ΠΑΝΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΚΟΙΝΩΝΙΚΩΝ & ΠΟΛΙΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ: ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ

Π.Μ.Σ «ΔΙΚΑΙΟ, ΤΕΧΝΟΛΟΓΙΑ ΚΑΙ ΟΙΚΟΝΟΜΙΑ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ ΤΟΥ ΜΑΥΡΙΔΗ ΛΕΩΝΙΔΑ

Α.Μ.: 7117Μ081

ΘΕΜΑ ΕΡΓΑΣΙΑΣ:

«ΟΙ ΝΕΕΣ ΠΡΟΚΛΗΣΕΙΣ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ»

ΕΠΙΒΛΕΠΟΥΣΑ ΚΑΘΗΓΗΤΡΙΑ:

ΠΑΝΑΓΟΠΟΥΛΟΥ – ΚΟΥΤΝΑΤΖΗ ΦΕΡΕΝΙΚΗ

ΑΘΗΝΑ, ΦΕΒΡΟΥΑΡΙΟΣ 2019

ΠΕΡΙΕΧΟΜΕΝΑ

ΒΡΑΧΥΓΡΑΦΙΕΣ

- ΓΚΠΔ = Γενικός Κανονισμός Προστασίας Δεδομένων
- GDPR = General Data Protection Regulation
- κλπ = και λοιπά
- Βλ = Βλέπε
- αρ = άρθρο
- παρ = παράγραφος
- σελ = σελίδα
- εδ = εδάφιο
- στοιχ = στοιχείο
- πρβλ = παράβαλε
- αριθμ = αριθμός
- Πρωτ = Πρωτόκολλο
- Κ = Κανονισμός
- Ν ή ν = νόμος
- Σ = Σύνταγμα
- ΕΚ = Ευρωπαϊκές Κοινότητες
- ΕC = European Comission
- Κ. Δ. Διαδ = Κώδικας Διοικητικής Διαδικασίας
- ΕΕ = Ευρωπαϊκή Ένωση
- ΗΠΑ = Ηνωμένες Πολιτείες Αμερικής
- ΑΠΔΠΧ = Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
- π.χ = παραδείγματος χάριν
- ΥΠΔ = Υπεύθυνος Προστασίας Δεδομένων
- DPO = Data Protection Officer
- ΕΚΚΔΑ = Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης
- ΕΑΠΔ = Εκτίμηση Αντικτύπου για την Προστασία Δεδομένων
- ΑΠΔ = Αναλυτική Περιοδική Δήλωση

ΠΡΟΛΟΓΟΣ

Η παρούσα μεταπτυχιακή διπλωματική εργασία εκπονήθηκε στο πλαίσιο του μεταπτυχιακού προγράμματος «Δίκαιο, Τεχνολογία και Οικονομία», του τμήματος Δημόσιας Διοίκησης του Παντείου Πανεπιστημίου. Το θέμα της εν λόγω διπλωματικής ήταν «Οι νέες προκλήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων στην Δημόσια Διοίκηση» και έγινε μια προσπάθεια αποτίμησης της εφαρμογής του συνολικού έργου του Κανονισμού 679/2016/ΕΕ (ΓΚΠΔ) για την προστασία των προσωπικών δεδομένων. Το νέο στοιχείο που εισάγει ο Κανονισμός, είναι αυτό του Υπεύθυνου Προστασίας Δεδομένων, (ΥΠΔ) κάτι που θα αναλυθεί εκτεταμένα και στην συνέχεια. Στην συγκεκριμένη εργασία, (όπως προδίδει και ο ίδιος ο τίτλος της) δόθηκε περισσότερο έμφαση στον δημόσιο και όχι τόσο στον ιδιωτικό τομέα. Δηλαδή, επιχειρήθηκε η προσπάθειας ενσωμάτωσης του ΓΚΠΔ, καθώς φυσικά και του ΥΠΔ στους δημόσιους φορείς. Πιο συγκεκριμένα, εν πρώτοις, έγινε μια εισαγωγική αναφορά για τον Γενικό Κανονισμό Προστασίας Δεδομένων καθώς και μία ιστορική αναδρομή στους προ ισχύσαντες νόμους, τόσο τους κοινοτικούς όσο και τους εθνικούς φυσικά. Εν συνεχεία, πέρα από το κυρίως μέρος του πλαισίου του Γενικού Κανονισμού, καθώς και του Υπευθύνου Προστασίας Δεδομένων, παρουσιάστηκαν και τα «νέα δικαιώματα» που ‘δημιουργούνται’ από τον εν λόγω Κανονισμό. Τέλος, ασκήθηκε κριτική περί της εφαρμογής του Κανονισμού στον Δημόσιο Τομέα και εισήχθη η προβληματική στο κατά πόσο μπορεί να εφαρμοστεί.

Σ’αυτό το σημείο, πέρα από την επεξήγηση της ροής που είχε η διπλωματική μου εργασία, θα ήθελα να εκφράσω τις ευχαριστίες μου για τους καθηγητές του μεταπτυχιακού. Όλοι συντέλεσαν, στο να έχουμε μια όμορφη, ομαλή και δημιουργική χρονιά. Ιδιαίτερα θα ήθελα να ευχαριστήσω την κ. Παναγοπούλου – Κουτνατζή που με συμβούλευσε και με κατεύθυνε ως προς το θέμα και μέσα από την διαρκή επικοινωνία μας στάθηκε αρωγός στην προσπάθειά μου, για την ομαλή εκπόνηση της εργασίας.

ΠΕΡΙΛΗΨΗ

Στην συγκεκριμένη εργασία επιχειρήθηκε μία προσπάθεια παράθεσης – επεξήγησης του θεσμού του Γενικού Κανονισμού Προστασίας Δεδομένων κυρίως στην Δημόσια Διοίκηση. Δηλαδή εξετάσαμε πως λειτουργεί ή μάλλον πώς θα λειτουργήσει στο μέλλον στις δημόσιες υπηρεσίες. Αυτό βέβαια δεν σημαίνει ότι για τον ιδιωτικό τομέα υφίσταται διαφορετικό καθεστώς. Με την εισαγωγή της εργασίας προσπαθούμε να συνειδητοποιήσουμε πόσο σημαντική είναι η προστασία των προσωπικών δεδομένων για το άτομο. Η ιστορική αναδρομή, θα μας δείξει ότι η προστασία αυτών των δεδομένων ήταν ανέκαθεν μέλημα των ανθρώπων. Στην συνέχεια, θα αναλυθεί εν συντομία η προγενέστερη καταργηθείσα από τον Γενικό Κανονισμό, Οδηγία 95/46/ΕΚ ώστε να γίνει γνωστό το προ ισχύον νομοθετικό καθεστώς. Ο Υπεύθυνος Επεξεργασίας δεν είναι μια καινούρια έννοια. Αναφερόμαστε σε κάθε έναν δημόσιο φορέα που επεξεργάζεται τα προσωπικά δεδομένα των πολιτών. Αντιθέτως, καινούρια έννοια είναι ο Υπεύθυνος Προστασίας Δεδομένων (έννοια που εισήχθη με τον Γενικό Κανονισμό). Ο θεσμός αυτός είναι αρμόδιος για την προστασία, τον έλεγχο των προσωπικών δεδομένων καθώς και για την ενημέρωση τόσο των δημοσίων φορέων όσο και των πολιτών. Ακολουθούν κάποια παραδείγματα δημοσίων φορέων για την εφαρμογή του GDPR, (όπως αυτό του Υπουργείου Υγείας) και επισημαίνονται τα πρόστιμα –διοικητικά και μη- τα οποία επιβάλλονται στους μη συμμορφωμένους δημόσιους φορείς ή επιχειρήσεις. Δίνεται ιδιαίτερη έμφαση στα δικαιώματα των πολιτών που «γεννιούνται» από τον Γενικό Κανονισμό, καθώς αυτά έχουν καθοριστικό ρόλο για την αποτελεσματική, ολοκληρωτική και σωστή εφαρμογή του. Τέλος, οι ευρωπαϊκές αποφάσεις (αν και εδώ δεν αναφερόμαστε σε δημόσιους φορείς) που ολοκληρώνουν το κείμενο, σκοπό έχουν να δείξουν την σημαντικότητα της προστασίας των προσωπικών δεδομένων.

SUMMARY

In this work, was made an attempt to give an explanation of the institution of the General Data Protection Regulation, mainly to the Public Administration.

That is, we looked at how it works or, rather, it will work in the future in public services. This does not, of course, mean that the private sector has a different status. With the introduction of the work we try to realize how important it is to protect the personal data for the individual.

The historical background will shows that protecting this data has always been a concern for people. Subsequently, the earlier repealed by the General Regulation, Directive 95/46 / EC, was briefly analyzed in order to make known the pre-existing legislative regime. The Editor is not a new concept. We refer to any public body that processes the personal data of citizens. Instead, the new concept is the Data Protection Officer (concept introduced by the General Regulation).

This institution is responsible for the protection, control of personal data and for the information of both public bodies and citizens. There are some examples of public entities for the implementation of the GDPR (such as the Ministry of Health) and the fines - administrative and non-imposed - imposed on non-compliant public bodies and businesses. Special emphasis is placed on the rights of citizens who are "born" by the General Regulation, as they have a key role to play for its effective, complete and correct implementation. Finally, the European decisions (although here we are not referring to public bodies) that complete the text, will intend to show the importance of protecting personal data.

§1. - ΕΙΣΑΓΩΓΗ

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ.), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων. Τα δεδομένα αυτά εξαιτίας των χαρακτηριστικών τους δεν πρέπει να τίθενται στην ευχέρεια οποιουδήποτε καθώς πρόκειται για πολύ προσωπικές πληροφορίες και επομένως πρέπει να προστατεύονται από τη συλλογή και επεξεργασία τρίτων. Η προστασία των δεδομένων σχετίζεται με την προστασία της προσωπικότητας και της ιδιωτικής ζωής των ατόμων. Επειδή όμως η ιδιωτική ζωή δεν περιορίζεται στο σπίτι αλλά επεκτείνεται και σε όλες του είδους τις δραστηριότητες του ατόμου, η προστασία των προσωπικών του δεδομένων θα πρέπει να επεκτείνεται και εκεί. Μια κύρια και πολύ σημαντική και αναπόφευκτη για την επιβίωση του ατόμου δραστηριότητα είναι αυτή της εργασίας.

Η προστασία δεδομένων των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, είναι θεμελιώδες δικαίωμα. Το θεμελιώδες αυτό δικαίωμα, έχει συγκεκριμένο περιεχόμενο[1], αλλά η σχετική νομοθεσία είναι δυναμική και εξελίσσεται καθώς καλύπτει οριζόντια πολλές όψεις της οικονομικής, επαγγελματικής, κοινωνικής και ιδιωτικής δράσης αφού συνδέεται αρρήκτως με τα δεδομένα της τεχνολογίας. Το άρθρο 8 παράγραφος 1 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης («Χάρτης») και το άρθρο 16 παράγραφος 1 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ) ορίζουν ότι κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Η τεχνολογία επιτρέπει τόσο σε ιδιωτικές επιχειρήσεις όσο και σε δημόσιες αρχές να κάνουν χρήση δεδομένων προσωπικού χαρακτήρα σε πρωτοφανή κλίμακα για την επιδίωξη των δραστηριοτήτων τους. Τα φυσικά πρόσωπα ολοένα και περισσότερο δημοσιοποιούν προσωπικές πληροφορίες και τις καθιστούν διαθέσιμες σε παγκόσμιο

[1] Λεωνίδας Κοτσαλής, Κωνσταντίνος Μενουδάκος, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, GDPR», Εισαγωγή Κωνσταντίνος Μενουδάκος.

επίπεδο. Η τεχνολογία έχει αλλάξει τόσο την οικονομία όσο και την κοινωνική ζωή και θα πρέπει να διευκολύνει περαιτέρω την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης και τη διαβίβαση σε τρίτες χώρες και διεθνείς οργανισμούς, διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα. Εντούτοις, η οικονομική και κοινωνική ολοκλήρωση της Ευρωπαϊκής Ένωσης, οι ραγδαίες τεχνολογικές εξελίξεις, η παγκοσμιοποίηση με τις εντεινόμενες ροές εργασίας, δεδομένων και κεφαλαίου, συντέλεσαν στην κατάργηση της Οδηγίας 95/46/ΕΚ και στη θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), ώστε τα κράτη – μέλη της Ε.Ε. να αποκτήσουν ένα πιο ισχυρό και συνεκτικό πλαίσιο προστασίας δεδομένων με στόχο την ασφάλεια δικαίου και την προώθηση της ψηφιακής αγοράς.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων, (ΓΚΠΔ) στα αγγλικά GDPR (General Data Protection Regulation) αφορά στην διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης. Στις 16 Απριλίου 2016 ψηφίστηκε από το Ευρωπαϊκό Κοινοβούλιο ο Γενικός Κανονισμός Προστασίας Δεδομένων, νομοθέτημα άμεσης εφαρμογής σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης. Ο γενικός κανονισμός για την προστασία δεδομένων («ΓΚΠΔ») που τέθηκε εν τέλει σε εμαρμογή στις 25 Μαΐου 2018, παρέχει ένα εκσυγχρονισμένο πλαίσιο συμμόρφωσης για την προστασία των δεδομένων στην Ευρώπη με βάση τη λογοδοσία. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα[2] θα πρέπει να προορίζεται να εξυπηρετεί τον άνθρωπο. Το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας. Ο παρών κανονισμός σέβεται όλα τα θεμελιώδη δικαιώματα και τηρεί τις ελευθερίες και αρχές που αναγνωρίζονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες, ιδίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και πληροφόρησης, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία. Στο επίκεντρο αυτού του νέου νομικού πλαισίου θα βρίσκονται για

[2] Βλ. Ιστοσελίδα www.lawspot.gr.

πολλούς οργανισμούς οι υπεύθυνοι προστασίας δεδομένων, οι οποίοι θα διευκολύνουν τη συμμόρφωση με τις διατάξεις του ΓΚΠΔ. Σύμφωνα με τον ΓΚΠΔ, ορισμένοι υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία υποχρεούνται να ορίσουν υπεύθυνο προστασίας δεδομένων. Η υποχρέωση αυτή ισχύει για όλες τις δημόσιες αρχές και φορείς (ανεξαρτήτως του είδους δεδομένων που επεξεργάζονται), καθώς και για άλλους οργανισμούς που έχουν ως κύρια δραστηριότητα τη συστηματική παρακολούθηση φυσικών προσώπων σε μεγάλη κλίμακα, ή την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα σε μεγάλη κλίμακα. Ενδέχεται, πάντως, να υπάρξουν οργανισμοί που θα κρίνουν σκόπιμο να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, ακόμη και σε περιπτώσεις στις οποίες ο ΓΚΠΔ δεν απαιτεί ρητώς τον ορισμό υπευθύνου προστασίας δεδομένων. Η ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 («ομάδα του άρθρου 29») ενθαρρύνει τέτοιου είδους εθελοντικές ενέργειες. Μάλιστα ο κανονισμός θέτει ισχυρότερη βάση από την οδηγία 95/46/ΕΚ για μεγαλύτερη συνεκτικότητα, καθώς ο κανονισμός ισχύει άμεσα στα κράτη μέλη. Αν και οι εποπτικές αρχές λειτουργούν «με πλήρη ανεξαρτησία» (άρθρο 52) σε σχέση με τις εθνικές κυβερνήσεις, τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία, οφείλουν να συνεργάζονται «με σκοπό να διασφαλίσουν τη συνεκτικότητα της εφαρμογής και της επιβολής του παρόντος κανονισμού» (άρθρο 57 παράγραφος 1 στοιχείο ζ). Ο κανονισμός απαιτεί μεγαλύτερη συνεκτικότητα από την οδηγία 95/46/ΕΚ κατά την επιβολή κυρώσεων. Σε διασυνοριακές περιπτώσεις, η συνεκτικότητα επιτυγχάνεται κυρίως μέσω του μηχανισμού συνεργασίας και σε ορισμένο βαθμό μέσω του μηχανισμού συνεκτικότητας που προβλέπει ο νέος κανονισμός. Η έννοια του υπευθύνου προστασίας δεδομένων δεν είναι καινούργια. Αν και η οδηγία 95/46/ΕΚ δεν επέβαλλε σε κανέναν οργανισμό την υποχρέωση να ορίσει υπεύθυνο προστασίας δεδομένων, η συγκεκριμένη πρακτική αναπτύχθηκε παρόλα αυτά σε αρκετά κράτη μέλη στο πέρασμα του χρόνου. Πριν από την έγκριση του ΓΚΠΔ, η ομάδα του άρθρου 29 ήταν της γνώμης ότι ο υπεύθυνος προστασίας δεδομένων συνιστά ακρογωνιαίο λίθο της λογοδοσίας και ότι ο ορισμός του μπορεί να διευκολύνει τη συμμόρφωση και επιπλέον να αποτελέσει ανταγωνιστικό πλεονέκτημα για τις επιχειρήσεις. 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 μεταξύ των διαφόρων ενδιαφερομένων (π.χ., εποπτικές αρχές, υποκείμενα των δεδομένων και επιχειρησιακές μονάδες του ίδιου οργανισμού). Οι υπεύθυνοι προστασίας δεδομένων δεν φέρουν προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης με τον ΓΚΠΔ. Ο ΓΚΠΔ καθιστά σαφές ότι είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τις διατάξεις του (άρθρο 24 παράγραφος 1). Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Ο ρόλος του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι επίσης καθοριστικός όσον αφορά την αποτελεσματική εκτέλεση των καθηκόντων του υπευθύνου προστασίας δεδομένων. Ο ορισμός υπευθύνου προστασίας δεδομένων είναι μεν το πρώτο βήμα, όμως πρέπει επιπλέον να του δοθούν επαρκής αυτονομία και πόροι για να είναι σε θέση να ασκήσει αποτελεσματικά τα καθήκοντά του. Ο ΓΚΠΔ αναγνωρίζει τον υπεύθυνο προστασίας δεδομένων ως καίρια συνιστώσα του νέου συστήματος διακυβέρνησης δεδομένων και θεσπίζει τις προϋποθέσεις για τον ορισμό, τη θέση και τα καθήκοντά του. Οι παρούσες κατευθυντήριες γραμμές επιδιώκουν να αποσαφηνίσουν τις σχετικές διατάξεις του ΓΚΠΔ ώστε αφενός να βοηθήσουν τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να συμμορφωθούν με τη νομοθεσία, και αφετέρου να συνδράμουν τους υπεύθυνους προστασίας δεδομένων στην άσκηση του ρόλου τους. Οι κατευθυντήριες γραμμές παρέχουν επίσης συστάσεις για βέλτιστες πρακτικές, με βάση την εμπειρία που έχουν αποκτήσει στον συγκεκριμένο τομέα ορισμένα κράτη μέλη. Η ομάδα του άρθρου 29 θα παρακολουθεί την εφαρμογή των εν λόγω κατευθυντήριων γραμμών και ενδέχεται επίσης να τις συμπληρώνει και να τις εμπλουτίζει κατά περίπτωση.

§1.1 - *Ιστορική αναδρομή*

Στον κλασσικό κατάλογο ελευθεριών και δικαιωμάτων του ανθρώπου[3], όπως ήδη διαμορφώθηκε ήδη από τα φιλελεύθερα συνταγματικά δικαιώματα του 18ου αιώνα, περιλαμβάνεται το δικαίωμα στην ιδιωτική ζωή. Το δικαίωμα αυτό αναγνωρίζεται και από την Οικουμενική Διακήρυξη Δικαιωμάτων του Ανθρώπου του Οργανισμού Ηνωμένων Εθνών του έτους 1948, καθώς και από την Ευρωπαϊκή Σύμβαση

[3] Λεωνίδας Κοτσαλής, Κωνσταντίνος Μενουδάκος, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, GDPR», Εισαγωγή Κωνσταντίνος Μενουδάκος

Δικαιωμάτων του Ανθρώπου του έτους 1950. Από τη δεκαετία του 1970 εμφανίζεται στη νομοθεσία των ευρωπαϊκών χωρών και των ΗΠΑ το δικαίωμα προστασίας των προσωπικών δεδομένων ως εξειδίκευση του δικαιώματος στην ιδιωτική ζωή.

Το 1981 καταρτίστηκε από το Συμβούλιο της Ευρώπης η διεθνής σύμβαση 108 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η σύμβαση έχει τεθεί σε ισχύ από τις 1/10/1985, ημερομηνία κατά την οποία συγκέντρωσε τις απαιτούμενες 5 υπογραφές και κυρώσεις από τα εθνικά κράτη. Η σύμβαση είχε υπογραφεί από την Ελλάδα στις 17/2/1983 και στη συνέχεια κυρώθηκε με τον ν. 2068/1992 και τέθηκε σε ισχύ από την 1.12.1995.

Από την ημερομηνία θέσης σε εφαρμογή του ΓΚΠΔ, καταργήθηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και το μεγαλύτερο μέρος των διατάξεων του εθνικού Ν. 2472/1997 για την Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, που ενσωμάτωσαν στην ελληνική έννομη τάξη τις διατάξεις της Οδηγίας αυτής.

Αντίθετα, παραμένουν σε ισχύ, δυνάμει και του άρθρου 95 του ΓΚΠΔ[4], οι διατάξεις της Οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, που έχουν ενσωματωθεί στην ελληνική έννομη τάξη με τις διατάξεις του Ν. 3471/2006 για την προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997.

Με το ν. 3861/2010, εισήχθη η υποχρέωση ανάρτησης των αναφερόμενων στο άρθ. 2 παρ. 4, πράξεων των κυβερνητικών και διοικητικών οργάνων στο διαδίκτυο, με σκοπό, κατά την αιτιολογική έκθεση αυτού, την επίτευξη της μέγιστης δημοσιότητας της κυβερνητικής πολιτικής και της διοικητικής δράσης, προς διασφάλιση της διαφάνειας της κρατικής δράσης και κατ' αποτέλεσμα της υπευθυνότητας, της ευθύνης και της λογοδοσίας εκ μέρους των φορέων άσκησης της δημόσιας εξουσίας. Παράλληλα με το

[4] Βλ. Ιστοσελίδα Υπουργείου Υγείας, Οδηγός Προετοιμασίας – Βασικές Κατευθύνσεις για ΓΚΠΔ, www.moh.gov.gr.

θεσμό αυτό ενισχύεται η δυνατότητα των πολιτών να απολαύσουν και να ασκήσουν το συνταγματικά κατοχυρωμένο δικαίωμα της πληροφόρησης.

Η κατά τις διατάξεις του ν. 3861/2010 ανάρτηση στο διαδίκτυο των αναφερόμενων στο αρθ. 2 διοικητικών πράξεων, όταν σε αυτές περιέχονται δεδομένα προσωπικού χαρακτήρα, συνιστά, εν όλω ή εν μέρει, αυτοματοποιημένη επεξεργασία, κατά την έννοια τόσο του ισχύοντος νομικού πλαισίου όσο και κατά το νέο Ευρωπαϊκό Κανονισμό.

Από τη διατύπωση του ν. 3861/2010[5] στο άρθρο 5, προκύπτει, ότι σε ότι αφορά τα απλά προσωπικά δεδομένα, η επεξεργασία πραγματοποιείται νόμιμα, για καθορισμένο, εκ των προτέρων, σαφή και νόμιμο σκοπό και είναι επιτρεπτή, χωρίς τη συγκατάθεση των υποκειμένων, δηλαδή των φυσικών προσώπων, των οποίων τα προσωπικά δεδομένα γίνονται αντικείμενο επεξεργασίας, εφόσον αυτή είναι αναγκαία για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας που επιβάλλεται από νόμο.

§1.2 – *Η Οδηγία 1/2011/ΕΕ*[6]

Η λήψη και επεξεργασία δεδομένων προσωπικού χαρακτήρα[7] με συστήματα βιντεοεπιτήρησης[8] συνιστά περιορισμό του ατομικού δικαιώματος προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών δεδομένων, το οποίο καθιερώνεται από το άρθρο 9Α του Συντάγματος. Έτσι η εγκατάσταση και λειτουργία συστημάτων βιντεοεπιτήρησης σε χώρους που δεν είναι δημόσιοι αλλά είναι προσβάσιμοι στο κοινό πρέπει να γίνεται μετά από ουσιαστική αξιολόγηση της αναγκαιότητας της συγκεκριμένης επεξεργασίας σε σχέση (α) με τον κίνδυνο που ο υπεύθυνος επεξεργασίας επιδιώκει να αντιμετωπίσει και (β) με το μέγεθος της επίπτωσης στην ιδιωτική ζωή των προσώπων που αφορά. Η αξιολόγηση αυτή θα πρέπει να περιλαμβάνει και τη διερεύνηση ηπιότερων μέσων ασφάλειας προσώπων και αγαθών. Η παρούσα Οδηγία εφαρμόζεται στην επεξεργασία δεδομένων εικόνας ή/και ήχου που πραγματοποιείται μέσω συστημάτων βιντεοεπιτήρησης από πάσης φύσεως δημόσιους φορείς ή από φυσικά ή νομικά πρόσωπα για τον σκοπό της

[5] Βλ, Ιστοσελίδα «Διαύγεια» (Διαύγεια και Προσωπικά Δεδομένα), www.governet.gr.
[6] Βλ. Οδηγία 1/2011.
[7] Αναλύθηκε η εν λόγω Οδηγία 1/2011/ΕΕ, όπως και η επόμενη, 680/2016/ΕΕ, διότι αφορούν τα προσωπικά δεδομένα (σε ένα γενικότερο πλαίσιο εισαγωγής) και κατ'επέκταση την προστασία αυτών. Ο Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016/ΕΕ θα τοποθετηθεί στην συνέχεια, καθώς και η Οδηγία που αντικατέστησε αυτός, 95/46/ΕΚ.
[8] Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Αριθμ. Πρωτ. Γ/ΕΞ/2274/31.03.2011.

προστασίας προσώπων ή/και αγαθών στον οποίο εντάσσονται και ειδικές περιπτώσεις παροχής υπηρεσιών υγείας. Ειδικότερα:

α) Προστασία προσώπων ή/και αγαθών. Ο σκοπός της προστασίας προσώπων ή/και αγαθών δικαιολογείται από το έννομο συμφέρον ή την νομική υποχρέωση του ιδιοκτήτη ή του διαχειριστή ενός χώρου να προστατεύσει τον χώρο καθώς και τα αγαθά που ευρίσκονται στον χώρο αυτό από παράνομες πράξεις. Το ίδιο ισχύει και για την ασφάλεια της ζωής, της σωματικής ακεραιότητας, της υγείας καθώς και της περιουσίας τρίτων που νομίμως ευρίσκονται στον επιτηρούμενο χώρο.

β) Παροχή υπηρεσιών υγείας. Η παροχή υπηρεσιών υγείας αφορά την παρακολούθηση βαριά ψυχικά ή νοητικά ασθενών που εκτιμάται ότι μπορούν να προκαλέσουν βλάβη στην υγεία τους ή σε τρίτους και την παρακολούθηση ασθενών σε Μονάδες Εντατικής Θεραπείας. Ο σκοπός αυτός μπορεί να επιδιώκεται μόνο από νοσηλευτικά ιδρύματα, ψυχιατρικά ιδρύματα, ιδρύματα περίθαλψης ατόμων με αναπηρίες και παρόμοιους φορείς παροχής υπηρεσιών υγείας. Η παρακολούθηση πρέπει να πραγματοποιείται από πρόσωπα που δεσμεύονται από το επαγγελματικό απόρρητο

§1.3 – *Η Οδηγία 2016/680/ΕΕ*

. Η παρούσα οδηγία[9] θεσπίζει τους κανόνες που αφορούν στην προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.

Σύμφωνα με την παρούσα οδηγία, τα κράτη μέλη προστατεύουν τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων και, ειδικότερα, το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα και διασφαλίζουν ότι η ανταλλαγή δεδομένων προσωπικού χαρακτήρα μεταξύ αρμοδίων αρχών εντός της Ένωσης, εφόσον η ανταλλαγή αυτή απαιτείται από το ενωσιακό δίκαιο ή το δίκαιο των κρατών μελών, δεν μπορεί να περιοριστεί ούτε να απαγορευτεί για λόγους που σχετίζονται με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

[9] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 171-173.

Η παρούσα οδηγία δεν εμποδίζει τα κράτη μέλη να προβλέπουν ισχυρότερες διασφαλίσεις από αυτές που θεσπίζονται σε αυτή για την προστασία των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων σε ό,τι αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές.

