2019

Problem based training on the data protection reform package in GR and CY – TRAIN-GR-CY

769169 — TRAIN-GR-CY — REC-DATA-2016/REC-DATA-2016-01

ΠΡΟΤΥΠΟ ΚΩΔΙΚΑ ΠΡΑΚΤΙΚΗΣ

ΓΙΑ ΤΗ ΔΙΕΥΚΟΛΥΝΣΗ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ ΠΡΟΣ ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ο Κώδικας Πρακτικής δημιουργήθηκε με τη χρηματοδότηση του Προγράμματος Δικαιώματα, Ισότητα και Ιθαγένεια της Ευρωπαϊκής Ένωσης (2014-2020). Το περιεχόμενο του Κώδικα αντιπροσωπεύει αποκλειστικά τις απόψεις του συγγραφέα, ο οποίος φέρει την ευθύνη του. Η Ευρωπαϊκή Επιτροπή δεν φέρει καμία ευθύνη από τη χρήση των πληροφοριών που περιλαμβάνονται στον Κώδικα.

ΠΡΟΤΥΠΟ ΚΩΔΙΚΑ ΠΡΑΚΤΙΚΗΣ

ΓΙΑ ΤΗ ΔΙΕΥΚΟΛΥΝΣΗ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ ΠΡΟΣ ΤΟ ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Εισαγωγική σημείωση

Το παρόν Πρότυπο εκπονήθηκε για λογαριασμό του Κέντρου Ευρωπαϊκού Συνταγματικού Δικαίου – Ίδρυμα Θεμιστοκλή και Δημήτρη Τσάτσου, στο πλαίσιο του έργου 'PROBLEM BASED TRAINING ON THE DATA PROTECTION REFORM PACKAGE IN GR AND CY — TRAIN-GR-CY'.

Ήδη από τον σχεδιασμό του παραπάνω έργου είχε προβλεφθεί ως παραδοτέο ένα τέτοιο Πρότυπο Κώδικα Πρακτικής. Κατά την εκτέλεση όμως του έργου επιβεβαιώθηκε πέρα από κάθε αμφιβολία ότι η εκπόνηση Κωδίκων Πρακτικής, εν είδει χρηστικών Οδηγών, σε σχέση κάθε φορά με μια συγκεκριμένη δραστηριότητα και τις ιδιαιτερότητες που παρουσιάζει, μπορεί να διευκολύνει σε πολύ μεγάλο βαθμό την προσπάθεια συμμόρφωσης προς το πλαίσιο προστασίας των προσωπικών δεδομένων.

Διαπιστώθηκε επίσης ότι περιεχόμενο ενός τέτοιου Κώδικα ενδείκνυται να είναι αφενός – για όλες τις περιπτώσεις – η βασική ενημέρωση για το ισχύον νομικό πλαίσιο (Κανονισμός 2016/679 και εθνική νομοθεσία) και αφετέρου τα ειδικότερα κάθε φορά θέματα που πρέπει να λαμβάνονται υπόψη, μαζί με πρακτικές οδηγίες/κατευθύνσεις για την ορθή αντιμετώπιση των κυριότερων ζητημάτων που κατά περίπτωση αναφύονται λόγω των ιδιαιτεροτήτων του εκάστοτε αντικειμένου δραστηριότητας.

Όπως προαναφέρθηκε, η εκπόνηση τέτοιων Κωδίκων μπορεί να γίνεται σε σχέση κάθε φορά με μια συγκεκριμένη δραστηριότητα, οριζόντια ή κάθετα. Επομένως, μπορεί να αφορά σε μια συγκεκριμένη ομάδα επαγγελματιών, καθ' όλο το εύρος της δραστηριότητάς τους, για όλες δηλαδή τις πλευρές της που μπορεί να σχετίζονται με επεξεργασίες δεδομένων προσωπικού χαρακτήρα (π.χ. Κώδικας Πρακτικής για δικηγόρους ή συμβολαιογράφους). Θα μπορούσε επίσης να αφορά στο έργο των ίδιων των Υπευθύνων Προστασίας Δεδομένων γενικά ή ειδικότερα, των απασχολούμενων σε μια συγκεκριμένη δραστηριότητα (π.χ. Κώδικας Πρακτικής για τους Υπεύθυνους Προστασίας Δεδομένων στις ασφαλιστικές επιχειρήσεις). Μπορεί όμως ν' αφορά και μόνο σ' έναν μεγάλο οργανισμό του δημόσιου τομέα (όπου μάλιστα δεν υπάρχει και η δυνατότητα χρήσης Κώδικα Δεοντολογίας) ή σε μια πολυάνθρωπη επιχείρηση του ιδιωτικού τομέα, χωρίς ασφαλώς να αποκλείεται και η εκπόνηση τέτοιων Κωδίκων και για

μικρότερης κλίμακας χρήστες.

Το Πρότυπο Κώδικα Πρακτικής που ακολουθεί καταρτίσθηκε στο πλαίσιο του προαναφερόμενου έργου, με στόχο να αποτελέσει πρότυπο ως προς τη δομή του για την εκπόνηση διαφόρων Κωδίκων Πρακτικής, κατά τα προαναφερόμενα (στο κείμενο αναγράφονται κάθε φορά οι χρήστες για τους οποίους προορίζεται ο Κώδικας, π.χ. των Δικηγόρων ή του Οργανισμού). Το βασικό ζητούμενο ήταν η συγκρότηση μιας δομής που να μπορεί να χρησιμοποιηθεί στο σύνολο, ει δυνατόν, των περιπτώσεων. Ουσιαστικό περιεχόμενο, όπου αποσπασματικά υπάρχει, παρατίθεται μόνο για σκοπούς επεξηγηματικούς, προκειμένου δηλαδή να γίνει καλύτερα κατανοητό το αντικείμενο του αντίστοιχου πεδίου. Τα παραδείγματα συνήθως επιλέγονται από την άσκηση της δικηγορίας, ως αντικείμενο δραστηριότητας, δεδομένης της μεγαλύτερης εξοικείωσης των συμμετεχόντων στο έργο με το συγκεκριμένο αντικείμενο και της εξ αυτής ευχερέστερης κατανόησης της δομής του Προτύπου και των σκοπών που επιδιώκονται κάθε φορά.

Σε κάποια σημεία το Πρότυπο Κώδικα περιλαμβάνει ορισμένες συστάσεις καλών πρακτικών ("Συστήνεται..."), έχοντας κατά νου ότι πρόκειται συνήθως για σημεία σημαντικά σε κάθε δραστηριότητα, για τα οποία καλό είναι ένας τέτοιος Κώδικας να παρέχει συγκεκριμένες συστάσεις.

Στην εκπόνηση αυτού του Προτύπου Κώδικα Πρακτικής που ακολουθεί, συμμετείχαν όλοι οι εταίροι του έργου (Κέντρο Ευρωπαϊκού Συνταγματικού Δικαίου, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Πανεπιστήμιο Κύπρου, Εργαστήριο Νομικής Πληροφορικής της Νομικής Σχολής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, Γραφείο Επιτρόπου για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα). Ιδιαίτερη μνεία θα πρέπει να γίνει στην Επίτροπο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της Κύπρου, κυρία Ειρήνη Λοϊζίδου Νικολαΐδου, για την πολύτιμη συμβολή της όσον αφορά το Κυπριακό πλαίσιο. Στην εκπόνηση του Κώδικα συμμετείχαν ενεργά και πολλοί από τους συμμετέχοντες στο έργο, εργαζόμενοι σε τρεις επαγγελματικές ομάδες στόχους (δικαστές, δικηγόροι, Υπεύθυνοι Προστασίας Δεδομένων) από την Ελλάδα και την Κύπρο. Ιδιαίτερες ευχαριστίες πρέπει να αποδοθούν στους κκ. Ε. Βρακατσέλη, Α. Καρεκλά, Ξ. Κασάπη, Δ. Κολιό, Χ. Κότιο, Π. Μπουρλετίδου, Π. Συρίγο, Κ. Τουμπάνου και Α. Χριστοφόρου. Τη συγγραφή του Προτύπου, λαμβάνοντας υπόψη τα προσχέδια, τις προτάσεις και τις παρατηρήσεις τους,

έκανε ο δικηγόρος και μέλος του Επιστημονικού Συμβουλίου του Ιδρύματος, Παναγιώτης Περάκης.

Πέραν των ανωτέρω, για τη συγγραφή χρησιμοποιήθηκαν κείμενα σχετικά με τη συμμόρφωση στο αντικείμενο δραστηριότητας που επιλέχθηκε για την άντληση παραδειγμάτων (άσκηση δικηγορίας), όπως ιδίως το «Εγχειρίδιο (Manual) Εφαρμογής Γενικού Κανονισμού Προσωπικών Δεδομένων (GDPR) για Δικηγόρους κατά την Άσκηση του Δικηγορικού Λειτουργήματος», που εκπονήθηκε για λογαριασμό του ΔΣΑ από το Εργαστήριο Νομικής Πληροφορικής του ΕΚΠΑ (συντάκτες Λ. Μήτρου, Γ. Γιαννόπουλος, Φ. Παναγοπούλου, Α. Βαρβέρης), το σχέδιο «Κώδικα Δεοντολογίας για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από Δικηγόρους/Δικηγορικές Εταιρείες», αλλά και άλλα αντίστοιχα κείμενα (“Οδηγοί”) άλλων κρατών.

Τέλος, σημειώνεται ότι το κεφάλαιο για τους Υπεύθυνους Προστασίας Δεδομένων έχει μεγαλύτερη έκταση σε σχέση με τα υπόλοιπα, αξιοποιώντας μέρος της δουλειάς που πραγματοποίησε η αντίστοιχη ομάδα στο πλαίσιο του έργου και κρίνοντας ότι θα μπορούσε η δουλειά αυτή να είναι χρήσιμη σε κάθε περίπτωση, χωρίς βεβαίως αυτό να σημαίνει πως πρέπει πάντοτε να διατηρείται σε όλη την έκτασή του.

Πίνακας περιεχομένων

Εισαγωγική σημείωση i

Α΄ ΜΕΡΟΣ 1

Β' ΜΕΡΟΣ 2

1. Εισαγωγή 2
2. Βασικοί ορισμοί 3
3. Ειδικότεροι ορισμοί 6
4. Βασικές αρχές 7
5. Βάσεις Νομιμότητας Επεξεργασίας 12
6. Τα δικαιώματα των Υποκειμένων 15
7. Υποχρεώσεις υπευθύνων και εκτελούντων επεξεργασίες 22
8. Ειδικότερα θέματα 43
9. Κυρώσεις 44

CHECK LIST 45

Γ΄ ΜΕΡΟΣ 47

Δ΄ ΜΕΡΟΣ 49

Επισήμανση

- Ο παρών Κώδικας είναι ένας άτυπος Οδηγός, με σκοπό τη διευκόλυνση εκπλήρωσης των υποχρεώσεων που επιβάλλει το ανωτέρω νομικό πλαίσιο.
- Ο παρών Κώδικας δεν είναι Κώδικας Δεοντολογίας του άρθρου 40 του Κανονισμού 2016/679.
- Το περιεχόμενο του παρόντος Κώδικα περιλαμβάνει συγκεκριμένα μόνο σημεία, χωρίς να καλύπτει το σύνολο των θεμάτων που ρυθμίζει η νομοθεσία.
- Όπου υπάρχει ασάφεια ή αντίθεση του περιεχομένου του παρόντος Κώδικα με τις προβλέψεις της νομοθεσίας, ισχύουν οι τελευταίες.
- Η τήρηση του παρόντος Κώδικα σε καμιά περίπτωση δεν απαλλάσσει από τις υποχρεώσεις εκ του ανωτέρω Κανονισμού και της εκάστοτε εθνικής νομοθεσίας.

Α΄ ΜΕΡΟΣ

Πριν από τη θέση σε εφαρμογή του παρόντος Προτύπου

Συστήνεται

- Πριν από τη συγγραφή του Κώδικα και την οριστικοποίηση του περιεχομένου του, η αναζήτηση τυχόν άλλων αντίστοιχων Κωδίκων ή Οδηγών ή ακόμη και τυχόν υπαρχόντων Κωδίκων Δεοντολογίας, που αφορούν στην ίδια αυτή δραστηριότητα, εντός της χώρας που πρόκειται να εφαρμοστεί ο Κώδικας ή σε άλλες χώρες που εφαρμόζεται ο Κανονισμός 2016/679 (εφεξής "ο Κανονισμός"). Η αξιοποίηση της ήδη υπάρχουσας εμπειρίας και η ομοιόμορφη πρακτική διευκολύνει τη συμμόρφωση.

- Η πραγματοποίηση διαδικασίας διαβούλευσης με τους εμπλεκόμενους (π.χ. με την δικηγορική κοινότητα), με την ανάρτηση του Προτύπου Κώδικα και τη λήψη σχολίων και προτάσεων. Η ίδια διαδικασία είναι καλό να ακολουθείται και σε κάθε επικαιροποίηση του Κώδικα.

- Μετά την οριστικοποίηση του περιεχομένου του παρόντος Κώδικα και αφού προηγηθούν τα ανωτέρω, πριν από τη θέση του σε εφαρμογή και ενδεχομένως (ανάλογα αν υπάρχουν πολλές και ουσιώδεις αλλαγές), πριν από κάθε επικαιροποίησή του, η αποστολή του στην εθνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα για τυχόν σχόλια.

