ΚΥΡΙΑ ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ 2016/679

ΚΑΤΑΝΟΗΣΗ ΤΩΝ ΒΑΣΙΚΩΝ ΑΡΧΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ως δεδομένα προσωπικού χαρακτήρα σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΓΚΠΔ) ορίζεται 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.

Η διεύρυνση του ορισμού των προσωπικών δεδομένων στον ΓΚΠΔ έχει ως συνέπεια να συμπεριλαμβάνονται και άλλα είδη προσωπικών δεδομένων, πέρα από τα προσωπικά δεδομένα πελατών και τρίτων προσώπων, όπως π.χ., διευθύνσεις IP που συλλέγει μία ιστοσελίδα ενός βρεφονηπιακού σταθμού.

Ο ορισμός, δε, αυτός ισχύει τόσο για την αυτοματοποιημένη όσο και για τη μη αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων. Εκτός όμως από τα προσωπικά δεδομένα πελατών, οι οντότητες επεξεργάζονται και δεδομένα των υπαλλήλων και συνεργατών τους. Με αυτό το πνεύμα, το πρώτο βήμα για μια Οντότητα είναι να διασφαλίσει ότι η συμμόρφωση θα αντιμετωπίσει το σύνολο των δεδομένων που κατέχει και τα οποία εμπίπτουν στον ορισμό των προσωπικών δεδομένων. Επιπλέον, το προσωπικό της οντότητας (υπάλληλοι) θα πρέπει να κατανοήσει τις βασικές αρχές προστασίας και να μελετήσει σε βάθος τις πτυχές του ΓΚΠΔ που άπτονται τόσο των υποχρεώσεων κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα όσο και των επιμέρους δικαιωμάτων των υποκειμένων των δεδομένων.

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

➢ Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε θεμιτή και νόμιμη επεξεργασία.

➢ Τα προσωπικά δεδομένα πρέπει να υπόκεινται σε επεξεργασία μόνο για έναν ή περισσότερους συγκεκριμένους και νόμιμους σκοπούς και δε θα πρέπει να υποβάλλονται σε περαιτέρω επεξεργασία με οποιονδήποτε τρόπο ασυμβίβαστο προς τον σκοπό ή τους σκοπούς αυτούς.

➢ Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι επαρκή, συναφή και όχι υπερβολικά σε σχέση με το σκοπό ή τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

➢ Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και, όπου χρειάζεται, να ενημερώνονται.

➢ Τα προσωπικά δεδομένα που υποβάλλονται σε επεξεργασία για οποιονδήποτε σκοπό ή σκοπούς δεν πρέπει να διατηρούνται για περισσότερο από το χρονικό διάστημα που είναι απαραίτητο για το σκοπό αυτό ή για τους σκοπούς αυτούς.

➢ Πρέπει να λαμβάνονται κατάλληλα τεχνικά και οργανωτικά μέτρα κατά της μη εξουσιοδοτημένης ή παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κατά της τυχαίας απώλειας, καταστροφής ή ζημίας προσωπικών δεδομένων.

➢ Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να αποδείξει την συμμόρφωσή του με τις απαιτήσεις του ΓΚΠΔ (αρχή της λογοδοσίας).

➢ Τα δεδομένα προσωπικού χαρακτήρα δεν μεταφέρονται σε χώρα ή έδαφος εκτός της Ε.Ε, εκτός εάν εξασφαλίζεται επαρκές επίπεδο προστασίας των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις ειδικές προϋποθέσεις που ορίζονται στον ΓΚΠΔ. Η εταιρεία θα πρέπει να είναι προετοιμασμένη σε περίπτωση που το υποκείμενο των δεδομένων ασκήσει τα δικαιώματα που του παρέχει ο ΓΚΠΔ, υιοθετώντας κατάλληλες πρακτικές και διαδικασίες.