§ 2. - Η ΟΔΗΓΙΑ 95/46/ΕΚ

Η οδηγία 95/46/ΕΚ[10] του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου επιδίωκε την εναρμόνιση της προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον αφορά τις δραστηριότητες επεξεργασίας και τη διασφάλιση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα μεταξύ κρατών μελών. Η Οδηγία 95/46/ΕΚ κάλυπτε οποιαδήποτε μορφή επεξεργασίας των προσωπικών δεδομένων ανεξάρτητα από την τεχνολογία της εποχής. Τα μέτρα για τις ηλεκτρονικές επικοινωνίες σε συνδυασμό με τους γενικούς κανόνες προστασίας των δεδομένων, δεν παρείχαν την κατάλληλη προστασία των δεδομένων[11] ανεξάρτητα από την τεχνολογία που χρησιμοποιείτο. Συνεπώς, θα έπρεπε να προβλεφθούν τα κατάλληλα μέτρα, τα οποία θα ανάγκαζαν τους κατασκευαστές του εξοπλισμού των ηλεκτρονικών επικοινωνιών να κατασκευάζουν προϊόντα τα οποία θα διασφάλιζαν την προστασία των προσωπικών δεδομένων των ατόμων και συνεπώς θα διασφάλιζαν την ασφάλεια των προσωπικών δεδομένων των ασθενών. Η Ελλάδα ενσωμάτωσε την Οδηγία 95/46-ΕΚ με τον νόμο 2472/1997.

§ 2.1 - *Πρόσβαση στα δημόσια έγγραφα*

Η Αρχή[12] Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής Αρχή) ερμηνεύοντας τις κρίσιμες διατάξεις (άρθρο 5 του ν. 2472/1997 και άρθρο 5 Κ.Δ.Διαδ)

[10] Βλ. άρ 3 ΓΚΠΔ.
[11] Βλ. άρ 6 Οδηγίας 95/46/ΕΚ (γενικές αρχές).
[12] Όπου «Αρχή» εννοείται η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία θα αναλυθεί στη συνέχεια.

έχει κρίνει, με σειρά γνωμοδοτικών της εγγράφων, ότι η επεξεργασία προσωπικών δεδομένων (όπως είναι και η ανακοίνωση δεδομένων κάποιου προσώπου σε τρίτους μέσω της πρόσβασης στα δημόσια έγγραφα) επιτρέπεται και χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων (του προσώπου δηλαδή στο οποίο τα δεδομένα αφορούν), εάν είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπευθύνου επεξεργασίας, η οποία επιβάλλεται από το νόμο. Τέτοια υποχρέωση του υπευθύνου επεξεργασίας η Αρχή θεωρεί ότι προβλέπεται από τις διατάξεις του άρθρου 5 ΚΔΔιαδ για το δικαίωμα (και αντίστοιχη αξίωση) πρόσβασης στα δημόσια έγγραφα («διοικητικά» κατά το άρθρο 5 παρ. 1 και «ιδιωτικά» που φυλάσσονται από δημόσιες αρχές κατά το άρθρο 5 παρ. 2), όταν τα έγγραφα αυτά δεν αναφέρονται στην ιδιωτική ή οικογενειακή ζωή τρίτου και δεν παραβλάπτεται απόρρητο προβλεπόμενο από ειδικές διατάξεις (άρθρο 5 παρ. 3). Ως διοικητικά έγγραφα θεωρεί, μάλιστα, λαμβάνοντας υπόψη τη νομολογία του Συμβουλίου της Επικρατείας και του Νομικού Συμβουλίου του Κράτους, και όσα έγγραφα δεν προέρχονται μεν από δημόσιες υπηρεσίες, αλλά χρησιμοποιήθηκαν ή ελήφθησαν υπόψη για τον καθορισμό της διοικητικής δράσης ή τη διαμόρφωση γνώμης ή κρίσης διοικητικού οργάνου.

Ερμηνεύοντας ειδικότερα τη διάταξη του άρθρου 5 παρ. 3 ΚΔΔιαδ, η οποία επιδιώκει να ρυθμίσει τη σχέση ανάμεσα στην πρόσβαση στα δημόσια έγγραφα και στην προστασία των προσωπικών δεδομένων προβλέποντας ότι «*το κατά τις προηγούμενες παραγράφους δικαίωμα δεν υφίσταται στις περιπτώσεις που το έγγραφο αφορά την ιδιωτική ή οικογενειακή ζωή τρίτου ή αν παραβλάπτεται απόρρητο το οποίο προβλέπεται από ειδικές διατάξεις», έχει κρίνει ότι η έννοια της «ιδιωτικής ή οικογενειακής ζωής*» δεν ταυτίζεται αλλά είναι στενότερη της έννοιας των προσωπικών δεδομένων, αντιπαρατάσσεται στη «*δημόσια ζωή*» και αφορά μια γενικά παραδεκτή, σύμφωνα με τις κοινωνικές αντιλήψεις, «*σφαίρα του απορρήτου*» του ατόμου. Δέχεται, συγκεκριμένα, ότι όλα τα προσωπικά δεδομένα δεν είναι ικανά εκ της φύσεως τους να θίξουν την ιδιωτική ζωή κάποιου προσώπου, ενώ ως δυνάμενα να επιφέρουν τέτοιο αποτέλεσμα θα πρέπει να αντιμετωπίζονται κυρίως τα ευαίσθητα δεδομένα, όπως εκείνα που σχετίζονται με τη φυλετική ή εθνική προέλευση, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τα σχετικά με την υγεία και τη σεξουαλική ζωή ενός προσώπου δεδομένα. Η επεξεργασία των ευαίσθητων δεδομένων, εξάλλου, είναι νόμιμη μόνο υπό τις αυστηρότερες προϋποθέσεις του άρθρου 7 του ν. 2472/1997, το οποίο προβλέπει την έκδοση προηγούμενης άδειας της Αρχής.

Στην περίπτωση, αντίθετα, που στα δημόσια έγγραφα περιέχονται προσωπικά δεδομένα τρίτων προσώπων, τα οποία σχετίζονται με την ιδιωτική ή οικογενειακή τους ζωή (χωρίς να είναι ευαίσθητα δεδομένα), εφαρμόζεται η διάταξη του άρθρου 5 παρ. στοιχ. ε΄ του ν. 2472/1997, σύμφωνα με την οποία επιτρέπεται η χορήγησή τους σε τρίτο χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων, όταν η χορήγηση τους είναι απολύτως αναγκαία για την ικανοποίηση του εννόμου συμφέροντος που επιδιώκει ο τρίτος και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα, και ταυτόχρονα δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

§2.2 – *Πρόσβαση στα στοιχεία του καταγγέλλοντος*

Η Αρχή δέχεται πλήθος ερωτημάτων από δημόσιες υπηρεσίες σχετικά με τη νομιμότητα χορήγησης στους καταγγελλόμενους αντιγράφων των σε βάρος τους καταγγελιών που υποβάλλονται για διερεύνηση και κρίση. Συγκεκριμένα, ζητείται η γνώμη της Αρχής σχετικά με τη νομιμότητα χορήγησης του ονόματος και των λοιπών στοιχείων επικοινωνίας του καταγγέλλοντος ή την τυχόν υποχρέωση για την απαλοιφή τους από το σώμα της καταγγελίας όταν αυτή δίδεται στον καθ' ου η καταγγελία.

Η Αρχή σε απόφαση της (με αριθμό 73/2010) έκρινε σχετικά ότι «ο καθ' ου[13] η καταγγελία, ως υποκείμενο των δεδομένων που τον αφορούν, δηλαδή της υποβληθείσας σε δημόσια υπηρεσία καταγγελίας, έχει δικαίωμα πρόσβασης όχι μόνο στο κείμενο της καταγγελίας αλλά και σε κάθε πληροφορία σχετική με την προέλευση (πηγή) των δεδομένων αυτών». Η Αρχή καθορίζοντας περαιτέρω την έννοια της προέλευσης υπογράμμισε ότι τα στοιχεία ταυτοποίησης του καταγγέλλοντος, όπως το όνομα και η διεύθυνση του, συνιστούν προέλευση των δεδομένων.

Το εν λόγω δικαίωμα πρόσβασης, εντούτοις, υπόκειται και σε ορισμένους περιορισμούς. Οι δύο πρώτοι αναφέρονται στο άρθρο 12 παρ. 5 του ν. 2472/1997, και αφορούν σε λόγους εθνικής ασφάλειας ή εξακρίβωσης ιδιαίτερα σοβαρών εγκλημάτων. Περαιτέρω περιορισμοί προκύπτουν από το άρθρο 5 παρ. 3 του ΚΔΔιαδ (ν. 2690/1999) στις περιπτώσεις που το έγγραφο αφορά ιδιωτική ή οικογενειακή ζωή τρίτου ή παραβλάπτεται απόρρητο, προβλεπόμενο από ειδικές διατάξεις, ή όταν η πρόσβαση είναι δυνατόν να δυσχεράνει ουσιωδώς την έρευνα της υπόθεσης σχετικά με

[13] Βλ. Ιστοσελίδα Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.

την τέλεση εγκλήματος ή διοικητικής παράβασης. Επιπλέον περιορισμοί αναφέρονται στην ύπαρξη ειδικών διατάξεων που επιβάλλουν ή επιτρέπουν ενδεχομένως απόλυτη ή μερική τήρηση μυστικότητας καθώς και στην περίπτωση που η γνωστοποίηση των στοιχείων του καταγγέλλοντος δύναται να απειλήσει το υπέρτατο έννομο αγαθό της ζωής του.

Σε κάθε περίπτωση και με δεδομένο ότι και ο καταγγέλλων είναι ομοίως υποκείμενο των δεδομένων που περιέχονται στην καταγγελία, θα πρέπει να ενημερώνεται με κάθε πρόσφορο τρόπο κατά το χρόνο υποβολής της καταγγελίας του για τη δυνατότητα του καθ' ου να έχει πρόσβαση στα στοιχεία αυτής. Ο καταγγέλλων ο οποίος δεν επιθυμεί να αποκαλυφθεί η ταυτότητά του θα πρέπει εξαρχής να επικαλείται και να αιτιολογεί εγγράφως τους σχετικούς λόγους, ώστε να εξετάζονται αρμοδίως από τη δημόσια υπηρεσία.

§2.3- *Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)*

Με αφορμή τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) που υιοθετήθηκε τον Απρίλιο του 2016 και τέθηκε σε εφαρμογή την 25η Μαΐου 2018, έχει υπάρξει έντονη δραστηριότητα πολλών φορέων (κερδοσκοπικών και μη) για παροχή συμβουλευτικών υπηρεσιών αναφορικά με τις απαιτήσεις συμμόρφωσης του ΓΚΠΔ, προετοιμασία και προσφορά εκπαιδευτικών προγραμμάτων που ως στόχο έχουν την κατάρτιση επαγγελματιών σε θέματα που άπτονται του ΓΚΠΔ και των αρμοδιοτήτων /υποχρεώσεων του Υπεύθυνου Επεξεργασίας Δεδομένων (DPO), καθώς και για παροχή υπηρεσιών πιστοποίησης.

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (*ΑΠΔΠΧ*)[14], γνωστή (ανεπίσημα) και ως Αρχή Προστασίας Προσωπικών Δεδομένων, είναι συνταγματικά κατοχυρωμένη ανεξάρτητη διοικητική Αρχή[15]. Ιδρύθηκε με τον Νόμο 2472/1997 «*για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*», ο οποίος ενσωματώνει στο ελληνικό δίκαιο την ευρωπαϊκή οδηγία 95/46/ΕΚ[1]. Η οδηγία αυτή θέτει κανόνες για την προστασία

[14] Για τις 'δραστηριότητες' της εν λόγω Αρχής, βλ. §2.1 και §2.2.
[15] Βλ. Ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.

των προσωπικών δεδομένων σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης. Η λειτουργία της Αρχής ξεκίνησε στις 10 Νοεμβρίου 1997.

Η Αρχή, σύμφωνα με την παρ. 1 του άρθρου 20 του ιδρυτικού της νόμου 2472/1997, εξυπηρετείται από Γραμματεία, η οποία λειτουργεί σε επίπεδο Διεύθυνσης, και αποτελείται από τρία τμήματα: 1. Το τμήμα Ελεγκτών, 2. Το τμήμα Επικοινωνίας και 3. Το τμήμα Διοικητικών και Οικονομικών Υποθέσεων.

§2.4 - *Γιατί Κανονισμός και όχι Οδηγία;*

Αν και η επιλογή του Κανονισμού από την Ευρωπαϊκή Ένωση δεν έμεινε χωρίς αρνητική κριτική, οι λόγοι[16] για τους οποίους η ΕΕ αποφάσισε να ρυθμίσει το ζήτημα της προστασίας των Προσωπικών Δεδομένων με Κανονισμό και όχι με Οδηγία, είναι εύκολα αντιληπτοί. Ενόψει των ταχύτατων τεχνολογικών εξελίξεων και της ραγδαίας αύξησης των (προσωπικών) δεδομένων, τα οποία είναι πλέον εύκολα διαθέσιμα μέσω του διαδικτύου, της διαρκούς διαβίβασης δεδομένων μεταξύ εταιρειών του ίδιου ομίλου επιχειρήσεων - ή και διαφορετικών - εντός και εκτός των κρατών της Ένωσης, καθώς και της ανάγκης διαμοιρασμού πληροφοριών μεταξύ δημόσιων υπηρεσιών, η ΕΕ βρέθηκε μπροστά σε μια από τις μεγαλύτερες προκλήσεις της σύγχρονης εποχής. Κρίθηκε, επιτακτική η ανάγκη ύπαρξης μίας νέας, ενιαίας και (όσο το δυνατόν πιο) λεπτομερούς προσέγγισης, με κανόνες που θα ρυθμίζουν την προστασία των δεδομένων (μέσα, σκοπό/αποτέλεσμα, κύρωση) με τέτοιο τρόπο που δεν θα επιτρέπει την εκμετάλλευση προσωπικών δεδομένων για σκοπούς αθέμιτους εντός των ορίων της Ένωσης, ενώ παράλληλα θα υποχρεώνει όλα τα κράτη-μέλη να επιβάλλουν κανόνες με κοινά μέσα ελεγχόμενης, αν όχι εγγυημένης, αποτελεσματικότητας.

§2.5 - *Διαφορά Οδηγίας 95/46/ΕΚ – Κανονισμού 679/2016/ΕΕ*

Ο Κανονισμός έχει 99 άρθρα και έκταση 5 φορές[17] μεγαλύτερη από την Οδηγία. Ο εμπλουτισμός του κανονιστικού «οπλοστασίου» έχει ως κύριο σκοπό να βελτιώσει την παρεχόμενη προστασία στα υποκείμενα των, με το να θέσει πιο αυστηρά χρονικά όρια στην αποθήκευση των δεδομένων, να επεκτείνει το εδαφικό πεδίο εφαρμογής κ.ά. Η δεύτερη διαφορά είναι ότι στον Κανονισμό δίνεται έμφαση στην πρόληψη αντί για την

[16] Βλ. Ιστοσελίδα www.lawspot.gr.
[17] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 8-9.

καταστολή (Οδηγία) και ότι προσθέτει έναντι της προγενέστερης Οδηγίας ρητά στην ειδική κατηγορία δεδομένων τα βιομετρικά και τα γενετικά δεδομένα, ο χαρακτηρισμός των οποίων παλαιότερα ως ευαίσθητων δεδομένων δεν ήταν αδιαμφισβήτητος. Η πρόληψη διασφαλίζεται ακόμη, με μηχανισμούς αυτοδέσμευσης των υπεύθυνων επεξεργασίας, όπως ο κώδικας δεοντολογίας. Ακόμα, αναδεικνύεται η σημασία της τεχνοκρατικής συνιστώσας στην ορθή διαχείριση των δεδομένων και απονέμεται πιο ενεργός ρόλος στο υποκείμενο των δεδομένων:

Κατοχυρώνεται, το δικαίωμα αντίρρησης, το «δικαίωμα στη λήθη», το δικαίωμα πρόσβασης και άλλα δικαιώματα που θα εξεταστούν στην συνέχεια. «Ο Κανονισμός[18] διευκρινίζει το συνταγματικά αυτονόητο της ελλείψεως κυριαρχίας στα ατομικά δικαιώματα υπογραμμίζοντας ότι σε περίπτωση συγκρούσεως θα λαμβάνει χώρα στάθμιση επί τη βάσει της αρχής της αναλογικότητας». Σημαντικότερη καινοτομία προς αυτή την κατεύθυνση αποτελεί ο θεσμός της μελέτης αντικτύπου (data privacy impact assessment) για την επιστημονική εκτίμηση των πιθανών κινδύνων και την αξιολόγηση των εγγυήσεων και των μέτρων προστασίας.

Προτού προχωρήσουμε σε περαιτέρω ανάλυση θεματικών ενοτήτων, κρίνεται απαραίτητο να παραθέσουμε κάποιους ορισμούς – έννοιες που θα λειτουργήσουν ως μια ομαλή μετάβαση για την συνέχεια.

§3. - ΟΡΙΣΜΟΙ

«**Κανονισμοί»**: Οι κανονισμοί είναι νομικές πράξεις που ορίζονται στο άρθρο 288[19] της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ). Έχουν γενική ισχύ, είναι δεσμευτικοί ως προς όλα τα μέρη τους και ισχύουν άμεσα σε όλες τις χώρες της Ευρωπαϊκής Ένωσης (ΕΕ). Ανήκει στο παράγωγο δίκαιο της ΕΕ, εγκρίνεται από τα θεσμικά όργανα της ΕΕ με βάση τις ιδρυτικές Συνθήκες και αποσκοπεί στην ενιαία εφαρμογή της νομοθεσίας της ΕΕ σε όλες της χώρες της. Ο κανονισμός θεσπίζεται βάσει νομοθετικής διαδικασίας. Είναι μια νομοθετική πράξη που εγκρίνεται από το Συμβούλιο και το Κοινοβούλιο με τη συνήθη ή την ειδική νομοθετική διαδικασία.

[18] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ», σελ 24.
[19] Βλ. Ιστοσελίδα Ευρωπαϊκής Ένωσης, www.europa.eu.

Απευθύνεται σε αφηρημένες κατηγορίες προσώπων και όχι σε αναγνωρίσιμους αποδέκτες. Το στοιχείο αυτό τον διαφοροποιεί από την απόφαση, η οποία ορίζεται στο άρθρο 288 της ΣΛΕΕ[20].

«**Οδηγίες**»: Οι οδηγίες είναι νομοθετικές πράξεις που ορίζουν έναν στόχο τον οποίο πρέπει να επιτύχουν όλες οι χώρες της ΕΕ. Ωστόσο, εναπόκειται σε κάθε χώρα να θεσπίσει τους δικούς της νόμους για την επίτευξη των στόχων αυτών. Δεν έχει άμεση ισχύ όπως ο Κανονισμός είναι δεσμευτική μόνο ως προς το αποτέλεσμα[21]. Ένα παράδειγμα είναι η οδηγία της ΕΕ για τα δικαιώματα των καταναλωτών, η οποία ενδυναμώνει τα δικαιώματα των καταναλωτών σε όλη την ΕΕ.

«**Δεδομένα προσωπικού χαρακτήρα**»: κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

«Επεξεργασία»: 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.

«Εκτελών την επεξεργασία»: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

«**Υπεύθυνος επεξεργασίας**» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η 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

[20] Δονάτος Παπαγιάννης, «Ευρωπαϊκό Δίκαιο», 5η έκδοση, σελ 288
[21] Δονάτος Παπαγιάννης, «Ευρωπαϊκό Δίκαιο», 5η έκδοση, σελ 291

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.

«Κύρια εγκατάσταση» Το άρθρο 4 σημείο 16) του γενικού κανονισμού για την προστασία δεδομένων ορίζει την «κύρια εγκατάσταση» ως εξής:

- όταν πρόκειται για υπεύθυνο επεξεργασίας με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση, εκτός εάν οι αποφάσεις όσον αφορά τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα λαμβάνονται σε άλλη εγκατάσταση του υπευθύνου επεξεργασίας στην Ένωση και η εγκατάσταση αυτή έχει την εξουσία εφαρμογής των αποφάσεων αυτών, οπότε ως κύρια εγκατάσταση θεωρείται η εγκατάσταση στην οποία έλαβε τις αποφάσεις αυτές, -

- όταν πρόκειται για εκτελούντα την επεξεργασία με εγκαταστάσεις σε περισσότερα του ενός κράτη μέλη, ο τόπος της κεντρικής του διοίκησης στην Ένωση ή, εάν ο εκτελών την επεξεργασία δεν έχει κεντρική διοίκηση στην Ένωση, η εγκατάσταση του εκτελούντος την επεξεργασία στην Ένωση στην οποία εκτελούνται οι κύριες δραστηριότητες επεξεργασίας στο πλαίσιο των δραστηριοτήτων εγκατάστασης του εκτελούντος την επεξεργασία, στον βαθμό που ο εκτελών την επεξεργασία υπόκειται σε ειδικές υποχρεώσεις δυνάμει του παρόντος κανονισμού.

«**Δημόσιες Αρχές»** θεωρούνται οι Αρχές του Δημόσιου και ευρύτερου Δημόσιου τομέα συμπεριλαμβανομένων όλων των ανεξάρτητων Αρχών και των Αρχών τοπικής αυτοδιοίκησης, Δικαστικές Αρχές όταν δεν ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας και Βουλή των Αντιπροσώπων.

Αρμόδια αρχή»: α) κάθε δημόσια αρχή αρμόδια για τη διερεύνηση, τη διακρίβωση, βεβαίωση ή τη δίωξη εγκλημάτων β) κάθε δημόσια αρχή αρμόδια για την εκτέλεση ποινικών κυρώσεων γ) κάθε δημόσια αρχή αρμόδια για την πρόληψη εγκλημάτων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους· δ) κάθε άλλος οργανισμός ή φορέας, στον οποίο ο νόμος αναθέτει ρόλο δημόσιας αρχής και την εκτέλεση δημόσιων εξουσιών για τους σκοπούς της πρόληψης, της διερεύνησης, της διακρίβωσης, βεβαίωσης ή της δίωξης εγκλημάτων ή

της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους.

«**Γενετικά δεδομένα»:** τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

«**Βιομετρικά δεδομένα**»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.

«**Δεδομένα που αφορούν την υγεία**»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

«Βασικές δραστηριότητες»: Ως «βασικές δραστηριότητες» μπορούν να θεωρηθούν οι καίριες πράξεις για την επίτευξη των στόχων του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Σ' αυτές συμπεριλαμβάνονται επίσης όλες οι δραστηριότητες που επιτελούνται όταν η επεξεργασία δεδομένων αποτελεί αναπόσπαστο μέρος της δραστηριότητας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Για παράδειγμα, η επεξεργασία ιατρικών δεδομένων, όπως οι ιατρικοί φάκελοι ασθενών, θα πρέπει να θεωρείται ως μία από τις βασικές δραστηριότητες κάθε νοσοκομείου. Κατά συνέπεια, τα νοσοκομεία οφείλουν να ορίσουν υπεύθυνο προστασίας δεδομένων**.**

§4. - ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΚΑΝΟΝΙΣΜΟΥ

Σύμφωνα με το άρθρο 3 Κ, το πεδίο εφαρμογής του Κανονισμού εκτείνεται στις δραστηριότητες εγκαταστάσεως υπευθύνου επεξεργασίας ή εκτελούντος την

επεξεργασία που λαμβάνει χώρα εντός ΕΕ[22], αλλά και στις δραστηριότητες εγκαταστάσεως υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία εκτός ΕΕ, όταν η επεξεργασία αφορά υποκείμενα δεδομένων που βρίσκονται εντός ΕΕ. Ουσιαστικά υιοθετείται η αρχή του τόπου εγκαταστάσεως του οργανισμού (ή της επιχειρήσεως) αλλά και του υποκειμένου των δεδομένων. Δηλαδή, ο Κανονισμός μπορεί να ισχύει για κάποιον που είναι εγκατεστημένος στις Η.Π.Α και επεξεργάζεται δεδομένα πολιτών εντός της ΕΕ. «Με τον τρόπο αυτό ο Κανονισμός αποσκοπεί στο να αλλάξει την προστασία δεδομένων προσωπικού χαρακτήρα παγκοσμίως».[23] Όμως εάν κάποιος υπήκοος ΕΕ, είναι εγκατεστημένος εκτός ΕΕ (π.χ Η.Π.Α) και τα δεδομένα του επεξεργάζονται από κάποιον που βρίσκεται και αυτός εκτός ΕΕ, τότε ο Κανονισμός 679/2016 δεν εφαρμόζεται γι'αυτόν.

§4.1 – *Διαβίβαση δεδομένων εκτός ΕΕ*

Στον σημερινό παγκοσμιοποιημένο κόσμο, γίνονται διασυνοριακές διαβιβάσεις μεγάλου όγκου δεδομένων προσωπικού χαρακτήρα[24], τα οποία ορισμένες φορές αποθηκεύονται σε διακομιστές σε διαφορετικές χώρες. Η προστασία που προσφέρει ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) συνοδεύει τα δεδομένα, πράγμα που σημαίνει ότι οι κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα εξακολουθούν να ισχύουν ανεξάρτητα από το πού καταλήγουν τα δεδομένα. Αυτό ισχύει επίσης όταν τα δεδομένα διαβιβάζονται σε χώρα που δεν ανήκει στην ΕΕ (τρίτη χώρα). Ο ΓΚΠΔ παρέχει διαφορετικά εργαλεία που πλαισιώνουν τις διαβιβάσεις δεδομένων από την ΕΕ προς τρίτη χώρα: Ορισμένες φορές, μια τρίτη χώρα μπορεί, μέσω απόφασης της Ευρωπαϊκής Επιτροπής («απόφαση επάρκειας»), να κηρυχθεί ως προσφέρουσα επαρκές επίπεδο προστασίας , πράγμα που σημαίνει ότι επιτρέπεται να διαβιβασθούν δεδομένα σε άλλη εταιρεία στην εν λόγω τρίτη χώρα χωρίς να απαιτείται από τον εξαγωγέα δεδομένων να παρέχει περαιτέρω εγγυήσεις ή να υπόκειται σε επιπλέον όρους. Με άλλα λόγια, οι διαβιβάσεις σε μια «επαρκή» τρίτη χώρα εξομοιώνονται με διαβίβαση δεδομένων εντός της ΕΕ. Σε περίπτωση που δεν υπάρχει απόφαση επάρκειας, μπορεί να γίνει διαβίβαση με την παροχή κατάλληλων εγγυήσεων και με την προϋπόθεση ότι τα φυσικά πρόσωπα έχουν

[22] Φερενίκη Παναγοπούλου-Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων, 679/2016/ΕΕ» σελ 26-27

[23] Φερενίκη Παναγοπούλου-Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων, 679/2016/ΕΕ» σελ 26-27.

[24] Βλ. Ιστοσελίδα Ευρωπαϊκής Επιτροπής, www.europa.eu

στη διάθεσή τους εκτελεστά δικαιώματα και πραγματικά ένδικα μέσα. Τέτοιες κατάλληλες εγγυήσεις περιλαμβάνουν τα εξής: στην περίπτωση ομίλου επιχειρήσεων ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα, οι εταιρείες μπορούν να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα με βάση τους αποκαλούμενους δεσμευτικούς εταιρικούς κανόνες συμβατικές ρυθμίσεις με τον αποδέκτη των δεδομένων προσωπικού χαρακτήρα, μέσω της χρήσης, για παράδειγμα, τυποποιημένων συμβατικών ρητρών που έχουν λάβει την έγκριση της Ευρωπαϊκής Επιτροπής. Ένα άλλο «εργαλείο» του ΓΚΠΔ για την διαβίβαση δεδομένων εκτός ΕΕ είναι η τήρηση ενός κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης παράλληλα με τη λήψη δεσμευτικών και εκτελεστών δεσμεύσεων από τον αποδέκτη, σχετικά με την εφαρμογή κατάλληλων εγγυήσεων για την προστασία των δεδομένων που διαβιβάζονται. Τέλος, εάν προβλέπεται διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα που δεν υπόκειται σε απόφαση επάρκειας και εάν δεν υπάρχουν κατάλληλες εγγυήσεις, μπορεί να γίνει διαβίβαση με βάση ορισμένες εξαιρέσεις για συγκεκριμένες καταστάσεις, για παράδειγμα, όταν ένα φυσικό πρόσωπο συγκατατέθηκε ρητώς στην προτεινόμενη διαβίβαση αφού του παρασχέθηκαν όλες οι απαραίτητες πληροφορίες σχετικά με τους κινδύνους που αυτή ενέχει.

Οι 4 βασικοί πυλώνες της εργασίας είναι οι εξής: α) ο Υπεύθυνος Επεξεργασίας, β) ο Υπεύθυνος Προστασίας Δεδομένων, γ) η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων στη Δημόσια Διοίκηση και δ) τα δικαιώματα που προκύπτουν από τον Κανονισμό. Προτού αναλυθεί ο πρώτος «πυλώνας», βέλτιστο θα ήταν να παραθέσουμε κάποιους κανόνες αυτοδέσμευσης των Υπευθύνων Επεξεργασίας[25], τους Κώδικες Δεοντολογίας.

