπίπτει στην αντίληψη του ιατρού ή του αποκαλύπτει ο ασθενής ή οι τρίτοι στο πλαίσιο ασκήσεως των καθηκόντων του και αφορά στον ασθενή ή τους οικείους του, κατά το άρθρο 13 του ν. 3418/2005 (Κώδικα Ιατρικής Δεοντολογίας) και κατ' επέκταση κάθε πληροφορία που

[93] Δ. Σιδέρης, Επίσχεση εργασίας, 2019, σ. 121 = sakkoulas-online
[94] https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eidikeskatigories/dedomenaugeias
[95] Φ. Παναγοπούλου, Χορήγηση δεδομένων υγείας με άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ): μία θεσμική αποτίμηση, ΕφημΔΔ 6/2015.755-771 = sakkoulas-online

προστατεύεται από το ιατρικό απόρρητο, είναι σημαντικό να διευκρινιστεί πως δεν συνιστά απαραιτήτως ευαίσθητο δεδομένα υγείας[96].

8.1 Τα δεδομένα υγείας και η συλλογή τους

Όπως παρατίθεται λεπτομερώς στην αιτιολογική σκέψη 35 ΓΚΠΔ στα δεδομένα υγείας περιλαμβάνονται πληροφορίες σχετικά με το φυσικό πρόσωπο που συλλέγονται κατά την εγγραφή για υπηρεσίες υγείας, τα οποία μπορεί να συνίστανται σε έναν αριθμό, ένα σύμβολο ή ένα χαρακτηριστικό ταυτότητας που αποδίδεται σε φυσικό πρόσωπο με σκοπό την πλήρη ταυτοποίηση του φυσικού προσώπου για σκοπούς υγείας.

Επιπλέον περιλαμβάνονται πληροφορίες που προκύπτουν από εξετάσεις ή αναλύσεις σε μέρος ή ουσία του σώματος, μεταξύ άλλων από γενετικά δεδομένα και βιολογικά δείγματα και περαιτέρω κάθε πληροφορία, παραδείγματος χάριν, σχετικά με ασθένεια, αναπηρία, κίνδυνο ασθένειας, ιατρικό ιστορικό, κλινική θεραπεία ή τη φυσιολογική ή βιοϊατρική κατάσταση του υποκειμένου των δεδομένων, ανεξαρτήτως πηγής, παραδείγματος χάριν, από ιατρό ή άλλο επαγγελματία του τομέα της υγείας, νοσοκομείο, ιατρική συσκευή ή διαγνωστική δοκιμή in vitro.

Η συλλογή των δεδομένων υγείας περιορίζεται μόνο σε δεδομένα που είναι απαραίτητα για τη θεραπεία. Περεταίρω η συλλογή πρόσθετων πληροφοριών και η διαβίβαση των πληροφοριών σε τρίτους (συμπεριλαμβανομένων των συγγενών του ενδιαφερόμενου προσώπου) επιτρέπεται μόνο με τη ρητή συγκατάθεση του ασθενούς ή εάν αυτό επιτρέπεται από τη νομοθεσία.

Οι πληροφορίες που λαμβάνουν οι γιατροί και το προσωπικό του νοσοκομείου υπόκεινται σε ιατρικό απόρρητο ή ειδικό επαγγελματικό απόρρητο. Εκτός δηλαδή από την προστασία δεδομένων, η υποχρέωση εμπιστευτικότητας πρέπει πάντα να τηρείται στον τομέα της υγειονομικής περίθαλψης. Επομένως, μια παράβαση μπορεί επίσης να διωχθεί σύμφωνα με το ποινικό δίκαιο .

[96] Πέτρο Τσαντίλας/Χαρίκλεια Λάτσιου, Το ιατρικό απόρρητο υπό το πρίσμα της προστασίας των προσωπικών δεδομένων, ΕΔΚΑ 2011, σ. 161 επ. (163 επ.).

8.2 Η τεχνολογία στον τομέα της υγείας

Δεδομένου πως η πρόοδος της τεχνολογίας έχει επηρεάσει κάθε πτυχή της ζωής μας και δεν θα μπορούσε ο τομέας της υγείας να αποτελέσει εξαίρεση σε αυτό. Τα δεδομένα της υγείας πλέον ψηφιοποιούνται, διευκολύνοντας σε μεγάλο βαθμό τους γιατρούς και τα νοσοκομεία. Αναλυτικότερα, τα έγγραφα υγείας μπορούν πλέον να αποθηκευτούν στο ηλεκτρονικό αρχείο ασθενών (ePA) και με τη συγκατάθεση του ασθενή οι γιατροί να έχουν πρόσβαση σε αυτά.