ΚΑΤΑΝΟΗΣΗ & ΕΦΑΡΜΟΓΗ ΤΗΣ ΑΡΧΗΣ ΤΗΣ ΛΟΓΟΔΟΣΙΑΣ

Η αρχή της λογοδοσίας εισάγεται για πρώτη φορά με τον ΓΚΠΔ και στηρίζει την προσέγγιση που πρέπει να υιοθετήσουν μεταξύ άλλων και οι οντότητες για τη συμμόρφωσή τους. Δεν αρκεί πλέον η συμμόρφωση με τις απαιτήσεις προστασίας προσωπικών δεδομένων, αλλά οι οντότητες πρέπει να επιδείξουν και τον τρόπο συμμόρφωσής τους. Μόλις γίνει κατανοητή η ουσία της αρχής της λογοδοσίας, είναι σαφές ότι οι οντότητες πρέπει να τεκμηριώνουν τη λήψη αποφάσεων σχετικά με τις διαδικασίες που ακολουθούν για την προστασίας των προσωπικών δεδομένων που επεξεργάζονται

Η οντότητα, ως υπεύθυνος επεξεργασίας, σύμφωνα με τον Κανονισμό 2016/679, οφείλει να τηρεί τις υποχρεώσεις που επιβάλλει ο Κανονισμός, ήτοι:

1. Να τηρεί αρχείο δραστηριοτήτων επεξεργασίας.

2. Στα πλαίσια εφαρμογής του ΓΚΠΔ μια οντότητα θα πρέπει να αναθεωρήσει τις τρέχουσες διαδικασίες ενημέρωσης των υποκειμένων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων και να θέσει σε εφαρμογή ένα σχέδιο για την πραγματοποίηση των απαραίτητων αλλαγών όπου αυτό κρίνεται αναγκαίο. Κατά το στάδιο συλλογής προσωπικών δεδομένων, θα πρέπει να δοθούν συγκεκριμένες και σαφείς πληροφορίες στα υποκείμενα, όπως π.χ. ο χρόνος και τρόπος με τον οποίο θα χρησιμοποιηθούν οι πληροφορίες τους, η νόμιμη βάση και ο σκοπός της επεξεργασίας καθώς επίσης και τα δικαιώματά τους ως υποκείμενα.

Για το σκοπό αυτό, θα πρέπει κάθε οντότητα να διαθέτει έντυπο ενημέρωσης των πελατών, σύμφωνα με το άρθρο 13 του Κανονισμού. Η οντότητα α δεν οφείλει να λαμβάνει συναίνεση από τους πελάτες της, εκτός αν πρόκειται να κάνει χρήση δεδομένων και για άλλους σκοπούς, πέρα από την τήρηση αρχείου με σκοπό την διεκπεραίωση της εντολής.

3. Θα πρέπει να σέβεται στην πράξη τα δικαιώματα των πελατών του, για τα οποία οφείλει να τον ενημερώνει, σύμφωνα με τα παραπάνω, ήτοι:

Α) Δικαίωμα πρόσβασης. Το δικαίωμα να γνωρίζει αν τα προσωπικά του δεδομένα υφίστανται επεξεργασία, πως και για ποιο σκοπό.

Β) Δικαίωμα διόρθωσης. Το δικαίωμα να ζητήσει τη διόρθωση προσωπικών δεδομένων που είναι ανακριβή ή ελλιπή.

Γ) Δικαίωμα διαγραφής. Το δικαίωμα να ζητήσει διαγράφη των προσωπικών του δεδομένων. Ισχύει περιορισμένα και μόνο μετά το πέρας της εντολής, εφόσον δεν είναι πλέον απαραίτητα τα δεδομένα αυτά.

Δ) Δικαίωμα περιορισμού της επεξεργασίας δεδομένων.

Ε) Δικαίωμα στη φορητότητα. Το δικαίωμα να σταλούν τα δεδομένα ηλεκτρονικά (εφόσον τηρούνται ηλεκτρονικά) σε άλλο εκπαιδευτικό φορέα.

Χρόνος άσκησης των δικαιωμάτων: 1 μήνας

Όταν αρνείται να ικανοποιήσει τα δικαιώματα αυτά ή καθυστερεί να τα ικανοποιήσει πρέπει να εξηγήσει τους λόγους καθυστέρησης.