Β' ΜΕΡΟΣ

Κυρίως μέρος

Τα κύρια σημεία του νομικού πλαισίου και η εφαρμογή τους

1. Εισαγωγή

Από την 25η Μαΐου 2018 τέθηκε σε εφαρμογή ο Γενικός Κανονισμός Προστασίας Δεδομένων 2016/679 (εφεξής ΓΚΠΔ ή Κανονισμός). Ο Κανονισμός έχει ευρύτατο πεδίο εφαρμογής, οφείλουν δε, να συμμορφώνονται σ' αυτόν τόσο ο ιδιωτικός όσο και ο δημόσιος τομέας.

Ο Κανονισμός εφαρμόζεται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, δηλ. κάθε πληροφορίας που αναφέρεται σ' ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (εν ζωή). Ο Κανονισμός εφαρμόζεται και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης.

Όπως προαναφέρθηκε, ο παρών Κώδικας δεν εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα θανόντων. Εάν όμως, τα δεδομένα προσωπικού χαρακτήρα θανόντων μπορούν να προσδιορίσουν ή να συσχετιστούν με δεδομένα προσωπικού χαρακτήρα ταυτοποιημένων ή ταυτοποιήσιμων φυσικών προσώπων εν ζωή, τότε νοούνται και πρέπει να αντιμετωπίζονται ως δεδομένα προσωπικού χαρακτήρα των προσώπων αυτών.

Ήδη στην Ελλάδα, μετά την θέση σε εφαρμογή του Κανονισμού, ψηφίστηκε ο ν. 4624/2019, ο οποίος ρυθμίζει σημεία του Κανονισμού τα οποία είχαν αφεθεί στη διακριτική ευχέρεια του εθνικού νομοθέτη.

Έως τότε, το βασικό νομοθέτημα για την προστασία των προσωπικών δεδομένων στο πλαίσιο της ελληνικής νομοθεσίας ήταν ο ν. 2472/1997, σύμφωνα με τις διατάξεις του οποίου ιδρύθηκε και η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εφεξής "ΑΠΔΠΧ") η

οποία παρέμεινε ως η ελληνική εποπτική Αρχή για την προστασία των προσωπικών δεδομένων και κατά την έννοια του Κανονισμού.

Στην Κύπρο η αντίστοιχη βασική εθνική νομοθεσία είναι ο νόμος 125(I)/2018, ενώ εθνική Αρχή είναι ο Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα («ΕΠΔΠΧ»).

2. Βασικοί ορισμοί

Στο παραπάνω νομικό πλαίσιο οι παρακάτω όροι έχουν την ακόλουθη σημασία:

1. **«Δεδομένα προσωπικού χαρακτήρα»**: κάθε πληροφορία που αφορά (εξαρχής) ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»).

2. **«Ταυτοποιήσιμο φυσικό πρόσωπο»**: 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 (on-line) 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.

3. **«Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα»**: δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά και βιομετρικά δεδομένα που αποτελούν αντικείμενο επεξεργασίας με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία και δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό, ενώ ιδιαίτερη κατηγορία αποτελούν τα δεδομένα που αφορούν σε ποινικά αδικήματα και καταδίκες.

4. **«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.

5. **«Σύστημα αρχειοθέτησης»**: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

6. **«Αποδέκτης»**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι.

7. **«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.

8. **«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.

9. **«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.

10. «Δεδομένα που αφορούν ποινικά αδικήματα και καταδίκες»: δεδομένα που αφορούν ποινικές διώξεις, συμπεριλαμβανομένων των προκαταρκτικών εξετάσεων, ποινικές διαδικασίες, καταδίκες καθώς και μέτρα ασφαλείας.

11. «Υπεύθυνος επεξεργασίας»: 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 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.

12. «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.

13. «Τρίτος»: οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

14. «Συγκατάθεση» του υποκειμένου των δεδομένων: κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν.

15. «Ψευδωνυμοποίηση»: η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο, ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές

πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

16. «Κατάρτιση προφίλ»: 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.

17. «Παραβίαση δεδομένων προσωπικού χαρακτήρα»: η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

3. Ειδικότεροι ορισμοί

Παραθέστε τους σύμφωνα με τον νόμο ορισμούς κρίσιμων εννοιών του εκάστοτε συγκεκριμένου πεδίου στο οποίο αφορά ο Κώδικάς σας, όπως ορίζονται στο σχετικό κανονιστικό πλαίσιο. Π.χ., αν ο Κώδικας αναφέρεται στο επάγγελμα του δικηγόρου στην Ελλάδα (ισχυόντων αναλόγως κάθε φορά εφεξής των όσων αντιστοίχως προβλέπει το θεσμικό πλαίσιο της Κύπρου):

- **«Δικηγορική εταιρεία»**: η αστική επαγγελματική εταιρεία που συστήνεται μεταξύ εν ενεργεία δικηγόρων κατά τα οριζόμενα στο άρθρο 49 του ελληνικού Κώδικα Δικηγόρων.

- **«Δικηγόρος»**: το πρόσωπο που έχει αποκτήσει τη δικηγορική ιδιότητα κατά τα οριζόμενα στο άρθρο 4 του ελληνικού Κώδικα Δικηγόρων.

- **«Σύμβαση εντολής»**: η έννομη σχέση ιδιωτικού δικαίου μεταξύ

δικηγόρου/ δικηγορικής εταιρείας και εντολέα με αντικείμενο την εκπροσώπηση και υπεράσπιση του εντολέα σε κάθε δικαστήριο, αρχή ή υπηρεσία ή εξωδικαστικό θεσμό, η παροχή νομικών συμβουλών και γνωμοδοτήσεων ή η ανάληψη έργου που προβλέπεται ή επιτρέπεται από τον Κώδικα Δικηγόρων κ.λπ.

4. Βασικές αρχές

Το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων προβλέπει και επιβάλλει να γίνονται πάντα σεβαστές οι αρχές που αναφέρονται παρακάτω.

Κεντρικό γνώρισμα του θεσμικού πλαισίου είναι ότι ο κάθε υπεύθυνος επεξεργασίας, όπως και κάθε εκτελών επεξεργασία, οφείλει να είναι σε θέση ανά πάσα στιγμή να αποδεικνύει ότι κάθε επιμέρους επεξεργασία προσωπικών δεδομένων που διενεργεί γίνεται σε πλήρη συμμόρφωση με τον Κανονισμό και τις τυχόν πρόσθετες ή ειδικότερες προβλέψεις της εθνικής νομοθεσίας και ότι έχει λάβει όλα τα αναγκαία γι' αυτό μέτρα, σύμφωνα με την **αρχή της λογοδοσίας**.

Συνεπώς, επιβάλλεται η συνεχής και επιμελής καταγραφή και τεκμηρίωση κάθε ενέργειας που σχετίζεται με τη συμμόρφωση προς το νομικό πλαίσιο. Το σχετικό βάρος εν προκειμένω πέφτει στο πρόσωπο που έχει αναλάβει την παρακολούθηση της τήρησης του παρόντος Κώδικα (βλ. παρακάτω).

Με την επιφύλαξη τήρησης κάθε φορά και της επίσης θεμελιώδους **αρχής της αναλογικότητας**, η οποία, εκτός των άλλων, επιβάλλει σε κάθε περίπτωση την επιλογή του ηπιότερου για τα υποκείμενα μέσου (ήτοι, την λύση που συνεπάγεται μικρότερη απειλή για τα δικαιώματά του), οι λοιπές βασικές αρχές του νομικού πλαισίου είναι τα δεδομένα να:

- Συλλέγονται για προκαθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο προς τους σκοπούς αυτούς (**αρχή του σκοπού**).
- Υποβάλλονται σε σύννομη και θεμιτή επεξεργασία και με διαφανή

τρόπο σε σχέση με το υποκείμενο των δεδομένων (**αρχές της νομιμότητας, αντικειμενικότητας και διαφάνειας**).

- Είναι κατάλληλα, συναφή και περιορίζονται στο αναγκαίο μέτρο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία (**αρχή της ελαχιστοποίησης των δεδομένων**).

- Είναι ακριβή και όταν είναι αναγκαίο να επικαιροποιούνται πρέπει να λαμβάνονται όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας (**αρχή της ακρίβειας**).

- Διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα (**αρχή της ελάχιστης διάρκειας**).

- Υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, όπως μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων (**αρχή της ακεραιότητας και εμπιστευτικότητας**).

Παραδείγματα εφαρμογής των παραπάνω αρχών στο πλαίσιο της συγκεκριμένης δραστηριότητας:

Παρατίθενται συγκεκριμένες περιπτώσεις που σχετίζονται με την εφαρμογή των ανωτέρω αρχών στην καθημερινή πρακτική της συγκεκριμένης δραστηριότητας στην οποία αφορά ο Κώδικας. Για παράδειγμα, σε σχέση με την άσκηση της δικηγορίας:

Ως προς τη θεμιτή και νόμιμη συλλογή, την αρχή της αναλογικότητας και της ελαχιστοποίησης των δεδομένων:

- Οι Δικηγόροι/ Δικηγορικές Εταιρείες διασφαλίζουν ότι υποβάλλουν σε επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι κατάλληλα και συναφή και περιορίζονται στο αναγκαίο μέτρο

για την επίτευξη των σκοπών της - συγκεκριμένης κάθε φορά – επεξεργασίας.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες επεξεργάζονται δεδομένα προσωπικού χαρακτήρα εφόσον και στο μέτρο που η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (ιδίως) ενώπιον δικαστηρίου, διοικητικού ή πειθαρχικού οργάνου και εν γένει για την εκτέλεση και στο πλαίσιο της εντολής που έχουν λάβει από τους εντολείς/πελάτες τους. Δεν χρησιμοποιούν, επικαλούνται ή εν γένει επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, τα οποία – ανεξάρτητα από την ακρίβειά / αλήθειά τους- δεν έχουν σχέση με το αντικείμενο της δίκης ή / και της υπό χειρισμό υπόθεσης.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες μπορούν να έχουν πρόσβαση, να συλλέγουν και να επεξεργάζονται κάθε είδους προσωπικά δεδομένα τρίτου υπό την προϋπόθεση ότι τα δεδομένα αυτά προέρχονται είτε από δημόσια προσβάσιμη πηγή/αρχή είτε από νόμιμο αρχείο τηρούμενο από δικαστικές ή άλλες αρχές του δημόσιου τομέα.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες διασφαλίζουν ότι χρησιμοποιούν, επικαλούνται και εν γένει επεξεργάζονται ως αποδεικτικά μέσα δεδομένα προσωπικού χαρακτήρα, η συλλογή των οποίων έχει γίνει με νόμιμο και θεμιτό τρόπο, τηρουμένων των κανόνων, εγγυήσεων και διαδικασιών του νόμου.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες χρησιμοποιούν, επικαλούνται και εν γένει επεξεργάζονται ως αποδεικτικά μέσα δεδομένα προσωπικού

χαρακτήρα, τα οποία είναι πρόσφορα και αναγκαία για να υποστηρίξουν αξιώσεις, δικαιώματα και ισχυρισμούς των εντολέων τους.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες δεσμεύονται να μην χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα που περιέχονται σε έγγραφα, αποδεικτικά στοιχεία κ. α. που αποτελούν μέρος άλλης δικογραφίας, χωρίς την προηγούμενη ενημέρωση και συγκατάθεση των υποκειμένων των δεδομένων.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες δεσμεύονται να απέχουν από την επίκληση ή αναφορά δεδομένων προσωπικού χαρακτήρα με σκοπό τη δημιουργία [δυσμενών] εντυπώσεων για τα πρόσωπα στα οποία αυτά αναφέρονται ή για σκοπούς εντυπωσιασμού.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες δύνανται να χρησιμοποιούν, να επικαλούνται ή εν γένει να χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα, τα οποία είναι απαραίτητα για την αξιολόγηση της αξιοπιστίας των ισχυρισμών και αποδεικτικών μέσων που επικαλούνται οι διάδικοι, μάρτυρες και εν γένει οι παράγοντες της δίκης.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες δεσμεύονται να απέχουν από την χρήση, επίκληση και εν γένει επεξεργασία δεδομένων προσωπικού χαρακτήρα προσώπων που δεν αποτελούν διαδίκους/παράγοντες της δίκης ιδίως εάν πρόκειται για δεδομένα προσωπικού χαρακτήρα που ανήκουν στις ειδικές κατηγορίες του άρθρου 9 ΓΚΠΔ, αφορούν ποινικά αδικήματα και καταδίκες ή αναφέρονται σε ανηλίκους, εκτός, εάν αυτό είναι απολύτως απαραίτητο για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων και δεν υπερισχύουν τα δικαιώματα των προσώπων, τα δεδομένα των οποίων χρησιμοποιούνται για τον ως άνω σκοπό.