Από την άλλη οι εφαρμογές υγείας και τα wearables[97] υποστηρίζουν τη θεραπεία ενός ευρέος φάσματος ασθενειών και οι ασθενείς έχουν την ευκαιρία να λάβουν εξειδικευμένες συμβουλές και βοήθεια από τα ιατρεία μέσω του Διαδικτύου.

Προϋπόθεση όμως για τη χρήση τέτοιων εφαρμογών αποτελεί η ψηφιακή ανταλλαγή δεδομένων μεταξύ ιατρείων, νοσοκομείων και φαρμακείων, η οποία οδηγεί σε διαρκή επεξεργασία δεδομένων υγείας. Ταυτόχρονα, η αυτοματοποιημένη επεξεργασία δεδομένων υγείας προσφέρει μεγάλες ευκαιρίες και πολλές δυνατότητες. Ενδεικτικά αφενός οι γιατροί έχουν τη δυνατότητα μέσω αυτών των πληροφοριών να ενεργήσουν με μεγαλύτερη ακρίβεια και να αποφύγουν την παροχή κάποιας λανθασμένης θεραπείας και αφετέρου οι επιστήμονες μπορούν να ανακαλύψουν αιτίες ασθένειας και καλύτερες μεθόδους θεραπείας, καθώς τα δεδομένα υγείας, που συλλέγονται μέσω των εφαρμογών, τους παρέχουν όγκο πληροφοριών για μεγαλύτερο δείγμα του πληθυσμού.

8.3 Η προστασία των δεδομένων υγείας

Ανάλογα με την ευαισθησία των δεδομένων, τίθενται υψηλές απαιτήσεις για την προστασία και την ασφάλεια αυτών. Τα δεδομένα υγείας είναι ένας από τους ειδικούς τύπους προσωπικών δεδομένων που περιγράφονται στο άρθρο 9 του ΓΚΠΔ και ως εκ τούτου ανήκουν στην κατηγορία των ευαίσθητων προσωπικών δεδομένων. Λόγω αυτού απαιτείται η θέσπιση υψηλών προτύπων ασφαλείας, που να εξασφαλίζουν την προστασία

[97] Πρόκειται για φορητές και έξυπνες συσκευές, οι οποίες δύνανται να μετρούν τους καρδιακούς παλμούς, τα επίπεδα ζαχάρου, την ποιότητα ύπνου κ.α. και εφαρμόζονται στο δέρμα του ατόμου.

αυτών των δεδομένων και ακόμη περισσότερο την προστασία τους κατά την ψηφιακή υγειονομική περίθαλψη.

Με τον όρο ψηφιακή υγειονομική περίθαλψη εννοείται η επεξεργασία μεγάλων ποσοτήτων δεδομένων υγείας για σκοπούς ανάλυσης. Ο κύριος στόχος είναι η βελτίωση της πρόληψης, της διάγνωσης και των θεραπειών συνδυάζοντας την ψηφιακή τεχνολογία και την παραδοσιακή ιατρική. Η έννοια της ψηφιακής υγειονομικής περίθαλψης συμπορεύεται με τον ρυθμό της ψηφιοποίησης και υποστηρίζεται επίσης από τεχνολογίες όπως η τεχνητή νοημοσύνη. Για παράδειγμα, οι εικόνες μαστογραφίας ψηφιοποιούνται και εξετάζονται για ανωμαλίες από την τεχνητή νοημοσύνη.

Συχνά όμως οι πληροφορίες που συνδέονται με την κατάσταση της υγείας κάποιου ασθενή μπορεί να καταλήξουν στο διαδίκτυο. Αυτό αποτελεί ένα γεγονός με ιδιαίτερα αρνητικές συνέπειες, διότι ορισμένοι ασθενείς αντιμετωπίζουν αυξημένο κίνδυνο διακρίσεων και στιγματισμού, σε περίπτωση δημοσιοποίησης των στοιχείων αυτών.