§5. - ΚΩΔΙΚΕΣ ΔΕΟΝΤΟΛΟΓΙΑΣ

Οι κώδικες δεοντολογίας προβλέπονται στο άρ. 40 ΓΚΠΔ και αποσκοπούν στο να διευκολύνεται η ουσιαστική εφαρμογή του Κανονισμού[26], ρυθμίζοντας ειδικές υποχρεώσεις τόσο υπευθύνων επεξεργασίας όσο και εκτελούντων την επεξεργασία, ειδικούς τομείς δραστηριότητας Ως εκ τούτου, οι κώδικες δεοντολογίας δεν εκπονούνται από μεμονωμένους υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία, αλλά από ενώσεις ή άλλους φορείς που εκπροσωπούν

[25] Μια πρώτη ιδέα για τον Υπεύθυνο Επεξεργασίας είδαμε στην παράγραφο 3, «ορισμοί».
[26] Βλ. Ιστοσελίδα Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.

κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία. Συνεπώς, η εν λόγω έννοια του κώδικα δεοντολογίας του άρ. 40 είναι διαφορετική από οποιονδήποτε άλλον κώδικα δεοντολογίας έχει τυχόν ήδη θεσπίσει υπεύθυνος επεξεργασίας για τις πράξεις επεξεργασίας προσωπικών δεδομένων που διενεργεί. Οι κώδικες δεοντολογίας δεν είναι υποχρεωτικοί αλλά προαιρετικοί. Κατά την κατάρτιση ενός κώδικα δεοντολογίας ή κατά την τροποποίηση ή την επέκταση ενός τέτοιου κώδικα, ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία θα πρέπει να διαβουλεύονται με τα ενδιαφερόμενα μέρη, μεταξύ άλλων και με υποκείμενα των δεδομένων, όπου αυτό είναι εφικτό, και να λαμβάνουν υπόψη όσες παρατηρήσεις υποβάλλονται και όσες απόψεις διατυπώνονται στο πλαίσιο αυτών των διαβουλεύσεων. Λοιπά στοιχεία που λαμβάνονται υπόψη κατά την κατάρτιση ενός κώδικα περιγράφονται στο αρ. 40 παρ. 2 ΓΚΠΔ. Το σχέδιο ενός τέτοιου κώδικα πρέπει να υποβάλλεται στην Αρχή, η οποία γνωμοδοτεί για το αν ο εν λόγω κώδικας είναι σύμφωνος με τον Κανονισμό και τον εγκρίνει εφόσον κρίνει ότι παρέχει επαρκείς εγγυήσεις (είτε πρόκειται για αρχικό κώδικα είτε για τροποποίηση υπάρχοντα). Ένας εγκεκριμένος από την Αρχή κώδικας δεοντολογίας, εφόσον τηρείται από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία, δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας (άρ. 24 παρ. 3 ΓΚΠΔ) ή ως στοιχείο για να αποδειχθεί ότι ο εκτελών την επεξεργασία παρέχει επαρκείς διαβεβαιώσεις σύμφωνα με τις παρ. 1 και 4 του άρ. 28 (άρ. 28 παρ. 5). Όταν η Αρχή εγκρίνει έναν κώδικα, τον καταχωρίζει και τον δημοσιεύει.

§6.- ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Ο νέος Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπεύθυνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη αρχή της διαφάνειας στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα αρχή της λογοδοσίας, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων. Σύμφωνα με το νόμο ο υπεύθυνος επεξεργασίας έχει την ευθύνη να εξασφαλίσει επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων**.** Η Αρχή

συμβουλεύει τους υπευθύνους επεξεργασίας στην κατάρτιση κωδίκων δεοντολογίας για την επεξεργασία προσωπικών δεδομένων και ζητά την υποβολή τους καθώς και την υποβολή σχεδίων ασφαλείας και/ή σχεδίων έκτακτης ανάγκης ιδιαίτερα στις περιπτώσεις όπου πραγματοποιείται επεξεργασία ευαίσθητων προσωπικών δεδομένων.

- Ο Κώδικας Δεοντολογίας περιέχει κανόνες αυτοδέσμευσης επαγγελματικών ομάδων, που περιλαμβάνουν τον τρόπο χειρισμού προσωπικών δεδομένων. Ο κώδικας αυτός πρέπει να είναι δεσμευτικός ως προς την τήρηση του από τους υπαλλήλους του υπευθύνου επεξεργασίας ή τα μέλη της επαγγελματικής ομάδας.

- Το Σχέδιο Ασφάλειας[27] (Security Plan) είναι ένα έγγραφο στο οποίο περιγράφεται η πολιτική ενός οργανισμού για την κάλυψη των βασικών απαιτήσεων ασφάλειας, καθώς επίσης και τα κύρια τεχνικά, διοικητικά και οργανωτικά μέτρα ασφάλειας που εφαρμόζονται ή/και πρόκειται να εφαρμοστούν. Το Σχέδιο Ασφάλειας αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων και πρέπει να εφαρμόζεται με ακρίβεια για την προστασία των ευαίσθητων προσωπικών δεδομένων που τηρούνται από τον οργανισμό. Η σύνταξη του Σχεδίου θα πρέπει να γίνεται από υπεύθυνο πρόσωπο, ορισμένο από τον οργανισμό και να υπογράφεται από τη Διοίκηση του εν λόγω οργανισμού.

- Το Σχέδιο Έκτακτης Ανάγκης[28] (Disaster recovery plan and contingency plan) είναι ένα έγγραφο που αναφέρεται στα μέτρα προστασίας, ανάκαμψης και αποκατάστασης ενός συστήματος πληροφοριών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, εξωτερικές επιθέσεις/ εισβολές, κλπ. Το Σχέδιο Έκτακτης Ανάγκης συμπληρώνει το Σχέδιο Ασφαλείας ενός οργανισμού και αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων. Η σύνταξη του Σχεδίου θα πρέπει να γίνεται από υπεύθυνο πρόσωπο, ορισμένο από τον οργανισμό και να υπογράφεται από τη Διοίκηση του εν λόγω οργανισμού.

[27] Βλ. Ιστοσελίδα Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.
[28] Βλ. Ιστοσελίδα Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.

Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να είναι να είναι σε θέση να αποδείξει τη συμμόρφωση του με τις προβλέψεις του Γενικού Κανονισμού, με όλες τις άλλες αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, είναι νόμιμη, εφόσον είναι αναγκαία για την εκπλήρωση των καθηκόντων και την άσκηση των αρμοδιοτήτων που έχουν ανατεθεί στον υπεύθυνο επεξεργασίας από τον νόμο ή με ανάθεση κατ' εξουσιοδότηση νόμου. Ευθύνη του υπεύθυνου επεξεργασίας νοείται ως η υποχρέωση του να λαμβάνει όλα τα αναγκαία απαραίτητα τεχνικά και οργανωτικά μέτρα λαμβάνοντας υπόψη ασφαλώς τους κινδύνους οι οποίοι υφίστανται για τις επεξεργασίες τις οποίες πραγματοποιεί. Επίσης, να λαμβάνει, να καταρτίζει κατάλληλες πολιτικές προστασίας δεδομένων. Κάθε οργανισμός, φορέας του δημοσίου, εταιρεία που έχει για τους σκοπούς της, για τις δραστηριότητές της προσωπικά δεδομένα και τα επεξεργάζεται, χαρακτηρίζεται υπεύθυνος επεξεργασίας. Αν εμπλακεί στην επεξεργασία οποιοσδήποτε τρίτος (π.χ outsource), αυτός ο τρίτος λέγεται «εκτελών την επεξεργασία». Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών, συνοδεύεται από αιτιολόγηση για την καθυστέρηση.

Σύμφωνα με το άρ. 33 του Κανονισμού (ΕΕ) 2016/679, οι υπεύθυνοι επεξεργασίας, σε περίπτωση που συμβεί περιστατικό παραβίασης προσωπικών δεδομένων από το οποίο ενδέχεται να προκληθεί κίνδυνος στα δικαιώματα και τις ελευθερίες των προσώπων τα οποία αφορά το περιστατικό, οφείλουν να γνωστοποιήσουν το εν λόγω περιστατικό στην Αρχή.

Η γνωστοποίηση αυτή πρέπει να γίνεται αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που ο υπεύθυνος επεξεργασίας ενημερωθεί για το περιστατικό. Η γνωστοποίηση πρέπει να περιέχει σύνολο σχετικών πληροφοριών (φύση/έκταση του

περιστατικού, κατηγορίες προσώπων που επλήγησαν, αιτία και συνέπειες αυτού, ενέργειες που έγιναν προς αντιμετώπισή του, κ.ά.). Ακόμα και αν οι σχετικές αυτές πληροφορίες δεν είναι όλες διαθέσιμες κατά την υποβολή της γνωστοποίησης, αυτή θα πρέπει να υποβληθεί ως αρχική και να ακολουθήσει στο μέλλον, χωρίς αδικαιολόγητη καθυστέρηση, επικαιροποίησή της (με υποβολή συμπληρωματικής γνωστοποίησης).

Επισημαίνεται ότι ακόμα και αν το περιστατικό δεν μπορεί να προκαλέσει κίνδυνο για τα φυσικά πρόσωπα που αφορά, οπότε και δεν απαιτείται η υποβολή της ως άνω γνωστοποίησης στην Αρχή, ο υπεύθυνος επεξεργασίας οφείλει σε κάθε περίπτωση να τηρεί δικό του εσωτερικό σχετικό αρχείο.

Περαιτέρω, σύμφωνα με το άρ. 34 του Κανονισμού (ΕΕ) 2016/679, όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τα οποία αφορά το περιστατικό, τότε ο υπεύθυνος επεξεργασίας οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά. Αυτή η ανακοίνωση είναι ανεξάρτητη της προαναφερθείσας γνωστοποίησης στην Αρχή (η οποία γνωστοποίηση στην Αρχή υποβάλλεται ακόμα και αν ο σχετικός κίνδυνος δεν κρίνεται ως υψηλός). Η ανακοίνωση στα φυσικά πρόσωπα θα πρέπει να γίνει με τον πλέον πρόσφορο και αποτελεσματικό τρόπο, με τη μορφή προσωποποιημένης πληροφόρησης και όχι μέσω κάποιας γενικού χαρακτήρα ανακοίνωσης, στο βαθμό που αυτό είναι εφικτό.

Σημειώνεται ότι η Αρχή δύναται σε κάθε περίπτωση να δώσει εντολή στον υπεύθυνο επεξεργασίας να ενημερώσει τα φυσικά πρόσωπα για το περιστατικό (άρ. 58 παρ. 2 ε' Κανονισμού).

§6.1 - *«Παλιές και νέες υποχρεώσεις»*

Η Οδηγία 95/46/ΕΚ εστιάζει στο απόρρητο και στην ασφάλεια της επεξεργασίας. Συγκεκριμένα, το άρθρο 17 προβλέπει ότι «ο υπεύθυνος της επεξεργασίας πρέπει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία από τυχαία ή παράνομη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, ιδίως αν η επεξεργασία συμπεριλαμβάνει και διαβίβαση των δεδομένων μέσων δικτύου, και από κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικών χαρακτήρα. Τα μέτρα αυτά, πρέπει να εξασφαλίζουν λαμβανομένης

υπόψη της τεχνολογικής εξέλιξης και του κόστους εφαρμογής τους, επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που απορρέουν από την επεξεργασία και την φύση των δεδομένων που απολαύουν προστασίας..»

Συγκριτικά, ο ΓΚΠΔ προβλέπει την γενικότερη ευθύνη του υπευθύνου επεξεργασίας. Σύμφωνα με το άρθρο 24: «Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα, προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα Κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο».

Συνεπώς, ο Γενικός Κανονισμός κατοχυρώνει μια σειρά από έννοιες που δεν έχουν χρησιμοποιηθεί στο παρελθόν και της επαυξάνει προς τη κατεύθυνση της διακυβέρνησης για τα προσωπικά δεδομένα (Personal Data Governance).

§6.2 - *Προστασία δεδομένων κατά τον σχεδιασμό*[29] *(«Data protection by design»)*

Ο Κανονισμός[30] επιβάλλει την εφαρμογή προϊόντων και υπηρεσιών (ηλεκτρονικών και μη) που κατά τον αρχικό σχεδιασμό τους δημιουργούν φιλικές συνθήκες για την προστασία των δεδομένων. Οι οργανισμοί[31] ενθαρρύνονται να εφαρμόζουν τεχνικά και οργανωτικά μέτρα, στα αρχικά στάδια του σχεδιασμού των πράξεων επεξεργασίας, με τέτοιον τρόπο ώστε να διασφαλίζονται οι αρχές ιδιωτικού απορρήτου και προστασίας δεδομένων ήδη από την αρχή. («προστασία δεδομένων ήδη από τον σχεδιασμό») Για παράδειγμα, στις υπηρεσίες ηλεκτρονικής κοινωνικής δικτύωσης πρέπει να δίνεται η δυνατότητα να επιλέγονται ρυθμίσεις που θα προστατεύουν περισσότερο τα προσωπικά σας δεδομένα ή για την χρήση ψευδωνυμοποίησης (αντικατάσταση

[29] Φερενίκη Παναγοπούλου-Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων, 679/2016/ΕΕ», σελ 32.
[30] Βλ. άρ 25 Κ.
[31] Βλ. άρθρο 25 και αιτιολογική σκέψη 78 του ΓΚΠΔ.

προσωπικά ταυτοποιήσιμου υλικού με τεχνητά αναγνωριστικά στοιχεία) και κρυπτογράφησης. (κωδικοποίηση μηνυμάτων έτσι ώστε μόνο όσοι είναι εξουσιοδοτημένοι να μπορούν να τα διαβάζουν).

§6.3 - *Προστασία δεδομένων εξ ορισμού[32] («Data protection by default»)*

Ο Κανονισμός[33] επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, εξ ορισμού[34], υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας. Εξ ορισμού, δηλαδή οι οργανισμοί θα πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με το υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής (π.χ. μόνο τα απαραίτητα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία, σύντομη περίοδος αποθήκευσης, περιορισμένη προσβασιμότητα) έτσι ώστε εξ ορισμού τα δεδομένα προσωπικού χαρακτήρα να μην είναι προσβάσιμα από αόριστο αριθμό φυσικών προσώπων («προστασία δεδομένων εξ ορισμού»). Για παράδειγμα, μια πλατφόρμα κοινωνικής δικτύωσης θα πρέπει να ενθαρρύνεται να ορίζει τις ρυθμίσεις των προφίλ των χρηστών έτσι ώστε να προστατεύουν όσο το δυνατόν περισσότερο το ιδιωτικό απόρρητο, για παράδειγμα, περιορίζοντας από την αρχή την προσβασιμότητα στα προφίλ των χρηστών έτσι ώστε να μην είναι προσβάσιμα εξ ορισμού από αόριστο αριθμό ατόμων.

§6.4 - *Επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον*

Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 παράγραφος 1 του Κανονισμού επιτρέπεται, όταν είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον και ο υπεύθυνος επεξεργασίας λαμβάνει τα ανάλογα προς τον κίνδυνο μέτρα σύμφωνα με την παράγραφο 3 του παρόντος άρθρου. «Ο υπεύθυνος επεξεργασίας, συνεκτιμώντας[35] το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της εκάστοτε επεξεργασίας και τη φύση

[32] Φερενίκη Παναγοπούλου-Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων, 679/2016/ΕΕ», σελ 32.
[33] Βλ. άρ 25 Κ.
[34] Βλ.Ιστοσελίδα της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.
[35] Βλ. Ιστοσελίδα Υπουργείου Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων, www.opengov.gr.

και κατηγορία των δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται στο αρχειακό υλικό, λαμβάνει κατάλληλα και ανάλογα οργανωτικά και τεχνικά μέτρα που διασφαλίζουν τη συμμόρφωση προς τις αρχές της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως η αρχή της ελαχιστοποίησης, και προστασίας των δεδομένων αυτών, ιδίως αναφορικά με τα πρόσωπα τα οποία έχουν πρόσβαση και λαμβάνουν γνώση των δεδομένων αυτών και τους όρους πρόσβασης σε αυτά». Κατά παρέκκλιση από το άρθρο 16 του Κανονισμού το υποκείμενο των δεδομένων δεν έχει δικαίωμα διόρθωσης των δεδομένων προσωπικού χαρακτήρα που το αφορούν, (όπως έχει επισημανθεί, εφόσον η άσκησή του είναι πιθανό να καταστήσουν αδύνατη ή να παρακωλύσουν σοβαρά την επίτευξη των σκοπών αρχειοθέτησης προς το δημόσιο συμφέρον ή την άσκηση δικαιωμάτων τρίτων. Εάν το υποκείμενο των δεδομένων αμφισβητεί βάσιμα την ακρίβεια των δεδομένων προσωπικού που το αφορούν και τηρούνται για τους ανωτέρω σκοπούς δύναται να αιτηθεί την κατάθεση συμπληρωματικών δεδομένων, τα οποία κατά την κρίση του υπευθύνου επεξεργασίας μπορούν να ενταχθούν κατά διακριτό τρόπο στο αρχειακό υλικό. Όπως επίσης είναι δυνατό να περιοριστούν τα δικαιώματα των υποκειμένων (κατά παρέκκλιση από τα οριζόμενα άρθρα 18, 19, 20 και 21 του Κανονισμού) εφόσον τα εν λόγω δικαιώματα είναι πιθανό να καταστήσουν αδύνατη ή να παρακωλύσουν σοβαρά την επίτευξη των ειδικών σκοπών αρχειοθέτησης προς το δημόσιο συμφέρον.

§6.5 -*Τήρηση αρχείων δραστηριοτήτων*[36]

Ο υπεύθυνος και ο εκτελών την επεξεργασία οφείλουν, βάσει του άρθρου 30 του Κανονισμού, να τηρούν εγγράφως ή ηλεκτρονικά αρχείο δραστηριοτήτων επεξεργασιών τους όταν ο οργανισμός (ή η επιχείρηση) απασχολεί άνω των 250 ατόμων[37], η επεξεργασία δημιουργεί κινδύνους για τα δεδομένα. Το εν λόγω αρχείο τίθεται στην διάθεση της εποπτικής αρχής κατόπιν αιτήματος της προς άσκηση των αρμοδιοτήτων της.

§6.6 - *Εκτίμηση επιπτώσεων και προηγούμενη διαβούλευση*

Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες

[36] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 33.
[37] Βλ. άρ 30 Κ .

δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων (Data protection impact assessment). Όταν βάσει της διενεργηθείσας εκτίμησης επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εποπτική Αρχή.

§6.7 - Αρχή της Λογοδοσίας

Ο Γενικός Κανονισμός εισάγει την αρχή της Λογοδοσίας[38] (Accountability), σύμφωνα με την οποία οι υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία (οργανισμοί/φορείς/επιχειρήσεις), που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα, οφείλουν να διαμορφώνουν τις διαδικασίες και τα τεχνικά και οργανωτικά συστήματά τους κατά τέτοιο τρόπο ώστε να μπορούν να αποδεικνύουν, ανά πάσα στιγμή, τόσο ενώπιον των εποπτικών αρχών όσο και των δικαστηρίων, ότι είναι πλήρως συμμορφωμένοι με όσα προβλέπει ο νέος Κανονισμός. Η αρχή της λογοδοσίας συνιστά ακρογωνιαίο λίθο του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ). 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 τα βοηθά να αποδεικνύουν τη λογοδοσία, ορισμένα εκ των οποίων πρέπει να τίθενται σε εφαρμογή υποχρεωτικά. Η αρχή της Λογοδοσίας αποτελεί και πρέπει να αποτελεί την σημαντικότερη αρχή για τον υπεύθυνο επεξεργασίας .Η εισαγωγή αυτής της αρχής μετατοπίζει το «βάρος της απόδειξης», όσον αφορά τη νομιμότητα της επεξεργασίας και τη συμμόρφωση με τον ΓΚΠΔ, από τις αρχές προστασίας δεδομένων στους ίδιους τους υπευθύνους επεξεργασίας ή τους εκτελούντες.

Σ'αυτό το σημείο θα ακολουθήσουν και κάποιες επιμέρους αρχές επεξεργασίας που ισχύουν και θα πρέπει να ισχύουν για κάθε Δημόσιο Τομέα – Φορέα.

[38] Βλ. Ιστοσελίδα Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, www.dpa.gr.

§6.8 -*Επιμέρους Αρχές Επεξεργασίας*[39]

- Νομιμότητα, αντικειμενικότητα και διαφάνεια: (laufulness, fairness and transparency) τα προσωπικά δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων
- Περιορισμός του σκοπού: (purpose limitation) τα προσωπικά δεδομένα συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς
- Ελαχιστοποίηση των δεδομένων: (data minimisation) τα προσωπικά δεδομένα, είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία
- Ακρίβεια: (accuracy) τα προσωπικά δεδομένα είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται (όσο το δυνατόν άμεσα)
- Περιορισμός της περιόδου αποθήκευσης: (storage limitation) τα προσωπικά δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται
- Ακεραιότητα και εμπιστευτικότητα: (integrity and confidentiality) απαίτηση εγγύησης για την ενδεδειγμένη ασφάλεια των δεδομένων από σειρά κινδύνων, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων.

§6.9 – *Εκτελών την επεξεργασία*

Ο εκτελών την επεξεργασία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα μόνο εκ μέρους του υπεύθυνου επεξεργασίας. Όταν η επεξεργασία πρόκειται να διενεργηθεί για λογαριασμό υπευθύνου επεξεργασίας, ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις[40] για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται

[39] Βλ. εκδδα, καινότομο εργαστήριο «Γενικός Κανονισμός Προστασίας Δεδομένων, το νέο τοπίο και οι υποχρεώσεις της Δημόσιας Διοίκησης».
[40] Βλ. Ιστοσελίδα. www.lawspot.gr

η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων. Ο εκτελών την επεξεργασία είναι συνήθως τρίτος εκτός εταιρείας[41] (το ίδιο ισχύει και για τον δημόσια τομέα, δηλαδή τις δημόσιες διοικήσεις και τους δημοσίους φορείς). Ωστόσο, στην περίπτωση ομίλων επιχειρήσεων, μια επιχείρηση μπορεί να ενεργεί ως εκτελούσα την επεξεργασία για λογαριασμό άλλης επιχείρησης. Τα καθήκοντα του εκτελούντος την επεξεργασία προς τον υπεύθυνο επεξεργασίας πρέπει να καθορίζονται σε σύμβαση ή άλλη νομική πράξη.

§6.10 - *Ορισμός Υπευθύνου Προστασίας Δεδομένων*

Ο υπεύθυνος επεξεργασίας οφείλει να ορίσει, βάσει του άρθρου 37 του Κανονισμού, υπεύθυνο προστασίας δεδομένων (data protection officer)[42] σε περίπτωση δημοσίων υπηρεσιών και επεξεργασίας μεγάλης κλίμακας[43]. Ο θεσμός αυτός αποσκοπεί στην ανάθεση της προστασίας δεδομένων των υποκειμένων. Ο κομβικός ρόλος του DPO στον Γενικό Κανονισμό Προστασίας Δεδομένων, θα αναλυθεί ευθύς αμέσως.

§7. - ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Όπως προαναφέρθηκε, με τον Γενικό Κανονισμό επιχειρείται η συνολική αναβάθμιση του πλαισίου προστασίας προσωπικών δεδομένων, προκειμένου να εξασφαλιστεί τόσο η ουσιαστική προστασία των ατόμων σε ένα διαρκώς μεταβαλλόμενο τεχνολογικό περιβάλλον, όσο και η ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα. Για να επιτύχει τους σκοπούς αυτούς εισάγει μία σειρά από καινοτόμες διατάξεις, μεταξύ των οποίων και ο θεσμός του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer ή DPO). Ο Υπεύθυνος Προστασίας Δεδομένων[44] (DPO) 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 είναι συμβουλευτικός (όχι αποφασιστικός**)** και δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία

[41] Βλ. Ιστοσελίδα Ευρωπαϊκής Επιτροπής, ec.europa.eu
[42] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 34.
[43] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 34.
[44] Βλ. άρ 37 και 38 του ΓΚΠΔ.

διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Ο DPO μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών (εξωτερικός συνεργάτης). Σε κάθε περίπτωση, μπορεί να συνεπικουρείται από ομάδα, εφόσον απαιτείται. Συνιστάται δε να είναι εγκατεστημένος εντός ΕΕ, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην ΕΕ. Ο Υπεύθυνος Προστασίας Δεδομένων αποτελεί καινοφανής θέση για το ελληνικό δημόσιο. Λειτουργεί εκτός ιεραρχίας και δημοσιοϋπαλληλικής δομής. Λογοδοτεί απευθείας στο υψηλότερο επίπεδο του φορέα. Μπορεί να ασκεί τα καθήκοντα με παράλληλη ανάθεση μέσα στο φορέα ή σε παράλληλους φορείς, αρκεί να μην υπάρχει ασυμβίβαστο. Ο Υπεύθυνος Προστασίας Δεδομένων πρέπει να γνωρίζει πολύ καλά το αντικείμενο του Φορέα.

Σε δημόσιες αρχές και φορείς μπορεί να ορίζεται ένας υπεύθυνος επεξεργασίας ή και περισσότεροι ή πολλοί φορείς μπορούν να ορίσουν ένα μόνο ΥΠΔ, λαμβάνοντας υπόψη κάθε φορά το μέγεθος και την οργανωτική τους δομή, δηλαδή αν ένα Υπουργείο έχει πάρα πολλές γενικές διευθύνσεις ή αν έχει λίγες ή και το μέγεθος τον αριθμό των υπαλλήλων και τον αριθμό των αρχείων επεξεργασίας. Σύμφωνα με τις «Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων» της Ομάδας του άρθρου 29 της Οδηγίας 95/46/ΕΚ, στην έννοια της δημόσιας αρχής ή δημόσιου φορέα που υποχρεούται να ορίσει υπεύθυνο προστασίας δεδομένων εμπίπτουν και άλλα φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου που εκπληρώνουν δημόσια καθήκοντα ή ασκούν δημόσια εξουσία, όπως υπηρεσίες δημοσίων μεταφορών, ύδρευσης και παροχής ενέργειας, οδικές υποδομές, δημόσια ραδιοτηλεόραση, κατασκευή εργατικών κατοικιών, ή πειθαρχικά όργανα για νομοθετικά κατοχυρωμένα επαγγέλματα. Η δραστηριότητα του υπεύθυνου προστασίας καλύπτει όλες τις πράξεις επεξεργασίας που διενεργούνται στο φορέα και περιλαμβάνει και αυτές που δεν σχετίζονται άμεσα με την εκπλήρωση δημόσιου καθήκοντος ή άσκησης δημόσιας εξουσίας (π.χ διαχείριση βάσης δεδομένων). Σύμφωνα, με την ίδια γνώμη της Ομάδας του άρθρου 29, για τον προσδιορισμό της μεγάλης κλίμακας επεξεργασίας πρέπει να λαμβάνονται υπόψη: α) ο αριθμός των εμπλεκόμενων υποκειμένων είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του πληθυσμού β) ο

όγκος και το εύρος των δεδομένων γ) η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας δ) η γεωγραφική έκταση της επεξεργασίας. Σύμφωνα με τα παραπάνω κριτήρια, μπορεί να εξαχθεί αν είναι υποχρεωτικός ή όχι ο ορισμός του υπεύθυνου προστασίας δεδομένων.

Ο ορισμός DPO στηρίζεται στην αρχή της εθελοντικής ανάληψης καθηκόντων. Συνεπώς, από 01/09/2018, εφόσον δεν έχει οριστεί DPO στη βάση της εθελοντικής ανάληψης καθηκόντων, θα πρέπει να απευθύνει πρόσκληση εκδήλωσης ενδιαφέροντος προς το προσωπικό του φορέα για υποβολή υποψηφιότητας σχετικά με την ανάληψη καθηκόντων DPO και αναπλήρωση αυτού, οπότε ο DPO και ο αναπληρωτής θα πρέπει να επιλέγουν μεταξύ ενδεχομένως περισσοτέρων υποψηφίων, μετά από μοριοδότηση και οπωσδήποτε στη βάση επαγγελματικών προσόντων και, ιδίως στη βάση της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης καθηκόντων.