Ως προς την αρχή της ακρίβειας και της επικαιροποίησης των δεδομένων προσωπικού χαρακτήρα.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα, τα οποία υποβάλλουν σε επεξεργασία είναι ακριβή και όταν είναι αναγκαίο, επικαιροποιούνται.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες προνοούν, ώστε τα δεδομένα προσωπικού χαρακτήρα, και ιδίως αυτά τα οποία αφορούν ειδικές κατηγορίες δεδομένων ή ποινικά αδικήματα ή καταδίκες, η ακρίβεια, πληρότητα και επικαιροποίηση των οποίων δεν έχει διαπιστωθεί, δεν υφίστανται επεξεργασία, εκτός της αποθήκευσης. Τα δεδομένα αυτά δεν επιτρέπεται ιδίως να δημοσιοποιούνται ή να διατίθενται, διαβιβάζονται ή/και να ανακοινώνονται σε τρίτους, έως ότου διαπιστωθεί η ακρίβειά τους ή πραγματοποιηθεί η απαιτούμενη διόρθωση ή /και επικαιροποίηση.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες υιοθετούν κατάλληλα μέτρα και διαδικασίες για την εξέταση ανακριβών δεδομένων προσωπικού χαρακτήρα και την διόρθωση, διαγραφή ή επικαιροποίηση αυτών. Εφόσον πρόκειται για δεδομένα προσωπικού χαρακτήρα που αφορούν σε εντολείς τους ή προσκομιζόμενα από αυτούς, η παροχή σχετικής διαβεβαίωσης εκ μέρους των αποτελεί μία υποχρεωτική διαδικασία που καλύπτει κατ' αρχήν την αντίστοιχη υποχρέωση.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες, όταν διαπιστώσουν ή λάβουν γνώση της ανακρίβειας ή της ανάγκης επικαιροποίησης των δεδομένων προσωπικού χαρακτήρα, τα οποία επεξεργάζονται, προβαίνουν χωρίς – αδικαιολόγητη – καθυστέρηση σε όλες τις αναγκαίες ενέργειες για την άμεση διαγραφή, διόρθωση ή επικαιροποίηση των δεδομένων προσωπικού χαρακτήρα, τα οποία είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας.

Ως προς τον χρονικό περιορισμό της διατήρησης των δεδομένων προσωπικού χαρακτήρα:

- Οι Δικηγόροι/Δικηγορικές Εταιρείες διατηρούν τα δεδομένα προσωπικού χαρακτήρα υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το χρονικό διάστημα που απαιτείται για τους σκοπούς της εκάστοτε επεξεργασίας, άλλως για το διάστημα που τυχόν απαιτείται από ρητή διάταξη νόμου. Με την πάροδο του διαστήματος αυτού οι Δικηγόροι/Δικηγορικές Εταιρείες οφείλουν να προβούν στην ασφαλή διαγραφή των δεδομένων προσωπικού χαρακτήρα και καταστροφή των αντίστοιχων εγγράφων ή στην επιστροφή αυτών στα υποκείμενα των δεδομένων.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες επιτρέπεται να προβαίνουν σε περαιτέρω διατήρηση των δεδομένων προσωπικού χαρακτήρα, εφόσον αυτό/ αυτή είναι αναγκαίο/ αναγκαία για την εκπλήρωση νομικής υποχρέωσης, όπως η εκπλήρωση υποχρεώσεων από τη φορολογική νομοθεσία.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες επιτρέπεται να διατηρούν τα

δεδομένα προσωπικού χαρακτήρα και πέραν του διαστήματος που απαιτείται για την εκπλήρωση του αρχικού σκοπού επεξεργασίας για τους σκοπούς της θεμελίωσης, άσκησης και υποστήριξης νομικών αξιώσεων. Σε κάθε περίπτωση το διάστημα τήρησης δεν θα υπερβαίνει τα είκοσι (20) έτη από το χρονικό σημείο κατά το οποίο οι Δικηγόροι/ Δικηγορικές Εταιρείες θα έπρεπε να διαγράψουν τα δεδομένα λόγω της εκπλήρωσης του αρχικού σκοπού, πλην των κατωτέρω περιπτώσεων της παρ. 5.

- Οι Δικηγόροι/Δικηγορικές Εταιρείες επιτρέπεται να διατηρούν περαιτέρω τα δεδομένα προσωπικού χαρακτήρα για μεγαλύτερο χρονικό διάστημα, εφόσον τα υποκείμενα των δεδομένων έχουν δώσει τη συγκατάθεσή τους, αφού προηγουμένως έχουν ενημερωθεί.

- Η περαιτέρω διατήρηση των δεδομένων προσωπικού χαρακτήρα για χρονικό διάστημα μεγαλύτερο από αυτά που προβλέπονται στις προηγούμενες παραγράφους επιτρέπεται στους Δικηγόρους/ στις Δικηγορικές Εταιρείες, εφόσον τα δεδομένα υποβάλλονται σε επεξεργασία για στατιστικούς ή ερευνητικούς σκοπούς, υπό την προϋπόθεση ότι ανωνυμοποιούνται ή λαμβάνονται κατάλληλα και επαρκή οργανωτικά και τεχνικά μέτρα για την ασφαλή τήρησή τους.

5. Βάσεις Νομιμότητας Επεξεργασίας

Για να είναι σύννομη κάποια επεξεργασία προσωπικών δεδομένων θα πρέπει να συντρέχει έστω και μία από τις παρακάτω προϋποθέσεις:

Α. Το υποκείμενο των δεδομένων έχει συναινέσει. Για τη συγκατάθεση (συναίνεση και συγκατάθεση είναι ταυτόσημες έννοιες και μπορούν να χρησιμοποιούνται και οι δύο) ισχύουν τα εξής:

- Η συγκατάθεση του υποκειμένου των δεδομένων παρέχεται ελεύθερα, με δήλωση ή με σαφή θετική ενέργεια του υποκειμένου, εν πλήρη επιγνώσει των όρων και σκοπών της επεξεργασίας και πρέπει να είναι συγκεκριμένη και αναμφίβολη. Όταν πρόκειται για την επεξεργασία δεδομένων ειδικών κατηγοριών ή δεδομένων που αφορούν ποινικά αδικήματα και καταδίκες, η συγκατάθεση πρέπει να είναι ρητή (explicit). Η συγκατάθεση δεν αποκλείεται να παρέχεται ηλεκτρονικά ή/και με

προφορική δήλωση, με όλες όμως τις συνακόλουθες αποδεικτικές δυσχέρειες, ιδίως στην τελευταία περίπτωση.

- Η συγκατάθεση ανακαλείται ελεύθερα, η δε ανάκλησή της πρέπει να διασφαλίζεται ότι μπορεί να γίνει τουλάχιστον το ίδιο εύκολα όσο και η χορήγησή της. Το υποκείμενο των δεδομένων ενημερώνεται για το δικαίωμα ανάκλησης της συγκατάθεσης πριν από τη χορήγησή της, όπως και ότι σε περίπτωση που ανακληθεί, η επεξεργασία που πραγματοποιείται πριν από την ανάκληση παραμένει νόμιμη. Επίσης, σε περίπτωση ανάκλησης, το υποκείμενο ενημερώνεται αν δεδομένα του αποτέλεσαν αντικείμενο περαιτέρω επεξεργασίας ή αν θα υπάρξει συνέχιση της επεξεργασίας στηριζόμενη σε άλλες νομικές βάσεις, όπως είναι η εκπλήρωση νομικής υποχρέωσης ή η αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος.

Συστήνεται

- Για όλες τις περιπτώσεις που στο πλαίσιο της συγκεκριμένης δραστηριότητας ενδέχεται ως βάση επεξεργασίας να χρησιμοποιηθεί η συγκατάθεση του υποκειμένου, να προδιατυπωθούν συγκεκριμένες φόρμες συγκατάθεσης κατά περίπτωση, οι οποίες να πληρούν όλες τις προϋποθέσεις του νόμου προκειμένου ακολούθως να τίθενται στη διάθεση των υποκειμένων.

- Όταν η συγκατάθεση παρέχεται με ηλεκτρονικά μέσα, να εξασφαλίζεται σε συνεργασία με τον αρμόδιο τεχνικό η ταυτοποίηση του προσώπου που συγκατατίθεται και η αυθεντικότητα/ακεραιότητα του ηλεκτρονικού εγγράφου/δήλωσης.

- Ενόψει της αρχής της λογοδοσίας, να δημιουργηθεί και να τηρείται από τον ΥΠΔ ή το επιφορτισμένο με την παρακολούθηση της τήρησης του παρόντος Κώδικα πρόσωπο αρχείο των συγκαταθέσεων/ δηλώσεων με τρόπο, ώστε να προκύπτει αδιαμφισβήτητα και με σαφήνεια η ταυτότητα του προσώπου που συγκατατέθηκε, η ύπαρξη ενημέρωσης πριν από την παροχή της συγκατάθεσης, ο τρόπος λήψης της συγκατάθεσης και ο χρόνος παροχής αυτής.

Β. Η επεξεργασία να είναι αναγκαία για εκτέλεση σύμβασης στην οποία το υποκείμενο είναι συμβαλλόμενο μέρος.

Παράδειγμα: Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης εντολής προς τον Δικηγόρο ή τη Δικηγορική Εταιρεία, συμπεριλαμβανομένων των πράξεων επεξεργασίας που απαιτούνται. Η σύμβαση εντολής περιλαμβάνει τους όρους υπό τους οποίους πραγματοποιείται η επεξεργασία και την απαραίτητη ενημέρωση των συμβαλλομένων υποκειμένων των δεδομένων σύμφωνα με τα οριζόμενα στον ΓΚΠΔ και περιλαμβάνει ενημέρωση για τον σκοπό, τη νομική βάση της επεξεργασίας, τις κατηγορίες δεδομένων προσωπικού χαρακτήρα, τους αποδέκτες, την προβλεπόμενη ή εκτιμώμενη διάρκεια τήρησης των δεδομένων, τα δικαιώματα των προσώπων, την ενημέρωση ως προς τα ένδικα βοηθήματα και μέσα).

Γ. Η επεξεργασία είναι αναγκαία για συμμόρφωση με νόμιμη υποχρέωση του υπεύθυνου επεξεργασίας.

Παράδειγμα: Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση των Δικηγόρων και των δικηγορικών εταιρειών που υπάγονται στον παρόντα Κώδικα με τις υποχρεώσεις που επιβάλλονται από την εκάστοτε ισχύουσα νομοθεσία, ιδίως τη φορολογική νομοθεσία, τη νομοθεσία που ρυθμίζει την άσκηση του δικηγορικού λειτουργήματος και τη νομοθεσία για την καταπολέμηση της νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες,

Δ. Η επεξεργασία να απαιτείται για την διαφύλαξη ζωτικού συμφέροντος του υποκειμένου κι εκείνο αδυνατεί να δώσει τη συναίνεσή του.

Ως ζωτικό συμφέρον νοείται αυτό που είναι ουσιώδες για τη ζωή του Υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα με βάση το ζωτικό συμφέρον άλλου φυσικού προσώπου θα πρέπει να διενεργείται καταρχήν μόνο εάν είναι πρόδηλο ότι η επεξεργασία δεν μπορεί να έχει άλλη νομική βάση.

Ε. Η επεξεργασία να απαιτείται στο πλαίσιο καθήκοντος που έχει ανατεθεί στον υπεύθυνο επεξεργασίας προς υπηρέτηση δημοσίου συμφέροντος ή άσκησης δημόσιας εξουσίας.

ΣΤ. Η επεξεργασία είναι αναγκαία για τη διαφύλαξη των εννόμων συμφερόντων του υπευθύνου επεξεργασίας ή τρίτου, εκτός αν από τη σχετική στάθμιση προκύπτει ότι τα έννομα συμφέροντα του υποκειμένου είναι υπέρτερα.

Ως έννομο συμφέρον νοείται και η αναγνώριση, άσκηση και υπεράσπιση δικαιώματος ιδίως ενώπιον δικαστηρίου, διαιτητικού οργάνου, πειθαρχικού οργάνου και μηχανισμού διαμεσολάβησης.

ΠΡΟΣΟΧΗ: Τα παραπάνω ισχύουν εφόσον δεν πρόκειται για ειδικές κατηγορίες δεδομένων, των οποίων κατ' αρχήν απαγορεύεται η επεξεργασία, εκτός αν συντρέχουν κάποιες πολύ πιο αυστηρές προϋποθέσεις.

Συστήνεται

Για τις περιπτώσεις επεξεργασίας ειδικών κατηγοριών δεδομένων που συνήθως ανακύπτουν στο πλαίσιο της συγκεκριμένης δραστηριότητας να εκδοθούν από τον Υπεύθυνο Προστασίας Δεδομένων, εάν υπάρχει (βλ. παρακάτω) άλλως από το επιφορτισμένο με την παρακολούθηση της τήρησης του παρόντος Κώδικα πρόσωπο, η τυποποίηση των περιπτώσεων αυτών και η θέσπιση σχετικών διαδικασιών που θα εφαρμόζονται κάθε φορά, για κάθε επεξεργασία τέτοιων δεδομένων.

6. Τα δικαιώματα των Υποκειμένων

Τα δικαιώματα των υποκειμένων είναι τα εξής:

- **Δικαίωμα πρόσβασης και ενημέρωσης:** Το υποκείμενο των δεδομένων δικαιούται να γνωρίζει αν δεδομένα του υφίστανται επεξεργασία, με ποιο τρόπο και για ποιον σκοπό.
- **Δικαίωμα διόρθωσης - επικαιροποίησης:** Το υποκείμενο των

δεδομένων δικαιούται να ζητήσει τη διόρθωση ανακριβών / ελλιπών δεδομένων.

- **Δικαίωμα διαγραφής (δικαίωμα στη λήθη):** Το υποκείμενο των δεδομένων δικαιούται να ζητήσει τη διαγραφή εφόσον τα δεδομένα δεν είναι πλέον απαραίτητα και εφόσον η επεξεργασία δεν δικαιολογείται σύμφωνα με τον νόμο.
- **Δικαίωμα περιορισμού της επεξεργασίας.**
- **Δικαίωμα εναντίωσης στην επεξεργασία.**
- **Δικαίωμα φορητότητας.**
- **Δικαίωμα αντίθεσης σε αυτοματοποιημένηατομική λήψη αποφάσεων,** περιλαμβανομένης και της κατάρτισης προφίλ.

