

ΜΑΘΗΜΑ: Στοιχεία Δικαίου της Πληροφορίας

Τίτλος: Οδηγός και ανάλυση δυνατοτήτων νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα στις ηλεκτρονικές επικοινωνίες

Σπυρίδων Βαρούμας, AM: 3170243

Κωνσταντίνος Ιωάννης Κορναράκης, AM: 3170074

Ηλίας Μπεζαντάκος, AM: 3160241

2021

Περιεχόμενα:

1.Εισαγωγή	3
2. Ορισμοί	3
2.1 Η έννοια των προσωπικών δεδομένων	3
2.2 Η έννοια της επεξεργασίας των προσωπικών δεδομένων	6
2.3 Η έννοια του υποκειμένου	6
2.4 Η έννοια του υπεύθυνου επεξεργασίας	6
2.5 Η έννοια του υπευθύνου προστασίας δεδομένων	7
2.6 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα	7
2.7 Μορφές ηλεκτρονικής επικοινωνίας	8
3. Οδηγός Επεξεργασίας Προσωπικών Δεδομένων	8
3.1 Οι ευθύνες των παρόχων ηλεκτρονικών υπηρεσιών	9
3.1.1 Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας	9
3.1.2 Η αρχή του σκοπού	9
3.1.3 Η αρχή της ελαχιστοποίησης των δεδομένων	10
3.1.4 Η αρχή της ακρίβειας	10
3.1.5 Η αρχή του περιορισμού της περιόδου αποθήκευσης	10
3.1.6 Η αρχή της ακεραιότητας και εμπιστευτικότητας	10
3.1.7 Η αρχή της αναλογικότητας	10
3.1.8 Η αρχή της λογοδοσίας	10
3.2 Βήματα επεξεργασίας προσωπικών δεδομένων	11
4. Επίλογος	17
Περίληψη	17

1.Εισαγωγή

Η τεχνολογία έχει γίνει αναπόσπαστο κομμάτι της ζωής του ανθρώπου σε κάθε πτυχή της ζωής του, καθώς αποτελεί σημαντικό παράγοντα στην εκπαίδευση, την εργασία, την ψυχαγωγία και την αλληλεπίδρασή του με τον υπόλοιπο κόσμο. Η ραγδαία εξέλιξη της τεχνολογίας και των παράγωγων μέσων της έχει επιφέρει μια νέα τάξη πραγμάτων στους χρήστες και στους συνδρομητές υπηρεσιών ηλεκτρονικών επικοινωνιών. Τα δεδομένα που ανταλλάσσονται καθημερινά, σε παγκόσμιο επίπεδο, μέσα από τις ηλεκτρονικές επικοινωνίες είναι παραπάνω από δισεκατομμύρια ενώ η επεξεργασία τους, είναι μια διαδικασία που παρουσιάζει ιδιαίτερο ενδιαφέρον από την στιγμή που μπορεί το περιεχόμενο των πληροφοριών να αποτελέσει σημαντική γνώση για πολλούς φορείς, που κυρίως προσπαθούν να αποτρέψουν εγκλήματα ή γενικά παράνομες ενέργειες. Για την νόμιμη επεξεργασία και συλλογή προσωπικών δεδομένων μέσω των ηλεκτρονικών επικοινωνιών είναι απαραίτητη η συμμόρφωση των φορέων με τον Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) (ΕΕ) 2016/679, όπως επίσης και η τήρηση του νόμου 3471/2006, ο οποίος ρυθμίζει την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και εφαρμόζεται ως ειδικότερος του Κανονισμού. Επομένως, προκειμένου οι φορείς να έχουν την δυνατότητα την νόμιμης επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να ακολουθήσουν μια σειρά οδηγιών και βημάτων που θα αναλυθούν παρακάτω.

2. Ορισμοί

2.1 Η έννοια των προσωπικών δεδομένων

Προσωπικά δεδομένα^{1,2} είναι, σύμφωνα με τον Κανονισμό, και την Οδηγία 2016/680/ΕΕ, κάθε πληροφορία που αναφέρεται στο πρόσωπό του κάθε ατόμου, για παράδειγμα το ονοματεπώνυμο και το επάγγελμά του ατόμου, η οικογενειακή του κατάσταση, η ηλικία, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, το θρήσκευμά του, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και προτιμήσεις, η εργασία του (προϋπηρεσία, εργασιακή συμπεριφορά κλπ.), η οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά) και οι τυχόν ποινικές του διώξεις και καταδίκες. Στα προσωπικά δεδομένα δεν λογίζονται τα στατιστικής φύσεως συγκεντρωτικά στοιχεία, από τα οποία δεν μπορούν πλέον να προσδιοριστούν τα υποκείμενα των δεδομένων.

Τα προσωπικά δεδομένα χωρίζονται στις εξής κατηγορίες³, όπως αυτά έχουν χαρακτηριστεί και εκδοθεί από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα:

¹ [Άρθρο 4 ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων. Privacy/Privazy according to plan.](#) (Άρθρο 4 ΕΕ Γενικός Κανονισμός για την Προστασία Δεδομένων, παράγραφος 1 (τελευταία πρόσβαση 09/04/2021))

² [Άρθρο 03 – Ορισμοί | Υπουργείο Δικαιοσύνης](#) (Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679: Άρθρο 3 Ορισμοί, παράγραφος α) (τελευταία πρόσβαση 09/04/2021))

³ <https://www.nirris.gr/gdpr/katigories-prosopikon-dedomenon/> (τελευταία πρόσβαση 09/04/2021)

Ομάδα Α: Μη ευαίσθητα προσωπικά δεδομένα:

1. Στοιχεία Αναγνώρισης:
 - 1.1. Προσωπικά στοιχεία
 - 1.2. Επίσημα στοιχεία Ληξιαρχείου
 - 1.3. Καταγωγή
 - 1.4. Στοιχεία Ταυτότητας (π.χ υπηκοότητα)
 - 1.5. Λοιπά στοιχεία αναγνώρισης
2. Προσωπικά χαρακτηριστικά:
 - 2.1. Φυσικά χαρακτηριστικά
 - 2.2. Ενδιαφέροντα, συνήθειες
 - 2.3. Μετακινήσεις – ταξίδια
 - 2.4. Στοιχεία προσωπικότητας
 - 2.5. Λοιπά στοιχεία προσωπικών χαρακτηριστικών
3. Οικογενειακές συνθήκες:
 - 3.1. Έγγαμος βίος
 - 3.2. Οικογενειακή κατάσταση
 - 3.3. Κοινωνικές επαφές
 - 3.4. Λοιπά στοιχεία οικογενειακών συνθηκών
4. Εκπαίδευση:
 - 4.1. Δεδομένα ακαδημαϊκής δραστηριότητας
 - 4.2. Τομείς ειδίκευσης και πιστοποιητικά
 - 4.3. Σπουδαστικό / Μαθητικό Αρχείο
 - 4.4. Εγγραφή σε επιτροπές
 - 4.5. Επαγγελματική ειδίκευση
 - 4.6. Λοιπά στοιχεία
5. Οικονομική κατάσταση:
 - 5.1. Έσοδα, περιουσιακά στοιχεία, επενδύσεις
 - 5.2. Απολογισμός εξόδων
 - 5.3. Δάνεια, υποθήκες, πιστώσεις
 - 5.4. Επιδόματα, εργασιακά προνόμια, επιχορηγήσεις
 - 5.5. Δεδομένα ασφάλισης, σύνταξης γήρατος
 - 5.6. Αγαθά και υπηρεσίες που προσφέρονται στο άτομο
 - 5.7. Αγαθά και υπηρεσίες που προσφέρει το άτομο
 - 5.8. Τραπεζικοί λογαριασμοί, πιστωτικές κάρτες
 - 5.9. Κληρονομιά
 - 5.10. Αποζημίωση
 - 5.11. Λοιπά στοιχεία οικονομικής κατάστασης
6. Εργασία:
 - 6.1. Παρούσα εργασία
 - 6.2. Δεδομένα Πρόσληψης
 - 6.3. Ιστορικό εργασίας
 - 6.4. Εργασιακή συμπεριφορά
 - 6.5. Περιγραφή εργασίας

- 6.6. Αξιολόγηση εργασίας
- 6.7. Εκπαιδευτικό αρχείο
- 6.8. Δεδομένα ασφάλειας
- 6.9. Αμοιβές και κρατήσεις
- 6.10. Εργασιακές παροχές
- 6.11. Λοιπά στοιχεία εργασίας
- 7. Δεδομένα ηλεκτρονικών επικοινωνιών:
 - 7.1. Δεδομένα θέσης
 - 7.2. Δεδομένα κίνησης

Ομάδα Β: Προσωπικά Ευαίσθητα Δεδομένα

- 1. Φυλετική ή Εθνική προέλευση:
 - 1.1. Εθνική Καταγωγή
 - 1.2. Μειονότητες
 - 1.3. Φυλετική προέλευση
- 2. Πολιτικά Φρονήματα:
 - 2.1. Δεδομένα πολιτικών πεποιθήσεων
- 3. Θρησκευτικές Πεποιθήσεις:
 - 3.1. Δεδομένα θρησκευτικής πίστης
- 4. Φιλοσοφικές Πεποιθήσεις:
 - 4.1. Δεδομένα φιλοσοφικών πεποιθήσεων
- 5. Συνδικαλιστική δράση:
 - 5.1. Συνδικαλιστική δραστηριότητα
- 6. Υγεία:
 - 6.1. Φυσική κατάσταση
 - 6.2. Πνευματική κατάσταση
 - 6.3. Ανικανότητες και αναπηρίες
 - 6.4. Διαιτητικές ή άλλες σχετικές ανάγκες
 - 6.5. Ιατρικό ιστορικό ασθενούς
 - 6.6. Χορήγηση φαρμάκων
 - 6.7. Λοιπά στοιχεία υγείας
- 7. Κοινωνική πρόνοια (για φορείς με συναφή αντικείμενο):
 - 7.1. Ασφάλιση
 - 7.2. Σύνταξη
- 8. Ερωτική ζωή:
 - 8.1. Σεξουαλική ζωή
- 9. Ποινικές διώξεις:
 - 9.1. Καταγγελίες
 - 9.2. Διώξεις
 - 9.3. Διοικητικά μέτρα
 - 9.4. Διοικητικές ποινές
- 10. Καταδίκες:
 - 10.1. Αποφάσεις δικαστηρίων

10.2. Ποινικό Μητρώο

2.2 Η έννοια της επεξεργασίας των προσωπικών δεδομένων

Σύμφωνα με το νόμο, επεξεργασία προσωπικών δεδομένων⁴ είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

2.3 Η έννοια του υποκειμένου

Υποκείμενο των προσωπικών δεδομένων⁵ είναι το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή να προσδιοριστεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

2.4 Η έννοια του υπεύθυνου επεξεργασίας

Υπεύθυνος επεξεργασίας⁶ είναι το φυσικό ή νομικό πρόσωπο, ή δημόσια αρχή, ή υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

⁴ [Άρθρο 03 – Ορισμοί | Υπουργείο Δικαιοσύνης](#) (Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679: Άρθρο 3 Ορισμοί, παράγραφος β) (τελευταία πρόσβαση 24/04/2021))

⁵ [Τι είναι το Υποκείμενο των δεδομένων](#) (τελευταία πρόσβαση 24/04/2021)

⁶ [Άρθρο 03 – Ορισμοί | Υπουργείο Δικαιοσύνης](#) (Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679: Άρθρο 3 Ορισμοί, παράγραφος ζ) (τελευταία πρόσβαση 24/04/2021))

2.5 Η έννοια του υπευθύνου προστασίας δεδομένων

Ο υπεύθυνος προστασίας δεδομένων (DPO)⁷, σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ), είναι το πρόσωπο που διευκολύνει τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και μεσολαβεί μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων). Ο ρόλος του υπευθύνου προστασίας δεδομένων είναι συμβουλευτικός, και όχι αποφασιστικός, και δεν φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό.