§7.1 - *Γενικό πλαίσιο λειτουργικής ανεξαρτησίας ή αυτονομίας*

Ο Γενικός Κανονισμός Προστασίας Δεδομένων ορίζει το πλαίσιο, εντός του οποίου παρέχονται από τον υπεύθυνο ή τον εκτελούντα την επεξεργασία στον ΥΠΔ οι προϋποθέσεις για την πραγματική και ανεξάρτητη άσκηση των καθηκόντων του. Πιο συγκεκριμένα: πλήρη και πραγματική ενημέρωσή του για όλα τα θέματα προσωπικών δεδομένων, πρόσβασή του σε κάθε είδους δεδομένα και πρόσκλησή του σε κάθε σχεδιαζόμενη πράξη επεξεργασίας προσωπικών δεδομένων, πρόσβασή του στους αναγκαίους πόρους για την υλοποίηση της αποστολής του, παροχή επαρκούς χρόνου για την εκτέλεση των καθηκόντων του, τήρηση απορρήτου ή εμπιστευτικότητας χωρίς να αποτελεί αποτρεπτικό παράγοντα επικοινωνίας και συμβουλής με την εποπτική αρχή και τέλος, διατήρηση της εμπειρογνωσίας του μέσω της συνεχούς ενημέρωσης και εκπαίδευσης για τους εσωτερικούς ΥΠΔ.

§7.2 - *Οικονομική αυτοτέλεια*

Παρά το ότι δεν μπορεί να γίνει τυπικά λόγος για «οικονομική ανεξαρτησία» του Υπεύθυνου Προστασίας Δεδομένων, με την στενή έννοια, είτε στο πλαίσιο παροχής

παροχής ανεξάρτητων εξωτερικών υπηρεσιών, είτε στο πλαίσιο της σύμβασης εργασίας, εν τούτοις μπορεί να γίνει σαφώς λόγος για «οικονομική αυτοτέλειά»[45] του, ως ένα επιπλέον στοιχείο που μειώνει την εξάρτησή του στο πλαίσιο της άσκησης των καθηκόντων του. Ο σχεδιασμός και η έγκριση ενός ιδιαιτέρου προϋπολογισμού εντός της εταιρίας που περιλαμβάνει τις αμοιβές και τους αναγκαίους πόρους για την επιτέλεση των καθηκόντων του ΥΠΔ συνιστά έμπρακτη στήριξη και διασφάλιση της ανεξαρτησίας του.

§7.3 - *Προσωπική ανεξαρτησία*

Στο πλαίσιο της διασφάλισης της λειτουργικής ανεξαρτησίας του ΥΠΔ, κατοχυρώνεται κατ'άρ. 38 παρ. 3 Κανονισμού η προσωπική ανεξαρτησία του με την προϋπόθεση ότι δεν απολύεται, ούτε υφίσταται κυρώσεις από τον υπεύθυνο ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του. Ένας Υπεύθυνος προστασίας δεδομένων που λαμβάνει εγκαίρως τον μισθό του ή το τίμημα από την παροχή υπηρεσιών, που του παρέχονται οι κατ' αρ. 38 παρ 2 Κανονισμού απαραίτητοι πόροι για την άσκηση των καθηκόντων του και την διατήρηση της εμπειρογνωσίας του, που δεν απειλείται με απόλυση, ούτε απολύεται επειδή επιτέλεσε τα καθήκοντά του, αφήνεται ελεύθερος να λειτουργήσει αντικειμενικά, ανεξάρτητα και αυτόνομα. Άλλωστε ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων. Δεν απολύεται, ούτε υφίσταται κυρώσεις[46] από τον υπεύθυνο επεξεργασίας επειδή επιτέλεσε τα καθήκοντά του. «Είναι αυτονόητο ότι η ανεξαρτησία δεν είναι αυτοσκοπός[47]». Είναι συνθήκη για την ορθή ενάσκηση των καθηκόντων και προκειμένου ο ΥΠΔ να ασκεί αποτελεσματικά το καθήκον του για συμβουλευτικές παρεμβάσεις σχετικά με την συμμόρφωση προς τις διατάξεις για την προστασία δεδομένων. Ωστόσο, κάθε εγγύηση που ενισχύει τον ανεξάρτητο ρόλο του είναι θετική, εφόσον βεβαίως κατοχυρώνεται με σταθερότητα και στους κανονισμούς εσωτερικής λειτουργίας της οντότητας στην οποία θητεύει, ως όροι της σύμβασης παροχής υπηρεσιών καθώς και ως αντίληψη όλων των στελεχών με τα οποία συνεργάζεται.

[45] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 122-124.
[46] Βλ. άρ 38 παρ 3 ΓΚΠΔ.
[47] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 124.

§7.4 - *Απαγόρευση κατοχής θέσης που συνεπάγεται σύγκρουση συμφερόντων*

Οι εγγυήσεις ανεξαρτησίας του ΥΠΔ, ολοκληρώνονται με την απαγόρευση κατοχής θέσης ή ρόλου[48] που συνεπάγεται σύγκρουση συμφερόντων (άρ. 38 παρ 5 εδ. β΄ Κανονισμού), ήτοι θέσης από την οποία καθορίζεται ο σκοπός και τα μέσα επεξεργασίας των προσωπικών δεδομένων, ή ρόλου που αφορά την εκπροσώπηση της επιχείρησης ή την υπεράσπιση των επιλογών που έλαβαν χώρα από την επιχείρηση. Στην περίπτωση αυτή, το ίδιο το πρόσωπο δεν μπορεί να κατέχει ταυτόχρονα θέση «εσωτερικού ελεγκτή» και «ελεγχόμενου». Δηλαδή, σε περίπτωση διορισμού ομάδας ΥΠΔ, ενδείκνυται το νομικό προσωπικό της να μην παρέχει παράλληλα νομικές υπηρεσίες στον υπεύθυνο ή εκτελούντα την επεξεργασία, προκειμένου να μην τεθεί σε αμφισβήτηση το καθεστώς ανεξαρτησίας του ΥΠΔ.

§7.5 - *Υποχρεωτικός ορισμός*

Σύμφωνα με το άρθρο 37 παράγραφος 1 του ΓΚΠΔ, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός σε τρεις συγκεκριμένες περιπτώσεις : α) όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα. 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· ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα . Στις ακόλουθες υποενότητες, η ομάδα του άρθρου 29 παρέχει καθοδήγηση σχετικά με τα κριτήρια και την ορολογία που χρησιμοποιείται στο άρθρο 37 παράγραφος 1. Εκτός από τις περιπτώσεις όπου είναι προφανές ότι ένας οργανισμός δεν υποχρεούται να ορίσει υπεύθυνο προστασίας δεδομένων, η ομάδα του άρθρου 29 συνιστά στους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να καταγράφουν την εσωτερική ανάλυση που διενεργούν προκειμένου να προσδιορίσουν αν πρέπει ή όχι να διοριστεί υπεύθυνος προστασίας δεδομένων, ώστε να μπορούν να αποδείξουν ότι λήφθηκαν δεόντως υπόψη οι σχετικοί παράγοντες . Η εν λόγω ανάλυση αποτελεί μέρος της απαιτούμενης τεκμηρίωσης δυνάμει της αρχής της λογοδοσίας. Μπορεί να ζητηθεί από την εποπτική αρχή και θα πρέπει να επικαιροποιείται όταν κρίνεται απαραίτητο, για παράδειγμα αν οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία

[48] Λεωνίδας Κοτσαλής, Κωνσταντίνος Μενουδάκος, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων, GDPR», σελ 214.

αναλαμβάνουν νέες δραστηριότητες ή παρέχουν νέες υπηρεσίες που εμπίπτουν ενδεχομένως στις περιπτώσεις του άρθρου 37 παράγραφος 1. Όταν ένας οργανισμός ορίζει υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι απαιτήσεις των άρθρων 37 έως 39 ως εάν ο ορισμός να ήταν υποχρεωτικός. Οι οργανισμοί που δεν υποχρεούνται, βάσει της νομοθεσίας, να ορίσουν υπεύθυνο προστασίας δεδομένων και που δεν επιθυμούν να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση μπορούν κάλλιστα να απασχολούν υπαλλήλους ή εξωτερικούς συμβούλους επιφορτισμένους με καθήκοντα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Σ' αυτές τις περιπτώσεις, είναι σημαντικό να διασφαλίζεται ότι δεν υπάρχει σύγχυση ως προς τον τίτλο, το καθεστώς, τη θέση και τα καθήκοντα των εν λόγω υπαλλήλων ή συμβούλων. Θα πρέπει, επομένως, να διευκρινίζεται, τόσο στο πλαίσιο της ενδοεταιρικής επικοινωνίας, όσο και στις αρχές προστασίας δεδομένων, τα υποκείμενα των δεδομένων και το ευρύ κοινό, ότι ο εν λόγω υπάλληλος ή σύμβουλος δεν φέρει τον τίτλο του «υπευθύνου προστασίας δεδομένων». Ο ορισμός, υποχρεωτικός ή εθελοντικός, του υπευθύνου προστασίας δεδομένων γίνεται για όλες τις πράξεις επεξεργασίας που διενεργούνται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Εκτός όμως από τον Γενικό Κανονισμό Προστασίας Δεδομένων, η υποχρέωση για διορισμό ΥΠΔ περιλαμβάνεται και στο «άρθρο 32[49] της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών 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».

§7.6 - *Ενημερωτικός και συμβουλευτικός ρόλος*

Ο ΥΠΔ ενημερώνει και συμβουλεύει[50] τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων[51]. Ο υπεύθυνος επεξεργασίας

[49] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 82-84.
[50] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 136-138.
[51] Βλ άρ. 39 παρ 1 στοιχείο β' ΓΚΠΔ.

αναθέτει στον ΥΠΔ να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας και τους υπαλλήλους που διενεργούν επεξεργασία για τις υποχρεώσεις τους σύμφωνα με την παρούσα Οδηγία.

§7.7 - *Από κοινού ορισμός*

Όμιλος επιχειρήσεων ή περισσότεροι δημόσιοι φορείς, λαμβάνοντας υπόψη το μέγεθος και την οργανωτική τους δομή, μπορούν να ορίσουν έναν μόνο DPO, υπό την προϋπόθεση να είναι διαθέσιμος και εύκολα προσβάσιμος σε κάθε εγκατάσταση ή φορέα είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας και σε γλώσσα που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων.

§7.8 - *Μεγάλη κλίμακα*

Σύμφωνα με το άρθρο 37 παράγραφος 1 στοιχεία β) και γ), για να ενεργοποιηθεί η υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να διενεργείται σε μεγάλη κλίμακα. Ο ΓΚΠΔ δεν ορίζει τι συνιστά επεξεργασία μεγάλης κλίμακας. Παρόλα αυτά στην αιτιολογική σκέψη 91 παρέχονται κάποιες οδηγίες για το συγκεκριμένο θέμα . Είναι γεγονός ότι δεν είναι δυνατό να προσδιοριστεί με ακρίβεια ούτε η ποσότητα των δεδομένων που υποβάλλονται σε επεξεργασία ούτε το πλήθος των εμπλεκόμενων φυσικών προσώπων, ώστε να δοθεί ένας αριθμός που να ισχύει σε όλες τις περιπτώσεις. Δεν αποκλείεται, πάντως, να αναπτυχθεί με τον καιρό τυποποιημένη πρακτική για τον ακριβέστερο προσδιορισμό, με πιο συγκεκριμένους και/ή ποσοτικούς όρους, του τι συνιστά «μεγάλη κλίμακα» σε σχέση με ορισμένους τύπους συνήθων δραστηριοτήτων επεξεργασίας. Η ομάδα του άρθρου 29 σκοπεύει μάλιστα να συμβάλει προς την κατεύθυνση αυτή μέσω της ανταλλαγής και της δημοσιοποίησης παραδειγμάτων των κατώτατων ορίων που εφαρμόστηκαν σε διάφορες περιπτώσεις για τον ορισμό υπευθύνου προστασίας δεδομένων.

§7.9 - *Τακτική και συστηματική παρακολούθηση*

Η έννοια της τακτικής και συστηματικής παρακολούθησης των υποκειμένων των δεδομένων δεν ορίζεται μεν στον ΓΚΠΔ, όμως στην αιτιολογική σκέψη 24 αναφέρεται η έννοια της «παρακολούθησης της συμπεριφοράς των υποκειμένων των δεδομένων» στην οποία περιλαμβάνονται ξεκάθαρα όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, μεταξύ άλλων, και για σκοπούς συμπεριφορικής διαφήμισης. Η έννοια της παρακολούθησης δεν περιορίζεται, πάντως, στο επιγραμμικό περιβάλλον και η επιγραμμική παρακολούθηση θα πρέπει να θεωρείται ως ένα μόνο παράδειγμα παρακολούθησης της συμπεριφοράς των υποκειμένων των δεδομένων.

§7.10 - *Ορισμός εξωτερικού υπευθύνου προστασίας δεδομένων*

Σύμφωνα με το άρθρο 37 παράγραφος 6, ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή «να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών». Αυτό σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων, μπορεί να είναι εξωτερικός και σ' αυτή την περίπτωση τα καθήκοντα του μπορούν να ασκηθούν βάσει σύμβασης παροχής υπηρεσιών, η οποία συνάπτεται με φυσικό πρόσωπο ή οργανισμό.

Σύμφωνα με το άρθρο 37 παράγραφος 6, ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή «να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών». Αυτό σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι εξωτερικός, και σ' αυτήν την περίπτωση, τα καθήκοντά του μπορούν να ασκηθούν βάσει σύμβασης παροχής υπηρεσιών η οποία συνάπτεται με φυσικό πρόσωπο ή οργανισμό.

§8. - ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29

Η ομάδα εργασίας του άρθρου 29[52] είναι η ανεξάρτητη ευρωπαϊκή ομάδα εργασίας που χειριζόταν θέματα σχετικά με την προστασία της ιδιωτικής ζωής και των δεδομένων προσωπικού χαρακτήρα έως τις 25 Μαΐου 2018 (έναρξη ισχύος του ΓΚΠΔ). Η ομάδα εργασίας επικροτεί την πρόταση της Ευρωπαϊκής Επιτροπής, η οποία υποβλήθηκε στις 10 Ιανουαρίου 2017, σχετικά με έναν κανονισμό για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες. Η ομάδα εργασίας επικροτεί το γεγονός ότι ως κανονιστικό μέσο επελέγη ο κανονισμός. Με τον τρόπο αυτό διασφαλίζεται η ομοιομορφία των κανόνων σε ολόκληρη την ΕΕ και παρέχεται σαφήνεια για τις εποπτικές αρχές και τους οργανισμούς. Επιπλέον, διευκολύνεται η εξασφάλιση συνοχής με τον γενικό κανονισμό για την προστασία δεδομένων (ΓΚΠΔ). Η εν λόγω συνοχή υποστηρίζεται περαιτέρω με την επιλογή να διοριστεί ως αρμόδια αρχή για την επιβολή των κανόνων σχετικά με την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες η ίδια αρχή που είναι αρμόδια για την παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ. Ταυτόχρονα, είναι θετική η επιλογή (της διατήρησης) μιας συμπληρωματικής νομοθετικής πράξης. Η προστασία του απορρήτου των επικοινωνιών και του τερματικού εξοπλισμού έχει ιδιαίτερα χαρακτηριστικά τα οποία δεν εξετάζονται στον ΓΚΠΔ. Ως εκ τούτου, απαιτούνται συμπληρωματικές διατάξεις σχετικά με αυτά τα είδη υπηρεσιών, προκειμένου να διασφαλιστεί η επαρκής προστασία του θεμελιώδους δικαιώματος στην προστασία της ιδιωτικής ζωής και του απορρήτου των επικοινωνιών, συμπεριλαμβανομένου του απορρήτου του τερματικού εξοπλισμού. Εν προκειμένω, η ομάδα εργασίας τάσσεται σθεναρά υπέρ της βασισμένης σε αρχές προσέγγισης που επελέγη στην πρόταση κανονισμού και που προβλέπει ευρείες απαγορεύσεις και περιορισμένες εξαιρέσεις, καθώς και υπέρ της στοχευμένης εφαρμογής της έννοιας της συγκατάθεσης.

Η ομάδα εργασίας συνιστά ο τερματικός εξοπλισμός και το λογισμικό να παρέχουν εξ ορισμού ρυθμίσεις προστασίας της ιδιωτικής ζωής, καθώς και σαφείς επιλογές στους χρήστες για την επιβεβαίωση ή την αλλαγή των προεπιλεγμένων αυτών ρυθμίσεων κατά την εγκατάσταση. Οι ρυθμίσεις πρέπει να είναι εύκολα προσβάσιμες κατά τη χρήση. Οι χρήστες πρέπει να έχουν τη δυνατότητα να παρέχουν ειδική συγκατάθεση

[52] Βλ. Ιστοσελίδα Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, edpb.europa.eu

μέσω των ρυθμίσεων του φυλλομετρητή τους. Οι προτιμήσεις όσον αφορά την ιδιωτική ζωή δεν θα πρέπει να περιορίζονται στην παρέμβαση τρίτων ή στα cookies. Η ομάδα εργασίας συνιστά θερμά να καταστεί υποχρεωτική η τήρηση του προτύπου απαγόρευσης της παρακολούθησης (Do Not Track).

§8.1 - *Ομάδα εργασίας του άρθρου 29 και ΥΠΔ*

Η Ομάδα Εργασίας του άρθρου 29[53], στις «Κατευθυντήριες γραμμές για τους ΥΠΔ» ερμηνεύει τον όρο «τακτική παρακολούθηση»[54] ως συνεχιζόμενη παρακολούθηση ή εμφανιζόμενη σε τακτά διαστήματα για συγκεκριμένη χρονική περίοδο ή επαναλαμβανόμενη σε προκαθορισμένο χρόνο. Ως προς τον όρο «συστηματική παρακολούθηση»[55] η Ομάδα Εργασίας δέχεται ότι αυτό μπορεί να σημαίνει ότι εφαρμόζεται από ένα σύστημα ή είναι προκαθορισμένη, οργανωμένη ή εφαρμόζουσα μέθοδο ή ότι αποτελεί μέρος γενικότερου σχεδιασμού για την συλλογή δεδομένων και διεξάγεται ως μέρος μιας στρατηγικής. Ως παραδείγματα «τακτικής και συστηματικής παρακολούθησης» η Ομάδα Εργασίας αναφέρει την λειτουργία ενός τηλεπικοινωνιακού δικτύου, την παροχή τηλεπικοινωνιακών υπηρεσιών, την προώθηση διαφημιστικών μηνυμάτων ηλεκτρονικού ταχυδρομείου σε άτομα που επισκέφθηκαν ήδη έναν διαδικτυακό τόπο, γενικώς τις δραστηριότητες προώθησης προϊόντων με τη χρήση προσωπικών δεδομένων, την δημιουργία προφίλ και βαθμολόγησης για την αξιολόγηση κινδύνων.

Επίσης, ο ΥΠΔ έχει καθήκον συνεργασίας με την εποπτική αρχή[56]. Έτσι, σύμφωνα με τις «Κατευθυντήριες γραμμές για τους ΥΠΔ» η Ομάδα Εργασίας του άρθρου 29 αναφέρει ότι αυτό το καθήκον, «επιβεβαιώνει το ρόλο του ΥΠΔ ως διευκολύνοντος την προστασία δεδομένων»[57]. Ο ΥΠΔ διευκολύνει την πρόσβαση της εποπτικής Αρχής στα έγγραφα και τις πληροφορίες του οργανισμού, προκειμένου να ασκήσει τις ελεγκτικές, διορθωτικές, αδειοδοτικές και συμβουλευτικές αρμοδιότητές της. Ο ΥΠΔ δεσμεύεται από καθήκον εχεμύθεια και εμπιστευτικότητας σύμφωνα με το δίκαιο της Ένωσης και του κράτους μέλους. Ωστόσο, η υποχρέωση τήρησης του απορρήτου και

[53] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 123.
[54] Βλ. Κεφάλαιο «Υπεύθυνος Προστασίας Δεδομένων», τακτική και συστηματική παρακολούθηση.
[55] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 95-96.
[56] Βλ. άρθρο 39 παρ 1 δ ΓΚΠΔ.
[57] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 186-187.

της εμπιστευτικότητας δεν απαγορεύει στον ΥΠΔ να επικοινωνεί και να ζητά συμβουλή από την εποπτική Αρχή.

§9. - ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους. Η ΕΑΠΔ αποτελεί σημαντικό εργαλείο για την πλήρωση της υποχρέωσης λογοδοσίας, καθώς παρέχει συνδρομή στους υπεύθυνους επεξεργασίας όχι μόνον προκειμένου να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και για να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσης προς τον κανονισμό (βλ. επίσης άρθρο 24)5 . Με άλλα λόγια, η ΕΑΠΔ είναι μια διαδικασία εμπέδωσης και απόδειξης της συμμόρφωσης. Βάσει του ΓΚΠΔ, η μη συμμόρφωση με τις απαιτήσεις ΕΑΠΔ μπορεί να οδηγήσει στην επιβολή προστίμων από την αρμόδια εποπτική αρχή. Η παράλειψη διενέργειας ΕΑΠΔ σε επεξεργασία που υπόκειται σε απαίτηση διενέργειας ΕΑΠΔ (άρθρο 35 παράγραφος 1 και παράγραφοι 3-4), η διενέργεια ΕΑΠΔ με εσφαλμένο τρόπο (άρθρο 35 παράγραφος 2 και παράγραφοι 7-9) ή η μη διαβούλευση με την αρμόδια εποπτική αρχή εφόσον απαιτείται [άρθρο 36 παράγραφος 3 στοιχείο ε)] μπορούν να επιφέρουν διοικητικό πρόστιμο ύψους έως 10 εκατ. ευρώ ή, σε περίπτωση επιχείρησης, έως 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

§9.1 - *Εκτίμηση Αντικτύπου και Υπεύθυνος Επεξεργασίας*

Προκειμένου να ενισχυθεί η συμμόρφωση[58] προς τον παρόντα κανονισμό όταν οι πράξεις επεξεργασίας ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας θα πρέπει να ευθύνεται για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, ώστε να αξιολογήσει, ιδίως, την προέλευση, τη φύση, την πιθανότητα και τη σοβαρότητα του εν λόγω κινδύνου. Το αποτέλεσμα της εκτίμησης θα πρέπει να λαμβάνεται υπόψη όταν καθορίζεται ποια μέτρα ενδείκνυται να ληφθούν ώστε να αποδειχθεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύμφωνη με τον παρόντα κανονισμό. Εάν η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων υποδεικνύει ότι οι πράξεις επεξεργασίας συνεπάγονται υψηλό κίνδυνο που ο υπεύθυνος επεξεργασίας δεν μπορεί να μετριάσει με τα κατάλληλα μέτρα από άποψη διαθέσιμης τεχνολογίας και κόστους εφαρμογής, θα πρέπει να πραγματοποιείται διαβούλευση με την αρχή ελέγχου πριν από την επεξεργασία.

§9.2 - *Εκτίμηση Αντικτύπου και ΥΠΔ*

Ο ΥΠΔ έχει ως καθήκον να παρέχει συμβουλές, όταν ζητείται όσον αφορά την εκτίμηση αντικτύπου[59] σχετικά με την προστασία των δεδομένων και να παρακολουθεί την υλοποίησή της. Η Αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου. Ανακοινώνει τον εν λόγω κατάλογο στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων. Η Αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η υποχρέωση διενέργειας της εκτίμησης αντικτύπου βαρύνει βέβαια τον Υπεύθυνο Επεξεργασίας και όχι τον Υπεύθυνο Προστασίας Δεδομένων. Ωστόσο, σύμφωνα με τις «Κατευθυντήριες γραμμές για τους ΥΠΔ» της Ομάδας Εργασίας του άρθρου 29, ο ΥΠΔ μπορεί να παίξει έναν πολύ σημαντικό ρόλο συντρέχοντας τον υπεύθυνο επεξεργασίας στο θέμα αυτό.

[58] Βλ. Ιστοσελίδα, www.lawspot.gr.
[59] Βασίλης Σωτηρόπουλος, «Υπεύθυνος Προστασίας Δεδομένων», σελ 182-186.

§10. - «ΔΗΜΟΣΙΑ ΑΡΧΗ Η΄ ΔΗΜΟΣΙΟΣ ΦΟΡΕΑΣ» ΣΤΟΝ ΓΚΠΔ

Αρχικά να τονισθεί ότι, κάθε δημόσια διοίκηση[60] υπόκειται στους κανόνες του ΓΚΠΔ όταν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που αφορούν φυσικό πρόσωπο. Ο ΓΚΠΔ δεν ορίζει τι συνιστά «δημόσια αρχή ή δημόσιο φορέα». Το σχέδιο του ελληνικού εφαρμοστικού νόμου του Γενικού Κανονισμού Προστασίας Δεδομένων αναφέρει για τον «δημόσιο φορέα»: «*οι κρατικές ή δημόσιες αρχές, κεντρικές και περιφερειακές, αυτοτελείς δημόσιες υπηρεσίες, νομικά πρόσωπα δημοσίου δικαίου, ανεξάρτητες και ρυθμιστικές διοικητικές αρχές, οι κρατικές ή δημόσιες επιχειρήσεις και οργανισμοί, τα νομικά πρόσωπα ιδιωτικού δικαίου που ανήκουν στο κράτος ή επιχορηγούνται από κατά 50% τουλάχιστον του ετήσιου προϋπολογισμού τους ή η διοίκησή τους ορίζεται από αυτό, οι οργανισμοί τοπικής αυτοδιοίκησης πρώτου και δευτέρου βαθμού και τα νομικά πρόσωπα και επιχειρήσεις αυτών*». Εν ολίγοις, αναγνωρίζεται ότι ως δημόσιοι φορείς μπορεί να είναι και οι φορείς που τυπικά ανήκουν στον ιδιωτικό τομέα, αλλά ασκούν δημόσιες αρμοδιότητες.

Σύμφωνα με την οργανική θεωρία[61] στην έννοια της διοικητικής αρχής εντάσσεται κάθε όργανο της δημόσιας αρχής, άμεσο ή έμμεσο ατομικό ή συλλογικό. Επιπλέον, του έχει ανατεθεί η άσκηση διοικητικής εξουσίας και αρμοδιοτήτων κατά το νόμο για την έκδοση εκτελεστών πράξεων. Η ικανότητα έκδοσης «εκτελεστών» διοικητικών πράξεων αποτελεί, αυτόχρημα, εννοιολογικό στοιχείο της οργανικής έννοιας της διοικητικής αρχής, αλλά και κάθε νομικού προσώπου δημοσίου δικαίου, όπως είναι οι οργανισμοί τοπικής αυτοδιοίκησης αφενός και τα διακεκριμένα νομικά πρόσωπα, που ασκούν διοίκηση αφετέρου ή αυτοτελείς υπηρεσίες ενός απ' αυτά που παρουσιάζουν τα ως άνω χαρακτηριστικά. Για τον προσδιορισμό της έννοιας δεν λαμβάνεται υπόψιν η νομική φύση των δραστηριοτήτων του οργάνου, αλλά η νομική οργανωτική μορφή του οργάνου που τις εκδίδει. Αρκεί ο φορέας που εξέδωσε τις πράξεις να είναι διοικητικό όργανο.

Συνεπώς, η έννοια της αρχής αναφέρεται στην οργανωτική έννοια της Διοίκησης. Με την έννοια ότι η Διοίκηση αποτελείται από ένα σύνολο διοικητικών αρχών και

[60] Βλ. Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα «Προετοιμασία και Υποχρεώσεις Δημοσίων Αρχών».
[61] Ανδρομάχη Μαρκαντωνάτου – Σκαλτσά, «Δημόσια Διοίκηση και Συλλογικά Όργανα», σελ 34-36

υπηρεσιών που ανήκουν στην εκτελεστική εξουσία, και το Κράτος ασκεί τις διοικητικές του λειτουργίες μέσω των αρχών αυτών, π.χ. υπουργεία, ή μέσω των αρχών που είναι ενταγμένες σε αυτοτελείς νομικές ενότητες. Τα συλλογικά όργανα της πολιτείας, μπορεί να είναι γνωμοδοτικά και δεν αποτελούν στην κυριολεξία «διοικητικές αρχές», όταν αναφερόμαστε στα οργανικά πλαίσια των κρατικών υπηρεσιών.

Κατά τη νομολογία ως δημόσια αρχή νοείται, όχι μόνο κάθε εγκεκριμένη κρατική υπηρεσία της δημόσιας διοίκησης, που έχει οργανική ενότητα και αυτοτελή κύκλο αρμοδιοτήτων, αλλά και κάθε νομικό πρόσωπο δημοσίου δικαίου, όπως είναι π.χ., ο οργανισμός τοπικής αυτοδιοίκησης αφενός και τα διακεκριμένα καθ' ύλην νομικά πρόσωπα που ασκούν διοίκηση αφετέρου.

Επίσης, το ευρωπαϊκό δίκαιο θεωρεί ως «δημόσιες αρχές» τα πρόσωπα ή τους φορείς του δημοσίου δικαίου, όσο και τα τα πρόσωπα ή τους φορείς του ιδιωτικού δικαίου. Η ιδιότητα του δημοσίου ή του ιδιωτικού ενός φορέα ή ενός προσώπου δεν είναι καθοριστική. Αυτό που ενδιαφέρει[62] είναι η φύση των εξουσιών που ασκεί.