6.1. Ως προς το δικαίωμα ενημέρωσης:

Α. Όταν δεδομένα συλλέγονται από το υποκείμενο, ο υπεύθυνος επεξεργασίας *κατά τη λήψη τους* παρέχει στο υποκείμενο τουλάχιστον την παρακάτω πληροφόρηση:

- Την ταυτότητα και στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας.
- Τον σκοπό ή τους σκοπούς της επεξεργασίας.
- Τη νόμιμη βάση επεξεργασίας.
- Τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα που θα αποτελέσουν αντικείμενο επεξεργασίας.
- Τους αποδέκτες / κατηγορίες αποδεκτών των δεδομένων.
- Την τυχόν πρόθεση διαβίβασης των δεδομένων σε τρίτη χώρα και τις νομικές προϋποθέσεις με βάση τις οποίες μπορεί να γίνει κάτι τέτοιο.
- Τη διάρκεια τήρησης των δεδομένων.
- Τα παραπάνω δικαιώματα κάθε υποκειμένου.
- Την ύπαρξη δικαιώματος καταγγελίας στην ΑΠΔΠΧ.

- Το δικαίωμα άσκησης ενδίκων βοηθημάτων και μέσων.
- Το κατά πόσο η παροχή των δεδομένων είναι υποχρεωτική.
- Την τυχόν ύπαρξη αυτοματοποιημένης λήψης αποφάσεων για το υποκείμενο, συμπεριλαμβανομένης της τυχόν κατάρτισης προφίλ.

Β. Σε κάθε περίπτωση επεξεργασίας δεδομένων για σκοπό διαφορετικό από αυτόν που χορηγήθηκαν πρέπει προηγουμένως να ενημερώνονται τα υποκείμενα των δεδομένων.

Γ. Η ενημέρωση πρέπει να παρέχεται κατά τρόπο σαφή, κατανοητό και ευσύνοπτο, λαμβάνοντας κάθε φορά υπόψη τα ιδιαίτερα χαρακτηριστικά του υποκειμένου των δεδομένων και του πλαισίου της επεξεργασίας.

Δ. Όταν υποβάλλεται σχετικό αίτημα από υποκείμενο δεδομένων, ο υπεύθυνος επεξεργασίας, αφού επιβεβαιώσει την ταυτότητα του αιτούντος, παρέχει την αιτηθείσα ενημέρωση χωρίς καθυστέρηση και πάντως *εντός μηνός από την παραλαβή του αιτήματος*. Η εν λόγω προθεσμία μπορεί να παραταθεί, το ανώτερο, κατά δύο μήνες, εφόσον αυτό απαιτείται, ενόψει της πολυπλοκότητας του αιτήματος και του αριθμού των εκκρεμών λοιπών αιτημάτων. Στην περίπτωση αυτή το υποκείμενο των δεδομένων ενημερώνεται για την εν λόγω παράταση εντός μηνός από την παραλαβή του αιτήματος, καθώς και για τους λόγους της καθυστέρησης.

Ιδιαίτερη επιμέλεια πρέπει να καταβάλλεται προκειμένου οι αιτούμενες πληροφορίες να παρέχονται μόνο στο υποκείμενο των δεδομένων ή σε εξουσιοδοτημένο από αυτό πρόσωπο. Για τον σκοπό αυτό, απαιτείται η διαπίστωση της ταυτότητας με τον κατά περίπτωση ενδεικνυόμενο και ασφαλή τρόπο. Μη ικανοποίηση αιτήματος για ενημέρωση, εν όλω ή εν μέρει, επιτρέπεται μόνον εφόσον στην κατά τις προηγούμενες παραγράφους ενημέρωση εφόσον το υποκείμενο των δεδομένων διαθέτει ήδη τις πληροφορίες αυτές ή ο περιορισμός της πρόσβασης επιβάλλεται για/ σχετίζεται με τη θεμελίωση, άσκηση, υποστήριξη ή εκτέλεση νομικών

αξιώσεων και η ενημέρωση και η άσκηση των δικαιωμάτων αυτών θα παρέβλαπτε σοβαρά ή θα καθιστούσε αδύνατη την εκπλήρωση των σκοπών αυτών.

Σε περίπτωση αιτημάτων προδήλως αβασίμων ή υπερβολικών, επιτρέπεται η μη ικανοποίησή τους ή η επιβολή ευλόγου τέλους.

6.2. Ως προς το δικαίωμα διαγραφής

Οι υπεύθυνοι επεξεργασίας δεν υποχρεούνται να διαγράψουν τα δεδομένα, εφόσον η επεξεργασία είναι απαραίτητη:

- Για την τήρηση νομικής υποχρέωσης που επιβάλλει την επεξεργασία βάσει του ενωσιακού ή εθνικού δικαίου, όπως ιδίως στις περιπτώσεις της τήρησης της φορολογικής νομοθεσίας.

- Για σκοπούς ιστορικής ή επιστημονικής έρευνας ή στατιστικούς σκοπούς, εφόσον η διαγραφή των δεδομένων προσωπικού χαρακτήρα είναι πιθανόν να καταστήσει αδύνατη ή να εμποδίσει σε μεγάλο βαθμό την επίτευξη των εν λόγω σκοπών και εφόσον λαμβάνονται τα προβλεπόμενα στον νομοτεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων, όπως η ψευδωνυμοποίηση ή η ανωνυμοποίηση.

- Για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων του υπευθύνου επεξεργασίας ή για την απόκρουση υφιστάμενων ή δυνητικών νομικών αξιώσεων του υποκειμένου των δεδομένων ή τρίτων.

- Όταν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει ή διαβιβάσει τα δεδομένα προσωπικού χαρακτήρα, τα οποία υποχρεούται να διαγράψει, υποχρεούται, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, να ενημερώσει τους υπευθύνους επεξεργασίας και εκτελούντες επεξεργασία που επεξεργάζονται τα εν λόγω δεδομένα για το αίτημα του υποκειμένου των δεδομένων, ώστε οι τελευταίοι να προβούν με τη σειρά τους σε διαγραφή συνδέσμων ή αντίγραφων ή αναπαραγωγών των δεδομένων αυτών, με την επιφύλαξης [της ύπαρξης] άλλης νομικής βάσης που δικαιολογεί την περαιτέρω τήρησή τους.

- Ιδιαίτερη μέριμνα καταβάλλεται για την ανταπόκριση στο δικαίωμα

διαγραφής, ιδίως εάν πρόκειται για δεδομένα προσωπικού χαρακτήρα ανηλίκων, οι οποίοι επιθυμούν την διαγραφή/ ασκούν το δικαίωμα διαγραφής των εν λόγω δεδομένων.

6.3. Ως προς το δικαίωμα περιορισμού της επεξεργασίας

Τα υποκείμενα των δεδομένων έχουν δικαίωμα να ζητήσουν τον περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που τα αφορούν στις περιπτώσεις που ακολουθούν. Στις περιπτώσεις αυτές η επεξεργασία είναι δυνατή μόνο εάν το υποκείμενο έχει δώσει ρητή και ειδική συγκατάθεση για την κατ' εξαίρεση χρήση, η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, η επεξεργασία είναι απαραίτητη για την προστασία δικαιωμάτων τρίτων (φυσικών ή νομικών προσώπων) ή για λόγους σημαντικού δημόσιου συμφέροντος. Συγκεκριμένα, περιορισμός της επεξεργασίας μπορεί να ζητηθεί:

- Όταν η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων. Στην περίπτωση αυτή ο υπεύθυνος επεξεργασίας προβαίνει σε περιορισμό της επεξεργασίας για το χρονικό διάστημα που απαιτείται προκειμένου να επαληθευτεί η ακρίβεια των δεδομένων.

- Όταν η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσης τους.

- Όταν ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα για τους σκοπούς της επεξεργασίας αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

- Όταν το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 του Κανονισμού, έως ότου επαληθευτεί κατά πόσον οι νόμιμοι λόγοι για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που επικαλείται ο υπεύθυνος επεξεργασίας

υπερισχύουν έναντι των λόγων εναντίωσης που επικαλείται το υποκείμενο των δεδομένων, για το χρονικό διάστημα **που απαιτείται για την επαλήθευση.**

Συστήνεται

- Ο προκαθορισμός συγκεκριμένων διαδικασιών για τις περιπτώσεις περιορισμού της επεξεργασίας, όπως μέτρα περιορισμού και ελέγχου της πρόσβασης στα εν λόγω δεδομένα ή τήρηση αυτών σε διακριτό φορέα/αρχείο επεξεργασίας ή/και αποθήκευσης, όπως και η λήψη κάθε άλλου κατάλληλου μέτρου. Πρέπει πάντοτε να διασφαλίζεται και να γίνεται εμφανές σε όλους που υπό κανονικές συνθήκες μπορούν να αποκτούν πρόσβαση στα δεδομένα αυτά ότι πλέον τελούν υπό καθεστώς περιορισμού της επεξεργασίας.
- Η ανάθεση σε συγκεκριμένο πρόσωπο, με συγκεκριμένο τρόπο, αφενός της γνωστοποίησης του περιορισμού σε όσους τυχόν έχουν γίνει αποδέκτες των υπό περιορισμό της επεξεργασίας δεδομένων, όπως και της ανακοίνωσης στο υποκείμενο της άρσης του περιορισμού, πριν από αυτήν την άρση. Το πρόσωπο αυτό συστήνεται να είναι ο ΥΠΔ, αν υπάρχει, άλλως το πρόσωπο που έχει επιφορτισθεί με την παρακολούθηση της τήρησης του παρόντος Κώδικα.

6.4. Ως προς το δικαίωμα στη φορητότητα των δεδομένων

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και έχει παράσχει στον υπεύθυνο επεξεργασίας και να του ζητά να διαβιβάζει χωρίς αντίρρηση τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας, όταν η επεξεργασία είχε θεμελιωθεί στη συγκατάθεση του υποκειμένου ή αφορά στην εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας και διενεργείται με αυτοματοποιημένα μέσα.

Ο υπεύθυνος επεξεργασίας είτε παρέχει στο υποκείμενο τα δεδομένα προσωπικού χαρακτήρα που αιτείται, είτε τα διαβιβάζει σε άλλον υπεύθυνο

επεξεργασίας, με τη χρήση δομημένου, κοινώς χρησιμοποιούμενου και αναγνώσιμου από μηχανήματα μορφότυπου, εφόσον είναι τεχνικά εφικτό.

Το αίτημα για τη φορητότητα των δεδομένων προσωπικού χαρακτήρα δεν ικανοποιείται όταν πρόκειται για επεξεργασία που είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Σε κάθε περίπτωση, η ικανοποίηση του δικαιώματος δεν πρέπει να επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων προσώπων.

Συστήνεται

Στις παρακάτω περιπτώσεις δικαιολογείται η μη ικανοποίηση του δικαιώματος στη φορητότητα:

(*Παρατίθενται συγκεκριμένες περιπτώσεις στο πλαίσιο της συγκεκριμένης δραστηριότητας που δικαιολογείται η μη ικανοποίηση του δικαιώματος στη φορητότητα)*.

6.5. Ως προς το δικαίωμα εναντίωσης

Το υποκείμενο των δεδομένων δικαιούται να εναντιωθεί, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν, όταν αυτή βασίζεται στο άρθρο 6 παρ. 1 στοιχ. ε΄ ή στ΄ του Κανονισμού.

Ο υπεύθυνος επεξεργασίας ικανοποιεί το δικαίωμα εναντίωσης και δεν υποβάλλει πλέον τα εν λόγω δεδομένα σε επεξεργασία, εκτός εάν αποδείξει ότι συντρέχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία, οι οποίοι υπερισχύουν των συμφερόντων και των δικαιωμάτων του υποκειμένου των δεδομένων ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.

Εάν πρόκειται για επεξεργασία για σκοπούς εμπορικής προώθησης,

συμπεριλαμβανομένης της κατάρτισης προφίλ, αν σχετίζεται με απευθείας εμπορική προώθηση, το υποκείμενο δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων του.

7. Υποχρεώσεις υπευθύνων και εκτελούντων επεξεργασίες

Οι υπεύθυνοι και εκτελούντες επεξεργασίες έχουν τη γενική υποχρέωση τήρησης όλων των διατάξεων του νομικού πλαισίου, με την αυξημένη υποχρέωση λογοδοσίας που προαναφέρθηκε.

Κάποιες από τις σημαντικές υποχρεώσεις τους είναι οι ακόλουθες:

7.1. Εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων που διασφαλίζουν ότι κάθε επεξεργασία γίνεται σύμφωνα με τον Κανονισμό.

Ειδικά για την ασφάλεια: Ως ασφάλεια δεδομένων προσωπικού χαρακτήρα νοείται αφενός η εμπιστευτικότητα (απόρρητο) και αφετέρου η ακεραιότητα και διαθεσιμότητα.

Το άρθρο 32 του Κανονισμού παραθέτει ενδεικτικά ορισμένα μέτρα ασφαλείας (όπως η ψευδωνυμοποίηση και η κρυπτογράφηση), αυτά όμως πάντοτε πρέπει να λαμβάνονται με βάση τη συγκεκριμένη κάθε φορά περίπτωση.

Τα μέτρα ασφάλειας πρέπει να είναι κατάλληλα και ανάλογα των κινδύνων. Κατά τον ειδικότερο προσδιορισμό τους πρέπει να λαμβάνονται υπ' όψιν ιδίως οι τελευταίες τεχνολογικές εξελίξεις, ο αριθμός των εργαζομένων, ο όγκος εργασιών, ο αριθμός των συνεργατών και των πελατών, το κόστος εφαρμογής, η φύση και η κατηγορία των δεδομένων που υποβάλλονται σε επεξεργασία, το πλαίσιο της επεξεργασίας και οι ειδικότεροι σκοποί αυτής.