Συγκεκριμένα τα καθήκοντα του υπευθύνου προστασίας δεδομένων είναι:

- α) να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας και τους υπαλλήλους που διενεργούν επεξεργασία για τις υποχρεώσεις τους σύμφωνα με τον παρόντα νόμο και άλλες διατάξεις του εθνικού δικαίου ή του δικαίου της Ένωσης σχετικά με την προστασία των δεδομένων·
- β) να παρακολουθεί τη συμμόρφωση με τις ρυθμίσεις του παρόντος νόμου, άλλες διατάξεις του εθνικού δικαίου ή του δικαίου της Ένωσης σχετικά με την προστασία των δεδομένων και με τις πολιτικές του υπεύθυνου επεξεργασίας σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας και των σχετικών ελέγχων·
- γ) να παρέχει συμβουλές, έπειτα από σχετικό αίτημα, όσον αφορά στην εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων και να παρακολουθεί τη συμμόρφωση σύμφωνα με το άρθρο 42 του παρόντος νόμου.
- δ) να συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα·
- ε) να ενεργεί ως σημείο επικοινωνίας για την Αρχή για ζητήματα που σχετίζονται με την επεξεργασία, συμπεριλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 43 του παρόντος νόμου, και να διαβουλεύεται ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

2.6 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Για την αμεσότερη και ταχύτερη προστασία των πολιτών από την επεξεργασία προσωπικών δεδομένων θεωρήθηκε αναγκαία η ίδρυση μιας Αρχής που θα εποπτεύει και θα ασχολείται αποκλειστικά με αυτό το αντικείμενο, έτσι το 1997 με τον Νόμο 2472/1997 ιδρύεται η Αρχή και ονομάζεται Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)^{8,9}. Η Αρχή είναι αρμόδια για την παρακολούθηση της εφαρμογής των διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ), με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων που τα αφορούν και τη διευκόλυνση της ελεύθερης

⁷ [Υπεύθυνος Προστασίας Δεδομένων \(DPO\)](#) (τελευταία πρόσβαση 26/04/2021)

⁸ [Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα](#) (τελευταία πρόσβαση 26/04/2021)

⁹ [Αρμοδιότητες, καθήκοντα και εξουσίες](#) (τελευταία πρόσβαση 26/04/2021)

κυκλοφορίας των δεδομένων στην Ένωση (άρθρο 51 παρ. 1, αιτ. 123 του ΓΚΠΔ). Μερικές ακόμα από τις αρμοδιότητές της είναι η έκδοση οδηγιών και αποφάσεων και η γνωμάτευση για κάθε ρύθμιση που αφορά την επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

2.7 Μορφές ηλεκτρονικής επικοινωνίας

Η ηλεκτρονική επικοινωνία¹⁰ έχει πολλές διαφορετικές μορφές, κάποιες από αυτές είναι ευρέως γνωστές στον σύγχρονο άνθρωπο και χρησιμοποιούνται από εκείνον ως μέσο επικοινωνίας στην καθημερινότητα του, άλλες από αυτές είναι λιγότερο συνηθισμένες και οικίες στο μέσο άνθρωπο. Παρόλα αυτά όλες οι μορφές ηλεκτρονικής επικοινωνίας έχουν σημαντικούς κινδύνους για τα προσωπικά δεδομένα του χρήστη και είναι σημαντικό να αναφερθούν.

Οι μορφές ηλεκτρονικής επικοινωνίας είναι οι εξής:

- E-mail
- Fax
- Τηλεδιασκέψεις μέσω εφαρμογών (π.χ Skype Meetings, Microsoft Teams, Zoom)
- Αυτόματες τηλεφωνικές κλήσεις, όπου ακούγεται μαγνητοφωνημένο μήνυμα
- SMS και MMS
- Τηλεφωνικές κλήσεις (σταθερής και κινητής τηλεφωνίας)
- Cookies
- Spamming

3. Οδηγός Επεξεργασίας Προσωπικών Δεδομένων

Οι λόγοι που γίνεται η επεξεργασία των προσωπικών δεδομένων αφορούν τα συμφέροντα και των υποκειμένων επεξεργασίας δεδομένων, αλλά και όσων τα επεξεργάζονται.

Η συλλογή δεδομένων και η επεξεργασία τους μέσω των ηλεκτρονικών επικοινωνιών μπορεί να είναι απαραίτητη προκειμένου κάποιος να μπορέσει να συμμετάσχει σε διαδικτυακές συνομιλίες, να δημοσιεύσει ή να αναρτήσει σχόλια, καθώς διάφορες ιστοσελίδες απαιτούν την αποδοχή επεξεργασίας δεδομένων για παράδειγμα με τη δημιουργία και σύνδεση σε λογαριασμό ή με την αποδοχή cookies. Παράλληλα οι φορείς που επιθυμούν να διαφημιστούν διαδικτυακά, λαμβάνοντας κάποια στοιχεία μπορούν να προβάλουν στο χρήστη περιεγχόμενο ανάλογο των προτιμήσεών του. Άλλες περιπτώσεις συλλογής στοιχείων προσωπικού χαρακτήρα είναι οι ηλεκτρονικές αγοραπωλησίες, διάφοροι διαγωνισμοί που λαμβάνουν χώρα διαδικτυακά, η υποβολή αναφορών ή παραπόνων σε μια ιστοσελίδα και η ενημέρωση μέσω ηλεκτρονικού ταχυδρομείου σχετικά με οτιδήποτε νέο υπάρχει σε έναν οργανισμό, ένα ηλεκτρονικό κατάστημα ή κάποιο site ενημέρωσης.

¹⁰ [Άρθρο 4 - Οδηγία 1/2010 της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - Πολιτική επικοινωνία με χρήση ηλεκτρονικών μέσων επικοινωνίας](#) (τελευταία πρόσβαση 26/04/2021)

Για να είναι νόμιμη η επεξεργασία που γίνεται στα προσωπικά δεδομένα πρέπει οι υπεύθυνοι επεξεργασίας να τηρούν τη σχετική νομοθεσία, οι αρχές και τα βήματα της οποίας περιγράφονται παρακάτω.