Στην αντιμετώπιση αυτών των κινδύνων, αλλά και στο ζήτημα ασφάλειας των δεδομένων των ασθενών η συμβολή του ΓΚΠΔ είναι καθοριστικής σημασίας. Ο νομοθέτης της Ένωσης επιδίωξε την αποσαφήνιση της έννοιας των δεδομένων υγείας. Όπως αναφέρεται και ανωτέρω τα δεδομένα που αφορούν την υγεία εμπίπτουν στο άρθρο 9 του Κανονισμού και στις ειδικές κατηγορίες δεδομένων που αυτός προβλέπει. Γίνεται εξαρχής εμφανής η βούληση του νομοθέτη για απαγόρευση της επεξεργασίας αυτών, απαγόρευση όχι απόλυτη, καθώς άρεται από την συγκατάθεση του υποκειμένου.

Η συγκατάθεση εν προκειμένω για να θεωρηθεί έγκυρη δεν αρκεί να συγκεντρώνει τα χαρακτηριστικά του άρθρου 4 του ΓΚΠΔ, δηλαδή να είναι αποτέλεσμα ενημέρωσης, ελεύθερη και αδιαμφισβήτητη. Σύμφωνα με την παράγραφο 2 του άρθρου 9 του ΓΚΠΔ θα πρέπει η συγκατάθεση του υποκειμένου να είναι ρητή και να καλύπτει το σύνολο των δραστηριοτήτων επεξεργασίας που διενεργείται για τον ίδιο σκοπό ή για τους ίδιους σκοπούς[98]. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, θα πρέπει να δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς[99].

[98] Λ. Μήτρου, Τα δεδομένα υγείας στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, σε: Όμιλος Μελέτης Ιατρικού Δικαίου και Βιοηθικής, Προστασία δεδομένων υγείας, 2018, σ. 12 = sakkoulas-online

[99] Αιτιολογική σκέψη 32 ΓΚΠΔ

Εγείρονται ερωτήματα, όπως είναι λογικό, σχετικά με το εάν ένας ασθενής, ο οποίες πολλές φορές λόγω της κατάστασης του αντιμετωπίζει ζητήματα κατανόησης, είναι σε θέση αφενός να ενημερωθεί και αφετέρου να παράσχει την συγκατάθεση του για επεξεργασία των δεδομένων του. Επίσης η σχέση ασθενούς και γιατρού αναμφίβολα είναι μία σχέση που παρουσιάζει μία ενδεχομένη εξάρτηση και συνεπώς ανισορροπία ισχύος.

Βέβαια η συγκατάθεση δεν συνιστά την μόνη εξαίρεση για την άρση της απαγόρευσης επεξεργασίας στον τομέα της υγείας. Για παράδειγμα η επεξεργασία καθίσταται απαραίτητη όταν υπάρχουν λόγοι δημοσίου συμφέροντος ή λόγοι που αφορούν την ικανότητα εργασίας ενός ατόμου. Βέβαια σύμφωνα με το άρθρο 9 παρ. 4 του Κανονισμού παρέχεται η εξουσία στον εθνικό νομοθέτη να διατηρήσει ή και να θεσπίσει περαιτέρω όρους και περιορισμούς, ειδικά για την επεξεργασία δεδομένων που αφορούν την υγεία, όπως και των βιομετρικών και των γενετικών δεδομένων.

Αξίζει να υπογραμμισθεί ότι μετά τη θέση σε ισχύ του ΓΚΠΔ την 25η.05.2018 και τον νόμο 4624/2019, η λήψη της προηγούμενης άδειας από την Αρχή ως προϋπόθεση για τη νομιμότητα της επεξεργασίας, κατά το άρθρο 7 παρ. 2 του νόμου 2472/1997, δεν έχει πλέον εφαρμογή και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα δεν έχει πια αρμοδιότητα χορήγησης των αδειών της διάταξης αυτής[100].

100 https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/eidikeskatigories/dedomenaugeias/epexergasia_dedomenwn_ugeias

Συμπεράσματα

Ο Γενικός Κανονισμός Προστασίας Δεδομένων αποτελεί μία νομοθετική καινοτομία που συμπορεύεται με την ραγδαία τεχνολογική εξέλιξη της εποχής μας, η οποία διαρκώς φέρνει στο προσκήνιο καινούργιες προκλήσεις αλλά και νέα ζητήματα, που άπτονται σε όλο το φάσμα του δικαίου. Είναι γεγονός πως η φιλοσοφία του Κανονισμού άπτεται των σκοπών του. Έτσι εξηγείται γιατί στο επίκεντρο του ενωσιακού νομοθέτη κατά τη σύνταξη του Κανονισμού τέθηκε το υποκείμενο των δεδομένων και το πως θα μπορέσει να διασφαλιστεί και να επεκταθεί η προστασία αυτού και των δικαιωμάτων του σε ένα κόσμο, που τα προσωπικά δεδομένα χρησιμοποιούνται ευρέως σε πολλούς τομείς.