4. Να έχει πρωτόκολλο και να τηρεί μια διαδικασία για τη διαχείριση των περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα και ειδικότερα για την γνωστοποίηση των περιστατικών παραβίασης προσωπικών δεδομένων (πχ παραβίαση ασφαλείας (hacking), μόλυνση με κακόβουλο λογισμικό (όπως ransomware), απώλεια USB, φορητού υπολογιστή κλπ., στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και για την ενημέρωση των φυσικών προσώπων τα οποία αφορά το περιστατικό, όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες τους (σχετικές φόρμες επισυνάπτονται).

5. Με βάση τον ΓΚΠΔ κάθε εταιρεία οφείλει όπως προαναφέρθηκε πέρα από την υιοθέτηση πολιτικών προστασίας της ιδιωτικότητας να λάβει μέτρα για να διασφαλίσει την ασφάλεια, ακεραιότητα και την εμπιστευτικότητα της επεξεργασίας των προσωπικών δεδομένων.

Ειδικότερα, θα πρέπει να ληφθούν τα εξής μέτρα, ενδεικτικώς αναφερόμενα, ασφαλείας δεδομένων:

i. Να γίνεται χρήση ασφαλών κωδικών (προτεινόμενο ελάχιστο μήκος αποτελούν οι 8 χαρακτήρες που να περιλαμβάνει αριθμούς, γράμματα και σύμβολα) για ασφαλή είσοδο (log-in) σε συστήματα (υπολογιστές, Wi-Fi).

ii. Οι κωδικοί δεν πρέπει να είναι κάπου καταγεγραμμένα στην πραγματική τους μορφή (ούτε σε φυσικό ούτε σε ηλεκτρονικό αρχείο).
iii. Πρέπει να υπάρχει προστασία από κακόβουλο λογισμικό όλων των υπολογιστών της εταιρείας (τόσο των προσωπικών υπολογιστών όσο και των διακομιστών (servers)) που τηρούν ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα και να υπάρχουν εγκατεστημένα ενημερωμένα αντιβιοτικά προγράμματα (antivirus)
iv. Αποφυγή χρήσης φορητών αποθηκευτικών μέσων (USB) και αποθήκευσης σε αυτά εμπιστευτικών εγγράφων
v. Χρήση σύγχρονων λειτουργικών συστημάτων και τακτική ενημέρωσή τους, (π.χ. δεν χρησιμοποιούμε Windows XP που δεν ενημερώνονται πλέον)
vi. Χρήση και ενεργοποίηση προγραμμάτων τειχών ασφαλείας (firewall) σε όλους τους υπολογιστές που τηρούνται ή επεξεργάζονται δεδομένα προσωπικού χαρακτήρα
vii. Αποφυγή «κατεβάσματος» από διαδίκτυο και χρήσης λογισμικών άγνωστης προέλευσης
viii. Λήψη αντιγράφων ασφάλειας (back-up) σε τακτά χρονικά διαστήματα
ix. Αποφυγή χρήσης ελευθέρων e-mail, π.χ. Yahoo, για αποστολή και λήψη ευαίσθητων δεδομένων, π.χ. ιατρικών πιστοποιητικών και εμπιστευτικών εγγράφων.
x. Κρυπτογράφηση του εσωτερικού σκληρού δίσκου του Ηλεκτρονικού Υπολογιστή
xi. Να αποφεύγεται η αποθήκευση δεδομένων προσωπικού χαρακτήρα σε υπολογιστές που έχουν σύνδεση με το διαδίκτυο
xii. Να αποφεύγεται η απομακρυσμένη πρόσβαση σε υπολογιστές που έχουν αποθηκευμένα προσωπικά δεδομένα και αν απαιτείται τέτοια θα πρέπει να γίνεται υπό την εποπτεία και έλεγχο και να καταγράφεται.
xiii. Κρυπτογράφηση εξωτερικών - φορητών μονάδων αποθήκευσης (π.χ. εξωτερικός σκληρός δίσκος, USB κ.ο.κ.) στους οποίους τηρούνται αρχεία με προσωπικά δεδομένα
xiv. Να εφαρμόζονται διαδικασίες αυτόματης αποσύνδεσης (μετά από ένα εύλογο χρονικό διάστημα αδράνειας) ή/και ενεργοποίηση της προφύλαξης οθόνης (screen saver) του υπολογιστή όπου υπάρχουν αποθηκευμένα προσωπικά δεδομένα – για την απενεργοποίηση της οποίας θα απαιτείται χρήση συνθηματικού.
xv. Να λαμβάνονται τα κατάλληλα μέτρα για τη φυσική ασφάλεια και προστασία των χώρων όπου υπάρχουν έγχαρτα αρχεία με προσωπικά δεδομένα