3.1 Οι ευθύνες των παρόχων ηλεκτρονικών υπηρεσιών

Οι υπεύθυνοι πάροχοι αναλαμβάνουν ένα ιδιαίτερα απαιτητικό έργο μέσα από το οποίο επωμίζονται σημαντικές ευθύνες. Είναι υπεύθυνοι για τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών στα δημόσια τηλεπικοινωνιακά δίκτυα, στους δρομολογητές και στους εξυπηρετητές οι οποίοι παρέχουν τη δυνατότητα πρόσβασης στο διαδίκτυο στο χρήστη. Οι υποχρεώσεις τους αναφέρονται αναλυτικά από τον νόμο για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679 και τον νόμο 3471/2006 ¹¹.

3.1.1 Η αρχή της νόμιμης, αντικειμενικής και διαφανούς επεξεργασίας

Ιδιαίτερα σημαντική προϋπόθεση για την επεξεργασία είναι η λήψη συγκατάθεσης του υποκειμένου, δηλαδή η συναίνεση και η έγκριση για τη διαδικασία αυτή, όπως και η ενημέρωσή του πριν τη λήψη της. Σύμφωνα με τον Κανονισμό η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν το υποκείμενο των δεδομένων έχει υποβάλλει τη συγκατάθεσή του. Παράλληλα τα δεδομένα θα πρέπει να συλλέγονται με θεμιτό τρόπο και μέσα, να είναι ακριβή και συναφή, ενώ θα πρέπει επίσης να διατηρούνται σε μορφή που προσδιορίζουν την ταυτότητα των υποκειμένων από τα οποία προήλθαν μόνο κατά τη διάρκεια της περιόδου που απαιτείται.

3.1.2 Η αρχή του σκοπού

Η συγκεκριμένη αρχή διασφαλίζει ότι το υποκείμενο έχει πλήρη επίγνωση των σκοπών της συλλογής και επεξεργασίας των δεδομένων του και δεν επιτρέπει την υποβολή των δεδομένων σε περαιτέρω επεξεργασία. Εξαίρεση αποτελεί η περαιτέρω επεξεργασία για σκοπούς αρχειοθέτησης που εξυπηρετούν το δημόσιο συμφέρον ή επιστημονικούς, ιστορικούς ή στατιστικούς σκοπούς, υπό τον όρο ότι οι μέθοδοι αποκλείουν την ταυτοποίηση των υποκειμένων των δεδομένων και παρέχουν τις κατάλληλες εγγυήσεις για την προστασία των δεδομένων τους.

¹¹ [Άρθρο 20 – Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα | Υπουργείο Δικαιοσύνης](#) (Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679: Άρθρο 20)(τελευταία πρόσβαση 30/04/2021)

3.1.3 Η αρχή της ελαχιστοποίησης των δεδομένων

Σύμφωνα με τη συγκεκριμένη αρχή ο όγκος των δεδομένων, αλλά και η διάρκεια τήρησης αυτών σε αρχείο, πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στα απολύτως απαραίτητα σε σχέση με τους αρχικούς σκοπούς για τους οποίους εκτελείται η επεξεργασία.

3.1.4 Η αρχή της ακρίβειας

Τα δεδομένα θα πρέπει σε κάθε περίπτωση να χαρακτηρίζονται από ακρίβεια και να είναι αληθή. Σε περίπτωση που αυτό απαιτείται θα πρέπει να ανανεώνονται και να επικαιροποιούνται, ενώ παράλληλα ενημερώνεται και το υποκείμενο για τις αλλαγές αυτές. Τέλος, πρέπει να μεριμνηθούν όλα τα κατάλληλα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα όταν αυτά είναι ανακριβή.

3.1.5 Η αρχή του περιορισμού της περιόδου αποθήκευσης

Η τήρηση αρχείου των δεδομένων πρέπει να περιορίζεται στο διάστημα που απαιτείται μέχρι το πέρας του σκοπού για τον οποίο λήφθηκαν εξ' αρχής. Στην περίπτωση όμως που είναι απαραίτητη η τήρηση μόνιμου αρχείου με τα δεδομένα αυτά, θα πρέπει να παρθούν τα κατάλληλα μέτρα για την προστασία τους καθώς και για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων.

3.1.6 Η αρχή της ακεραιότητας και εμπιστευτικότητας

Η επεξεργασία θα πρέπει να γίνεται με ασφάλεια ώστε να διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα, δηλαδή η αποφυγή απώλειας, καταστροφής, φθοράς, αλλοίωσης ή διαρροής τους από μη εξουσιοδοτημένους φορείς τους, είτε από λάθος.

3.1.7 Η αρχή της αναλογικότητας

Η αρχή αυτή επιβάλλει τη συνάφεια ανάμεσα στα δεδομένα που τηρούνται και στο σκοπό για τον οποίο συλλέγονται, καθώς και να είναι πρόσφορα και αναγκαία για την εκπλήρωση του σκοπού τους. Συμπερασματικά η αρχή αυτή οδηγεί στην ελαχιστοποίηση των δεδομένων στα απολύτως απαραίτητα.

3.1.8 Η αρχή της λογοδοσίας

Η αρχή αυτή αναφέρεται στην ευθύνη που φέρουν οι υπεύθυνοι επεξεργασίας και οι εκτελούντες της επεξεργασίας ως προς την απόδειξη της συμμόρφωσής τους προς τις υποχρεώσεις που θέτει ο Κανονισμός, αλλά και την ετοιμότητά τους να συμμορφωθούν. Οι υποχρεώσεις αυτές είναι μεταβαλλόμενες, αλλά εκτιμώνται πριν την έναρξη της επεξεργασίας βάσει της Εκτίμησης Αντικτύπου σχετικά με την προστασία των δεδομένων.