Για την αξιολόγηση των κινδύνων λαμβάνεται υπόψη ιδίως η πιθανότητα επέλευσής τους και η σοβαρότητα αυτών, κυρίως σε σχέση με τις επιπτώσεις που θα έχουν για την προστασία των προσωπικών δεδομένων και εν γένει για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

Συστήνεται

Να καταγραφούν κάποια αναγκαία μέτρα ασφαλείας και διαδικασίες για το συγκεκριμένο είδος δραστηριότητας.

Παραδείγματα:

- Παράθεση τεχνικών και οργανωτικών μέτρων για την ασφάλεια των δεδομένων και την προστασία τους ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση/ ανακοίνωση σε ή πρόσβαση από μη δικαιούμενα προς τούτο πρόσωπα.
- Δέσμευση συνεργατών με σχετικές συμβατικές ρήτρες.
- Διαβάθμιση και έλεγχος της πρόσβασης σε επεξεργασίες και αρχεία (συστήματα αρχειοθέτησης) που περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα.
- Μέτρα ασφαλούς καταστροφής των δεδομένων προσωπικού χαρακτήρα και των υλικών φορέων τους (βλ. ΑΠΔΠΧ Οδηγία 1/2005).
- Συστηματική και περιοδικά ελεγχόμενη προστασία από κακόβουλο λογισμικό, ιούς, επιθέσεις σε πληροφοριακά συστήματα, φθορά δεδομένων κ.α.
- Πολιτική φυσικής ασφάλειας των χώρων και πολιτική «καθαρού γραφείου» («κλείδωμα φακέλων», κλείδωμα υπολογιστών, προστασία εκτυπώσεων κ.α.
- Τήρηση εφεδρικών αντιγράφων ασφαλείας (back-up) σε τακτά χρονικά διαστήματα με χρήση κρυπτογράφησης.
- Πολιτικές περιορισμένης χρήσης φορητών και αφαιρούμενων συσκευών και τεχνικά μέτρα και διαδικασίες για την ορθή χρήση τους.

7.2. Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού

Η υποχρέωση αυτή κατ' αρχήν σημαίνει ότι τα κατάλληλα για την προστασία των δικαιωμάτων των υποκειμένων τεχνικά και οργανωτικά μέτρα και οι σχετικές εγγυήσεις πρέπει να λαμβάνονται εξ' αρχής από τους υπεύθυνους επεξεργασίας, ήδη από τον σχεδιασμό κάθε εφαρμογής. Μάλιστα, τα μέτρα αυτά κάθε φορά πρέπει να ανταποκρίνονται στο επίπεδο της τεχνικής εκείνης της χρονικής στιγμής ("state of the art").

Η υποχρέωση για προστασία εξ ορισμού σημαίνει ότι πρέπει από την αρχική λήψη της σχετικής απόφασης η επικείμενη επεξεργασία να περιορίζεται μόνο στα απολύτως αναγκαία δεδομένα για τους συγκεκριμένους σκοπούς.

Η εκπλήρωση αυτής της υποχρέωσης πιθανότατα μπορεί να συνεπάγεται και κάποιο κόστος. Το κόστος αυτό πρέπει να έχει προβλεφθεί στον σχετικό προϋπολογισμό του έργου. Τέλος, η υποχρέωση λογοδοσίας ισχύει και ως προς την τήρηση της συγκεκριμένης υποχρέωσης. Συνεπώς, πρέπει να παρέχεται στα υποκείμενα η δυνατότητα να ενημερωθούν για τον τρόπο εκπλήρωσής της.

7.3. Τήρηση αρχείου επεξεργασίας

Ήτοι, καταγραφή με συγκεκριμένο τρόπο, σύμφωνα με τα οριζόμενα στον Κανονισμό (άρθρο 30 ΓΚΠΔ), όλων των επεξεργασιών που λαμβάνουν χώρα. Η υποχρέωση αυτή συντρέχει όταν:

- Η διενεργούμενη επεξεργασία ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων.
- Η επεξεργασία δεν είναι περιστασιακή.
- Η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων ή επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Συστήνεται

Επειδή η τήρηση αυτού του αρχείου είναι πολύ σημαντική ως εργαλείο λογοδοσίας αλλά και γιατί αποτελεί ιδιαίτερα χρήσιμο μέσο συμμόρφωσης, η τήρηση του συγκεκριμένου αρχείου και η τακτική επικαιροποίησή του, ακόμη και αν δεν υφίσταται σχετική τυπική υποχρέωση εκ του Κανονισμού.

Το ελάχιστο περιεχόμενο του παραπάνω αρχείου επεξεργασίας περιλαμβάνει τα ακολούθα:

α) τα στοιχεία του υπευθύνου επεξεργασίας β) τους σκοπούς της επεξεργασίας

γ) την περιγραφή των κατηγοριών των υποκειμένων των δεδομένων

δ) την περιγραφή των κατηγοριών των προσωπικών δεδομένων (με ιδιαίτερη αναφορά στις ειδικές κατηγορίες και στην κατηγορία των δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα)

ε) τις κατηγορίες των (συνήθων) αποδεκτών των προσωπικών

δεδομένων, στους οποίους γνωστοποιήθηκαν/ γνωστοποιούνται συνήθως/ προβλέπεται να γνωστοποιούνται προσωπικά δεδομένα

στ) τις διαβιβάσεις σε τρίτες (εκτός ΕΕ/ΕΟΧ) χώρες ζ) τις προθεσμίες διαγραφής

η) όπου είναι δυνατόν, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας

Δεν προβλέπεται συγκεκριμένη φόρμα για το εν λόγω αρχείο (βλ. Σχετική φόρμα στην ιστοσελίδα των ΑΠΔΠΧ και ΕΠΔΠΧ).

7.4. Εκτίμηση επιπτώσεων (αντίκτυπου) της επεξεργασίας

Η διενέργεια εκτίμησης επιπτώσεων της επεξεργασίας απαιτείται όταν ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά σε ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών. Σε περιπτώσεις

υψηλού κινδύνου, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την εθνική Αρχή.

Κάθε τέτοια εκτίμηση πρέπει κατ' ελάχιστον να περιλαμβάνει:

α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας.

β) συσχέτιση με τη νομική βάση/θεμελίωση της επεξεργασίας, ιδίως εάν αυτή συνίσταται στο υπέρτερο έννομο συμφέρον.

γ) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς.

δ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

ε) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων,

περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας.

Συστήνεται

Να διενεργείται εκτίμηση αντικτύπου στις παρακάτω συνήθεις περιπτώσεις:

Παρατίθενται, εάν υπάρχουν, συγκεκριμένες περιπτώσεις στο πλαίσιο της συγκεκριμένης δραστηριότητας, για τις οποίες απαιτείται ή ενδείκνυται η διενέργεια εκτίμησης αντικτύπου.

7.5. Σύναψη συμβάσεων με εκτελούντες επεξεργασία

Ο Κανονισμός προβλέπει ως υποχρεωτική την ύπαρξη ορισμένων συμβατικών ρητρών στις συμβάσεις μεταξύ υπευθύνων και εκτελούντων επεξεργασίες.

Συστήνεται

Να καταγραφούν οι συνηθέστερες περιπτώσεις που στο πλαίσιο της συγκεκριμένης δραστηριότητας, οι υπεύθυνοι επεξεργασίας χρησιμοποιούν εκτελούντες επεξεργασία και να προδιατυπωθούν πρότυποι συμβατικοί όροι που θα ανταποκρίνονται με πληρότητα στις απαιτήσεις του Κανονισμού.

7.6. Υποχρέωση διευκόλυνσης των υποκειμένων για την άσκηση των δικαιωμάτων τους.

Συστήνεται

Να συνταχθούν έντυπα που θα διευκολύνουν τα υποκείμενα για την άσκηση των δικαιωμάτων τους (βλ. Παράρτημα).

7.7. Διορισμός Υπευθύνου Προστασίας Δεδομένων (ΥΠΔ)

Ο θεσμός του ΥΠΔ συνιστά δικλείδα ασφαλείας για τη διασφάλιση της αρχής της λογοδοσίας και η ύπαρξή του προσδίδει σαφές πλεονέκτημα στην διαδικασία συμμόρφωσης προς το νομικό πλαίσιο προστασίας των προσωπικών δεδομένων.

Ο ΥΠΔ είναι το φυσικό πρόσωπο ή νομικό πρόσωπό που διορίζεται από τον υπεύθυνο επεξεργασίας αλλά και από τον εκτελούντα την επεξεργασία, αναλαμβάνοντας τα περιγραφόμενα στον Κανονισμό καθήκοντα και αρμοδιότητες, προκειμένου να υποστηρίξει τη συμμόρφωση προς τις απαιτήσεις του Κανονισμού.

7.7.1. Υποχρεωτικός διορισμός ΥΠΔ

Ο διορισμός ΥΠΔ είναι υποχρεωτικός εάν:

α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας.

β) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή

γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών Δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες ή ποινικά αδικήματα.

Η έννοια της «*μεγάλης κλίμακας*» εξειδικεύτηκε και προσδιορίστηκε περαιτέρω από την Ομάδα Εργασίας του α 29. Παρόλο που δεν είναι δυνατόν να δοθεί ένας ακριβής αριθμός ως προς τον όγκο δεδομένων που τυγχάνουν επεξεργασίας προκειμένου να χαρακτηριστεί ως μεγάλης κλίμακας, οι ακόλουθοι παράγοντες πρέπει να λαμβάνονται υπόψη:

- Ο αριθμός των υποκειμένων - είτε απόλυτα, είτε ως ποσοστό του συνολικού πληθυσμού.
- Ο όγκος των Δεδομένων και/ή το εύρος των διαφορετικών Δεδομένων υπό επεξεργασία.
- Η Διάρκεια και μονιμότητα της επεξεργασίας.
- Η γεωγραφική έκταση της επεξεργασίας.

Παράδειγμα: χαρακτηριστικές περιπτώσεις επεξεργασίας σε μεγάλη κλίμακα είναι η επεξεργασία δεδομένων ασθενών σ' ένα νοσοκομείο, η επεξεργασία δεδομένων των πελατών μιας τράπεζας ή μιας ασφαλιστικής εταιρείας κ.λπ. Δεν είναι μεγάλη η κλίμακα της επεξεργασίας δεδομένων ασθενών από έναν ιδιώτη δικηγόρο ή έναν γιατρό.

Όσον αφορά στις έννοιες της τακτικής *και* συστηματικής παρακολούθησης, τα κατά περίπτωση στοιχεία που λαμβάνονται υπόψη, σύμφωνα πάλι με την Ομάδα Εργασίας του α 29, είναι κυρίως τα εξής:

Τακτική μπορεί να είναι η παρακολούθηση όταν:

- γίνεται διαρκώς ή σε τακτικά διαστήματα ή σε συγκεκριμένη περίοδο.
- επαναλαμβάνεται σε συγκεκριμένες στιγμές.
- συμβαίνει συνεχώς ή περιοδικά.

Συστηματική όταν λαμβάνει χώρα σύμφωνα με κάποιο σύστημα και:

- είναι προκαθορισμένη, οργανωμένη ή μεθοδική.
- γίνεται στο πλαίσιο γενικότερου σχεδίου για τη συλλογή δεδομένων.
- διενεργείται στο πλαίσιο στρατηγικής.

Παράδειγμα: περιπτώσεις τακτικής και συστηματικής παρακολούθησης δεδομένων υπάρχουν κατά την παροχή υπηρεσιών τηλεπικοινωνιών και σε δραστηριότητες μάρκετινγκ βάσει δεδομένων.

Σε περίπτωση αμφιβολίας περί της υποχρέωσης διορισμού ΥΠΔ, η Ομάδα Εργασίας του α 29 ενθαρρύνει τον οικειοθελή ορισμό ΥΠΔ.

Συστήνεται

(Ανάλογα με την περίπτωση) Στο πλαίσιο της συγκεκριμένης δραστηριότητας συστήνεται ή δεν συστήνεται ο ορισμός ΥΠΔ.

ΠΡΟΣΟΧΗ: Όταν διοριστεί ΥΠΔ οικειοθελώς, και πάλι αναλαμβάνει όλα τα καθήκοντα και τις υποχρεώσεις που θα είχε αν ήταν υποχρεωτικός ο διορισμός του.

ΠΡΟΣΟΧΗ: Η υποχρέωση διορισμού ΥΠΔ δεν είναι στατική ούτε εξετάζεται άπαξ: η τυχόν ανάληψη νέων δραστηριοτήτων ή ακόμη και στο πλαίσιο της ίδιας δραστηριότητας, η διενέργεια νέων επεξεργασιών, η χρήση νέων δεδομένων, η επέκταση της κλίμακας επεξεργασίας και άλλοι λόγοι μπορεί να καταστήσουν υποχρεωτικό τον διορισμό ΥΠΔ.

Εάν υπάρχει ΥΠΔ σε προαιρετική βάση, τυχόν τέτοια αλλαγή θα πρέπει να καταγραφεί και να γίνει σχετική μνεία ότι ο αρχικά οικειοθελής

διορισμός έχει πλέον καταστεί υποχρεωτικός.

7.7.2. Ιδιότητες και διαδικασία διορισμού

Ο ΥΠΔ μπορεί να είναι είτε εσωτερικός υπάλληλος, είτε εξωτερικός συνεργάτης, είτε εσωτερικός που υποστηρίζεται από εξωτερικό συνεργάτη. Η επιλογή εξαρτάται από διάφορους παράγοντες, όπως για παράδειγμα από τη φύση των δραστηριοτήτων επεξεργασίας, το μέγεθος του οργανισμού, τις ανάγκες υποστήριξης από τον ΥΠΔ αλλά και από οικονομικούς παράγοντες.