6. Να τηρείται πολιτική καθαρού γραφείου (Clean desk policy)

7. Να καταρτίζονται συμφωνίες εμπιστευτικότητας με τους υπαλλήλους

8. Να καταρτίζονται συμβάσεις με εκτελούντες την επεξεργασία

9. Να τηρείται πολιτική ασφαλούς καταστροφής εγγράφων και διαγραφής ψηφιακών δεδομένων.

10. Η ιστοσελίδα της οντότητας να διαθέτει πολιτική προστασίας δεδομένων και ενημέρωση για cookies (cookies policy) .

11. Η αποστολή newsletters της οντότητας πρέπει να διενεργείται με λήψη συγκατάθεσης τύπου double opt-in.

ΠΑΡΑΡΤΗΜΑ: ΠΟΛΙΤΙΚΗ ΚΑΘΑΡΟΥ ΓΡΑΦΕΙΟΥ

1. Πρέπει να διασφαλίζεται ότι όλοι οι φάκελοι εργαζομένων/Πελατών με ευαίσθητες/ εμπιστευτικές πληροφορίες σε έντυπη ή ηλεκτρονική μορφή είναι ασφαλισμένοι στο χώρο εργασίας στο τέλος της ημέρας σε ντουλάπια που ασφαλίζουν ή σε υπολογιστές που να διαθέτουν κρυπτογράφηση και κωδικούς ασφαλείας (passwords).
2. Οι υπολογιστές πρέπει να είναι κλειδωμένοι όταν ο χώρος εργασίας είναι μη κατειλημμένος.
3. Οι υπολογιστές πρέπει να κλείνουν με το πέρας της ημέρας εργασίας και να μην τίθενται απλώς σε αναστολή λειτουργίας.
4. Φάκελοι εργαζομένων/Πελατών με εμπιστευτικές ή ευαίσθητες πληροφορίες πρέπει να απομακρύνονται από το γραφείο και να κλειδώνονται σε ένα συρτάρι όταν δεν είναι κανείς στο γραφείο και στο τέλος της εργασιακής ημέρας.
5. Τα ντουλάπια με τα αρχεία εργαζομένων/πελατών πρέπει να μένουν κλειστά και κλειδωμένα όταν δεν γίνεται χρήση τους ή όταν δεν υπάρχει κανείς να τα προσέχει.
6. Τα κλειδιά με τα οποία ασφαλίζονται τα γραφεία και τα ντουλάπια που περιέχουν φακέλους με εμπιστευτικές πληροφορίες δεν πρέπει να αφήνονται σε γραφείο χωρίς επίβλεψη.
7. Οι φορητοί υπολογιστές πρέπει να είναι είτε κλειδωμένοι με καλώδιο ασφάλισης είτε να είναι ασφαλισμένοι σε συρτάρι ή άλλο χώρο.
8. Οι κωδικοί πρόσβασης δεν πρέπει να σημειώνονται σε αυτοκόλλητα χαρτάκια επάνω στον υπολογιστή ούτε να αφήνονται καταγεγραμμένοι σε θέση που έχουν άλλοι πρόσβαση.
9. Οι εκτυπώσεις κάθε είδους εμπιστευτικών εγγράφων πρέπει να απομακρύνονται άμεσα από τον εκτυπωτή.
10. Κατά την καταστροφή εγγράφων, θα πρέπει αυτά να τεμαχίζονται με ειδικές συσκευές ή με διάθεση για ασφαλή καταστροφή.
11. Κλειδώστε τις φορητές υπολογιστικές συσκευές όπως φορητούς υπολογιστές και tablets.
12. Οι συσκευές μαζικής αποθήκευσης, όπως δίσκους CDROM, DVD ή USB πρέπει να ασφαλίζονται με κρυπτογράφηση και να παραμένουν σε ασφαλή φύλαξη.