3.2 Βήματα επεξεργασίας προσωπικών δεδομένων

Ακολουθούν τα βήματα^{12,13} που πρέπει να ακολουθήσει ο υπεύθυνος επεξεργασίας για τη συμμόρφωση ως προς το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) προκειμένου να μπορεί να είναι νόμιμη η επεξεργασία των προσωπικών δεδομένων στις ηλεκτρονικές επικοινωνίες.

❖ **Διαμόρφωση συνείδησης προστασίας προσωπικών δεδομένων στον φορέα.**

Όλοι οι εργαζόμενοι, από την διοίκηση έως και τον απλό υπάλληλο, επιβάλλεται να γνωρίζουν στο βαθμό που είναι αναγκαίο για την ορθή άσκηση των καθηκόντων τους, τι επιτρέπεται και τι απαγορεύεται σχετικά με την επεξεργασία των προσωπικών δεδομένων. Ακόμα και αν έχουν ληφθεί όλα τα τεχνικά μέτρα προστασίας από έναν φορέα, με βάση τον Κανονισμό, εφόσον δεν υπάρξει εκπαίδευση του ανθρώπινου δυναμικού της, θα δημιουργούνται συνεχώς προβλήματα. Η ενημέρωση πρέπει να γίνεται σε τακτά χρονικά διαστήματα, ανάλογα με σχετικές αλλαγές στην νομοθεσία ή στις διαδικασίες του φορέα. Στο μέτρο του δυνατού ή του επιθυμητού, αποτελεί “καλή πρακτική” η διοργάνωση σχετικών σεμιναρίων.

❖ **Χαρτογράφηση των προσωπικών δεδομένα(data mapping).**

Αρχικά θα πρέπει να γίνει χαρτογράφηση των προσωπικών δεδομένων τα οποία ο φορέας επεξεργάζεται, τις πηγές από τις οποίες τα αντλεί και τους αποδέκτες τους, το σκοπό της επεξεργασίας, τα πληροφοριακά συστήματα που τηρούνται, κλπ. Ενδεικτικές πηγές είναι το site που ελέγχει ο εκάστοτε φορέας, ηλεκτρονικά αρχεία που διατηρεί καθώς και e-mail, social media, messaging apps. Όλα τα τελικά δεδομένα που αποκτήθηκαν, μετά την εκκαθάριση, πρέπει να οργανωθούν στα κατάλληλα αρχεία δραστηριοτήτων επεξεργασίας.

¹² [GDPR: 10 βήματα για να προετοιμάσεις την επιχείρησή σου](#) (τελευταία πρόσβαση 31/04/2021)

¹³ [12 βήματα συμμόρφωσης με τον GDPR](#) (τελευταία πρόσβαση 31/04/2021)

❖ **Αναθεώρηση της πολιτικής απορρήτου.**

Η πολιτική απορρήτου του φορέα θα πρέπει να αναθεωρηθεί, ώστε να είναι

συμβατή με τις διατάξεις του Κανονισμού. Για παράδειγμα δύο ερωτήματα που πρέπει να απαντηθούν μέσω την πολιτική απορρήτου είναι η εξής:

- Έχει προσδιοριστεί και καταγραφεί η νόμιμη βάση επεξεργασίας των προσωπικών δεδομένων και έχει συνδεθεί με συγκεκριμένο και ρητό σκοπό ή σκοπούς επεξεργασίας;
- Τηρείται η αρχή της «ελαχιστοποίησης των δεδομένων», δηλαδή γίνεται επεξεργασία των απολύτως αναγκαίων δεδομένων για την επίτευξη του εκάστοτε σκοπού επεξεργασίας, και όχι περισσότερων δεδομένων απ' ότι χρειάζεται;

Καθώς η πολιτική απορρήτου πρέπει να είναι ευρέως γνωστή, θα πρέπει να γίνει ανάρτηση της σε κάποια αρχική ιστοσελίδα, ώστε να την γνωρίζουν και τα εμπλεκόμενα υποκείμενα. Οι υπεύθυνοι επεξεργασίας, εκτός της ταυτότητάς τους και του τρόπου με τον οποίο σκοπεύουν να χρησιμοποιήσουν τα προσωπικά δεδομένα που συλλέγουν, υποχρεώνονται πλέον από τον Κανονισμό να γνωστοποιούν στο υποκείμενο των δεδομένων τη νόμιμη βάση επεξεργασίας των δεδομένων του, το χρόνο τήρησης τους και το δικαίωμα του για υποβολή καταγγελίας στην αρμόδια εποπτική αρχή.

❖ **Αναθεώρηση της πολιτικής του φορέα αναφορικά με τη λήψη της συγκατάθεσης.**

Η πολιτική του φορέα αναφορικά με τη λήψη της συγκατάθεσης θα πρέπει να αναθεωρηθεί, ώστε να είναι σύμφωνη προς τον Κανονισμό. Η συγκατάθεση καθίσταται πλέον υποχρεωτική. Θα πρέπει το αίτημα για συγκατάθεση του υποκειμένου να τίθεται κατά τρόπο σαφώς διακριτό από άλλα θέματα και η παροχή της συγκατάθεσης να είναι χωριστή από άλλους όρους και προϋποθέσεις. Αν η επεξεργασία αφορά πολλαπλούς σκοπούς, τότε να λαμβάνεται συγκατάθεση για όλους τους σκοπούς. Ακόμα θα πρέπει να γίνεται έλεγχος ηλικίας των υποκειμένων των δεδομένων και λήψης συγκατάθεσης των γονέων ή κηδεμόνων για κάθε επεξεργασία δεδομένων παιδιών. Τέλος αν κάποιος επιθυμεί να πρέπει να έχει το ακριβές αντίγραφο, να του παρέχεται εύκολα και άμεσα.