Η Ομάδα Εργασίας του άρθρου 29, αναφέρει τις περιπτώσεις των δημοσίων μεταφορών, της παροχής ενέργειας και νερού, τις οδικές υποδομές, την δημόσια υπηρεσία ραδιοτηλεοπτικών μεταδόσεων, τις υπηρεσίες δημόσιας στέγασης και τα πειθαρχικά όργανα για ρυθμισμένα επαγγέλματα. Επίσης να αναφερθεί ότι, απαιτείται να καταγραφούν πλήρως και επακριβώς οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα, που τυγχάνουν επεξεργασίας (συλλογή, καταχώριση, φύλαξη, διαβίβαση, κλπ.), από κάθε φορέα του δημοσίου τομέα, είτε υπέχει θέση υπευθύνου επεξεργασίας είτε εκτελούντος την επεξεργασία, καθώς επίσης τα συστήματα αρχειοθέτησης δεδομένων προσωπικού χαρακτήρα, τα οποία έχει συστήσει και τηρεί στο πλαίσιο της εκπλήρωσης της αποστολής του, σύμφωνα με τα οριζόμενα ιδίως στο άρθρο 30 ΓΚΠΔ. Και τούτο, ανεξάρτητα από κάθε υποβολή γνωστοποίησης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία έχει ήδη διενεργηθεί στο πλαίσιο του ακόμη ισχύοντος του Ν. 2472/1997. Οι κατηγορίες δεδομένων προσωπικού χαρακτήρα και τα συστήματα αρχειοθέτησης αφορούν όλες τις κατηγορίες ενδιαφερομένων υποκειμένων (φυσικών προσώπων). Η ομάδα του άρθρου 29 εκτιμά ότι η έννοια αυτή πρέπει να προσδιορίζεται από τα εθνικά δίκαια. Συνεπώς, δημόσιες αρχές και δημόσιοι

[62] Ανδρομάχη Μαρκαντωνάτου – Σκαλτσά, «Δημόσια Διοίκηση και Συλλογικά Όργανα», σελ 36

φορείς είναι μεν, μεταξύ άλλων, οι εθνικές, περιφερειακές και τοπικές αρχές, όμως στη συγκεκριμένη έννοια, δυνάμει των ισχυουσών διατάξεων των εθνικών δικαίων, περιλαμβάνονται κατά κανόνα και διάφοροι άλλοι φορείς δημοσίου δικαίου. Σ' αυτές τις περιπτώσεις, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός.

§ 10.1 – *Τα βήματα προετοιμασίας μιας Δημόσιας Αρχής ή Δημοσίου Φορέα για την εφαρμογή του ΓΚΠΔ*[63]

- Απαιτείται να καταγραφούν πλήρως και επακριβώς οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα, που τυγχάνουν επεξεργασίας (συλλογή, καταχώριση, φύλαξη, διαβίβαση, κλπ.), από κάθε φορέα του δημοσίου τομέα.

- Με βάση τα πορίσματα της προαναφερόμενης καταγραφής, απαιτείται να καταγραφούν οι ενέργειες που απαιτούνται, προκειμένου κάθε φορέας του δημοσίου τομέα, είτε ως υπεύθυνος επεξεργασίας είτε ως εκτελών την επεξεργασία, να συμμορφωθεί πλήρως προς το σύνολο των υποχρεώσεων, που απορρέουν από τις διατάξεις του ΓΚΠΔ, προκειμένου να διασφαλιστεί ο σεβασμός κάθε ενδιαφερομένου υποκειμένου δεδομένων προσωπικού χαρακτήρα, είτε πρόκειται για εργαζόμενο (με οποιαδήποτε εργασιακή σχέση) του φορέα, είτε για διοικούμενο.

- Εφόσον διαπιστωθεί η διενέργεια επεξεργασιών, από τις οποίες ενδέχεται να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τα οριζόμενα στο άρθρο 35 ΓΚΠΔ.

- Απαιτείται να σχεδιασθούν και να τεθούν σε λειτουργία διαδικασίες, οι οποίες να αποσκοπούν στη διασφάλιση ενός υψηλού επιπέδου προστασίας δεδομένων προσωπικού χαρακτήρα, σύμφωνα με τις γενικές αρχές του ΓΚΠΔ (άρθρο 25)

[63] Βλ. Ιστοσελίδα Εθνικού Κέντρου Δημόσιας Διοίκησης και Αυτοδιοίκησης, «Γενικός Κανονισμός Προστασίας Δεδομένων: Το νέο τοπίο και οι υποχρεώσεις της δημόσιας διοίκησης», www.ekdd.gr/images/seminaria/GDPR.pdf

- Απαιτείται, σύμφωνα με τα οριζόμενα ιδίως στα άρθρα 37 και 38 ΓΚΠΔ, όπως προαναφέρθηκε, να οριστεί σε κάθε δημόσιο φορέα, είτε υπέχει θέση υπευθύνου επεξεργασίας είτε εκτελούντος την επεξεργασία, Υπεύθυνος Προστασίας Δεδομένων, ο οποίος θα αναλάβει την άσκηση των καθηκόντων, που προβλέπονται στο άρθρο 39 ΓΚΔΠ και σε κάθε άλλη ρύθμιση σχετική με την προστασία δεδομένων προσωπικού χαρακτήρα. Ο DPO θα πρέπει ιδίως : α) να ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους εργαζόμενους, που διενεργούν επεξεργασίες, για τις υποχρεώσεις τους, που απορρέουν από το ΓΚΠΔ και από άλλες διατάξεις της ΕΕ εθνικές ρυθμίσεις σχετικά με την προστασία δεδομένων, β) να παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και να παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35 ΓΚΠΔ, γ) να συνεργάζεται με την εποπτική αρχή και να ενεργεί ως σημείο επικοινωνίας με την εποπτική αρχή και τα υποκείμενα των δεδομένων για όλα τα ζητήματα που σχετίζονται με την επεξεργασία.

§10.2 - *Δημόσια Αρχή ή Δημόσιος Φορέας κατά την Ομάδα Εργασίας του άρθρου 29*

Η Ομάδα Εργασίας του άρθρου 29 παραπέμπει επίσης στην έννοια των δημόσιων φορέων των άρθρων 2 παρ 1 και 2 της Οδηγίας 2003/98/ΕΚ για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα. Η εν λόγω Οδηγία[64] για να ορίσει την έννοια των φορέων του δημοσίου τομέα, όπως αυτό ορίζεται και από άλλες πηγές κοινοτικού δικαίου, ακολουθεί το «λειτουργικό» κριτήριο. Ο ορισμός που δίνει το άρθρο 4 παρ 1 και 2 του Ν. 3448/2006 με τον οποίο ενσωματώθηκε η ανωτέρω Οδηγία 2003/98/ΕΚ στο εσωτερικό δίκαιο είναι ο εξής: «φορείς του δημοσίου τομέα, νοούνται οι κρατικές αρχές, κεντρικές και περιφερειακές, οι ανεξάρτητες διοικητικές αρχές, οι Ο.Τ.Α πρώτου και δεύτερου βαθμού, τα λοιπά Ν.Π.Δ.Δ., οι οργανισμοί δημόσιου δικαίου και οι ενώσεις που σχηματίζονται από μία ή περισσότερες από τις αρχές ή από έναν ή

[64] Βασίλης Σωτηρόπουλος «Υπεύθυνος Προστασίας Δεδομένων», σελ 88.

περισσότερους από τους οργανισμούς δημοσίου δικαίου». «Ως οργανισμοί δημοσίου δικαίου, νοούνται εκείνοι που α) έχουν συσταθεί με συγκεκριμένο σκοπό την κάλυψη αναγκών γενικού συμφέροντος που δεν έχουν βιομηχανικό ή εμπορικό χαρακτήρα, β) έχουν νομική προσωπικότητα και γ) χρηματοδοτούνται για τη δραστηριότητά τους κατά κύριο λόγο από το Κράτος, τους Ο.Τ.Α. ή άλλους οργανισμούς δημοσίου δικαίου, είτε η διαχείρισή τους υπόκειται στην εποπτεία των ανωτέρω είτε διοικούνται, διευθύνονται ή εποπτεύονται από όργανο του οποίου ο μεγαλύτερος αριθμός των μελών διορίζεται από το Κράτος, τους Ο.Τ.Α ή άλλους οργανισμούς δημοσίου δικαίου».

§10.3 - *Δημόσια Αρχή ή Δημόσιος Φορέας και ΥΠΔ*

Η διάταξη του Γενικού Κανονισμού δεν διευκρινίζει ποιες «δημόσιες αρχές ή φορείς» οφείλουν να ορίσουν ΥΠΔ. Εξαιρεί τα δικαστήρια[65] κατά την ενάσκηση των δικαιοδοτικών τους αρμοδιοτήτων, αφήνοντας έτσι να εννοηθεί όμως ότι για την αρχειακή λειτουργία τους, οι Γραμματείες των Δικαστηρίων οφείλουν να ορίσουν ΥΠΔ, διότι η αρχειοθέτηση δεν εντάσσεται στην δικαιοδοτική αρμοδιότητα, αλλά στην διοικητική. Επίσης, σύμφωνα με τις διατάξεις της Οδηγίας 680/2016/ΕΕ, ΥΠΔ οφείλουν να ορίζουν οι αρχές που εφαρμόζουν την αντεγκληματική πολιτική: οι εισαγγελικές αρχές, οι αστυνομικές αρχές, οι λιμενικές αρχές. Δηλαδή ως προς αυτές τις δημόσιες αρχές είναι ξεκάθαρο ότι οφείλουν όλες να ορίσουν ΥΠΔ.

Το κατά πόσον σε κάθε Υπουργείο μπορεί να χρειάζονται και άλλοι ΥΠΔ είναι ζήτημα ανάλυσης των αρμοδιοτήτων ώστε να εντοπιστεί κατά πόσον υπάρχουν και άλλοι υπεύθυνοι επεξεργασίας. Άλλωστε το ερώτημα περί του εάν η υποχρέωση αφορά κάθε τμήμα ή κάθε διεύθυνση ή κάθε άλλη μονάδα του οργανισμού εσωτερικής υπηρεσίας, απαντάται από τον ορισμό του «υπευθύνου επεξεργασίας». Δεν παίζει κανένα ρόλο το «οργανικό κριτήριο» για τον καθορισμό του υπεύθυνου επεξεργασίας, διότι με την λογική του ότι όλο το Ελληνικό Δημόσιο αποτελεί ένα νομικό πρόσωπο, τότε θα αρκούσε ένας ΥΠΔ για όλα τα Υπουργεία. Η υποχρέωση όμως ορισμού αφορά κάθε «δημόσια αρχή». Δηλαδή κάθε Υπουργείο μπορεί να εντάσσεται στο νομικό πρόσωπο του Ελληνικού Δημοσίου, κάθε Υπουργείο όμως αποτελεί μια δημόσια αρχή. Ένας

[65] Βασίλης Σωτηρόπουλος «Υπεύθυνος Προστασίας Δεδομένων», σελ 85-88.

ΥΠΔ θα πρέπει για τον ίδιο λόγο να ορίζεται σε κάθε νομικό πρόσωπο δημοσίου δικαίου.

Η εκπλήρωση δημόσιου καθήκοντος και η άσκηση δημόσιας εξουσίας είναι δυνατή όχι μόνο από δημόσιες αρχές ή δημόσιους φορείς, αλλά και από άλλα φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου, σε διάφορους τομείς που απορρέουν από τους εθνικούς κανονισμούς κάθε κράτους μέλους, όπως οι υπηρεσίες δημόσιων μεταφορών, η ύδρευση και η παροχή ενέργειας, οι οδικές υποδομές, η δημόσια ραδιοτηλεόραση, η κατασκευή εργατικών κατοικιών, ή πειθαρχικά όργανα για νομοθετικά κατοχυρωμένα επαγγέλματα. Στις περιπτώσεις αυτές, τα υποκείμενα των δεδομένων είναι πιθανό να βρεθούν σε θέση που ομοιάζει πολύ με την επεξεργασία των δεδομένων τους από δημόσια αρχή ή δημόσιο φορέα. Συγκεκριμένα, είναι δυνατή η επεξεργασία δεδομένων για παρόμοιους σκοπούς και, ομοίως, τα φυσικά πρόσωπα έχουν συνήθως ελάχιστη ή καμία δυνατότητα επιλογής ως προς το εάν και το πώς θα υποβληθούν σε επεξεργασία τα δεδομένα τους. Είναι πιθανό, επομένως, να απαιτείται η πρόσθετη προστασία που παρέχει ο ορισμός υπευθύνου προστασίας δεδομένων. Μολονότι δεν προβλέπεται σχετική υποχρέωση σε τέτοιες περιπτώσεις, η ομάδα του άρθρου 29 συνιστά, ως ορθή πρακτική, στους οργανισμούς ιδιωτικού δικαίου που εκπληρώνουν δημόσια καθήκοντα ή ασκούν δημόσια εξουσία να ορίζουν υπεύθυνο προστασίας δεδομένων. Πιο συγκεκριμένα, απαιτείται, σύμφωνα με τα οριζόμενα ιδίως στα άρθρα 37 και 38 ΓΚΠΔ, να οριστεί σε κάθε δημόσιο φορέα, όπως προαναφέρθηκε, είτε υπέχει θέση υπευθύνου επεξεργασίας είτε εκτελούντος την επεξεργασία, Υπεύθυνος Προστασίας Δεδομένων[66], (*Data Protection Officer – DPO*), ο οποίος θα αναλάβει την άσκηση των καθηκόντων, που προβλέπονται στο άρθρο 39 ΓΚΔΠ και σε κάθε άλλη ρύθμιση σχετική με την προστασία δεδομένων προσωπικού χαρακτήρα. Η δραστηριότητα του εν λόγω υπευθύνου προστασίας δεδομένων καλύπτει όλες τις πράξεις επεξεργασίας που διενεργούνται, περιλαμβανομένων εκείνων που δεν σχετίζονται με την εκπλήρωση δημόσιου καθήκοντος ή την άσκηση επίσημης αρμοδιότητας (π.χ., τη διαχείριση βάσης δεδομένων υπαλλήλων).

[66] Βλ. Ιστοσελίδα Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης, «Εφαρμογή του Κανονισμού GDPR στον δημόσιο τομέα».

§10.4 *–Δημόσια Υγεία και ΓΚΠΔ*

Το Υπουργείο υγείας[67], στο πλαίσιο της προσπάθειας για τη συντονισμένη οργάνωση και προετοιμασία του συνόλου των εποπτευόμενων φορέων καθώς επίσης και των ιδιωτικών φορέων παροχής υπηρεσιών υγείας, σχετικά με την ανάγκη συμμόρφωσης σε σχέση με τα οριζόμενα στον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, προέβη, ως πρώτο βήμα, στον ορισμό Υπευθύνου Προστασίας Δεδομένων (DPO), σύμφωνα με τα οριζόμενα στις διατάξεις των άρθρων 37-39 του ΓΚΠΔ. Ο Υπεύθυνος Προστασίας Δεδομένων του Υπουργείου Υγείας θα αναλάβει και το έργο της συνδρομής και του συντονισμού των Υπευθύνων Προστασίας Δεδομένων, τους οποίος θα ορίσουν οι εποπτευόμενοι φορείς, όσον αφορά τις απαιτήσεις γενικής συμμόρφωσης προς τις διατάξεις του ΓΚΠΔ.

Ως δεύτερο βήμα, το Υπουργείο Υγείας προέβη στη σύνταξη σχετικής εγκυκλίου για την ενίσχυση των δράσεων συμμόρφωσης ως προς το ΓΚΠΔ, με περιεχόμενο:

- Τη συνοπτική παρουσίαση του ΓΚΠΔ και των θεμελιωδών αρχών του.
- Τις βασικές απαιτήσεις προετοιμασίας και εφαρμογής από την πλευρά των φορέων και παρόχων υπηρεσιών υγείας (δημόσιων και ιδιωτικών).
- Το πλαίσιο ανάθεσης καθηκόντων των Υπευθύνων Προσωπικών Δεδομένων (ΥΠΔ) και των αναπληρωτών τους καθώς επίσης και την οργάνωση διαδικασίας εσωτερικής πρόσκλησης εκδήλωσης ενδιαφέροντος από στελέχη των ιδίων των φορέων ή της διαδικασίας ανοικτών δημόσιων διαγωνισμών για την πλήρωση των θέσεων.
- Επιλογή από συνήθη ερωτήματα και προβληματισμούς, που έχουν ήδη τεθεί προς τον Υπεύθυνο Προστασίας Δεδομένων του Υπουργείου Υγείας από το διοικητικό και ιατρονοσηλευτικό προσωπικό σε σχέση με τις υποχρεώσεις των φορέων και τα δικαιώματα των ασθενών.
- Τη διαδικασία διενέργειας των απαιτούμενων Μελετών Αντικτύπου

[67] Βλ. Ιστοσελίδα Υπουργείου υγείας για GDPR, www.moh.gov.gr/articles/gdpr.

Στο πλαίσιο αυτό, η εγκύκλιος σαφώς δεν περιορίζεται μόνο στην περίπτωση των δημόσιων φορέων, αλλά δύναται να αποτελέσει και μια προσπάθεια παροχής βασικών οδηγιών σχετικά με τη συμμόρφωση προς το ΓΚΠΔ και των ιδιωτών παρόχων υπηρεσιών υγείας, στη λογική της εθνικής προετοιμασίας του τομέα της υγείας και της ενδυνάμωσης της προστασίας των πολιτών έναντι της επεξεργασίας δεδομένων τους προσωπικού χαρακτήρα. Το Υπουργείο Υγείας σχεδιάζει και υλοποιεί τη στρατηγική του με γνώμονα την προστασία των δεδομένων (ευαίσθητων και μη) προσωπικού χαρακτήρα, την απλοποίηση των διαδικασιών και τη μείωση της γραφειοκρατικής ταλαιπωρίας των πολιτών, τη λειτουργική εκπαίδευση των επαγγελματιών υγείας και την συντονισμένη ενδυνάμωση των εμπλεκομένων φορέων και παρόχων υπηρεσιών υγείας, με σκοπό τη συνολικότερη αναβάθμιση της ποιότητας των παρεχόμενων υπηρεσιών.

Οι πλέον ενδεδειγμένες νομικές βάσεις[68] για την επεξεργασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία είναι: (α) η παροχή ιατρικών υπηρεσιών κατά το άρθρο 9 παρ. 2 στοιχ. (η΄) του ΓΚΠΔ, είτε η εν λόγω παροχή ιατρικών υπηρεσιών στηρίζεται ειδικότερα σε νομικές ρυθμίσεις για την παροχή υπηρεσιών υγείας από φορείς του Δημοσίου τομέα είτε σε σύμβαση παροχής ιατρικών υπηρεσιών από φορέα του ιδιωτικού τομέα, (β) η εκπλήρωση δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας κατά το άρθρο 9 παρ. 2 στοιχ. (θ΄) του ΓΚΠΔ, (γ) η ανάγκη εκτέλεσης των υποχρεώσεων και άσκησης συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, (δ) η θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα κατά το άρθρο 9 παρ. 2 στοιχ. (στ΄) του ΓΚΠΔ, (ε) η ανάγκη εκπλήρωσης σκοπών αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπών επιστημονικής ή ιστορικής έρευνας ή στατιστικών σκοπών σύμφωνα με το άρθρο 89 παρ.1 του ΓΚΠΔ βάσει του δικαίου της 25 Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη

[68] Βλ. Ιστοσελίδα, Υπουργείο Υγείας, Οδηγός προετοιμασίας για τη συμμόρφωση προς το ΓΚΠΔ, www.ispatras.gr

διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Η συγκατάθεση του υποκειμένου είναι απαραίτητη νομική βάση για τη σύννομη επεξεργασία δεδομένων του προσωπικού χαρακτήρα στον τομέα της υγείας μόνο όταν αυτή απαιτείται ρητά από διάταξη νόμου, πχ. για τη συμμετοχή σε δραστηριότητες επιστημονικής έρευνας στο πλαίσιο κλινικών δοκιμών (Πρβλ. αιτιολογική σκέψη 161 του ΓΚΠΔ). Στις περιπτώσεις όπου απαιτείται ρητά η συγκατάθεση του υποκειμένου για την επεξεργασία ευαίσθητων δεδομένων του προσωπικού χαρακτήρα, αυτή πρέπει επιπλέον να είναι έγγραφη. Συνεπώς, δεν επιτρέπεται η άρνηση παροχής υπηρεσιών υγείας με το επιχείρημα ότι το υποκείμενο των δεδομένων αρνήθηκε να παράσχει τη συγκατάθεσή του για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, καθόσον η νομική βάση για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα είναι καταρχήν η παροχή ιατρικών υπηρεσιών κατά το άρθρο 9 παρ. 2 στοιχ. (η΄) του ΓΚΠΔ. Δεν πρέπει να συγχέεται η υποχρέωση έγγραφης ενημέρωσης των υποκειμένων (άρθρα 12-14 ΓΚΠΔ) με τη λήψη συγκατάθεσης για την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα.

§10.5 – *Εθνική Τράπεζα της Ελλάδος και GDPR*[69]

Ένα από τα σημαντικότερα στοιχεία για την προστασία των προσωπικών δεδομένων σε ηλεκτρονικές πλατφόρμες είναι αυτό των cookies. Cookies[70] Η Τράπεζα μπορεί να συγκεντρώνει στοιχεία αναγνώρισης των επισκεπτών /χρηστών του δικτυακού της τόπου χρησιμοποιώντας αντίστοιχες τεχνολογίες, όπως cookies ή /και την παρακολούθηση διευθύνσεων Πρωτοκόλλου Internet (IP). Τα cookies είναι μικρά αρχεία κειμένου που αποθηκεύονται στο σκληρό δίσκο κάθε επισκέπτη /χρήστη και δεν λαμβάνουν γνώση οποιουδήποτε εγγράφου ή αρχείου από τον υπολογιστή του. Χρησιμοποιούνται για τη διευκόλυνση πρόσβασης του επισκέπτη /χρήστη όσον αφορά στη χρησιμοποίηση συγκεκριμένων υπηρεσιών ή /και σελίδων του δικτυακού τόπου, για στατιστικούς λόγους και προκειμένου να καθορίζονται οι περιοχές οι οποίες είναι

[69] Στην συγκεκριμένη υποενότητα δεν θα επιχειρήσουμε να αναλύσουμε κάτι που έχει ήδη ειπωθεί αναφορικά με τους δημόσιους φορείς, αλλά θα επισημάνουμε κάτι διαφορετικό.

[70] Τα **cookies** είναι μικρά αρχεία κειμένου τα οποία αποθηκεύονται στον φυλλομετρητή μας κατά την πλοήγησή μας στο διαδύκτιο Σκοπός τους είναι να ειδοποιούν τον ιστότοπο που επισκέπτεται ο χρήστης, για την προηγούμενη δραστηριότητά του.[1] Συνήθως περιγράφουν στοιχεία μας όπως όνομα χρήστη (user name) και συνθηματικό πρόσβασης (password) με σκοπό κατά την επίσκεψή μας στον ίδιο ιστότοπο αργότερα, να μας "θυμάται" και να μην χρειάζεται να κάνουμε σύνδεση.

χρήσιμες ή δημοφιλείς, καθώς και για να εκτιμάται η αποτελεσματικότητα της ιστοσελίδας και να βελτιωθούν οι επιδόσεις του δικτυακού τόπου. Τα στοιχεία αυτά μπορεί να περιλαμβάνουν επίσης τον τύπο του φυλλομετρητή (browser) που χρησιμοποιεί ο επισκέπτης /χρήστης, το είδος του υπολογιστή, το λειτουργικό του σύστημα, τους παροχείς διαδικτυακών υπηρεσιών και λοιπές πληροφορίες τέτοιου είδους. Επιπλέον, το πληροφοριακό σύστημα του δικτυακού τόπου συλλέγει αυτόματα πληροφορίες σχετικά με τις τοποθεσίες που επισκέπτεται ο επισκέπτης /χρήστης και σχετικά με τους συνδέσμους σε ιστοχώρους τρίτων που ενδέχεται να επιλέξει μέσω της χρήσης του δικτυακού τόπου της Τράπεζας[71]. Ο επισκέπτης /χρήστης του δικτυακού τόπου μπορεί να ρυθμίσει το πρόγραμμα του για πλοήγηση στο Διαδίκτυο (web browser) κατά τέτοιο τρόπο ώστε είτε να τον προειδοποιεί για τη χρήση των cookies σε συγκεκριμένες υπηρεσίες είτε να μην επιτρέπει την αποδοχή της χρήσης cookies σε καμία περίπτωση. Για το σκοπό αυτό μπορεί να ανατρέξει στις οδηγίες του φυλλομετρητή δικτύου του ή στην οθόνη βοήθειας για να πληροφορηθεί περισσότερα σχετικά με αυτές τις λειτουργίες. Για παράδειγμα, στον Internet Explorer, μπορεί να μεταβεί στο Tools /Internet Options /Security and Privacy για να προσαρμόσει το φυλλομετρητή στις απαιτήσεις του.

§10.6 - *Εποπτική αρχή*

«Κάθε κράτος μέλος διασφαλίζει ότι μία ή περισσότερες ανεξάρτητες δημόσιες αρχές επιφορτίζονται[72] με την παρακολούθηση της εφαρμογής του παρόντος κανονισμού, με σκοπό την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας που τα αφορούν και τη διευκόλυνση της ελεύθερης κυκλοφορίας δεδομένων προσωπικού χαρακτήρα στην Ένωση». Κάθε εποπτική αρχή συμβάλλει στη συνεκτική εφαρμογή του παρόντος κανονισμού σε ολόκληρη την Ένωση. Για τον σκοπό αυτόν, οι εποπτικές αρχές συνεργάζονται μεταξύ τους και με την Επιτροπή. Άλλωστε η σύσταση εποπτικών αρχών στα κράτη μέλη, εξουσιοδοτημένων να εκτελούν τα καθήκοντά τους και να ασκούν τις εξουσίες τους με

[71] Βλ. Ιστοσελίδα, www.nbg.gr
[72] Βλ. άρ 51 ΓΚΠΔ.

πλήρη ανεξαρτησία, είναι ουσιώδης συνιστώσα της προστασίας των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων τους προσωπικού χαρακτήρα. Τα κράτη μέλη θα πρέπει να μπορούν να συστήσουν περισσότερες εποπτικές αρχές, ανάλογα με τη συνταγματική, οργανωτική και διοικητική δομή τους.

§11. - Η ΙΔΙΑΙΤΕΡΟΤΗΤΑ ΤΟΥ ΓΚΠΔ ΣΤΟΝ ΔΗΜΟΣΙΟ ΤΟΜΕΑ

§11.1 - *Διευκόλυνση ελέγχων*

Ο ΓΚΠΔ διευκολύνει τους ελέγχους[73]. Οι δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας δε θεωρούνται ως αποδεκτές (αρθ 4 παρ 9). Συνεπώς, δε τίθεται θέμα στο να λαμβάνουν αιτιολογημένα και περιορισμένα δεδομένα που είναι απαραίτητα για τις ελεγκτικές τους δραστηριότητες. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις εν λόγω δημόσιες αρχές θα πρέπει πάντα να συμμορφώνεται προς τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.

§11.2 - *Ιδιαιτερότητα στη Νομική βάση*

Ο ΓΚΠΔ παρουσιάζει ιδιαιτερότητα στο Δημόσιο Τομέα στη Νομική του βάση. Συγκεκριμένα, η συγκατάθεση στο Δημόσιο Τομέα είναι μειωμένης σημασίας σε σχέση με τον ιδιωτικό τομέα. Το Δημόσιο μπορεί/πρέπει να κάνει χρήση της διάταξης του αρθ 6 παρ 2 εδ ε΄ «η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Όμως, το δημόσιο, δεν μπορεί κατά κανόνα να κάνει χρήση της διάταξης αρθ 6 παρ 2 εδ στ΄ που αφορά το έννομο συμφέρον: η επεξεργασία των προσωπικών δεδομένων είναι απαραίτητη για τους σκοπούς των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος.