Ο ΥΠΔ παρέχει τις υπηρεσίες του βάσει σύμβασης παροχής υπηρεσιών (φυσικό ή νομικό πρόσωπο). Εφόσον πρόκειται για συνεργάτη ή μέλος του προσωπικού λαμβάνεται πρόνοια ώστε τα καθήκοντα του ΥΠΔ να μην είναι ασυμβίβαστα με τα άλλα καθήκοντα που του έχουν ανατεθεί.

Ο ορισμός του γίνεται εγγράφως, με σύμβαση ή με εσωτερική απόφαση. Στη σχετική πράξη ορισμού προσδιορίζεται η θέση, τα καθήκοντα και ο τρόπος άσκησής τους από τον ΥΠΔ. Ο ορισμός γίνεται για ορισμένο χρονικό διάστημα και μπορεί να ανανεώνεται. Ανάκληση του ορισμού ή παύση του ΥΠΔ επιτρέπεται μόνο εάν συντρέχει σοβαρός λόγος και σε καμία περίπτωση δεν επιτρέπεται επειδή ο Υπεύθυνος Προστασίας Δεδομένων επιτέλεσε τα καθήκοντά του.

Ο Υπεύθυνος Προστασίας Δεδομένων δεν λαμβάνει εντολές αναφορικά με την άσκηση των καθηκόντων του. Δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε (*ορθά και με συνέπεια*) τα καθήκοντά του.

Ο διορισμός ΥΠΔ ανακοινώνεται στην εθνική Αρχή, καθώς και στο κοινό, με δημόσια ανακοίνωση στην οποία ανακοινώνονται και τα στοιχεία επικοινωνίας μαζί του.

Τα ακόλουθα πρόσωπα δεν πρέπει να διορίζονται ΥΠΔ:

- Διοικητικά στελέχη, όπως ο διευθύνων σύμβουλος και ο οικονομικός διευθυντής *(να καταγραφούν περιπτώσεις)*.

- Οι διευθυντές των τμημάτων ανθρώπινου δυναμικού, πληροφορικής και μάρκετινγκ.
- Τυχόν άλλοι υπάλληλοι που δύνανται να καθορίζουν νέους σκοπούς επεξεργασίας και τα μέσα αυτής.

Όμιλος επιχειρήσεων μπορεί να διορίσει έναν μόνο ΥΠΔ, υπό την προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων.

7.7.3. Κριτήρια Επιλογής ΥΠΔ

Ο Κανονισμός είναι λακωνικός ως προς τα κριτήρια επιλογής του ΥΠΔ: αναφέρει στο άρθρο 37 παρ. 5 αυτού ότι «*Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39*».

Σύμφωνα με την Ομάδα Εργασίας του α 29, το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία.

Σε κάθε περίπτωση, ο ΥΠΔ θα πρέπει να διαθέτει τα ακόλουθα χαρακτηριστικά: Εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του Κανονισμού, γνώση των πράξεων επεξεργασίας που διενεργούνται, γνώση του τομέα των τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων, γνώση του τομέα δραστηριότητας και του οργανισμού, ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού. Επίσης, ο ΥΠΔ πρέπει να έχει την ευχέρεια (ως δυνατότητα που του δίνεται αλλά και ως υποχρέωση δική του) εύκολη και τακτικής πρόσβασης σε κάθε εγκατάσταση του οργανισμού που

πραγματοποιείται επεξεργασία προσωπικών δεδομένων.

Η έννοια αυτή της προσβασιμότητας ισχύει και ως προς αυτόν, ως προς τη δυνατότητα ευχερούς πρόσβασης στον ΥΠΔ από τα υποκείμενα και την εποπτική Αρχή.

Τυπικά ο ΥΠΔ δεν απαιτείται να είναι νομικός. Ωστόσο, πρέπει να ληφθεί υπόψη ότι ο Κανονισμός είναι ένα νομικό κείμενο που έχει γραφεί από νομικούς, στο πλαίσιο του οποίου τίθενται ζητήματα ερμηνείας και εφαρμογής στα οποία είναι δύσκολο να ανταποκριθεί ένας μη νομικός. Βεβαίως, αν και η άριστη γνώση του Κανονισμού είναι αναγκαία προϋπόθεση, δεν είναι από μόνη της επαρκής για να δικαιολογήσει την επιλογή του ΥΠΔ, ιδίως σε περιπτώσεις όπου ο οργανισμός διενεργεί επεξεργασία ιδιαίτερης φύσης δεδομένων, με τα οποία ο ΥΠΔ δεν έχει γνωσιολογική επαφή.

Παράδειγμα: Δικηγόρος με πολυετή εμπειρία στο δίκαιο προσωπικών δεδομένων βρίσκεται σε συζητήσεις με μεγάλη εταιρεία digital marketing για τη θέση του ΥΠΔ. Ωστόσο, ο ανωτέρω δικηγόρος δεν διαθέτει καθόλου εμπειρία σε θέματα ηλεκτρονικών υπολογιστών και διαδικτύου. Στην περίπτωση που αποφασίσει να λάβει το ρόλο του ΥΠΔ, θα πρέπει να εξοικειωθεί με τα θέματα του digital marketing, τις ιδιαίτερες δραστηριότητες επεξεργασίας της αγοράς και να υποστηρίζεται από τα στελέχη του οργανισμού.

Η Ευρωπαϊκή Ένωση ήδη από το 2010 είχε θέσει βέλτιστες πρακτικές για την επιλογή των ΥΠΔ των οργανισμών της (σημειώνεται ότι για την επεξεργασία προσωπικών δεδομένων από οργανισμούς της Ένωσης υπάρχει εδώ και χρόνια ο Κανονισμός (ΕΕ) 45/2001). Αντίστοιχες προϋποθέσεις θα πρέπει αναλογικά να τεθούν και για τους ΥΠΔ δημοσίων Αρχών και φορέων αλλά και εμπορικών επιχειρήσεων.

Συστήνεται

Ο ΥΠΔ να πληροί τις εξής προϋποθέσεις:

- Άριστη γνώση του Κανονισμού, της εθνικής νομοθεσίας προσωπικών δεδομένων και των αποφάσεων των εποπτικών Αρχών, καθώς και κατανόηση σε θέματα τεχνολογίας πληροφοριών και ασφάλειας πληροφοριών.
- Καλή κατανόηση της λειτουργίας του συγκεκριμένου κάθε φορά οργανισμού, και των δραστηριοτήτων επεξεργασίας αυτού, καθώς και γνώση του ειδικότερου τυχόν κανονιστικού πλαισίου που διέπει τη λειτουργία του.
- Δυνατότητα τακτικής επί τόπου επίσκεψης στους χώρους που εκτελούνται επεξεργασίες.
- Δυνατότητα συνεχούς προσβασιμότητας σ᾽ αυτόν από τα υποκείμενα (στην οποία συμπεριλαμβάνεται και η γλώσσα επικοινωνίας) και επικοινωνίας του με την εθνική εποπτική Αρχή.

ΠΡΟΣΟΧΗ: Δεν προβλέπεται πιστοποίηση ΥΠΔ, απαίτηση δε τέτοιας ως αναγκαίου προσόντος για την πλήρωση θέσης ΥΠΔ σε δημόσιο φορέα κρίθηκε παράνομη σε χώρα της ΕΕ.

7.7.4. Αρμοδιότητες και υποχρεώσεις του ΥΠΔ

Οι αρμοδιότητες του ΥΠΔ ορίζονται ρητά στο άρθρο 39 του Κανονισμού. Ειδικότερα, ο ΥΠΔ έχει τα ακόλουθα καθήκοντα:

- Να ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων.
- Να παρακολουθεί τη συμμόρφωση με τον Κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία

δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων.

- Να παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35 του Κανονισμού.

- Να συνεργάζεται με την εποπτική Αρχή.

- Να ενεργεί ως σημείο επικοινωνίας για την εποπτική Αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36 του Κανονισμού και να πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Ο ΥΠΔ ωστόσο, μπορεί να κληθεί (και σκόπιμο είναι να αναλάβει) να διεκπεραιώσει και άλλες υποχρεώσεις του οργανισμού που απορρέουν από τον Κανονισμό, όπως χαρακτηριστικά η τήρηση του αρχείου δραστηριοτήτων και ο σχεδιασμός της εσωτερικής πολιτικής για την επικαιροποίησή του, όταν προστίθενται νέες δραστηριότητες επεξεργασίας, ο συντονισμός των ενεργειών για τη δημιουργία πολιτικών ασφάλειας δεδομένων, πολιτικών επιχειρησιακής συνέχειας, πολιτικών απορρήτου, ειδικού σχεδίου διαχείρισης περιστατικών διαρροής ή παραβίασης και η τήρηση πρωτοκόλλου αιτημάτων των υποκειμένων.

Ο ΥΠΔ έχει ρόλο συμβουλευτικό και όχι αποφασιστικό: εναπόκειται στην διοίκηση του οργανισμού να λάβει τις αποφάσεις σχετικά με τις προτεινόμενες από τον ΥΠΔ ενέργειες.

Ο ΥΠΔ έχει πρόσβαση σε όλα τα αρχεία, ηλεκτρονικά και χειρόγραφα και σε όλα τα συστήματα που σχετίζονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

7.7.5. Δράση του ΥΠΔ εντός του οργανισμού

Όσον αφορά τη δράση του ΥΠΔ εντός του οργανισμού, το άρθρο 38 του Κανονισμού επιβάλει ορισμένες υποχρεώσεις προς τους οργανισμούς ως προς τη θέση και την ανεξαρτησία του ΥΠΔ. Ειδικότερα, οι οργανισμοί:

- Διασφαλίζουν ότι ο ΥΠΔ συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.

- Στηρίζουν τον ΥΠΔ στην άσκηση των καθηκόντων που αναφέρονται στο άρθρο 39, παρέχοντας απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του.

- Διασφαλίζουν ότι ο ΥΠΔ δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων, δεν απολύεται ούτε υφίσταται κυρώσεις από τον οργανισμό επειδή επιτέλεσε τα καθήκοντά του.

- Ο ΥΠΔ λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του Οργανισμού.

- Ο Οργανισμός υποχρεούται να δημιουργήσει κατάλληλες δομές και δίαυλο επικοινωνίας των υποκειμένων με τον ΥΠΔ κι εκείνος υποχρεούται να ανταποκρίνεται στα αιτήματά τους.

Τέλος, μεγάλη σημασία έχει ότι σύμφωνα με το άρθρο 38 παρ. 5, «*Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους*». Ο ΥΠΔ οφείλει να διατηρεί εμπιστευτικά όλα τα στοιχεία και τις πληροφορίες που διαθέτει κατά την εκτέλεση των αρμοδιοτήτων του. Αυτή η υποχρέωση δεν αποκλείεται να εκτείνεται και απέναντι στη διοίκηση του Οργανισμού. Ο ΥΠΔ οφείλει να μην ανακοινώνει ή αποκαλύπτει σε οποιονδήποτε τρίτο γεγονότα ή πληροφορίες που περιήλθαν σε γνώση

του από τη θέση του κατά την εκτέλεση των καθηκόντων του ή επ' ευκαιρία αυτών, όπως και να τηρεί γενικά απόλυτη εμπιστευτικότητα σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με την ισχύουσα νομοθεσία. Οι υποχρεώσεις αυτές υφίστανται και ύστερα από το πέρας του ορισμού του ως ΥΠΔ. Τυχόν ειδικότερες υποχρεώσεις εχεμύθειας επιβάλλονται/προβλέπονται στην πράξη ορισμού του.

7.7.6. Ενέργειες του ΥΠΔ – Βασικός Οδηγός

Α. Η πρώτη ερώτηση που θα πρέπει να απασχολήσει τον νέο ΥΠΔ είναι για ποιες δραστηριότητες επεξεργασίας ο οργανισμός δρα ως υπεύθυνος επεξεργασίας και για ποιες ως εκτελών την επεξεργασία. Η διάκριση είναι σημαντική για πολλούς λόγους, ο βασικός εκ των οποίων είναι η αντιμετώπιση των υποχρεώσεων του οργανισμού απέναντι στους αντισυμβαλλομένους του που απορρέουν από το άρθρο 28 του Κανονισμού.

Β. Η φύση των δραστηριοτήτων επεξεργασίας θα καθορίσει σε μεγάλο βαθμό και τις αρμοδιότητες του ΥΠΔ.

Γ. Επιπλέον, σκόπιμο είναι ο ΥΠΔ να γνωρίζει εκ των προτέρων τι κατηγορίες δεδομένων επεξεργάζεται ο οργανισμός, π.χ. οικονομικά δεδομένα, ιατρικά δεδομένα, δεδομένα μόνο εργαζομένων του οργανισμού ή και καταναλωτών.

Δ. Ο ΥΠΔ και ο εργοδότης του καλό είναι να συμφωνήσουν εκ των προτέρων για τυχόν άλλες αρμοδιότητες του ΥΠΔ, κατά τα προβλεπόμενα στο άρθρο 38 παρ. 6 του Κανονισμού: «Ο υπεύθυνος προστασίας δεδομένων μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων». Ενδεχομένως, τα «άλλα καθήκοντα» να μη συνεπάγονται σύγκρουση συμφερόντων, ωστόσο μπορεί να αποτρέπουν τον ΥΠΔ να εκτελεί τα καθήκοντά του εντός του οργανισμού.