❖ **Έλεγχος των υφιστάμενων διαδικασιών, αν έχουν υιοθετηθεί τα κατάλληλα οργανωτικά και τεχνικά μέτρα.**

Όλες οι υφιστάμενες διαδικασίες του φορέα θα πρέπει να ελεγχθούν, ώστε να διασφαλιστεί ότι συνάδουν με τους νέους και τους ήδη υφιστάμενους Κανονισμούς δικαιωμάτων των υποκειμένων των προσωπικών δεδομένων. Τα δικαιώματα αυτά είναι της ενημέρωσης, της πρόσβασης, της διόρθωσης, της διαγραφής(‘δικαίωμα στη λήθη’), στον περιορισμό της επεξεργασίας, στη φορητότητα των δεδομένων, της εναντίωσης και στην ανθρώπινη παρέμβαση. Οι διαδικασίες, που δεν έχουν την λειτουργικότητα για τα παραπάνω δικαιώματα, θα πρέπει να τροποποιηθούν αναλόγως. Επίσης ο φορέας θα πρέπει άμεσα, εύκολα και ανευ κόστους να ανταποκρίνεται σε αιτήματα των υποκειμένων για πρόσβαση στα δεδομένα τους, ιδίως μάλιστα αν αναμένονται πολλά τέτοια αιτήματα. Σε περίπτωση άρνησης

ικανοποίησης του δικαιώματος πρόσβασης ο υπεύθυνος επεξεργασίας οφείλει να εξηγήσει στο υποκείμενο των δεδομένων, το αργότερο σε έναν μήνα, το λόγο άρνησης, και ταυτόχρονα να ενημερώσει το υποκείμενο για το δικαίωμά του να υποβάλει καταγγελία στην αρμόδια εποπτική αρχή και να προσφύγει δικαστικά κατά του υπευθύνου επεξεργασίας. Στο μέτρο του δυνατού ή του επιθυμητού, αποτελεί “καλή πρακτική” η εγκατάσταση εφαρμογής που επιτρέπει την διαδικτυακή πρόσβαση του υποκειμένου στα προσωπικά του δεδομένα.

❖ **Εντοπισμός και ανάλυση κινδύνων και ελλείψεων.**

Κάθε φορέας οφείλει να εντοπίζει και να καταγράφει τους πιθανούς κινδύνους, καθώς και τις ελλείψεις που μπορεί να εντοπιστούν(risk analysis), για να είναι προετοιμασμένος για τη σωστή επεξεργασία των προσωπικών δεδομένων των υποκειμένων του. Αυτό επιτυγχάνεται με τη δημιουργία ενός πίνακα, ο οποίος περιέχει τις δραστηριότητες που εντοπίστηκαν με ελλείψεις, την σοβαρότητα τους με βάση των κινδύνων που ενέχουν και τις προτεινόμενες ενέργειες για την αντιμετώπισή τους.

❖ **Μέτρα ασφάλειας και αντιμετώπιση διαρροής δεδομένων.**

Έλεγχος αν ήδη υφίστανται ή πρέπει να υιοθετηθούν κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων, καθώς και κατάλληλες διαδικασίες για τον εντοπισμό και διερεύνηση των περιπτώσεων παραβίασης προσωπικών δεδομένων. Στην περίπτωση παραβίασης των συστημάτων ο υπεύθυνος έχει περιθώριο 72 ωρών να δηλώσει το περιστατικό στις αρμόδιες αρχές, αλλά και στα ενδιαφερόμενα υποκείμενα εφόσον η παραβίαση αυτή μπορεί να αποτελέσει ρίσκο για τα δικαιώματα και τις ελευθερίες τους. Η επιβολή προστίμου ελλοχεύει ακριβώς στις περιπτώσεις παραβίασης προσωπικών δεδομένων που ο υπεύθυνος επεξεργασίας παρέμεινε αδρανής.

❖ **Υιοθέτηση των προδιαγραφών Privacy by Default και Privacy by Design**

Όλες οι νέες υπηρεσίες θα πρέπει να σχεδιάζονται ώστε να περιέχουν εξ’ ορισμού την προστασία της ιδιωτικότητας. Τα μέτρα προστασίας εξ’ ορισμού και δια σχεδιασμού θα πρέπει να αποφασίζονται λαμβάνοντας υπόψη τις τεχνολογικές εξελίξεις αλλά και το κόστος εφαρμογής τους, καθώς την πιθανότητα και τη σοβαρότητα των κινδύνων που μπορεί να προκύψουν.

Παραδείγματα Privacy by Default:

- Η ελαχιστοποίηση των υπό επεξεργασία δεδομένων ως προς τον όγκο τους καθώς και ως προς την ένταση και έκταση της επεξεργασίας και τη διάρκεια τήρησης αυτών.
- Η παροχή στο χρήστη της δυνατότητας ο ίδιος ενεργά να προσδιορίζει την «ορατότητα» του προφίλ του.

Παραδείγματα της προστασίας δια σχεδιασμού (Privacy by Design) που αναφέρονται στο ίδιο το Προοίμιο του Κανονισμού:

- Πάλι η ελαχιστοποίηση της επεξεργασίας δεδομένων.
- Η ψευδωνυμοποίηση το συντομότερο δυνατόν.
- Η διαφάνεια όσον αφορά την επεξεργασία, ώστε να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία των δεδομένων του και να είναι

σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφαλείας.

❖ **Περίπτωση χρήσης Cookies.**

Συγκεκριμένα για τη χρήση των Cookies¹⁴, που είναι μικρά αρχεία με πληροφορίες που μία ιστοσελίδα αποθηκεύει στον υπολογιστή του χρήστη, με σκοπό την ανάκτηση τους για τη διευκόλυνση και την επιτάχυνση εργασιών ή την εξατομίκευση διαφημίσεων ισχύουν ξεχωριστές διατάξεις. Για την εγκατάστασή τους απαιτείται πάντοτε η συγκατάθεση του χρήστη μετά από την εμφάνιση αντίστοιχου μηνύματος και κατάλληλης ενημέρωσής του, σύμφωνα με την παράγραφο 5 του άρθρου 4 ν.3471/2006, όπως αυτή τροποποιήθηκε από το ν.4070/2012. Αυτό μπορεί να επιτευχθεί μέσω της ιστοσελίδας του παρόχου 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. Εναλλακτικά η λήψη μπορεί να γίνει και μέσω κατάλληλων ρυθμίσεων στο φυλλομετρητή ή άλλης εφαρμογής (ν.3471/2006). Επίσης, το υποκείμενο επεξεργασίας θα πρέπει να μπορεί να ανακαλέσει τη συγκατάθεσή του με τον ίδιο τρόπο με τον οποίο τη δήλωσε.