Είναι χαρακτηριστική η βαρύτητα που έχει η σαφής και ρητή συγκατάθεση του υποκειμένου για την επεξεργασία των προσωπικών του δεδομένων. Η προϋπόθεση αυτή ούτε αίρεται, ούτε παρακάμπτεται, με εξαίρεση φυσικά ορισμένους ρητά προβλεπόμενους λόγους, όπως για παράδειγμα το δημόσιο συμφέρον ή την επιστημονική έρευνα. Είναι εκεί η υποχρεωτικότητα της συγκατάθεσης για τονίζει το δικαίωμα του ατόμου στον ιδιωτικό του βίο και στα προσωπικά του δεδομένα, τα οποία συνδέονται με τη σειρά τους και με άλλα δικαιώματα ή ελευθερίες μεταξύ των οποίων είναι η ελευθερία της συνείδησης, η αξιοπρέπεια και η απαγόρευση των διακρίσεων. Όμως από μόνη της η τήρηση του Κανονισμού δεν αρκεί για την προστασία των δεδομένων, γι' αυτόν τον λόγο απαιτείται και το ίδιο το άτομο να ενημερώνεται για τα δικαιώματα του και να δείχνει την δέουσα προσοχή όταν πρόκειται να δώσει πληροφορίες του σε τρίτους.

Οι αλλαγές που έχουν επέλθει στην κοινωνία μας, αλλά και σε κάθε τομέα της ζωής μας, ως απότοκο της τεχνολογικής προόδου και του ολοένα και περισσότερο ψηφιοποιημένου κόσμου μας, μπορεί να επιλύουν καθημερινές ανάγκες και προβλήματα, όμως δημιουργούν σοβαρούς κινδύνους για την προστασία του ιδιωτικού μας βίου. Κάθε άλλο παρά ποτέ ελλοχεύει ο κίνδυνος για τα προσωπικά δεδομένα καθώς με τη χρήση αθέμιτων μέσων μπορεί να καταστεί εφικτή η χωρίς συναίνεση πρόσβαση σε προσωπικές και ευαίσθητες πληροφορίες τρίτων, γεγονός ικανό να δημιουργήσει προβλήματα με ιδιαίτερα δυσμενείς συνέπειες για το υποκείμενο των πληροφοριών. Εξάλλου το ίδιο εύκολο καθίσταται να υπάρξει διαρροή προσωπικών δεδομένων από επιχειρήσεις και φορείς, οι οποίοι είτε δεν τηρούν τα απαραίτητα πρότυπα προστασίας, είτε δεν

λαμβάνουν τα ενδεδειγμένα οργανωτικά και τεχνικά μέτρα, τα οποία προβλέπονται στον ΓΚΠΔ.

Πέραν τούτου οι προτιμήσεις του κάθε ατόμου, τα ζητήματα υγείας που ίσως αντιμετωπίζει ή η φαρμακευτική αγωγή που τυχόν λαμβάνει, ακόμη και άλλα στοιχεία του όπως το φύλο, η ηλικία ή η καταγωγή του δύναται να αποτελέσουν εφαλτήριο για την αύξηση των κερδών επιχειρήσεων και εταιρειών. Τα δεδομένα των υποκειμένων όχι μόνο μπορούν να γίνονται αντικείμενο ανταλλαγής μεταξύ εταιρειών διαφορετικών χωρών, εντός και εκτός την ΕΕ, αλλά και υφίσταται το ενδεχόμενο αυτά να υφαρπάζονται από τα υποκείμενα μέσω του διαδικτύου, χωρίς καν να το αντιληφθούν. Είναι πολλές οι μέθοδοι παραπλάνησης των χρηστών του διαδικτύου, και ακόμη περισσότεροι οι τρόποι παρακολούθησης της δραστηριότητας τους.