[73] Βλ. εκδδα, καινότομο εργαστήριο «Γενικός Κανονισμός Προστασίας Δεδομένων, το νέο τοπίο και οι υποχρεώσεις της Δημόσιας Διοίκησης», www.ekdd.gr

Τηρουμένων των αρμοδιοτήτων και εξουσιών των Δημοσίων Αρχών όπως ενδεχομένως απονέμονται από το Σύνταγμα της Ελλάδας, τις εθνικές, εναρμονιστικές, κυρωτικές νομοθεσίες, τις πρωτογενείς και τις συναφείς δευτερογενείς νομοθεσίες και την αποστολή τους οι Δημόσιες Αρχές προβαίνουν σε συλλογή και επεξεργασία (σε ηλεκτρονική και έντυπη μορφή) και διατήρηση συστημάτων αρχειοθέτησης (αρχεία) προσωπικών δεδομένων ήτοι των διοικούμενων, πολιτών, υπαλλήλων τους, αιτητών κ.α. Η νομική βάση και /ή νομιμότητα των επεξεργασιών που εκτελούν Δημόσιες Αρχές θα πρέπει να αναζητείται κυρίως στα στοιχεία (γ) ή (ε) της παρ.1 του άρθρου 6 του Κανονισμού.

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις: α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς, β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης, γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Ο σκοπός της επεξεργασίας καθορίζεται στην εν λόγω νομική βάση ή, όσον αφορά την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχείο ε), είναι η αναγκαιότητα της επεξεργασίας για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Η εν λόγω νομική βάση μπορεί να περιλαμβάνει ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού, μεταξύ άλλων: τις γενικές προϋποθέσεις που διέπουν τη σύννομη επεξεργασία από τον

υπεύθυνο επεξεργασίας, τα είδη των δεδομένων που υποβάλλονται σε επεξεργασία, τα οικεία υποκείμενα των δεδομένων, τις οντότητες στις οποίες μπορούν να κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα και τους σκοπούς αυτής της κοινοποίησης, τον περιορισμό του σκοπού· τις περιόδους αποθήκευσης και τις πράξεις επεξεργασίας και τις διαδικασίες επεξεργασίας, συμπεριλαμβανομένων των μέτρων για τη διασφάλιση σύννομης και θεμιτής επεξεργασίας.

§11.3 - *Ικανοποίηση των δικαιωμάτων των υποκειμένων*

- Κάθε Δημόσια Αρχή υπέχει υποχρέωση να ενημερώσει το προσωπικό και να καθιερώσει μηχανισμούς, να οργανώσει κατάλληλα την υπηρεσία με την απονομή ρόλων ώστε να διευκολύνεται η άσκηση των δικαιωμάτων των διοικούμενων τα οποία απορρέουν από τον Κανονισμό π.χ δικαίωμα ενημέρωσης, πρόσβασης κ.λπ αλλά και να επιτευχθεί σε κάθε περίπτωση η συμμόρφωση με τον Κανονισμό σε κάθε επίπεδο εντός της Δημόσιας Αρχής. Μια δημόσια διοίκηση[74] πρέπει να απαντά στα αιτήματα που υποβάλλονται από φυσικά πρόσωπα χωρίς αδικαιολόγητη καθυστέρηση και καταρχήν εντός ενός μηνός από τη λήψη του αιτήματος. Έχει το δικαίωμα να τους ζητήσει περαιτέρω πληροφορίες για να επαληθεύσει την ταυτότητα του προσώπου που υποβάλλει το αίτημα. Σε περίπτωση απόρριψης του αιτήματος, είναι υποχρεωτικό να ενημερώνεται το άτομο σχετικά με τους λόγους και σχετικά με το δικαίωμά του να υποβάλει καταγγελία ενώπιον της ΑΠΔ και να επιδιώξει έννομη προστασία. Απαιτείται να σχεδιαστούν και να τεθούν σε λειτουργία συστήματα διαχείρισης πληροφοριών και διαδικασίες που να αποσκοπούν στη διασφάλιση ενός υψηλού επιπέδου ασφάλειας των προσωπικών δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (data protection by design and by default) (άρθρο 25) αυστηρά προσαρμοσμένα στις βασικές αρχές της επεξεργασίας δεδομένων. Αναφορικά με το επίπεδο ασφάλειας των συστημάτων σε κάθε περίπτωση θα πρέπει να 7 εφαρμόζονται, μεταξύ άλλων, τα προβλεπόμενα στο

[74] Βλ. Ιστοσελίδα Ευρωπαϊκής Επιτροπής, «Δημόσιες Διοικήσεις και προστασία των δεδομένων», www.europa.eu.

(άρθρο 32) τεχνικά και οργανωτικά μέτρα ασφάλειας τα οποία να εξασφαλίζουν επίπεδο ασφάλειας των προσωπικών δεδομένων ανάλογο με τους κινδύνους στους οποίους εκτίθενται οι επεξεργασίες δεδομένων.

§11.4 - *Τι γίνεται όταν ένας δημόσιος φορέας δεν συμμορφώνεται με τους κανόνες προστασίας δεδομένων;*

Οι αρχές προστασίας[75] δεδομένων έχουν διαφορετικά εργαλεία στη διάθεσή τους σε περιπτώσεις μη συμμόρφωσης. Σε περίπτωση πιθανής παράβασης, μπορεί να εκδοθεί προειδοποίηση. Σε περίπτωση διαπιστωμένης παράβασης, ενδέχεται να επιβληθεί, π.χ., επίπληξη ή προσωρινή ή οριστική απαγόρευση της επεξεργασίας. Σε ορισμένες χώρες, οι δημόσιοι φορείς μπορεί επίσης να υπόκεινται σε διοικητικά πρόστιμα. Κάθε δημόσια διοίκηση θα πρέπει να ελέγξει την οικεία εθνική νομοθεσία για την προστασία των δεδομένων.

Τα φυσικά πρόσωπα μπορούν να ζητήσουν αποζημίωση εάν ένας δημόσιος φορέας έχει παραβιάσει τον ΓΚΠΔ με αποτέλεσμα να υποστούν υλική ζημία (π.χ. οικονομική απώλεια) ή μη υλική ζημία (π.χ. δυσφήμιση ή ψυχική οδύνη). Ο ΓΚΠΔ διασφαλίζει ότι θα τους καταβληθεί αποζημίωση, ανεξάρτητα από τον αριθμό των οργανισμών που συμμετείχαν στην επεξεργασία των δεδομένων τους. Η αξίωση αποζημίωσης μπορεί να εγερθεί είτε άμεσα στον υπαίτιο δημόσιο φορέα είτε ενώπιον των αρμόδιων εθνικών δικαστηρίων του οικείου κράτους μέλους της ΕΕ.

§11.5 – *Κριτική για την εφαρμογή του ΓΚΠΔ στους δημοσίους φορείς*

Οι περισσότεροι δημόσιοι φορείς της χώρας δεν έχουν προσαρμοστεί ακόμη με το καθεστώς του ΓΚΠΔ. Δηλαδή, δεν έχουν δημιουργήσει ή αναπροσαρμόσει διαδικασίες και πολιτική προστασίας, ώστε να διασφαλίσουν τη λειτουργία τους με τον προβλεπόμενο τρόπο και με τη μεγαλύτερη δυνατή ελαχιστοποίηση του κινδύνου παραβίασης των δεδομένων που επεξεργάζονται. Και αυτό έχει σημασία, αφενός διότι

[75] Βλ. Ιστοσελίδα Ευρωπαϊκής Επιτροπής, «Δημόσιες Διοικήσεις και προστασία των δεδομένων», www.europa.eu.

η παραβίαση μπορεί να οδηγήσει σε υψηλά πρόστιμα και αφετέρου, ίσως και κυριότερα, γιατί στο πλαίσιο της λειτουργίας των δήμων, τίθεται ουσιαστικό ζήτημα διατήρησης των σχέσεων εμπιστοσύνης με τους πολίτες στη βάση της καθημερινής συναλλαγής και επικοινωνίας. Οι δημόσιες αρχές διαχειρίζονται ένα τεράστιο εύρος προσωπικών δεδομένων, από τα απλά όπως το ονοματεπώνυμο, διεύθυνση, ΑΦΜ κλπ, όσο και ευαίσθητα, όπως δεδομένα υγείας και πρόνοιας, ακόμη και τα δεδομένα παιδιών. Οι δημόσιες αρχές με τα νομικά τους πρόσωπα οφείλουν αρχικά να κατανοήσουν την ανάγκη προσαρμογής στα δεδομένα του νέου ΓΚΠΔ και να μπουν σε διαδικασία να συμμορφωθούν, με τρόπο που θα διατηρεί τη λειτουργικότητά τους, αλλά και θα διασφαλίζει την ικανοποίηση των νέων, αυξημένων, υποχρεώσεων του ΓΚΠΔ. Αυτό θα συμβεί αρχικά, με το να αναγνωρίσουν τα προσωπικά δεδομένα και τις ενέργειες επεξεργασίας στις υπηρεσίες τους, ώστε να αποτυπώσουν την πραγματική κατάσταση σε μία, εν πολλοίς, αχαρτογράφητη διαδικασία. Αυτός ο «χάρτης» θα δώσει τη δυνατότητα στη συνέχεια, να εντοπίσουν τα κενά στην προστασία, τόσο στο επίπεδο των διαδικασιών, εντύπων, πολιτικών όσο και στα πληροφοριακά συστήματα που διαχειρίζονται, ώστε να λάβουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να οχυρώσουν τα δεδομένα που διατηρούν.

Ανάμεσα στις απαιτήσεις του νέου ΓΚΠΔ είναι ο εντοπισμός της νόμιμης βάσης επεξεργασίας των προσωπικών δεδομένων, η σαφής συγκατάθεση του υποκειμένου όπου αυτή κρίνεται αναγκαία, η εύκολη πρόσβαση, η δυνατότητα άσκησης δικαιωμάτων, όπως αυτά της πρόσβασης, διόρθωσης, διαγραφής, το δικαίωμα στον περιορισμό της επεξεργασίας, όπου είναι επιτρεπτό καθώς και το δικαίωμα στην εναντίωση. Και η ευθύνη δημόσιων φορέων (ή δημόσιων αρχών) ως υπεύθυνων επεξεργασίας, είναι αυξημένη αφού για το σύνολο των διαδικασιών και καθηκόντων που δρομολογούνται, είναι υπεύθυνοι να αποδεικνύουν ανά πάσα στιγμή τη συμμόρφωση με τις επιταγές του ΓΚΠΔ.

Παρότι, σε κάποια κράτη-μέλη της ΕΕ αντιμετωπίζονται δυσκολίες ως προς την συμμόρφωση στο νέο ΓΚΠΔ, δεν έχει προβλεφθεί περίοδος «παράτασης» εφαρμογής ή ανοχής. Αυτή είναι μία συνειδητή επιλογή από την πλευρά των αρμόδιων οργάνων της ΕΕ, ωστόσο δεν πρέπει να παραβλέπουμε ότι πρόκειται για την σημαντικότερη νομοθετική παρέμβαση στο χώρο των προσωπικών δεδομένων τα τελευταία 20 χρόνια, οπότε η πρώτη περίοδος είναι, ουσιαστικά, περίοδος προσαρμογής.

Προτού προχωρήσουμε στα διοικητικά πρόστιμα και εν συνεχεία στα δικαιώματα των υποκειμένων στον Κανονισμό, θα ήθελα να επισημάνω σ' αυτό το σημείο, ότι σχεδόν κάθε κεφάλαιο της παρούσας εργασίας αναλύθηκε σε σχέση με τον δημόσιο τομέα και την εφαρμογή του ΓΚΠΔ στον δημόσιο τομέα. Το ίδιο ισχύει φυσικά και για τον ΥΠΔ. Επιχειρήθηκε σε κάθε κεφάλαιο να γίνει αναφορά στον θεσμό του Υπευθύνου Προστασίας Δεδομένων π.χ, «ομάδα εργασίας του άρθρου 29 και ΥΠΔ», «εκτίμηση αντικτύπου και ΥΠΔ».

§12. - ΔΙΟΙΚΗΤΙΚΑ ΠΡΟΣΤΙΜΑ

Το άρθρο 83 του ΓΚΠΔ, με το τίτλο «Γενικοί Όροι Επιβολής Διοικητικών Προστίμων[76]» ορίζει ότι:

«Παραβάσεις των ακόλουθων διατάξεων επισύρουν, σύμφωνα με την παράγραφο 2, διοικητικά πρόστιμα έως 10 000 000 EUR ή, σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους…»

Με την θέσπιση δύο διαφορετικών μέγιστων ποσών όσον αφορά τα διοικητικά πρόστιμα[77] (10/20 εκατ. Ευρώ), ο Κανονισμός ήδη υποδεικνύει ότι η παράβαση ορισμένων διατάξεών του μπορεί να είναι πιο σοβαρή από την παράβαση άλλων. Ωστόσο, η αρμόδια εποπτική αρχή μπορεί να αποφασίσει ότι μια συγκεκριμένη περίπτωση μπορεί να αντιμετωπιστεί καλύτερα με την επιβολή κάποιου άλλου διοικητικού μέτρου αντί προστίμου π.χ. στην περίπτωση παράβασης ελάσσονος σημασίας κατά την παράγραφο 148 της αιτιολογικής έκθεσης. Επιπρόσθετα, πρέπει να σημειωθεί ότι οι παραβάσεις που από την φύση τους μπορεί να εμπίπτουν στην κατηγορία έως 10.000.000 ευρώ ή σε περίπτωση επιχειρήσεων έως το 2% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών (αρ.83 παρ. 4), μπορεί τελικά να εμπίπτουν σε υψηλότερη κατηγορία (20.000.000 ευρώ) σε ορισμένες περιπτώσεις. Αυτό θα ήταν πιθανό να συμβεί σε περίπτωση που οι εν λόγω παραβάσεις έχουν αντιμετωπιστεί κατά το παρελθόν με εντολή της εποπτικής αρχής (αρ. 58 παρ.2) προς

[76] Βλ. άρ 83 παρ 4 Κ.
[77] Βλ. Ιστοσελίδα, www.lawspot.gr.

την οποία ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δε συμμορφώθηκε (αρ. 83 παρ. 6). Η φύση της παράβασης, δηλαδή η έκταση ή ο σκοπός της σχετικής επεξεργασίας, καθώς και ο αριθμός των υποκειμένων των δεδομένων που έθιξε η παράβαση και ο βαθμός ζημίας που υπέστησαν, δείχνουν την βαρύτητα της παράβασης. Εάν τελεστούν πολλές διαφορετικές παραβάσεις σωρευτικά τότε η εποπτική αρχή θα μπορεί να επιβάλει διοικητικά πρόστιμα εντός του ορίου της βαρύτερης παράβασης. Η επιβολή προστίμου δεν εξαρτάται από την ικανότητα της εποπτικής αρχής να διαπιστώνει την ύπαρξη αιτιώδους συνάφειας μεταξύ της παράβασης και της υλική ζημίας.

Ακολουθούν τα βήματα μέχρι να φτάσουμε στα διοικητικά πρόστιμα:

• εάν η παράβαση είναι απλώς πιθανή, μπορεί να εκδοθεί προειδοποίηση

• εάν η παράβαση είναι διαπιστωμένη, ενδέχεται να επιβληθεί μεταξύ άλλων: α) επίπληξη, β) προσωρινή ή οριστική απαγόρευση της επεξεργασίας και γ) πρόστιμο μέγιστου ύψους 20 εκατομμυρίων ευρώ ή ίσο με το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης.

Το άρθρο 69 του ελληνικού σχεδίου νόμου, το οποίο έχει στόχο την εναρμόνιση του ελληνικού δικαίου με τον ΓΚΠΔ και φέρει τον τίτλο «Διοικητικά πρόστιμα και Γενικοί όροι επιβολής προστίμων» ορίζει συνοπτικά ότι:

- Η ΑΠΔΠΧ μπορεί να επιβάλλει τα διοικητικά πρόστιμα του άρθρου 83 του ΓΚΠΔ και σε δημόσιες αρχές και φορείς δημοσίου τομέα.

- Κατά τη λήψη απόφασης σχετικά με την επιβολή διοικητικού προστίμου, καθώς και σχετικά με το ύψος του διοικητικού προστίμου για κάθε μεμονωμένη περίπτωση, λαμβάνονται υπόψη τα κριτήρια και οι παράγοντες που απαριθμούνται στο άρθρο 83 του ΓΚΠΔ (βλ. ανωτέρω ενότητα 2 υπό τον τίτλο «ΑΡΘΡΟ 83 ΓΚΠΔ.»: π.χ. η φύση, η βαρύτητα και η διάρκεια της παράβασης, ο δόλος ή η αμέλεια που προκάλεσε την παράβαση, τυχόν σχετικές προηγούμενες παραβάσεις, οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση, κάθε άλλο επιβαρυντικό ή ελαφρυντικό στοιχείο εκ της συγκεκριμένης περιπτώσεως κ.λπ.)

- Σε περίπτωση που ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, για τις ίδιες ή για συνδεδεμένες πράξεις επεξεργασίας, παραβιάζει αρκετές διατάξεις του ΓΚΠΔ., το συνολικό ύψος του διοικητικού προστίμου δεν υπερβαίνει το ποσό που ορίζεται για τη βαρύτερη παράβαση.

- Οι πράξεις της ΑΠΔΠΧ με τις οποίες επιβάλλονται διοικητικά πρόστιμα συνιστούν εκτελεστό τίτλο και επιδίδονται στον υπεύθυνο επεξεργασίας ή τον εκτελούντα επεξεργασία ή τους εκπροσώπους αυτών.

- Η είσπραξη των προστίμων γίνεται κατά τις διατάξεις του Κώδικα Εισπράξεως Δημοσίων Εσόδων (ΚΕΔΕ).\

§12.1 - *Το περιεχόμενο των διοικητικών κυρώσεων - Η αρχή ne bis in idem*[78]

Σύμφωνα με τα ανωτέρω, το νομοθετικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση έχει τροποποιηθεί ριζικώς και εκτενώς βάσει των βασικών πυλώνων για νέους συνεκτικούς κανόνες δικαίου, απλουστευμένες διαδικασίες, συντονισμένες ενέργειες, ενεργή συμμετοχή των πλήρως ενημερωμένων υποκειμένων και εξουσίες ικανές να επιβάλουν τη συμμόρφωση στα νέα δεδομένα προστασίας, ιδίως με τη θέσπιση αυστηρών διοικητικών κυρώσεων.

Στο πλαίσιο αυτό, είναι σαφές ότι, αφενός οι εποπτικές αρχές πρέπει να διασφαλίζουν την αμεροληψία τους στην αποτελεσματική, αναλογική και αποτρεπτική επιβολή διοικητικών κυρώσεων, σύμφωνα με τις διατυπώσεις και το πνεύμα του Κανονισμού,

[78] Η αρχή "ne bis in idem" ή η απαγόρευση της διπλής διακινδύνευσης, σύμφωνα με την οποία δεν πρέπει να διώκεται ή να δικάζεται κανείς δύο φορές για τις ίδιες πράξεις, πραγματικά περιστατικά ή συμπεριφορά, κατοχυρώνεται ως ατομικό δικαίωμα στα διεθνή νομικά μέσα των ανθρώπινων δικαιωμάτων, όπως στο Διεθνές Σύμφωνο για τα Ατομικά και Πολιτικά Δικαιώματα (άρθρο 14, παράγραφος 7) της 19ης Δεκεμβρίου 1966, στο έβδομο πρωτόκολλο (άρθρο 4) της Σύμβασης για την Προάσπιση των Δικαιωμάτων του Ανθρώπου και των Θεμελιωδών Ελευθεριών και στον Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (άρθρο 50), αναγνωρίζεται δε από όλα τα νομικά συστήματα που διαπνέονται από την ιδέα σεβασμού και προστασίας των θεμελιωδών δικαιωμάτων. Αποτελεί ουσιαστική θωράκιση έναντι της καταχρηστικής άσκησης των κρατικών εξουσιών επί των πολιτών.

αφετέρου οι υπεύθυνοι και οι εκτελούντες την επεξεργασία δεδομένων έχουν αυξημένες υποχρεώσεις για την αποτελεσματική προστασία των προσωπικών δεδομένων, οι οποίες και διασφαλίζονται μέσω της γνώσης των πιθανών συνεπειών σε περίπτωση μη τήρησής τους. Πράγματι, τα διοικητικά πρόστιμα αποτελούν κεντρικό στοιχείο του νέου καθεστώτος επιβολής του Κανονισμού και ισχυρό εργαλείο στα χέρια των εποπτικών αρχών, συμπληρωματικώς με τα άλλα μέτρα που προβλέπονται στο άρθρο 58 του ΓΚΠΔ

Ωστόσο, η επιβολή και διοικητικών κυρώσεων (όπως και ποινικών κυρώσεων) για παραβάσεις εθνικών κανόνων δεν θα πρέπει να οδηγεί σε παραβίαση της αρχής ne bis in idem, όπως έχει νομολογιακώς ερμηνευτεί. Συνεπώς, σωρευτικώς επιπρόσθετη ποινή για το ίδιο αδίκημα δεν μπορεί να επιβάλει η εποπτική αρχή αν έχει επιβάλλει ποινή δικαστήριο ή άλλη αρχή. Βέβαια, η αθώωση / απαλλαγή από μία αρχή ή δικαστήριο δεν αποστερεί τη δυνατότητα της εποπτικής αρχής να επιληφθεί της υπόθεσης (βλ. αιτιολογική σκέψη 150 ΓΚΠΔ).

§13. - ΔΙΚΑΙΩΜΑΤΑ ΥΠΟΚΕΙΜΕΝΩΝ

Τα δικαιώματα του υποκειμένου[79] των δεδομένων συνιστούν έκφραση της πληροφοριακής αυτοδιάθεσης του υποκειμένου. Εντάσσονται στον «σκληρό πυρήνα» του δικαίου της προστασίας δεδομένων. Ωστόσο υπέρβαση του μοντέλου της πληροφοριακής αυτοδιάθεσης που εκφράζεται με τη συναίνεση του υποκειμένου, η οποία στην πράξη δίδεται χωρίς επίγνωση. Βασικός στόχος της αναθεώρησης του νομικού πλαισίου προστασίας δεδομένων είναι η επαύξηση των δικαιωμάτων των υποκειμένων των δεδομένων. Εισάγονται νέα δεδομένα, όπως το δικαίωμα στη λήθη, το δικαίωμα στη φορητότητα και η αντίταξη στη δημιουργία προφίλ. Συνεπώς, ενισχύονται τα δικαιώματα που κατοχυρώνονται στην Οδηγία 95/46. Η προστασία των δικαιωμάτων στον Κανονισμό φιλοξενείται στα άρθρα 12 έως 23.

Διαφάνεια (*Δικαίωμα ενημέρωσης*)

Το άρθρο 12[80] αναφέρεται στη διαφανή ενημέρωση, στις ανακοινώσεις και ρυθμίσεις για την άσκηση δικαιωμάτων των υποκειμένων. Ο γενικός κατάλογος των

[79] Βλ. άρ 12-23 Κ.

[80] Ιγγλεζάκης Ι. «Δικαιώματα του υποκειμένου των δεδομένων στον Κανονισμό 2016/679.

δικαιωμάτων του υποκειμένου των δεδομένων έχει ως αφετηρία τη γενική αρχή της διαφάνειας κατά την επεξεργασία προσωπικών δεδομένων «ή ορθότερα τη διαφανή[81] πολιτική ενημερώσεως με σκοπό τη διευκόλυνση της ασκήσεως των δικαιωμάτων εκ μέρους του υποκειμένου των δεδομένων αλλά και την παροχή συγκαταθέσεως». Ο υπεύθυνος επεξεργασίας παρέχει στο υποκείμενο των δεδομένων πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματος, δυνάμει των άρθρων 15 έως 22 χωρίς καθυστέρηση και σε κάθε περίπτωση εντός μηνός από την παραλαβή του αιτήματος. Οι πληροφορίες που πρέπει να παρέχονται στα υποκείμενα των δεδομένων σύμφωνα με τα άρθρα 13 και 14 μπορούν να παρέχονται σε συνδυασμό με τυποποιημένα εικονίδια προκειμένου να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο μια ουσιαστική επισκόπηση της σκοπούμενης επεξεργασίας. Όταν ζητείται από το υποκείμενο των δεδομένων, οι πληροφορίες μπορούν να δίνονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα. Οι πληροφορίες που παρέχονται σύμφωνα με τα άρθρα 13 και 14 και κάθε ανακοίνωση καθώς και όλες οι ενέργειες που αναλαμβάνονται σύμφωνα με τα άρθρα 15 έως 22 και το άρθρο 34 παρέχονται δωρεάν. Οι εργαζόμενοι έχουν δικαίωμα να απευθύνονται στον υπεύθυνο προστασίας δεδομένων και να διατυπώνουν ερωτήματα, παράπονα ή καταγγελίες σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της απασχόλησης. Η άσκηση του δικαιώματος αυτού και η άσκηση των δικαιωμάτων που προβλέπονται από τον Γενικό Κανονισμό Προστασίας Δεδομένων (άρθρα 12-22) δεν επιτρέπεται να άλλωστε να έχουν δυσμενείς συνέπειες για τον εργαζόμενο.

Ελεύθερη Συγκατάθεση

Ο ΓΚΠΔ δίνει ιδιαίτερη βαρύτητα στην συγκατάθεση του υποκειμένου για την χρήση προσωπικών δεδομένων, η οποία θα πρέπει να παρέχεται με σαφή θετική ενέργεια η οποία να συνιστά ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει ένδειξη της συμφωνίας του υποκειμένου (αιτιολογική σκέψη 32 του ΓΚΠΔ). Για να διασφαλιστεί ότι η συγκατάθεση έχει δοθεί ελεύθερα, δεν θα πρέπει να παρέχει έγκυρη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μια συγκεκριμένη

[81] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 58-60.

περίπτωση, όταν υπάρχει σαφής ανισότητα μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, ιδίως στις περιπτώσεις που ο υπεύθυνος επεξεργασίας είναι δημόσια αρχή και είναι επομένως σχεδόν απίθανο να έχει δοθεί η συγκατάθεση ελεύθερα σε όλες τις περιστάσεις αυτής της ειδικής κατάστασης. Η συγκατάθεση θεωρείται ότι δεν έχει παρασχεθεί ελεύθερα, εάν δεν επιτρέπεται να δοθεί χωριστή συγκατάθεση σε διαφορετικές πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ακόμη και αν ενδείκνυται στη συγκεκριμένη περίπτωση, ή όταν η εκτέλεση μιας σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, προϋποθέτει τη συγκατάθεση, ακόμη και αν η συγκατάθεση αυτή δεν είναι αναγκαία για την εν λόγω εκτέλεση.

Η συγκατάθεση θα μπορούσε να δοθεί με μία γραπτή δήλωση, με τη συμπλήρωση τετραγωνιδίου σε μια ιστοσελίδα. Έμφαση δίνεται στην θετική ενέργεια εκ μέρους του υποκειμένου οπότε η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση (αιτιολογική σκέψη 32 του ΓΚΠΔ).

Ο κανονισμός δεν αφήνει περιθώρια εξαιρέσεων αφού η συγκατάθεση θα πρέπει να αφορά συγκεκριμένα δεδομένα που θα υποβληθούν σε ορισμένη επεξεργασία για καθορισμένο χρονικό διάστημα. Για να διαφυλαχτεί η διαδικασία, ορίζεται επιπλέον ότι:

1. Το υποκείμενο μπορεί να αναιρέσει την συγκατάθεση του οποιαδήποτε στιγμή και ο υπεύθυνος της επεξεργασίας οφείλει να τον διευκολύνει στην συγκεκριμένη διαδικασία

2. Η συγκατάθεση δεν θεωρείται ελεύθερη αν υπάρχουν ξεκάθαρες σχέσεις εξουσίας μεταξύ του υποκειμένου και του υπεύθυνου (π.χ. ο υπεύθυνος της επεξεργασίας είναι δημόσια αρχή). Σε καμία περίπτωση η συγκατάθεση δεν θα πρέπει να είναι προϋπόθεση για την παροχή υπηρεσιών εκτός αν η χρήση δεδομένων είναι απαραίτητη για την παροχή της υπηρεσίας

3. Για κάθε άλλη χρήση των δεδομένων, το υποκείμενο θα πρέπει να ενημερώνεται και να δίνει την συγκατάθεση του εκ νέου

Ειδικότερα όσον αφορά ευαίσθητα δεδομένα, η συγκατάθεση θα πρέπει να δίνεται με ακόμη μεγαλύτερη σαφήνεια. Το άρθρο 9 για την «ειδική κατηγορία δεδομένων» απαγορεύει την

επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων[82] με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό (Άρθ. 9 του ΓΚΠΔ).

Εξαίρεση αποτελούν και πάλι οι περιπτώσεις προστασίας του ατόμου ή των οικείων του, η προστασία του δημόσιου συμφέροντος ή η συλλογή των δεδομένων στα πλαίσια άσκησης της δικαιοσύνης, επιστημονικών ή στατιστικών σκοπών και φυσικά, οι περιπτώσεις που το ίδιο το υποκείμενο έχει δημοσιοποιήσει τα δεδομένα.

Τέλος, το άρθρο 8 του κανονισμού απαγορεύει την χρήση προσωπικών δεδομένων παιδιών κάτω των 16 ετών χωρίς την ελεύθερη συγκατάθεση του γονέα.