Ε. Ο ΥΠΔ που τελικά αποφασίζει να αναλάβει τα καθήκοντα στον

οργανισμό πρέπει με ταχύτητα να ενημερωθεί για την υφιστάμενη κατάσταση και να εξοικειωθεί με τον χώρο, το προσωπικό και τον οργανισμό εν γένει.

ΣΤ. Ο ιδανικός σύμβουλος για τον νέο ΥΠΔ είναι ο προηγούμενος, αν υπήρχε. Ανεξάρτητα από τους λόγους αποχώρησής του, ο παλαιός ΥΠΔ είναι ουσιαστικά ο μόνος που γνωρίζει το επίπεδο συμμόρφωσης του οργανισμού, τις ελλείψεις και τις εκκρεμότητες. Ο νέος ΥΠΔ θα πρέπει να προσπαθήσει να έρθει σε επαφή με τον προκάτοχό του και για λόγους σχετικούς με τον οργανισμό εσωτερικά: από ποιον μπορεί να περιμένει βοήθεια, κατά πόσο ο ΥΠΔ αντιμετωπίζεται σαν περιττό βάρος και τροχοπέδη στο επιχειρείν ή αν μπορεί να προσδοκά αγαστή συνεργασία με τα τμήματα και τις μονάδες του Οργανισμού.

Ζ. Έλεγχος προγενέστερων εργασιών συμμόρφωσης. Ο νέος ΥΠΔ θα πρέπει να εξετάσει τις τυχόν ήδη διενεργηθείσες εργασίες και να φροντίσει για τη συμπλήρωση, επικαιροποίηση ή/και αναθεώρησή τους.

Η. Θα πρέπει να εξεταστεί από τον ΥΠΔ η τήρηση των πολιτικών του οργανισμού για το απόρρητο των προσωπικών δεδομένων και την ασφάλεια αλλά και το επίπεδο υλοποίησης των απαραίτητων ενεργειών, τόσο σε επίπεδο ηλεκτρονικών μέσων (π.χ. cyber security), όσο και σε επίπεδο φυσικής ασφάλειας (π.χ. χώροι προσβάσιμοι σε επισκέπτες, έλεγχοι φυσικής εισόδου σε χώρους εργασίας, βιντεοσκόπηση χώρων και εξοπλισμού).

Θ. Έλεγχος εκκρεμοτήτων ενώπιον της Αρχής και των Υποκειμένων. Από τη στιγμή της ενημέρωσης της Αρχής για την ανάθεση του ρόλου στον νέο πλέον ΥΠΔ, εκείνος θα βρεθεί αντιμέτωπος με όλα τα ζητήματα που ανακύπτουν από τον Κανονισμό. Μεταξύ άλλων, προβλήματα που μπορεί να αντιμετωπίσει ο νέος ΥΠΔ στα νέα του καθήκοντα είναι εκκρεμούσες ήδη υποθέσεις ενώπιον της Αρχής και υποβληθέντα αιτήματα των υποκειμένων για την άσκηση δικαιωμάτων τους. Τυχόν αιτήματα των υποκειμένων ως απόρροια άσκησης των δικαιωμάτων τους υπό τον Κανονισμό πρέπει να ικανοποιούνται στα χρονικά όρια που

προβλέπει κατά κανόνα ο Κανονισμός (καταρχήν τριάντα ημέρες). Ο ΥΠΔ θα πρέπει να εξετάσει τα ήδη υπάρχοντα αιτήματα, να τα χειριστεί με προτεραιότητα ανάλογα με τη δυσκολία τους και να επικοινωνήσει, εάν είναι απαραίτητο, με άλλα τμήματα του οργανισμού ώστε να τα εξυπηρετήσει: δεν πρέπει να παραβλέπεται ότι, μαζί με υπάρχοντα αιτήματα, βέβαιο είναι ότι θα υπάρξουν και νέα, όπως επίσης και πως η δυσκολία εκπλήρωσης των δικαιωμάτων, θα πρέπει να είναι βασικό κριτήριο ιεράρχησης από τον ΥΠΔ.

I. Συναντήσεις με υπευθύνους τμημάτων του Οργανισμού, εσωτερική διαβούλευση. Μόλις ο ΥΠΔ ολοκληρώσει τις ενέργειες που παρουσιάζονται ανωτέρω, σκόπιμο είναι να προχωρήσει σε εσωτερικές συναντήσεις με τους επικεφαλής των διαφόρων τμημάτων που διενεργούν επεξεργασία δεδομένων. Σε περιπτώσεις οργανισμών που απευθύνονται στη δράση τους σε φυσικά πρόσωπα π.χ. ασφαλιστικές εταιρείες, νοσοκομεία κ.α. πρώτο μέλημα θα μπορούσε να είναι η επικοινωνία με τους διευθυντές των εμπορικών τμημάτων, του τμήματος πωλήσεων, της εξυπηρέτησης πελατών κοκ., ώστε να εξεταστούν τα υπάρχοντα ζητήματα που ο ΥΠΔ διέγνωσε κατά τις πρώτες του μέρες στον οργανισμό. Εάν από την άλλη, ο οργανισμός δεν έχει συναλλαγές με φυσικά πρόσωπα, προτεραιότητα θα πρέπει να δοθεί σε θέματα ανθρωπίνου δυναμικού.

7.7.7. Δημιουργία κουλτούρας προστασίας δεδομένων

Οι υποχρεώσεις του ΥΠΔ είναι διττής φύσης: ο ΥΠΔ αφενός καλείται να καθοδηγήσει τον οργανισμό για τη σύμφωνη με τον Κανονισμό και τη σχετική νομοθεσία λειτουργία του κατά την επεξεργασία δεδομένων και αφετέρου να συντονίσει την ανάπτυξη κουλτούρας προστασίας των δεδομένων εντός του οργανισμού.

Ο ΥΠΔ θα είναι εκείνος που θα πρέπει να εμφυσήσει στο προσωπικό του Οργανισμού το αίσθημα ότι η προστασία των δεδομένων είναι μία πολύ σημαντική υπόθεση, κρίσιμη για το συνολικότερο συμφέρον του οργανισμού αλλά και ευρύτερα. Θα πρέπει να αναδείξει τους λόγους για

τους οποίους ο κάθε μεμονωμένος εργαζόμενος θα πρέπει να επιδείξει προσοχή στα δεδομένα που επεξεργάζεται απέναντι στον κίνδυνο απώλειας και αλλοίωσης, αναπτύσσοντας συνείδηση ατομικής ευθύνης στον καθένα προσωπικά.

Η ανωτέρω υποχρέωση του ΥΠΔ μπορεί να επιτευχθεί μέσα από τακτικές εκπαιδευτικές εκδηλώσεις: ο ίδιος ο ΥΠΔ μπορεί να διοργανώνει σεμινάρια και να εκπαιδεύει το προσωπικό, ιδίως σε μικρούς και ολιγάριθμους οργανισμούς. Αντίστοιχα σε μεγαλύτερους οργανισμούς, ο ΥΠΔ μπορεί να εκπαιδεύσει ή να φροντίσει για την εκπαίδευση επιλεγμένων στελεχών, π.χ. της διεύθυνσης ανθρωπίνου δυναμικού, οι οποίοι με τη σειρά τους θα αναλάβουν την επιμόρφωση των κατώτερων υπαλλήλων καθώς και των νέων εργαζομένων.

Η εκπαίδευση πρέπει να ξεκινά με τους νεοπροσλαμβανόμενους, οι οποίοι είναι δυνατό να ευαισθητοποιηθούν ευκολότερα και να υιοθετήσουν τις πολιτικές άμεσα και να συνεχίζει σε ετήσια βάση με το διαχωρισμό ομάδων με κοινό ενδιαφέρον και διαχείριση πελατών ή συναδέλφων, έως ότου καλυφθεί το σύνολο του Οργανισμού.

7.7.8. Επιμόρφωση και κατάρτιση ΥΠΔ

Η συνεχής επιμόρφωση και κατάρτιση του ΥΠΔ και των στελεχών που τον υποστηρίζουν στα καθήκοντά του είναι προϋπόθεση για να ανταποκριθεί στα καθήκοντά του. Το δίκαιο των προσωπικών δεδομένων είναι δυναμικό και βαίνει συνεχώς εξελισσόμενο: πρώτος από όλους, ο ίδιος ο ΥΠΔ θα πρέπει να επιδείξει μέγιστο ενδιαφέρον για τη συνεχιζόμενη κατάρτιση και επιμόρφωσή του. Ο οργανισμός οφείλει να στηρίζει υλικά την εκπαίδευση του ΥΠΔ, παρέχοντας στον ΥΠΔ πόρους για την διατήρηση της εμπειρογνωσίας του (άρθρο 38 παρ. 2 ΓΚΠΔ).

Παράλληλα, ο ΥΠΔ θα πρέπει να επιδείξει μέριμνα για την κατάρτισή του σε ζητήματα του κλάδου δραστηριότητας του οργανισμού του: σε περίπτωση θεσμικών αλλαγών π.χ. στο εργατικό δίκαιο, ο ΥΠΔ, είτε μόνος του είτε σε συνεργασία με τους νομικούς συμβούλους του οργανισμού, οφείλει να παρακολουθήσει τις εξελίξεις, ώστε να είναι σε θέση να εξετάσει

τις επιπτώσεις στις τυχόν σχετιζόμενες επεξεργασίες δεδομένων.

7.7.9. Συνοψίζοντας

- Ο ΥΠΔ εργάζεται με ανεξαρτησία και με γνώμονα την προστασία των προσωπικών δεδομένων, ακόμα και αν η άποψή του έρχεται σε αντίθεση με τη θέση του οργανισμού.
- Ο ΥΠΔ συμβουλεύει με τον καλύτερο δυνατό τρόπο για τα ζητήματα προσωπικών δεδομένων, με αντικειμενικότητα, τεκμηρίωση και διαφάνεια.
- Η επαγγελματική ευσυνειδησία του συνετού επαγγελματία επιτάσσει τη μη ανάληψη του ρόλου του ΥΠΔ, εφόσον δεν κρίνει ο ίδιος ότι πληροί τις απαραίτητες προϋποθέσεις.
- Ο ΥΠΔ φροντίζει για την επιμόρφωσή του και τη συνεχή του εκπαίδευση στο δίκαιο προσωπικών δεδομένων και την ασφάλεια πληροφοριών, παρακολουθώντας τις τεχνολογικές και λοιπές εξελίξεις στον κλάδο.
- Ο ΥΠΔ εμπλέκεται ενεργά σε κάθε ζήτημα που αφορά σε προσωπικά δεδομένα.
- Η ανάπτυξη κουλτούρας προσωπικών δεδομένων στον οργανισμό με κάθε πρόσφορο μέσο, είναι βασικό μέλημα του ΥΠΔ.
- Για τις ανάγκες της εκπλήρωσης των υποχρεώσεών του, ο ΥΠΔ ζητά από τον οργανισμό τους απαραίτητους πόρους, όπως χρόνο, υποδομή, κονδύλια και συνεργάτες.
- Ο ΥΠΔ οφείλει να λαμβάνει γνώση για το σύνολο των επεξεργασιών προσωπικών δεδομένων που κάνει ο οργανισμός από τον αρμόδιο Διευθυντή ή την Διοίκηση.
- Πριν πραγματοποιηθούν αλλαγές στην επεξεργασία δεδομένων και στην εισαγωγή νέων δραστηριοτήτων επεξεργασίας, ο ΥΠΔ συμβουλεύει τον οργανισμό για την εξ ορισμού και από το σχεδιασμό προστασία.

- Ο ΥΠΔ είναι εύκολα προσβάσιμος στα υποκείμενα, εντός και εκτός του οργανισμού, ενώ τα στοιχεία επικοινωνίας του είναι δημοσίως διαθέσιμα.

- Γίνεται τακτική ενημέρωση της διοίκησης του οργανισμού εκ μέρους του ΥΠΔ. *Στην προκειμένη περίπτωση συνιστάται η σύνταξη από τον ΥΠΔ….(π.χ. ετήσιων) εκθέσεων πεπραγμένων, ήτοι, (τον Ιανουάριο κάθε έτους για το προηγούμενο)*.

- Ο ΥΠΔ φροντίζει για τη διενέργεια τακτικών εσωτερικών ελέγχων για να εξασφαλίσει την τήρηση των βασικών αρχών και των υποχρεώσεων του Κανονισμού εντός του οργανισμού. *Στην προκειμένη περίπτωση τακτικοί έλεγχοι πρέπει να διενεργούνται κάθε π.χ. έξι (6) μήνες*.

- Στην αρχή κάθε έτους, ο ΥΠΔ προετοιμάζει σχέδιο δράσεων για τον επόμενο χρόνο, σύμφωνα με τις ανάγκες του οργανισμού, υποβάλλοντας τυχόν αιτήματά του για επιπλέον πόρους.

- Κατά την εξέταση αιτημάτων και καταγγελιών υποκειμένων, ο ΥΠΔ θα αντιμετωπίζει με αντικειμενικότητα το βάσιμο και νόμιμο του αιτήματος και θα ανταποκρίνεται έγκαιρα και με επαγγελματισμό στο αίτημα.

- Ο ΥΠΔ αποφεύγει οποιαδήποτε ανάληψη έργου ή καθήκοντος που μπορεί να δημιουργήσει κατάσταση σύγκρουσης συμφερόντων και απέχει από κάθε άλλη απασχόληση που θα μπορούσε να επιδράσει εις βάρος των καθηκόντων του.

- Ο ΥΠΔ τηρεί εμπιστευτικές όλες τις πληροφορίες τις οποίες διαχειρίζεται.