Αποδέκτες όλων των ανωτέρω αθέμιτων πρακτικών και παραπλανητικών ενεργειών δύναται να καταστούν και τα παιδιά. Ο Κανονισμός αναγνωρίζοντας την ιδιαίτερη κατάσταση στην οποία βρίσκονται τα παιδιά, τα οποία ευκολότερα συγκριτικά με τους ενήλικες εξαπατώνται και παραπλανώνται, έχει προβλέψει ειδικότερες ρυθμίσεις για αυτά. Περαιτέρω υπάρχουν και συγκεκριμένες απαγορεύσεις, όπως για παράδειγμα η απαγόρευση για την κατάρτιση εμπορικού προφίλ ιδίως για τους ανηλίκους, οι οποίες φανερώνουν την προσοχή που επέδειξε ο νομοθέτης προκειμένου να δημιουργήσει ένα πιο ασφαλές πλαίσιο για εκείνα.

Αυτά τα ζητήματα λοιπόν καλείται να επιλύσει ο Κανονισμός και έως σήμερα ανταπεξέρχεται σε αυτά επιτυχώς. Σημαντικό ρόλο φυσικά διαδραματίζουν στο έργο του τα κράτη μέλη και οι εποπτικές αρχές. Καθήκον τους είναι η διασφάλιση της τήρησης του ΓΚΠΔ, μέσω γνωμοδοτήσεων, κατευθυντήριων αλλά και επιβολή κυρώσεων, όπου αυτό κρίνεται αναγκαίο. Όσο όμως η τεχνολογία θα εξελίσσεται, οι ανάγκες θα πληθαίνουν και οι προκλήσεις θα αλλάζουν, τόσο πιο δύσκολο και περίπλοκο θα είναι το έργο του νομοθέτη. Για τον λόγο αυτόν αφενός οι εποπτικές αρχές οφείλουν να συνδράμουν στην προσπάθεια του για ένα ασφαλές πλαίσιο ανταλλαγής πληροφορίων, όπου πολίτες και δεδομένα προστατεύονται, και αφετέρου το κάθε άτομο ξεχωριστά να ενημερώνεται για τα δικαιώματα που διαθέτει και ενεργεί με σύνεση.

Βιβλιογραφία

Α. Σκουτέλη, Κλινικές δοκιμές φαρμάκων, 2021, § 14, σ. 405, αρ. 1316 = sakkoulas-online

Α. Σιανιώτη-Μαρούδη, Ασφαλιστικό Δίκαιο, Νομική Βιβλιοθήκη, 2017

Α. Σινανιώτη - Μαρούδη, Ι. Φαρσαρώτας, Ηλεκτρονική Τραπεζική, Εκδόσεις Σάκκουλα, 2005

Γ. Λαζαράκος σε: Σ. Βλαχόπουλος, Θεμελιώδη δικαιώματα, Νομική Βιβλιοθήκη, 2017

Γ. Πλιαβέσης, Η Προστασία των Προσωπικών Δεδομένων στη σχέση Τράπεζας – Πελάτη, Νομική Βιβλιοθήκη, 2019

Δ. Ζερδελής, Εργατικό Δίκαιο, 5η έκδ., 2022, § 21, σ. 1127, αρ. 123 = sakkoulas-online

Δ. Ζωγραφόπουλος σε Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

Δ. Κουκιάδης, Ο εργαζόμενος ως υποκείμενο προσωπικών δεδομένων κατά το Γενικό Κανονισμό Προστασίας Δεδομένων, 2019, σ. 55= sakkoulas-online

Ε. Τρούλη, Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων και Ευθύνη για Αποζημίωση, 2023, σ. 55, αρ. 66 = sakkoulas-online

Ι. Ιγγλεζάκης, Το δίκαιο της ψηφιακής οικονομίας, 2022 = sakkoulas-online

Ι. Ιγγλεζάκης, Δίκαιο της πληροφορικής - Συμπλήρωμα, 2016

Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, Νομική Βιβλιοθήκη, 2020

Κ. Λωσταράκου σε: Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

Λ. Μήτρου, Η αρχή τής Λογοδοσίας σε Υποχρεώσεις του υπευθύνου επεξεργασίας [Γ. Γίαννοπουλος, Λ. Μήτρου, Γ. Τσολίας], Συλλογίκος Τόμος Λ. Κοτσαλή – Κ. Μενουδάκου «Ο ΓΚΠΔ, Νομική διάσταση και πρακτική εφαρμογή », εκδ. Νομική Βιβλιοθήκη, 2018, σελ. 172 επ.