Δικαίωμα εναντίωσης

Το δικαίωμα της εναντίωσης[83] αποτελεί ένα από τα σημαντικότερα δικαιώματα όσον αφορά την προστασία των προσωπικών δεδομένων. Είναι το δικαίωμα με βάση το οποίο, μπορεί κάποιος να εναντιωθεί στην επεξεργασία προσωπικών δεδομένων από έναν οργανισμό, υπό την προϋπόθεση βέβαια ότι δεν θίγεται το δημόσιο συμφέρον. Στην 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 για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων. Ο υπεύθυνος επεξεργασίας πρέπει, το αργότερο κατά την πρώτη επικοινωνία με το υποκείμενο των δεδομένων, να ενημερώσει για την ύπαρξη του δικαιώματος αυτού με σαφήνεια και διακριτό τρόπο από τυχόν άλλες παρεχόμενες πληροφορίες. Επιπλέον, το δικαίωμα εναντίωσης μπορεί να ασκηθεί ανά

[82] Βλ. άρ 9 Κ

[83] Βλ. Ιστοσελίδα Αρχής Προστασίας δεδομένων Προσωπικού Χαρακτήρα, «Τα δικαιώματα μου», www.dpa.gr.

πάσα στιγμή στην επεξεργασία δεδομένων για σκοπούς απευθείας εμπορικής προώθησης.

Αρχή της εγγύτητας

Ο Κανονισμός υιοθετεί την αρχή της εγγύτητας προς το υποκείμενο των δεδομένων, προβλέποντας ρητά ότι κάθε πρόσωπο που θεωρεί ότι παραβιάζονται τα δικαιώματα του στην προστασία των δεδομένων του, έχει το δικαίωμα να υποβάλει καταγγελία σε οποιαδήποτε εποπτική αρχή (βλ. ενδεικτικά τόπος συνήθους διαμονής υποκειμένου, ή τόπος εργασίας του ή τόπος εικαζόμενης παράβασης).

Δικαίωμα στην ανθρώπινη παρέμβαση

Με αυτό το δικαίωμα μπορεί κάποιος να προβάλλει αντιρρήσεις όταν μια απόφαση που τον αφορά βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, και η απόφαση αυτή παράγει έννομα αποτελέσματα ή τον επηρεάζει σημαντικά.

Δικαίωμα προσβάσεως

Το άρθρο 15 Κ επικαιροποιεί το γνωστό ήδη από το άρθρο 12 της Οδηγίας 95/46/ΕΚ δικαίωμα του υποκειμένου να έχει πρόσβαση στα δεδομένα[84] που το αφορούν. Το δικαίωμα[85] στην ουσία, διευκολύνει το υποκείμενο να ελέγξει τη νομιμότητα της επεξεργασίας των δεδομένων του, αλλά και την άσκηση των δικαιωμάτων πληροφορήσεως, διαγραφής και αντιτάξεως. Το δικαίωμα αυτό εξυπηρετείται σε τέσσερα στάδια: στο στάδιο εξετάζεται εάν λαμβάνει χώρα επεξεργασία, στο δεύτερο στάδιο πως γίνεται η επεξεργασία, στο τρίτο στάδιο τι τυγχάνει επεξεργασίας και τέλος στο τέταρτο στάδιο με ποιο τρόπο πραγματοποιείται το δικαίωμα προσβάσεως.

Δικαίωμα διόρθωσης

Το υποκείμενο των δεδομένων έχει το δικαίωμα[86] να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της

[84] Βλ. άρ 15 Κ.
[85] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 68.
[86] Βλ. άρ. 16 Κ.

επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης. Το δικαίωμα αυτό[87] κατοχυρώνεται ρητά στο άρθρο 8 παρ 2 εδ. β΄του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ενώσεως, ενώ αποτελεί προέκταση του δικαιώματος προσβάσεως, καθώς μετά την πραγματοποίηση της προσβάσεως το υποκείμενο των δεδομένων δικαιούται σε διόρθωση ανακριβών δεδομένων. Βασική προϋπόθεση του δικαιώματος διορθώσεως είναι το αναληθές των δεδομένων, το οποίο εκτιμάται με αντικειμενικά κριτήρια. Παραβιάσεις[88] του δικαιώματος στη διόρθωση επιφέρουν κύρωση της επιβολής προστίμου 20.000.000 Ευρώ ή 4% του παγκοσμίου ετησίου κύκλου εργασιών της επιχειρήσεως, αναλόγως τι είναι υψηλότερο.

Ασφάλεια δεδομένων

Ο ΓΚΠΔ δίνει, επίσης, ιδιαίτερη βαρύτητα στην προστασία των προσωπικών δεδομένων και ορίζει συγκεκριμένα μέτρα ασφαλείας ώστε να προστατευτούν τα δικαιώματα των υποκειμένων των δεδομένων στο μέγιστο.

Λαμβάνοντας υπόψη τις συνθήκες, το κόστος, τα τεχνολογικά μέσα καθώς και τον βαθμό κινδύνου για τις ελευθερίες των υποκειμένων σε περίπτωση παραβίασης, ο υπεύθυνος οφείλει να εφαρμόζει μέτρα για την ασφάλεια των δεδομένων όπως ψευδωνυμοποίηση ή κρυπτογράφηση, διασφάλιση ομαλής λειτουργίας των συστημάτων επεξεργασίας, δυνατότητα αποκατάστασης σε περίπτωση φυσικού ή τεχνικού συμβάντος και τακτικός έλεγχος των μηχανισμών ασφαλείας.

Αν τα δεδομένα παραβιαστούν και ενδέχεται να προκληθεί παραβίαση των δικαιωμάτων των υποκειμένων, ο υπεύθυνος οφείλει να ενημερώσει την αρμόδια εποπτική αρχή εντός 72 ωρών περιγράφοντας την φύση της παραβίασης, τις συνέπειες που μπορεί να έχει για τα υποκείμενα των δεδομένων και τα ληφθέντα ή προτεινόμενα

[87] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 73.
[88] Φερενίκη Παναγοπούλου-Κουτνατζή «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016-ΕΕ», σελ 74.

μέτρα για την αντιμετώπιση του ζητήματος. Σε περίπτωση που ο υπεύθυνος δεν έχει λάβει τα μέτρα που αναφέρονται παραπάνω και η παραβίαση ενδέχεται να θέσει τα υποκείμενα σε υψηλό κίνδυνο, οφείλει, επιπλέον, να ενημερώσει τα ίδια τα υποκείμενα ή να δημοσιοποιήσει πληροφορίες για την παραβίαση (Άρθ. 33 και 34 του ΓΚΠΔ).

Επιπρόσθετα το Άρθρο 35 του κανονισμού προβλέπει και προληπτικά μέτρα για την ασφάλεια των υποκειμένων και για την εκτίμηση αντικτύπου. Σύμφωνα με το Άρθρο, αν η επεξεργασία δεδομένων υπάγεται σε κατηγορία που μπορεί να θέσει σε υψηλό κίνδυνο τα υποκείμενα, ο υπεύθυνος θα πρέπει να συμβουλευτεί τον υπεύθυνο προστασίας δεδομένων πριν προχωρήσει. Οι κατηγορίες υψηλού ρίσκου είναι, μεταξύ άλλων:

1. Η συστηματική και εκτενής παρακολούθηση προσωπικών πτυχών των υποκειμένων, όπως η κατάρτιση προφίλ, με σκοπό την λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα για το υποκείμενο
2. Η επεξεργασία ειδικής κατηγορίας δεδομένων σε μεγάλη κλίμακα και
3. Συστηματική παρακολούθηση δημοσίων χώρων σε μεγάλη κλίμακα

Η εφαρμογή των εν λόγω μέτρων αποτελεί πρόκληση για τους οργανισμούς που χειρίζονται δεδομένα, αφού σε περίπτωση μη τήρησης του κανονισμού, προβλέπονται πρόστιμα που φτάνουν τα 20 εκατομμύρια ευρώ. Πρόκληση, όμως, αποτελεί και για τα νομικά συστήματα των κρατών – μελών της Ένωσης που καλούνται να προτείνουν επιμέρους μέτρα ώστε να διευκολύνουν την εφαρμογή του κανονισμού στην επικράτεια τους και να διασφαλίσουν την δημιουργία εποπτικής αρχής που θα παρακολουθεί την εφαρμογή των μέτρων και θα φροντίζει για την ομαλή κυκλοφορία των δεδομένων στην Ένωση. Έτσι αν και ο Γενικός Κανονισμός για την Προστασία των Δεδομένων έρχεται ως ένα αυστηρό νομικό πλαίσιο με σκοπό την δημιουργία ενός ενιαίου καθεστώτος εντός της Ένωσης, επιτρέπει σε πολλά σημεία εναρμόνιση με το δίκαιο του κάθε κράτους – μέλους.

Το δικαίωμα στη λήθη

Αναφορικά με τα δικαιώματα, το «δικαίωμα στη λήθη[89]» που ίσως είναι το σημαντικότερο δικαίωμα στον νέο κανονισμό προστασίας προσωπικών δεδομένων, έχει περιορισμένη εφαρμογή στο Δημόσιο Τομέα. Με το δικαίωμα αυτό ενισχύεται η πληροφοριακή αυτοδιάθεση των φυσικών προσώπων σχετικά με τα δεδομένα που τους αφορούν και τα οποία δημοσιεύονται στο διαδίκτυο. Αντιμετωπίζεται το πρόβλημα της διαγραφής του ψηφιακού παρελθόντος του ατόμου, στην εποχή της «απόλυτης ψηφιακής μνήμης». Ουσιαστικά πρόκειται για ένα δικαίωμα 'διαγραφής': «το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα που το αφορούν χωρίς αδικαιολόγητη καθυστέρηση και ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση». Περαιτέρω, το δικαίωμα αυτό έχει ιδίως σημασία όταν το υποκείμενο των δεδομένων παρέσχε τη συγκατάθεσή του ως παιδί, όταν δεν είχε πλήρη επίγνωση των κινδύνων που ενέχει η επεξεργασία, και θέλει αργότερα να αφαιρέσει τα συγκεκριμένα δεδομένα προσωπικού χαρακτήρα, κυρίως από το διαδίκτυο. Το υποκείμενο των δεδομένων θα πρέπει να μπορεί να ασκήσει το εν λόγω δικαίωμα παρά το γεγονός ότι δεν είναι πλέον παιδί.

Επισημαίνεται, ωστόσο, ότι δεν πρόκειται για ένα απόλυτο δικαίωμα, καθώς η περαιτέρω διατήρηση των δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη, όταν είναι αναγκαία, για λόγους όπως για την άσκηση του δικαιώματος ελευθερίας της έκφρασης και ενημέρωσης, όπως προαναφέρθηκε, ή για τη συμμόρφωση με νομική υποχρέωση, για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Τέλος, σημειώνεται ότι για να είναι αποτελεσματικό το δικαίωμα διαγραφής, εάν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα προσωπικού χαρακτήρα και

[89] Βλ. Αρχή Προστασίας δεδομένων Προσωπικού Χαρακτήρα, «Τα δικαιώματα μου», www.dpa.gr.

υποχρεούται κατά τα ανωτέρω να τα διαγράψει, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, θα πρέπει να λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει σχετικά με το αίτημα διαγραφής τους υπευθύνους επεξεργασίας που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ώστε να διαγράψουν οποιουσδήποτε συνδέσμους ή αντίγραφα ή αναπαραγωγή των εν λόγω δεδομένων. Άλλωστε για να εφαρμοσθεί το δικαίωμα στη λήθη, πρέπει να συντρέχουν κάποιες συγκεκριμένες προϋποθέσεις. (π.χ τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα σε σχέση με τους σκοπούς για τους οποίους συλλέχθηκαν ή υποβλήθηκαν κατ'άλλο τρόπο σε επεξεργασία).

Συγκατάθεση των υποκειμένων

Η ομάδα εργασίας του άρθρου 29 επικροτεί άλλη μια κατηγορία βελτιώσεων που σχετίζονται με την εφαρμογή και την ερμηνεία της έννοιας της συγκατάθεσης. Πρώτον, επικροτείται η διευκρίνιση ότι η πρόσβαση στο διαδίκτυο και η (κινητή) τηλεφωνία συνιστούν θεμελιώδεις υπηρεσίες και ότι οι πάροχοι των υπηρεσιών αυτών δεν πρέπει να «αναγκάζουν» τους πελάτες τους να συναινούν σε οποιαδήποτε επεξεργασία δεδομένων η οποία δεν είναι αναγκαία για την παροχή της ίδιας της θεμελιώδους υπηρεσίας. Ειδικότερα, στην αιτιολογική σκέψη 18 σημειώνεται ότι οι βασικές υπηρεσίες ευρυζωνικής πρόσβασης στο διαδίκτυο και φωνητικών επικοινωνιών πρέπει να θεωρούνται θεμελιώδεις, γεγονός που σημαίνει, δεδομένης της εξάρτησης των προσώπων από την πρόσβαση στις εν λόγω υπηρεσίες, ότι η συγκατάθεση για την επεξεργασία των δεδομένων επικοινωνιών τους για τους συγκεκριμένους πρόσθετους σκοπούς (π.χ. επεξεργασία για σκοπούς διαφήμισης ή εμπορικής προώθησης) δεν μπορεί να είναι έγκυρη. Παράλληλα, η ομάδα εργασίας εκφράζει την ανησυχία ότι η διευκρίνιση αυτή είναι υπερβολικά περιορισμένη. Οι υπηρεσίες[90] που παρέχονται από ορισμένους παρόχους επιφυών υπηρεσιών (OTT) μπορούν επίσης να θεωρηθούν θεμελιώδεις και ο κανονισμός για την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες θα πρέπει επίσης να απαγορεύσει ειδικά τις επιλογές τύπου «όλα ή τίποτα» σε άλλες περιστάσεις.

[90] Βλ. Ομάδα εργασίας του άρ.29, σημείο 20.

Το Δικαίωμα στη φορητότητα

Το άρθρο 20 του ΓΚΠΔ[91] θεσπίζει ένα νέο δικαίωμα στη φορητότητα των δεδομένων, το οποίο συνδέεται μεν στενά με το δικαίωμα πρόσβασης αλλά διαφέρει από αυτό από πολλές απόψεις. Παρέχει στα υποκείμενα των δεδομένων τη δυνατότητα να λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα που έχουν παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζουν τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας. Στόχος αυτού του νέου δικαιώματος είναι να δώσει στο υποκείμενο των δεδομένων δύναμη και μεγαλύτερο έλεγχο επί των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Το «δικαίωμα στη φορητότητα» προσφέρει στα υποκείμενα των δεδομένων έναν εύκολο τρόπο να διαχειρίζονται τα ίδια τα προσωπικά τους δεδομένα. Τα διευκολύνει να διακινούν, να αντιγράφουν ή να μεταφέρουν, εύκολα, δεδομένα προσωπικού χαρακτήρα από ένα περιβάλλον τεχνολογιών πληροφορικής σε άλλο. Τα υποκείμενα των δεδομένων έχουν δικαίωμα να λάβουν τα δικά τους προσωπικά δεδομένα, τα οποία έχουν υποβληθεί σε επεξεργασία από έναν υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο (π.χ. XML, JSON, CSV, κ.λπ.). Έχουν επίσης το δικαίωμα να διαβιβάσουν τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας, χωρίς αντίρρηση από τον αρχικό υπεύθυνο. Σε περίπτωση που είναι τεχνικά εφικτό, μπορούν να ζητήσουν την απευθείας διαβίβαση των δεδομένων τους από έναν υπεύθυνο επεξεργασίας σε άλλον. Και σ'αυτό το δικαίωμα υπάρχουν κάποιες επιμέρους προϋποθέσεις για να ασκηθεί (π.χ η άσκηση του δικαιώματος δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων)

Όταν ένα πρόσωπο ασκεί το δικαίωμά του στη φορητότητα των δεδομένων, αυτό γίνεται με την επιφύλαξη κάθε άλλου δικαιώματός του (όπως άλλα δικαιώματα βάσει του ΓΚΠΔ). Ένα υποκείμενο των δεδομένων μπορεί να συνεχίσει να χρησιμοποιεί τις υπηρεσίες του υπευθύνου επεξεργασίας και να επωφελείται από αυτές ακόμη και μετά από μια πράξη φορητότητας δεδομένων. Η φορητότητα των δεδομένων δεν συνεπάγεται αυτομάτως διαγραφή των δεδομένων14 από τα συστήματα του υπευθύνου επεξεργασίας, και δεν επηρεάζει την αρχική περίοδο διατήρησης που ισχύει για τα

[91] Βλ. Ομάδα εργασίας του άρθρου 29, «Κατευθυντήριες γραμμές σχετικά με το δικαίωμα στη φορητότητα των δεδομένων, www.dataprotection.gov.cy.

διαβιβαζόμενα δεδομένα. Το υποκείμενο των δεδομένων μπορεί να ασκεί τα δικαιώματά του για όσο διάστημα ο υπεύθυνος επεξεργασίας συνεχίζει να επεξεργάζεται τα δεδομένα. Κατά τον ίδιο τρόπο, αν το υποκείμενο των δεδομένων επιθυμεί να ασκήσει το δικαίωμά διαγραφής το οποίο έχει («δικαίωμα στη λήθη» βάσει του άρθρου 17), η φορητότητα των δεδομένων δεν μπορεί να χρησιμοποιείται από τον υπεύθυνο επεξεργασίας ως δικαιολογία για την καθυστέρηση ή την άρνηση της διαγραφής.

Ο ΓΚΠΔ παρέχει αρκετά «εργαλεία» για να δικαιολογηθεί η νομική βάση για επεξεργασία δεδομένων προσωπικού χαρακτήρα. Επίσης, λόγω του ότι η «συγκατάθεση» και το «δικαίωμα στη λήθη» έχουν περιορισμένη εφαρμογή στο Δημόσιο -σε αντίθεση με τον ιδιωτικό τομέα-, το βάρος των νομικών αλλαγών από το ΓΚΠΔ δεν είναι ιδιαίτερα μεγάλο. Επομένως, ένας Δημόσιος φορέας που λειτουργεί ξεκάθαρα εντός εντός του πλαισίου των νομικά τεκμηριωμένων αρμοδιοτήτων του, μπορεί να αντιμετωπίσει τον ΓΚΠΔ με απλά και μεθοδικά βήματα. Ο ΓΚΠΔ πρέπει να αντιμετωπιστεί από το Δημόσιο ως ένα ακόμα βήμα για περισσότερη διαφάνεια της δημόσιας διοίκησης, ως μια ευκαιρία για να αυξηθεί η εμπιστοσύνη των πολιτών στη δημόσια διοίκηση.

Το Δικαίωμα λήψης δεδομένων προσωπικού χαρακτήρα

Το συγκεκριμένο δικαίωμα συνδέεται άμεσα με το δικαίωμα στη φορητότητα και ουσιαστικά αποτελεί υποκατηγορία του. Κατά πρώτον, η φορητότητα δεδομένων είναι το δικαίωμα του υποκειμένου των δεδομένων να λαμβάνει ένα υποσύνολο των δεδομένων προσωπικού χαρακτήρα που το αφορούν και έχουν υποβληθεί σε επεξεργασία από υπεύθυνο επεξεργασίας, και να αποθηκεύει τα δεδομένα αυτά για περαιτέρω προσωπική χρήση. Η αποθήκευση μπορεί να γίνεται σε ιδιωτική συσκευή ή ιδιωτικό υπολογιστικό σύννεφο, χωρίς, κατ' ανάγκη, διαβίβαση των δεδομένων σε άλλο υπεύθυνο επεξεργασίας. Υπό αυτή την έννοια, η φορητότητα των δεδομένων συμπληρώνει το δικαίωμα πρόσβασης. Μία ιδιαιτερότητα της φορητότητας των δεδομένων έγκειται στο γεγονός ότι προσφέρει στα υποκείμενα των δεδομένων έναν εύκολο τρόπο για τη διαχείριση και την εκ νέου χρήση των δεδομένων προσωπικού χαρακτήρα.

§13.1 – *Περιορισμοί δικαιωμάτων*

«Η άσκηση των δικαιωμάτων[92] που κατοχυρώνονται στον Κανονισμό υπόκειται στη ρήτρα περιορισμών του άρθρου 23 Κ. Το συγκεκριμένο άρθρο αναγνωρίζει τη διακριτική ευχέρεια στο ενωσιακό ή το εσωτερικό δίκαιο των κρατών μελών να περιορίσει μέσω νομοθετικού μέτρου το πεδίο εφαρμογής των δικαιωμάτων που προβλέπονται στα άρθρα 12 έως 22 Κ, όταν ένας τέτοιος περιορισμός σέβεται την ουσία των θεμελιωδών δικαιωμάτων και ελευθεριών και συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση υπέρτερων αγαθών». Οι περιορισμοί του άρθρου 23 του Κανονισμού περιέχουν τη ρήτρα της προστασίας του πυρήνα του δικαιώματος, σε αντίθεση με τους περιορισμούς του αντίστοιχου άρθρου της προγενέστερης Οδηγίας 95/46/ΕΚ. Ουσιαστικά, οι περιορισμοί που αφορούν τον ισχύοντα Κανονισμό, πρέπει αρχικά να μην παραβιάζουν τον πυρήνα του δικαιώματος, να εξυπηρετούν κάποιον από τους σκοπούς που αναφέρονται περιοριστικά στο άρθρο 23 παρ 1 και να εφαρμόζονται μόνο στα αναφερόμενα στο άρθρο 23 Κ δικαιώματα.

§13.2 – *Πότε τα δικαιώματα τίθενται σε περιορισμό;*

Τα δικαιώματα του Κανονισμού τίθενται σε περιορισμούς όταν αναφέρονται στην ασφάλεια του κράτους, την εθνική άμυνα, τη δημόσια ασφάλεια[93], την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, περιλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και την πρόληψη αυτών. Τέλος, περιορίζονται όταν σχετίζονται «με σημαντικούς στόχους[94] δημοσίου συμφέροντος της Ενώσεως ή κράτους μέλους, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων, της δημόσιας υγείας και της κοινωνικής ασφαλίσεως».

[92] Φερενίκη Παναγοπούλου – Κουτναζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ», σελ 114-117.
[93] Υπάρχουν περισσότεροι λόγοι σύμφωνα με τους οποίους περιορίζονται τα δικαιώματα του Κανονισμού. Αναφέρθηκαν μόνο όσοι είναι σχετικοί με τους «δημόσιους φορείς».
[94] Φερενίκη Παναγοπούλου – Κουτνατζή, «Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων 679/2016/ΕΕ», σελ 115.

§13.3 - *Περιορισμοί της ανακοίνωσης παραβίασης δεδομένων*

«Η ανακοίνωση της παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων που προβλέπεται στο άρθρο 34 του Κανονισμού, δεν πραγματοποιείται εφόσον η επεξεργασία πραγματοποιείται για σκοπού που σχετίζονται: με την εθνική άμυνα, την εθνική ασφάλεια, την δημόσια ασφάλεια, την πρόληψη, διερεύνηση, διακρίβωση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων, περιλαμβανομένης της προστασίας από απειλές κατά της δημόσιας ασφάλειας και πρόληψης αυτών». Επίσης η ανακοίνωση της παραβίασης δεν πραγματοποιείται όταν υπάρχουν περιπτώσεις που αναφέρονται σε οικονομικά, χρηματοοικονομικά συμφέροντα του Κράτους, συμπεριλαμβανομένων των νομισματικών, δημοσιονομικών και φορολογικών θεμάτων της δημόσιας υγείας και κοινωνικής ασφάλισης, ιδίως σε σχέση με την πραγματοποίηση των σχετικών ελέγχων και όταν υφίσταται άσκηση, υποστήριξη ή εκτέλεση νομικών αξιώσεων.

§13.4 - *Κατάρτιση προφίλ*

Το υποκείμενο των δεδομένων έχει το δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας , συμπεριλαμβανομένης της κατάρτισης προφίλ, η οποία παράγει έννομα αποτελέσματα που το αφορούν ή το επηρεάζει σημαντικά με παρόμοιο τρόπο. Η κατάρτιση προφίλ υπόκειται στους κανόνες του παρόντος κανονισμού που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως νομικοί λόγοι επεξεργασίας ή αρχές προστασίας δεδομένων. Σε αυτό το πλαίσιο, το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων που συστήνεται με τον παρόντα κανονισμό («Συμβούλιο Προστασίας Δεδομένων») θα πρέπει να έχει τη δυνατότητα να δίνει κατευθύνσεις. Προκειμένου να διασφαλισθεί δίκαιη και διαφανής επεξεργασία[95] σε σχέση με το υποκείμενο των δεδομένων, λαμβανομένων υπόψη των ειδικών συνθηκών και του πλαισίου εντός του οποίου πραγματοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κατάλληλες μαθηματικές ή στατιστικές διαδικασίες για την κατάρτιση του προφίλ, να εφαρμόζει τεχνικά και οργανωτικά μέτρα, ώστε να διορθώνονται οι παράγοντες που οδηγούν σε ανακρίβειες

[95] Βλ. Ιστοσελίδα, www.lawspot.gr.

σε δεδομένα προσωπικού χαρακτήρα και να ελαχιστοποιείται ο κίνδυνος σφαλμάτων, να καθιστά ασφαλή τα δεδομένα προσωπικού χαρακτήρα κατά τρόπο που να λαμβάνει υπόψη τους πιθανούς κινδύνους που συνδέονται με τα συμφέροντα και τα δικαιώματα του υποκειμένου των δεδομένων και κατά τρόπο που να προλαμβάνει, μεταξύ άλλων, τα αποτελέσματα διακρίσεων σε βάρος φυσικών προσώπων βάσει της φυλετικής ή εθνοτικής καταγωγής, των πολιτικών φρονημάτων, της θρησκείας ή των πεποιθήσεων, της συμμετοχής σε συνδικαλιστικές οργανώσεις, της γενετικής κατάστασης ή της κατάστασης της υγείας ή του γενετήσιου προσανατολισμού, ή μέτρων ισοδύναμου αποτελέσματος. Η αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ που βασίζονται σε ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα θα πρέπει να επιτρέπονται μόνο υπό ειδικές προϋποθέσεις.

Η κατάρτιση προφίλ είναι μια έννοια που προήλθε από τον χώρο της εγκληματολογίας, ωστόσο η δυνατότητα και επεξεργασίας μεγάλου όγκου δεδομένων, την καθιστά συνήθη πρακτική για κάθε είδους οργανισμό. Ο ΓΚΠΔ, στην προσπάθειά του να ενισχύσει τη δυνατότητα των δεδομένων να προστατεύσουν, τα προσωπικά τους δεδομένα, θέτει ορισμένους περιορισμούς στην αυτοματοποιημένη επεξεργασία δεδομένων και την λήψη αποφάσεων χωρίς την εμπλοκή του ανθρώπινου παράγοντα.

Σύμφωνα με το Άρθρο 4 του ΓΚΠΔ, η «κατάρτιση προφίλ» ορίζεται ως,

οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου.

§14. – ΑΠΟΦΑΣΕΙΣ[96]

§14.1 - *Google Spain κατά Costeja Gonzalez*

Στις 5 Μαρτίου 2010[97] ένας Ισπανός πολίτης, ο Mario Costeja Gonzalez, υπέβαλλε αίτηση κατά μίας ισπανικής εφημερίδας, της Google Spain SL και της Google Inc., ενώπιον της Ισπανικής Αρχής Προστασίας Προσωπικών Δεδομένων (AEPD). Ο αιτών διαμαρτυρόταν ότι οποιοσδήποτε χρήστης του διαδικτύου πληκτρολογούσε το ονοματεπώνυμό του στη μηχανή αναζήτησης της Google, θα λάμβανε ως αποτέλεσμα δύο δημοσιεύματα ισπανικής εφημερίδας σχετικά με μία διαταγή εκπλειστηριασμού του σπιτιού του. Ο αιτών ζητούσε η εφημερίδα να διαγράψει το όνομά του από τα σχετικά δημοσιεύματα και η Google να αφαιρέσει τα συγκεκριμένα προσωπικά του δεδομένα από τα αποτελέσματα που παρέχει στους χρήστες της.

Ισχυριζόταν ότι οι διαδικασίες αναγκαστικής εκτέλεσης κατά του σπιτιού του είχαν τερματισθεί οριστικά πολλά χρόνια πριν και οποιαδήποτε αναφορά σε αυτές δεν έχει καμία σχέση με το παρόν. Η Ισπανική Αρχή Προστασίας Προσωπικών Δεδομένων απέρριψε το αίτημα ως προς της ισπανική εφημερίδα, το έκανε όμως δεκτό ως προς τη Google. Σύμφωνα με την Αρχή, η εφημερίδα δεν υποχρεούνταν να ανακαλέσει τα δημοσιεύματα, καθώς τα τελευταία είχαν εκδοθεί νόμιμα κατά την ημερομηνία δημοσίευσής τους.