7.7.10. Υποχρέωση γνωστοποίησης παραβιάσεων δεδομένων προσωπικού χαρακτήρα

Όταν διαπιστώνεται παραβίαση δεδομένων προσωπικού χαρακτήρα υπό την έννοια του άρθρου 33 του Κανονισμού, ο υπεύθυνος επεξεργασίας γνωστοποιεί αμελλητί την παραβίαση στην αρμόδια εθνική Αρχή και μάλιστα, εφόσον είναι δυνατό, **εντός εβδομήντα δύο (72) ωρών από τη στιγμή που αποκτά γνώση της παραβίασης.** Στην περίπτωση που

δεν διαθέτει εξαρχής όλες τις ανωτέρω πληροφορίες, προβαίνει αμελλητί στη γνωστοποίηση κάποιων από αυτές και στη συνέχεια συμπληρώνει σταδιακά τις αναγκαίες πληροφορίες, χωρίς αδικαιολόγητη καθυστέρηση.

Η προαναφερόμενη υποχρέωση δεν υφίσταται όταν εκτιμάται ότι η συγκεκριμένη παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

Για την εκτίμηση του κινδύνου και της σοβαρότητας της παραβίασης λαμβάνονται μεταξύ άλλων υπόψη:

α) η φύση, ο όγκος, καθώς και η κατηγορία των δεδομένων προσωπικού χαρακτήρα που απετέλεσαν αντικείμενο της παραβίασης.

β) η δυνατότητα ταυτοποίησης των υποκειμένων των δεδομένων.

γ) η σοβαρότητα των συνεπειών της παραβίασης για τα υποκείμενα των δεδομένων.

δ) οι ιδιότητες, ο αριθμός και τα ειδικά χαρακτηριστικά των υποκειμένων (π.χ. κατηγορούμενοι, μάρτυρες, ανήλικοι κ.λπ.).

Σοβαρός κίνδυνος τεκμαίρεται ότι μπορεί να προκληθεί στις περιπτώσεις που η παραβίαση των δεδομένων προσωπικού χαρακτήρα μπορεί να προκαλέσει οποιαδήποτε σωματική, υλική ή ηθική - βλάβη σε φυσικά πρόσωπα, όπως ενδεικτικά στις ακόλουθες περιπτώσεις: κίνδυνος δημοσιοποίησης των δεδομένων, κίνδυνος για τη ζωή και την ακεραιότητα των υποκειμένων των δεδομένων, υποκλοπή ταυτότητας, προσβολή της τιμής και της προσωπικότητάς τους, σοβαρή οικονομική βλάβη ή βλάβη εννόμων συμφερόντων τους, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό ή άλλο απόρρητο που αναγνωρίζεται από τη νομοθεσία.

Σε περίπτωση απλώς απόπειρας παραβίασης δεδομένων, δεν δημιουργείται ενδεχόμενο πρόκλησης κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων και γι' αυτό δεν απαιτείται γνωστοποίηση της παραβίασης προς την Αρχή.

Για τις ανάγκες της γνωστοποίησης της παραβίασης στην Αρχή χρησιμοποιούνται τα σχετικά πρότυπα έντυπα (βλ. Παραρτήματα).

ΠΡΟΣΟΧΗ: Για τις περιπτώσεις μη γνωστοποίησης παραβιάσεων, επειδή κρίθηκε ότι δεν συνέτρεχε το ενδεχόμενο πρόκλησης κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων, πρέπει να τηρείται χωριστό αρχείο, στο οποίο καταγράφονται αυτές οι παραβιάσεις που έλαβαν χώρα αλλά δεν γνωστοποιήθηκαν στην Αρχή. Για καθεμία από τις παραβιάσεις καταγράφεται συνοπτική περιγραφή της, καθώς και οι λόγοι για τους οποίους κρίθηκε ότι δεν υπήρχε υποχρέωση γνωστοποίησης.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα η οποία ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, η παραβίαση ανακοινώνεται αμελλητί από τον υπεύθυνο επεξεργασίας στα υποκείμενα που θίγονται από την παραβίαση. Η υποχρέωση αυτή δεν ισχύει όταν συντρέχουν ορισμένες περιοριστικά αναφερόμενες στον Κανονισμό ειδικές περιπτώσεις (α 34 παρ. 3), ήτοι όταν ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας (όπως κρυπτογράφηση, περιορισμός της πρόσβασης σε φυσικό αρχείο κλπ.) και τα μέτρα αυτά πράγματι εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση καθιστώντας τα μη κατανοητά σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όταν στη συνέχεια έλαβε μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, καθώς και όταν η ανακοίνωση είναι αδύνατη ή προϋποθέτει δυσανάλογες προσπάθειες, οπότε γίνεται αντ' αυτής δημόσια ανακοίνωση ή κάτι παρόμοιο με το οποίο τα υποκείμενα μπορούν να ενημερωθούν αποτελεσματικά.

8. Ειδικότερα θέματα

Εδώ να παρατίθενται ζητήματα που αναφύονται ειδικά στο πλαίσιο της συγκεκριμένης δραστηριότητας στην οποία αφορά ο Κώδικας, π.χ.

- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα

ασκούμενων δικηγόρων.

- Διασυνοριακές ροές κατά την άσκηση της δικηγορίας.

- Συστήματα βιντεοεπιτήρησης [αν συνηθίζεται η χρήση τους κατά την άσκηση της δραστηριότητας στην οποία αφορά ο Κώδικας παραθέτουμε το σχετικό νομικό πλαίσιο -προβλέψεις Κανονισμού και εθνικής νομοθεσίας, το ζήτημα της εκτίμησης αντικτύπου, τις αποφάσεις και συστάσεις της Αρχής και των αρμόδιων ευρωπαϊκών φορέων- καθώς και συστάσεις καλής πρακτικής ("Συστήνεται...")] κ.λπ.

9. Κυρώσεις

Ο Κανονισμός προβλέπει, πέρα από τις αστικές αξιώσεις που μπορεί να εγείρει οποιοσδήποτε του οποίου τα προσωπικά δεδομένα παραβιάστηκαν, διοικητικές ποινές (πρόστιμα), τα οποία κλιμακώνονται ανάλογα με τη φύση της παραβίασης κατά περίπτωση και είναι δυνατόν να φτάσουν στο ποσό των 20.000.000 ευρώ ή στο 4% του συνολικού παγκόσμιου κύκλου εργασιών μιας επιχείρησης.

Ποινικές κυρώσεις προβλέπει η εθνική νομοθεσία.

CHECK LIST

Τα 15 βήματα προς τη συμμόρφωση

✓ Καταγράφουμε όλες τις επεξεργασίες προσωπικών δεδομένων τις οποίες διενεργούμε. Ιδιαίτερη προσοχή και ξεχωριστή αντιμετώπιση για τυχόν επεξεργασίες ειδικών κατηγοριών δεδομένων.

✓ Καταγράφουμε τον σκοπό κάθε μιας επεξεργασίας με ειλικρίνεια και πιστότητα.

✓ Δηλώνουμε τη νομική βάση στην οποία στηρίζεται κάθε επεξεργασία. Αποφεύγουμε στο ελάχιστο δυνατό να χρησιμοποιούμε ως βάση τη συγκατάθεση.

✓ Ελέγχουμε αν χρησιμοποιούμε σε κάθε περίπτωση τα κατάλληλα και ελάχιστα δυνατά δεδομένα, καθώς και αν τα δεδομένα που επεξεργαζόμαστε είναι επίκαιρα και ακριβή και θεσπίζουμε αντίστοιχες διαδικασίες περιοδικού ελέγχου.

✓ Καταγράφουμε για κάθε επεξεργασία ποιοι έχουν πρόσβαση στα δεδομένα και ελέγχουμε αν δικαιολογείται να έχουν.

✓ Ορίζουμε τον χρόνο διατήρησης των δεδομένων σε κάθε περίπτωση. Ορίζουμε ξεχωριστά τον χρόνο διατήρησης προσωπικών δεδομένων σε ορισμένες χαρακτηριστικές και πλέον συνήθεις περιπτώσεις, όπως των υποψηφίων για πρόσληψη, των εργαζομένων, των πρώην εργαζομένων, των προμηθευτών, των συνεργατών και των πελατών.

✓ Ελέγχουμε τις συνθήκες ασφαλείας γενικώς των εγκαταστάσεων και των συστημάτων και ορίζουμε υπεύθυνο ασφαλείας. Ελέγχουμε ειδικότερα τις συνθήκες αποθήκευσης ψηφιακών και μη αρχείων και θεσπίζουμε διαδικασίες ελέγχου και τακτικές επιθεωρήσεις.

✓ Προβλέπουμε διαδικασίες ασφαλούς καταστροφής όταν συμπληρώνεται κάθε φορά το σχετικό χρονικό διάστημα διατήρησης των δεδομένων και ορίζουμε υπευθύνους.

- ✓ Ελέγχουμε κάθε περίπτωση διαβίβασης δεδομένων σε τρίτες χώρες και τις προϋποθέσεις νομιμότητας κάθε μιας από αυτές.
- ✓ Ασχολούμαστε με προσοχή με τις προϋποθέσεις νομιμότητας της τυχόν λειτουργίας συστημάτων βιντεοεπιτήρησης.
- ✓ Θεσπίζουμε γενικές διαδικασίες για την εκάστοτε επιλογή των κατάλληλων τεχνικών και οργανωτικών μέτρων.
- ✓ Αναθεωρούμε τις συμβάσεις του προσωπικού, καθώς και τις συμβάσεις με συνεργάτες, προμηθευτές και συνεργάτες.
- ✓ Θεσπίζουμε διαδικασία ικανοποίησης των δικαιωμάτων των υποκειμένων και διαδικασία γνωστοποίησης παραβιάσεων.
- ✓ Ορίζουμε τακτικές εκπαιδεύσεις προσωπικού και άλλες δράσεις ευαισθητοποίησης στην προστασία προσωπικών δεδομένων.
- ✓ Ορίζουμε τακτική παρακολούθηση του αρχείου του άρθρου 30 του Κανονισμού.

Γ΄ ΜΕΡΟΣ

Μετά τη θέση σε εφαρμογή του Κώδικα

Γ΄1. Παρακολούθηση της εφαρμογής του παρόντος Κώδικα

Η παρακολούθηση της τήρησης των όσων προβλέπονται στον παρόντα Κώδικα ανατίθεται σ΄ ένα συγκεκριμένο πρόσωπο ή, εναλλακτικά, σε συγκεκριμένα πρόσωπα για συγκεκριμένα αντικείμενα.

Εάν επιλεγεί ένα πρόσωπο, αυτό πρέπει να είναι ο ΥΠΔ αν υπάρχει.

Γ΄2. Τακτική αναθεώρηση – επικαιροποίηση του παρόντος Κώδικα

Ο παρών Κώδικας πρέπει να ελέγχεται και αναθεωρείται κάθε διετία, καθώς και κάθε φορά που υπάρχουν αλλαγές στο νομικό πλαίσιο. Ανατίθεται η σχετική ευθύνη στο πρόσωπο που έχει οριστεί κατά τα οριζόμενα παραπάνω υπό Γ΄1.

Συστήνεται

- Πριν από κάθε αναθεώρηση του παρόντος Κώδικα να πραγματοποιείται διαβούλευση με τα πρόσωπα στα οποία αφορά η εφαρμογή του.
- Κάθε αναθεώρηση του Κώδικα να συνοδεύεται από μία εκδήλωση (ημερίδα-σεμινάριο) παρουσίασής του.
- Πριν από κάθε αναθεώρηση του Κώδικα να αποστέλλεται στην εθνική Αρχή για τυχόν σχόλια και παρατηρήσεις της.

Γ΄3. Θέσπιση κυρώσεων σε περιπτώσεις μη τήρησης του παρόντος Κώδικα

Η μη τήρηση των όσων ορίζονται στον παρόντα Κώδικα πρέπει να αποτελεί λόγο για την επέλευση κάποιου είδους δυσμενών συνεπειών για τους παραβάτες.

Εναπόκειται στη βούληση όποιου προσχωρεί στον Κώδικα να προσδιορίσει το είδος των συνεπειών αυτών, συστήνεται όμως να υπάρξει αφενός σύνδεση της υποχρέωσης τήρησής του με το πλαίσιο των γενικότερων υποχρεώσεων του προσωπικού και τους τυχόν λοιπούς εσωτερικούς Κανονισμούς και, αφετέρου, με το σύστημα αξιολόγησης.

Δ΄ ΜΕΡΟΣ

Παραρτήματα

1. Έντυπα διευκόλυνσης των υποκειμένων για την άσκηση των δικαιωμάτων τους

2. Φόρμες για την αντιμετώπιση περιστατικών παραβίασης

3. Νομικά κείμενα

4. Το κείμενο του Κανονισμού 2016/679

5. Το κείμενο του ν. 4624/2019

6. Ειδική νομοθεσία που αφορά στη συγκεκριμένη δραστηριότητα του *(π.χ. Κώδικας περί δικηγόρων)*.

7. Για την ανάγκη μελέτης αντικτύπου: Ομάδα Εργασίας του Άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5 Απριλίου 2017.

8. Για DPO: Ομάδα Εργασίας του Άρθρου 29, Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5 Απριλίου 2017.

9. Χαρακτηριστικές αποφάσεις της εθνικής Αρχής και των δικαστηρίων που αφορούν ειδικά στη δραστηριότητα που μας απασχολεί.


PROBLEM BASED TRAINING ON THE DATA
PROTECTION REFORM PACKAGE IN GR AND CY
DP
TRAINING ON THE DATA PROTECTION


Centre for
European
Constitutional
Law
Themistokles and Dimitris Tsatsos Foundation


University
of Cyprus


HELLENIC REPUBLIC
National and Kapodistrian
University of Athens
EST. 1837