Λ. Μήτρου, Τα δεδομένα υγείας στον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων, σε: Όμιλος Μελέτης Ιατρικού Δικαίου και Βιοηθικής, Προστασία δεδομένων υγείας, 2018, σ. 12 = sakkoulas-online

Πέτρος Τσαντίλας/Χαρίκλεια Λάτσιου, Το ιατρικό απόρρητο υπό το πρίσμα της προστασίας των προσωπικών δεδομένων, ΕΔΚΑ 2011, σ. 161 επ. (163 επ.).

Σ. Μαυρίδης, Το δικαίωμα στην προστασία δεδομένων προσωπικού χαρακτήρα κατά την οικοδόμηση μιας ευρωπαϊκής οικονομίας δεδομένων, 2024, σ. 65

Φ.Παναγοπούλου-Κουτνατζή, σε: Λ.Κοτσαλής- Κ.Μενουδάκος (επιμελ.), Γενικός Κανονισμός για την προστασία των Προσωπικών Δεδομένων (GDPR),Νομική διάσταση και πρακτική εφαρμογή, Νομική Βιβλιοθήκη, 2021, 2η έκδοση

Φ. Παναγοπούλου-Κουτνατζή, Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, 2017, σ. 122

Φ. Παναγοπούλου, Χορήγηση δεδομένων υγείας με άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ): μία θεσμική αποτίμηση, ΕφημΔΔ 6/2015.755-771 = sakkoulas-online

Αρθρογραφία

Β.-Α. Κόλλιας, Προβληματικές διατάξεις του ελληνικού νόμου για τα δεδομένα προσωπικού χαρακτήρα. Ο Ν.4624/2019 και η σχέση του με τον Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Αρμ 3-4/2019.265

Γ. Δελλής, Για μία αποτελεσματική δημόσια προστασία των προσωπικών δεδομένων: ο «θαυμαστός καινούργιος κόσμος» του Κανονισμού (ΕΕ) 679/2016, ΕφημΔΔ 1/2017.2

Ξένη Βιβλιογραφία

Mario Martini/Christian Drews/Paul Seeliger/ Quirin Weinzierl, Dark Patterns (2020) Σελ. 51 βλ. https://rsw.beck.de/docs/librariesprovider132/default-document-library/zfdr_heft_2021-01.pdf

Thaler, R. H., & Sunstein C. R. (2019). Nudge. Wie man kluge Entscheidungen anstößt. Berlin: Ullstein

Roman Meier, Dark Patterns, 13.04.2022, https://datenschutz.law/news/dark-patterns, abgerufen am 30.01.2024

Δικτυακοί τόποι

Κατευθυντήριες γραμμές 5/2020 σχετικά με τη συγκατάθεση βάσει του κανονισμού 2016/679 : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

Απόρρητο των ηλεκτρονικών επικοινωνιών, Δελτίο τύπου του Συμβουλίου της ΕΕ: https://www.consilium.europa.eu/el/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

Αρχή Προστασίας Προσωπικών Δεδομένων (Ελλάδα): https://www.dpa.gr

Αρχή Προστασίας Προσωπικών Δεδομένων (Αυστρία) https://www.dsb.gv.at/

Αρχή Προστασίας Προσωπικών Δεδομένων (Ιταλία) www.garanteprivacy.it

ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 04/2012 on Cookie Consent Exemption ,Adopted on 7 June 2012: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

Εκτελεστική απόφαση (ΕΕ) 2021/914 της Επιτροπής, της 4ης Ιουνίου 2021, σχετικά με τις τυπικές συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του

Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ): https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32021D0914

EDPB-EDPS Joint Opinion 2/2021 on standard contractual clauses for the transfer of personal data to third countries: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22021-standard_en

Κατευθυντήριες γραμμές 2/2020 σχετικά με το άρθρο 46 παράγραφος 2 στοιχείο α) και το άρθρο 46 παράγραφος 3 στοιχείο β) του κανονισμού 2016/679 για τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα μεταξύ δημόσιων αρχών και φορέων του ΕΟΧ και δημόσιων αρχών: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_el

Deceptive patterns: http://darkpatterns.org.

European Data Protection Board: https://edpb.europa.eu

https://www.lfd.niedersachsen.de/startseite/

https://www.lawspot.gr/nomika-nea/kanonismos-eprivacy-egkrithike-i-thesi-toy-symvoylioy-tis-ee-gia-toys-kanones-gia-tin