Αντίθετα, έκρινε ότι οι μηχανές αναζήτησης είναι επεξεργαστές προσωπικών δεδομένων και συνεπώς οι Google Spain και Google Inc. όφειλαν να προβούν σε διαγραφή προσωπικών δεδομένων, κατόπιν του αιτήματος του ενδιαφερομένου. Η Αρχή βάσισε την απόφασή της στην Οδηγία 1995/46 της ΕΕ. Κατόπιν τούτου, οι Google Spain και Google Inc. άσκησαν έφεση κατά της ανωτέρω απόφασης ενώπιον του Ισπανικού Ανώτατου Δικαστηρίου. Το τελευταίο απευθύνθηκε στο Δικαστήριο της Ευρωπαϊκής Ένωσης θέτοντας του μία σειρά από προδικαστικά ερωτήματα σχετικά με την ορθή εφαρμογή της Οδηγίας.

Τα προδικαστικά ερωτήματα αφορούσαν στο αν η Google εμπίπτει στην έννοια του επεξεργαστή δεδομένων και επίσης αν, ως μία Ευρωπαϊκή εταιρεία, εμπίπτει στις

[96] Αν και οι αποφάσεις δεν σχετίζονται τόσο με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων στη Δημόσια Διοίκηση, ωστόσο πρέπει να αναλυθούν, αφού οι περισσότερες αφορούν τα «νέα δικαιώματα» που προκύπτουν στον ΓΚΠΔ.
[97] Βλ. Ιστοσελίδα, www.homodigitalis.gr

διατάξεις της Οδηγίας. Σε περίπτωση θετικής απάντησης, ζητούνταν από το Ευρωπαϊκό Δικαστήριο να προσδιορίσει την ευθύνη της Google ως επεξεργαστή δεδομένων και να κρίνει εάν ένας πολίτης έχει το δικαίωμα να ζητήσει από την Google να διαγράψει τα προσωπικά του δεδομένα, δηλαδή δικαίωμα στη λήθη.

Το Δικαστήριο της Ευρωπαϊκής Ένωσης έκρινε ότι η Google είναι πράγματι επεξεργαστής δεδομένων, καθώς «συλλέγει προσωπικά δεδομένα, τα οποία στη συνέχεια καταγράφει, οργανώνει και αποθηκεύει στους διακομιστές της» και καθώς προσδιορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων. Το Δικαστήριο έκρινε επίσης ότι η Google Spain αποτελεί στην ουσία θυγατρική της Google Inc και συνεπώς η Google Inc. υπόκειται στην Οδηγία της ΕΕ.

Ένα από τα σημαντικότερα σημεία της απόφασης αφορά στις νομικές υποχρεώσεις που υπέχουν οι μηχανές αναζήτησης, όπως η Google, σύμφωνα με την Οδηγία. Το Δικαστήριο έκρινε σχετικά ότι οι μηχανές αναζήτησης έχουν δικαίωμα να επεξεργάζονται προσωπικά δεδομένα, όταν αυτό είναι απαραίτητο για να εξυπηρετηθεί το έννομο συμφέρον του κατόχου των δεδομένων ή τρίτων μερών.

Το δικαίωμα αυτό δεν είναι απόλυτο. Μπορεί να περιοριστεί όταν προσβάλλονται τα συμφέροντα ή τα θεμελιώδη δικαιώματα του υποκειμένου –ιδίως το δικαίωμά του στην ιδιωτική ζωή. Το Δικαστήριο υπογράμμισε ότι τα οικονομικά συμφέροντα της μηχανής αναζήτησης δεν είναι σε καμία περίπτωση αρκετά ώστε να περιορίσουν το δικαίωμα στην ιδιωτική ζωή. Το Δικαστήριο υπενθύμισε επίσης ότι το δικαίωμα στην ιδιωτική ζωή κατά κανόνα υπερέχει του δημοσίου συμφέροντος για πρόσβαση σε προσωπικά δεδομένα κάποιου μη δημοσίου προσώπου.

Το Δικαστήριο έκρινε ότι το υποκείμενο των δεδομένων έχει αναμφίβολα έννομο συμφέρον να αρνηθεί τη δημοσίευση των δεδομένων του, ακόμη και αν η δημοσίευση δεν είναι επιβλαβής για το ίδιο. Το δικαίωμά του αυτό βασίζεται στο δικαίωμά του στην ιδιωτική ζωή.

Συνεπώς, το υποκείμενο των προσωπικών δεδομένων –στη συγκεκριμένη περίπτωση ο κ. Costeja Gonzalez- δύναται να αξιώσει τη διαγραφή των δεδομένων του, αν οι πληροφορίες που δημοσιεύονται είναι «ανεπαρκείς, άσχετες ή όχι πλέον σχετικές, ή υπερβολικές σχετικά με τους σκοπούς [της επεξεργασίας] και σε συνάρτηση με το χρόνο που έχει παρέλθει». Σε αυτή την περίπτωση το υποκείμενο έχει το σχετικό

δικαίωμα, αλλά και ο κάτοχος των δεδομένων έχει την υποχρέωση να προβεί στη διαγραφή των δεδομένων. Το Δικαστήριο με αυτή του την απόφαση έκρινε ότι ο Mario Costeja Gonzalez είχε δικαίωμα να ζητήσει τη διαγραφή των δεδομένων του από την Google, ενώ η τελευταία είχε υποχρέωση να προβεί στη σχετική διαγραφή.

Αυτή η απόφαση συνεπώς αναγνώρισε το δικαίωμα στη λήθη για τα υποκείμενα των δεδομένων και ταυτόχρονα τη σχετική υποχρέωση του κατόχου των δεδομένων. Η απόφαση Google Spain κατά Costeja Gonzalez αποτελεί ορόσημο για την προστασία των προσωπικών δεδομένων σε ευρωπαϊκό, αλλά και σε παγκόσμιο επίπεδο. Η Google, η οποία αποτελεί έναν από τους μεγαλύτερους επεξεργαστές προσωπικών δεδομένων, έχει δημιουργήσει ένα σύστημα για την εύκολη και γρήγορη πρόσβαση των χρηστών της στο δικαίωμα στη λήθη.

§14.2 - *ΔΕΕ C-210/16*

Η συγκεκριμένη απόφαση[98] (ΔΕΕ C-210/16) αφορά ένας ευρέως γνωστό μέσο κοινωνικής δικτύωσης, το Facebook. Η θεματική της εν λόγω απόφασης είναι η εξής: «Από κοινού Υπεύθυνοι Επεξεργασίας το Facebook και ο διαχειριστής σελίδας στο Facebook για την επεξεργασία δεδομένων των επισκεπτών της σελίδας». Οι σελίδες (fan pages), είναι λογαριασμοί χρηστών, που μπορούν να δημιουργούνται στο facebook ή σε άλλα μέσα κοινωνικής δικτύωσης, από ιδιώτες, ή από επιχειρήσεις .Συγκεκριμένα, ο δημιουργός της σελίδας, ο οποίος έχει προηγουμένως εγγραφεί στο facebook, μπορεί να χρησιμοποιήσει την πλατφόρμα του εν λόγω μέσου κοινωνικής δικτύωσης για να προβάλει τις δραστηριότητες του στους χρήστες του facebook, καθώς και στα πρόσωπα που επισκέπτονται την σελίδα του και να διοχετεύσει κάθε είδους ανακοινώσεις στην αγορά των μέσων επικοινωνίας και της δημόσιας εκφράσεως .Οι διαχειριστές των σελίδων μπορούν να λαμβάνουν ανώνυμα στατιστικά στοιχεία, σχετικά με τους επισκέπτες των σελίδων αυτών, με την βοήθεια του εργαλείου facebook insight, το οποίο τίθεται δωρεάν στην διάθεση τους από το facebook, σύμφωνα με όρους χρήσεως, μη δυνάμενους να τροποποιηθούν .Τα στοιχεία αυτά συλλέγονται χάρη σε αναγνωριστικά αρχεία (cookies), τα οποία διαθέτουν το καθένα τον δικό του κωδικό χρήσεως, παραμένουν ενεργά επί δύο έτη και αποθηκεύονται από το facebook στον

[98] Βλ. Ιστοσελίδα, curia.europa.eu

σκληρό δίσκο του ηλεκτρονικού υπολογιστή, ή σε οποιαδήποτε άλλη συσκευή των επισκεπτών της σελίδας. Ο κωδικός χρήσεως, ο οποίος μπορεί να συσχετιστεί με τα δεδομένα συνδέσεως των εγγεγραμμένων χρηστών του facebook συλλέγεται και υποβάλλεται σε επεξεργασία κατά το άνοιγμα των σελίδων.

Το άρθρο 2 στοιχείο δ της Οδηγίας 95/46 δίνει στην έννοια ¨υπεύθυνος επεξεργασίας¨ ευρύ ορισμό, που καλύπτει κάθε φυσικό, ή νομικό πρόσωπο, δημόσια Αρχή, ή υπηρεσία, ή οποιονδήποτε άλλο φορέα, που μόνος του, ή από κοινού με άλλους καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Τόσο η Facebook Inc[99]. όσο και η Facebook Ireland συμμετέχουν στον καθορισμό των σκοπών και του τρόπου της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, συνεπώς οι δύο αυτές εταιρίες πρέπει να θεωρούνται από κοινού υπεύθυνες της εν λόγω επεξεργασίας. Στο στάδιο της συλλογής των δεδομένων προσωπικού χαρακτήρα από το Facebook προστίθεται και η ευθύνη του διαχειριστή της σελίδας. Το γεγονός ότι ο διαχειριστής της σελίδας χρησιμοποιεί την παρεχόμενη από το Facebook πλατφόρμα και επωφελείται των σχετικών υπηρεσιών (online συμπεριφορά των χρηστών, κατάρτιση προφίλ) δεν τον απαλλάσσει από τις υποχρεώσεις του όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα. Άλλωστε, αντίθετη ερμηνεία ενέχει κίνδυνο καταστρατηγήσεως των κανόνων περί προστασίας των δεδομένων προσωπικού χαρακτήρα.

[99] Βλ. ΔΕΕ C-210/16.

§14.3 - *ΔΕΕ C-25/17*

Tietosuojavaltuutettu κατά Jehovan todistajat - uskonnollinen yhdyskunta[100]:

Στις 17 Σεπτεμβρίου 2013 η Tietosuojalautakunta[101] (Φινλανδική Επιτροπή Προστασίας Δεδομένων) απαγόρευσε στη Jehovan todistajat – uskonnollinen yhdyskunta (θρησκευτική κοινότητα των μαρτύρων του Ιεχωβά στη Φινλανδία) να συλλέγει και να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο της ασκούμενης από τα μέλη της δραστηριότητας του κηρύγματος από πόρτα σε πόρτα χωρίς να τηρούνται οι νόμιμες προϋποθέσεις για την επεξεργασία των δεδομένων αυτών.

Τα μέλη της κοινότητας αυτής, στο πλαίσιο της δραστηριότητας κηρύγματος από πόρτα σε πόρτα, κρατούν σημειώσεις για τις επισκέψεις που πραγματοποιούν σε πρόσωπα άγνωστα στους ίδιους και στην εν λόγω κοινότητα. Στα συλλεγόμενα δεδομένα μπορούν να περιλαμβάνονται το όνομα και η διεύθυνση των προσώπων τα οποία προσεγγίζονται, καθώς και πληροφορίες σχετικά με τις θρησκευτικές τους πεποιθήσεις και την οικογενειακή τους κατάσταση. Τα δεδομένα συλλέγονται εν είδει υπομνηστικού σημειώματος και με σκοπό να είναι δυνατή η εύρεσή τους για μελλοντική ενδεχόμενη επίσκεψη, χωρίς τα πρόσωπα στα οποία αναφέρονται τα δεδομένα να έχουν συναινέσει ούτε να έχουν ενημερωθεί σχετικά. Η κοινότητα των μαρτύρων του Ιεχωβά και οι τοπικές δομές που εξαρτώνται από αυτή οργανώνουν και συντονίζουν την ασκούμενη από τα μέλη τους δραστηριότητα κηρύγματος από πόρτα σε πόρτα, καταρτίζοντας, μεταξύ άλλων, χάρτες βάσει των οποίων κατανέμονται οι περιοχές στα μέλη που μετέχουν στη δραστηριότητα κηρύγματος και καταγράφοντας τα μέλη αυτά και τον αριθμό των εντύπων της κοινότητας τα οποία μοίρασαν. Οι τοπικές δομές της κοινότητας των μαρτύρων του Ιεχωβά διαχειρίζονται, επίσης, κατάλογο των προσώπων που έχουν ζητήσει να μη δέχονται πλέον επισκέψεις κηρύγματος από μέλη της κοινότητας· τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται στον κατάλογο αυτό χρησιμοποιούνται από τα μέλη της κοινότητας.

Με την αίτηση προδικαστικής απόφασης το Korkein hallinto-oikeus (Ανώτατο Διοικητικό Δικαστήριο, Φινλανδία) ερωτά, κατ' ουσίαν, αν η κοινότητα υπόκειται

[100] Βλ. ΔΕΕ C-25/17.
[101] Βλ. Ιστοσελίδα, www.lawspot.gr.

στους κανόνες του ενωσιακού δικαίου προστασίας δεδομένων προσωπικού χαρακτήρα (και ειδικότερα στις διατάξεις της οδηγίας 95/46/ΕΚ), λόγω του ότι τα μέλη της, κατά την άσκηση της δραστηριότητας του κηρύγματος από πόρτα σε πόρτα, ενδέχεται να κρατήσουν σημειώσεις με το περιεχόμενο της συζήτησής τους και, ειδικότερα, σχετικές με τις θρησκευτικές πεποιθήσεις των προσώπων τα οποία επισκέφθηκαν.

Με αυτή την απόφασή του, το Δικαστήριο κρίνει, καταρχάς, ότι η δραστηριότητα κηρύγματος από πόρτα σε πόρτα την οποία ασκούν τα μέλη της κοινότητας των μαρτύρων του Ιεχωβά δεν εμπίπτει στις εξαιρέσεις που προβλέπει το ενωσιακό δίκαιο προστασίας δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, η δραστηριότητα αυτή δεν αποτελεί δραστηριότητα αποκλειστικά προσωπική ή οικιακή, στην οποία δεν εφαρμόζεται η εν λόγω νομοθεσία. Το γεγονός ότι η δραστηριότητα κηρύγματος από πόρτα σε πόρτα προστατεύεται από το θεμελιώδες δικαίωμα στην ελευθερία συνείδησης και θρησκείας, το οποίο κατοχυρώνεται στο άρθρο 10, παράγραφος 1, του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ, δεν έχει ως αποτέλεσμα να αποκτά η δραστηριότητα αυτή χαρακτήρα αποκλειστικά προσωπικό ή οικιακό, καθώς εξέρχεται από την ιδιωτική σφαίρα του μέλους θρησκευτικής κοινότητας το οποίο προβαίνει στη δραστηριότητα κηρύγματος.

§15. – Η ΠΡΟΣΤΙΘΕΜΕΝΗ ΑΞΙΑ ΤΟΥ ΓΚΠΔ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

Η εργασία «κινήθηκε» γύρω από τέσσερις βασικούς άξονες για την εκπόνησή της, αυτό:

- Του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) στο σύνολό του
- Του θεσμού του Υπεύθυνου Προστασίας Δεδομένων (DPO)
- Των δικαιωμάτων των υποκειμένων όπως διαμορφώνονται από τον ισχύον νομικό πλαίσιο
- Και της εφαρμογής των τριών παραπάνω πυλώνων στη Δημόσια Διοίκηση

Σ' αυτό το σημείο θα προσπαθήσουμε να απαριθμήσουμε τις σημαντικότατες αλλαγές[102] (προηγήθηκαν παραπάνω) που φέρνει ο Γενικός Κανονισμός Προστασίας Δεδομένων στη Δημόσια Διοίκηση.

Ορισμός του Υπεύθυνου Προστασίας Δεδομένων (ΥΠΔ)

Ο θεσμός του Υπεύθυνου Προστασίας Δεδομένων[103] είναι το σημαντικότερο στοιχείο που εισάγει ο νέος Κανονισμός 2016/679/ΕΕ. Είναι ένας θεσμός που δεν υπήρχε στην προ ισχύουσα οδηγία 95/46/ΕΚ και αποτελεί το «κλειδί» για την προστασία των δεδομένων των υποκειμένων αλλά και για την συμμόρφωση των υπευθύνων επεξεργασίας.

Ο ορισμός του ΥΠΔ είναι υποχρεωτικός σε όλους τους δημόσιους φορείς και τις δημόσιες αρχές (συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία) που επεξεργάζονται προσωπικά δεδομένα (άρθρα 37 και 38). Εξαίρεση αποτελούν τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.

[102] Το εν λόγω κεφάλαιο αποτελεί ουσιαστικά μία πρώτη «σύνοψη» της εργασίας, αφού αναλύει τα κυριότερα σημεία του ΓΚΠΔ στην Δημόσια Διοίκηση.
[103] Βλ. Κεφάλαιο 7 «Υπεύθυνος Προστασίας Δεδομένων».

Σχεδιασμός συγκεκριμένων διαδικασιών για την προστασία των προσωπικών δεδομένων.

Απαιτείται ο σχεδιασμός και η εφαρμογή συγκεκριμένων διαδικασιών που αποσκοπούν στην προστασία των προσωπικών δεδομένων. Συγκεκριμένα, η προστασία των προσωπικών δεδομένων πρέπει να διασφαλίζεται με συγκεκριμένες διαδικασίες ήδη από τον σχεδιασμό (by design), εξ ορισμού (by default). Επίσης, οι διαδικασίες αυτές οφείλουν να επικαιροποιούνται σε τακτά χρονικά διαστήματα.

Ενημέρωση της Αρχής Προστασίας Δεδομένων σε περίπτωση παραβίασης.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, πρέπει να ειδοποιηθεί η Αρχή Προστασίας Δεδομένων εντός 72 ωρών χωρίς αδικαιολόγητη καθυστέρηση. Επίσης, ενδέχεται να απαιτείται η ενημέρωση των υποκειμένων των προσωπικών δεδομένων που παραβιάστηκαν.

Σαφής ορισμός του σκοπού της επεξεργασίας προσωπικών δεδομένων.

Τα προσωπικά δεδομένα υπόκεινται σε επεξεργασία για τον σκοπό τον οποίο συλλέχθηκαν, ενώ περαιτέρω επεξεργασία για άλλο σκοπό απαιτεί την συγκατάθεση του υποκειμένου.

***Αρχή της λογοδοσία*ς**

Εισάγεται η αρχή της λογοδοσίας, σύμφωνα με την οποία οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία οφείλουν από κοινού να είναι συμμορφωμένοι με όσα προβλέπει ο κανονισμός, με τρόπο τέτοιο ώστε να μπορούν ανά πάσα στιγμή να το αποδεικνύουν. Στην περίπτωση ανάθεσης σε εξωτερικό οργανισμό (εκτελών την επεξεργασία) πρέπει να υφίσταται σύμβαση ή άλλη νομική πράξη που να εγγυάται πως ο εκτελών εφαρμόζει κατάλληλά οργανωτικά και τεχνικά μέτρα που ανταποκρίνονται στα πρότυπα του ΓΚΠΔ.

Εισαγωγή νέων δικαιωμάτων των υποκειμένων

Η αξία του Γενικού Κανονισμού Προστασίας Δεδομένων, φαίνεται φυσικά και στα δικαιώματα[104] που εισάγει ο ίδιος είτε αναφερόμαστε στη Δημόσια Διοίκηση είτε στον ιδιωτικό τομέα. Τα νέα δικαιώματα[105] τα οποία αναλύθηκαν παραπάνω είναι τα εξής:

- Δικαίωμα ενημερώσεως (γενική αρχή της διαφάνειας)
- Δικαίωμα προσβάσεως
- Δικαίωμα διορθώσεως
- Δικαίωμα διαγραφής (λήθης)
- Δικαίωμα περιορισμού της επεξεργασίας
- Δικαίωμα φορητότητας των δεδομένων
- Δικαίωμα εναντιώσεως
- Δικαίωμα στην ανθρώπινη παρέμβαση

Σημαντικότατο δικαίωμα είναι και αυτό της προστασίας των δικαιωμάτων των παιδιών, το οποίο όμως δεν συμπεριλήφθη στην εργασία.

Συνοψίζοντας, ο αντίκτυπος του ΓΚΠΔ στο δημόσιο τομέα είναι σημαντικός, καθώς αφορά την προσαρμογή ενός μεγάλου μέρους του τρόπου λειτουργίας του που αφορά την επεξεργασία προσωπικών δεδομένων. Οι αλλαγές[106] που επιβάλλει ο κανονισμός αφορούν τόσο το τεχνικό κομμάτι των διαδικασιών (π.χ. πληροφορικά συστήματα) όσο και τη δημιουργία μίας κουλτούρας που αποβλέπει στην προστασία των δεδομένων προσωπικού χαρακτήρα.

[104] Τα δικαιώματα αυτά είναι κατοχυρωμένα στο Γενικό Κανονισμό Προστασίας Δεδομένων.
[105] Φερενίκη Παναγοπούλου – Κουτναζή, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ», σελ 47-106.
[106] Βλ. Ιστοσελίδα, www.governet.gr (Η πύλη της Δημόσιας Διοίκησης).

ΣΥΜΠΕΡΑΣΜΑ

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016/ΕΕ, όπως προαναφέρθηκε, τέθηκε σε εφαρμογή στις 25 Μαΐου 2018. Τα ερωτήματα που απασχολούν σχετικά με τον εν λόγω Κανονισμό είναι τα παρακάτω: Κατά πόσο μπορεί να εφαρμοστεί ο Κανονισμός; Κατά πόσο μπορούν να συμμορφωθούν οι δημόσιες υπηρεσίες;[107] (αλλά και οι ιδιωτικές επιχειρήσεις). Πόσο χρόνο θα χρειαστούν οι πολίτες ώστε να τον ενσωματώσουν στην καθημερινότητα τους; Γνωρίζουν οι πολίτες τα δικαιώματα που προκύπτουν από τον Γενικό Κανονισμό; Είναι η Ελλάδα έτοιμη ώστε να ανταποκριθεί στις απαιτήσεις του;

Οι επιχειρήσεις μέχρι στιγμής 'προχωρούν' σε μια τυπική και σύντομη ενημέρωση για τον GDPR. Και αυτό διότι πρέπει να το κάνουν για να μην υπάρξουν κυρώσεις. Ως αποτέλεσμα αυτού, οι πολίτες να αδιαφορούν για τον Γενικό Κανονισμό και απλά να γνωρίζουν ίσως μόνο την ονομασία του, χωρίς φυσικά να έχουν αναρωτηθεί για το περιεχόμενο του. Παράλληλα όμως αναβαθμίζεται γενικότερα το προφίλ κάθε επιχείρησης που συμμορφώνεται στον κανονισμό αποδεικνύοντας με έμπρακτο τρόπο ότι σέβεται τα προσωπικά δεδομένα των πελατών της και επομένως αποκτά ένα ακόμα συγκριτικό πλεονέκτημα. Και έτσι ακριβώς εξασφαλίζει την επιχειρησιακή συνέχεια μειώνοντας τις πιθανότητες εκδήλωσης λειτουργικών κρίσεων μέσα στην επιχείρηση. Άλλωστε έχει αποδειχθεί ότι η βιωσιμότητα μιας επιχείρησης συνδέεται άμεσα με την ασφάλεια των πληροφοριακών της συστημάτων.

Η κοινωνία στο σύνολό της, ίσως να μην έχει συνειδητοποιήσει ακόμα την ύπαρξή του. Αναφερόμαστε σε ένα κείμενο τέτοιου βεληνεκούς, που από μόνο του αποτελεί βαρόμετρο για την προστασία των προσωπικών δεδομένων. Και αυτό γιατί; Διότι εισήχθη συν τοις άλλοις ο θεσμός του Υπεύθυνου Προστασίας Δεδομένων, κάτι που δεν υπήρχε στην προ ισχύουσα Οδηγία 95/46/ΕΚ. Ο Γενικός Κανονισμός, όπως τονίσθηκε σχετίζεται άμεσα με τον Υπεύθυνο Προστασίας. Κάθε Δημόσιος Φορέας, κάθε ιδιωτική επιχείρηση οφείλει να ορίσει έναν. Και εκεί ίσως υπάρχει ένα κώλυμα.

[107] Είχε προηγηθεί κριτική για τους δημόσιους φορείς για το πόσο μπορούν να εφαρμόσουν τον Κανονισμό. § 11.5 «Κριτική για την εφαρμογή του ΓΚΠΔ στους δημόσιους φορείς».

Ο θεσμός αυτός είναι καινούριος και η κοινωνία μέχρι στιγμής δεν ξέρει πώς να «συμπεριφερθεί». Άλλωστε, ανέκαθεν οτιδήποτε καινούριο, μας φαινόταν ξένο.

Το διάστημα είναι πολύ μικρό για να εξαχθούν αναλυτικά συμπεράσματα και ειδικά για κάτι τόσο σημαντικό που αφορά τα προσωπικά δεδομένα. Η Ελλάδα θα χρειαστεί χρόνο για να ενσωματώσει στην ουσία τον Κανονισμό, όπως και άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης. Μάλιστα σε κάποια κράτη-μέλη της ΕΕ αντιμετωπίζονται δυσκολίες ως προς την συμμόρφωση στο νέο ΓΚΠΔ, δεν έχει προβλεφθεί περίοδος «παράτασης» εφαρμογής ή ανοχής. Αυτή είναι μία συνειδητή επιλογή από την πλευρά των αρμόδιων οργάνων της ΕΕ, ωστόσο δεν πρέπει να παραβλέπουμε ότι πρόκειται για την σημαντικότερη νομοθετική παρέμβαση στο χώρο των προσωπικών δεδομένων τα τελευταία 20 χρόνια, οπότε η πρώτη περίοδος είναι, ουσιαστικά, περίοδος προσαρμογής.

Τέλος, οι πολίτες πρέπει να αντιληφθούν, ότι δεν πρόκειται για έναν απλό «νόμο» που θα εφαρμόζουν οι επιχειρήσεις ώστε να μην «τιμωρηθούν», αλλά για ένα κείμενο που «δημιουργήθηκε» για την ασφάλεια των προσωπικών τους δεδομένων. «Ο κανονισμός[108] θέτει νέα δεδομένα στο επιχειρείν προσπαθώντας να τυποποιήσει τις διαδικασίες προστασίας προσωπικών δεδομένων. Οι πολίτες θα πρέπει να αισθάνονται σιγουριά κάθε φορά που δίδουν τα προσωπικά τους δεδομένα ή είναι online, αξιοποιώντας τις νέες τεχνολογίες προς όφελός τους». Άλλωστε ο θεσμός του ΥΠΔ εισήχθη για να προστατεύσει τα δεδομένα των πολιτών και όχι για να λειτουργήσει ως φόβητρο και τιμωρός για δημόσιους φορείς και επιχειρήσεις.

[108] Βλ. Ιστοσελίδα, gdpr – greece.eu

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Κανονισμός (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 (Γενικός Κανονισμός για την Προστασία Δεδομένων).
- Παναγοπούλου – Κουτνατζή Φερενίκη, «Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2018», Αθήνα 2017
- Σωτηρόπουλος Βασίλης, «Υπεύθυνος Προστασίας Δεδομένων», Αθήνα 2017
- Παπαγιάννης Δονάτος, «Ευρωπαϊκό Δίκαιο», 5η έκδοση, Αθήνα 2016
- Κοτσαλής Λεωνίδας, Μενουδάκος Κωνσταντίνος, «Γενικός Κανονισμός για την Προστασία των Προσωπικών Δεδομένων (GDPR)», Αθήνα 2018
- Μαρκαντωνάτου – Σκαλτσά Ανδρομάχη, «Δημόσια Διοίκηση και Συλλογικά Όργανα», Αθήνα – Κομοτηνή 2005
- Υπουργείο Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων,σχέδιο Νόμου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα σε εφαρμογή του Κανονισμού (ΕΕ) 2016/679

Ιστοσελίδες

- www.dpa.gr (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
- www.lawspot.gr
- www.homodigitalis.gr
- www.europa.eu (Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης)
- www.curia.europa.eu (Δικαστήριο της Ευρωπαϊκής Ένωσης)
- www.gdpr-greece.eu - www.governet.gr
- www.ekdd.gr (Εθνικό Κέντρο Δημόσιας Διοίκησης και Αυτοδιοίκησης)
- www.ispatras.gr (Ιατρικός Σύλλογος Πάτρας)
- www.moh.gov.gr/articles/gdpr (Ιστοσελίδα Υπουργείου Υγείας για GDPR)