Εξαίρεση αποτελούν κάποιες περιπτώσεις, κατά τις οποίες η λήψη συγκατάθεσης δεν είναι απαραίτητη. Αυτές είναι, όπως αναφέρονται στην παράγραφο 5 του άρθρου 4 ν. 3471/2006¹⁵, οι περιπτώσεις που έχουν ως αποκλειστικό σκοπό τη «διενέργεια της διαβίβασης μίας επικοινωνίας μέσω δικτύου ηλεκτρονικών επικοινωνιών ή είναι αναγκαία για την παροχή υπηρεσίας της κοινωνίας της πληροφορίας, την οποία έχει ζητήσει ρητά ο χρήστης ή ο συνδρομητής». Μερικά παραδείγματα των παραπάνω περιπτώσεων είναι τα Cookies που είναι τεχνικά απαραίτητα κατά τη συμπλήρωση μιας ηλεκτρονικής φόρμας από τον χρήστη ή για την καταχώριση των αγορών του χρήστη σε ένα ηλεκτρονικό κατάστημα (π.χ. μέσω επιλογής «προσθήκη στο καλάθι») για την αυθεντικοποίηση του συνδρομητή ή χρήστη σε υπηρεσίες που την απαιτούν.

¹⁴ [Η χρήση cookies στο διαδίκτυο.](#) (τελευταία πρόσβαση 10/05/2021)

¹⁵ [Εξαίρεση από την υποχρέωση λήψης της συγκατάθεσης του συνδρομητή ή χρήστη](#) (τελευταία πρόσβαση 10/05/2021)

❖ **Ανεπιθύμητες ηλεκτρονικές επικοινωνίες – SPAM**

Με τον όρο “Spam”¹⁶ εννοούμε κάθε αζήτητη ηλεκτρονική επικοινωνία που αποστέλλεται με σκοπό την εμπορική προώθηση προϊόντων ή υπηρεσιών ή για κάθε άλλο διαφημιστικό σκοπό, χωρίς ο παραλήπτης να έχει δώσει τη συγκατάθεσή του για αυτό. Το spam στην Ελλάδα ρυθμίζεται από το αρ. 11 του Νόμου 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/EK για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Για την αποστολή μηνυμάτων spam με αυτοματοποιημένα μέσα, δηλαδή με μέσα με τα οποία η επικοινωνία πραγματοποιείται χωρίς ανθρώπινη παρέμβαση (μηνύματα ηλεκτρονικού ταχυδρομείου στο διαδίκτυο, μηνύματα σε δίκτυα κινητής τηλεφωνίας (SMS, MMS), φαξ), ισχύει το λεγόμενο σύστημα “opt-in”. Κατά το σύστημα αυτό η αποστολή των μηνυμάτων spam επιτρέπεται μόνο κατόπιν ρητής συγκατάθεσης του παραλήπτη, με ελάχιστες εξαιρέσεις. Πιο συγκεκριμένα εξαίρεση στον κανόνα αυτό, ειδικά για τα μηνύματα ηλεκτρονικού ταχυδρομείου, αποτελεί η περίπτωση στην οποία τα στοιχεία επικοινωνίας του παραλήπτη αποκτήθηκαν από τον αποστολέα νομίμως στο πλαίσιο παρόμοιας προηγούμενης συναλλαγής, κυρίως πώλησης παρόμοιων προϊόντων ή υπηρεσιών. Στην περίπτωση αυτή μηνύματα ηλεκτρονικού ταχυδρομείου μπορούν να αποστέλλονται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του. Απαραίτητη προϋπόθεση για την δυνατότητα αυτή αποτελεί η παροχή κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα του αποδέκτη να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή την χρήση (σύστημα “opt-out”). Τέλος, σε κάθε μήνυμα spam που αποστέλλεται, ακόμα και σε αυτά που στέλνονται με συγκατάθεση, πρέπει να αναγράφεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα, όπως επίσης και να παρέχεται ένας έγκυρος τρόπος τερματισμού της περαιτέρω αποστολής τέτοιων μηνυμάτων.

¹⁶ https://www.dpa.gr/portal/page?_pageid=33,127423&_dad=portal&_schema=PORTAL (τελευταία πρόσβαση 10/05/2021)

❖ **Επεξεργασία** **τηλεφωνικών** **κλήσεων**

Όσον αφορά τις τηλεφωνικές επικοινωνίες^{17,18}, η επεξεργασία δεδομένων είναι πιο δύσκολη διότι στο ελληνικό Σύνταγμα προστατεύει το απόρρητο της επικοινωνίας με οποιοδήποτε μέσο, καθώς θεωρείται απαραβίαστο, και βασίζεται στο άρθρο 19 του Συντάγματος, με το οποίο προβλέφθηκε και η σύσταση της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ). Σύμφωνα με τη διάταξη του άρθρου 19 παρ. 1 του Συντάγματος, η άρση του απορρήτου των επικοινωνιών είναι μια κατ' εξαίρεση επιτρεπόμενη διαδικασία, και είναι δυνατόν να ισχύσει για τις δικαστικές αρχές και όχι έναντι της διοίκησης για λόγους εθνικής ασφάλειας, για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων και πρέπει να τηρείται σε κάθε περίπτωση η αρχή της αναλογικότητας. Η συγκεκριμένη διαδικασία για την πραγμάτωση της συνταγματικής επιταγής εξειδικεύεται στο ν. 2225/1994 και στο ΠΔ 47/2005 ο οποίος, προβλέπει τους λόγους για τους οποίους η άρση του απορρήτου επιτρέπεται, τα όργανα που μπορούν να τη διατάξουν, τα χρονικά όρια εντός των οποίων μπορεί η άρση να πραγματοποιείται, τη διαδικασία που πρέπει να ακολουθείται σε κάθε περίπτωση, καθώς και τις σχετικές υποχρεώσεις των παρόχων υπηρεσιών και δικτύων επικοινωνίας. Σε νομοθετικό επίπεδο σχετικές με το απόρρητο των επικοινωνιών είναι οι ρυθμίσεις του Ν. 2225/1994, για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας, οι διατάξεις του Ν. 3115/2003, με τον οποίο συστάθηκε η ΑΔΑΕ, του Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, με το οποίο ρυθμίζονται θέματα προστασίας δεδομένων προσωπικών χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και οι διατάξεις του Ν. 3674/2008 σχετικά με τη διασφάλιση του απορρήτου της τηλεφωνικής επικοινωνίας. Σχετικά είναι και τα οριζόμενα στις διατάξεις του Ν. 4070/2012, η απόφαση υπ' αριθμ. 99/2017 (ΦΕΚ 4073/Β'/23.11.2017), ο Ν. 4411/2016, καθώς και ο Ν. 4055/2012. Νομοθετικές διατάξεις σχετικές με το απόρρητο των επικοινωνιών περιλαμβάνονται επίσης και στον Ποινικό Κώδικα, και ειδικότερα στα άρθρα 248-250 ΠΚ και 370-370Α, όπως ισχύουν, στα οποία προβλέπονται κυρώσεις για ταχυδρομικούς υπαλλήλους και υπαλλήλους τηλεπικοινωνιακών οργανισμών σε περίπτωση παραβίασης του απορρήτου των επιστολών και των τηλεφωνημάτων, αντίστοιχα. Για παράδειγμα, διάφοροι φορείς που συλλέγουν δεδομένα μέσω τηλεφωνικών γκάλοπ, ζητάνε την άδεια του εν δυνάμει υποκειμένου, για την ηχογράφηση της κλήσης. Έτσι έχουν την συγκατάθεση του υποκειμένου για την καταγραφή, επεξεργασία και αποθήκευση των δεδομένων.

¹⁷ [Άρση απορρήτου επικοινωνιών στα πλαίσια της ανάκρισης](#) (τελευταία πρόσβαση 10/05/2021)

¹⁸ [Υπηρεσίες προς πολίτες](#) (τελευταία πρόσβαση 10/05/2021)

4. Επίλογος

Η προστασία των δεδομένων προσωπικού χαρακτήρα είναι κύριας σημασίας, ειδικά σε ό,τι αφορά τις ηλεκτρονικές επικοινωνίες οι οποίες προσδεύουν διαρκώς μέσα από την ραγδαία εξέλιξη της τεχνολογίας. Αναμενόμενα, καθώς τα ίδια τα δεδομένα και η αγορά που διαμορφώνεται γύρω από αυτά διογκώνονται, αυξάνονται εκθετικά και οι κίνδυνοι παραβίασής τους, με εξαιρετικά δυσμενείς επιπτώσεις. Δεν είναι λίγες οι φορές που η υποκλοπή δεδομένων ή η αθέμιτη μεταχείρισή τους έχουν προκαλέσει μεγάλες επιπτώσεις και έχουν οδηγήσει σε τεράστιες δικαστικές υποθέσεις. Μαθαίνοντας από τα λάθη του παρελθόντος έχει δοθεί πλέον σημαντική βαρύτητα στο ζήτημα της προστασίας τους. Οι νόμοι που έχουν θεσπιστεί είναι αυστηροί και η συμμόρφωση σε αυτούς ελέγχεται από εξειδικευμένα πρόσωπα, ενώ κάθε παρεκτροπή συνεπάγεται υψηλά κόστη. Έτσι, απαιτείται η ύπαρξη ρυθμιστικών και κανονιστικών πλαισίων που να εφαρμόζουν την κείμενη νομοθεσία, προκειμένου να υπάρχει ουσιαστική προστασία των δικαιωμάτων προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας του ατόμου.

Περίληψη

Οι ραγδαίες τεχνολογικές εξελίξεις (διαδίκτυο, κινητή τηλεφωνία, big data) έχουν επηρεάσει μια πληθώρα τομέων της σύγχρονης ζωής του ανθρώπου. Μέσα σε λίγα μόλις χρόνια οι εξελίξεις αυτές οδήγησαν στην αύξηση της έκτασης και έντασης της συλλογής, ανταλλαγής και επεξεργασίας δεδομένων προσωπικού χαρακτήρα μέσω των ηλεκτρονικών επικοινωνιών από ιδιωτικές επιχειρήσεις και δημόσιες αρχές με γεωμετρική πρόοδο. Τα προσωπικά δεδομένα απέκτησαν μια έντονα εμπορική διάσταση, δημιουργώντας μια νέα παγκόσμια αγορά για την εύρυθμη λειτουργία της οποίας απαιτούνταν η ελεύθερη κυκλοφορία τους. Επιπλέον, μεταβλήθηκε ο τρόπος που τα ίδια τα φυσικά πρόσωπα χειρίζονται τα δεδομένα τους, δημοσιοποιώντας πλέον ολοένα και περισσότερο, αλλά και ευκολότερα, προσωπικές πληροφορίες μέσω των ηλεκτρονικών επικοινωνιών και κατ' επέκταση καθιστώντας τες διαθέσιμες προς εκμετάλλευση και παραβίαση. Για αυτόν τον λόγο, η προστασία των δεδομένων προσωπικού χαρακτήρα στην εποχή μας είναι αυξημένης σημασίας, δεδομένου ότι πρόκειται για ένα θεμελιώδες δικαίωμα του ανθρώπου. Οι φορείς που ενδιαφέρονται να χρησιμοποιήσουν προς επεξεργασία τα δεδομένα που διατίθενται μέσω των ηλεκτρονικών επικοινωνιών θα πρέπει να ακολουθήσουν κάποιες καθορισμένες οδηγίες και βήματα προκειμένου να μπορούν να προβούν στην νόμιμη επεξεργασία τους. Οι οδηγίες και τα βήματα για τη δυνατότητα νόμιμης επεξεργασίας δεδομένων προσωπικού