ΚΥΡΙΑ ΒΗΜΑΤΑ ΣΥΜΜΟΡΦΩΣΗΣ ΔΙΚΗΓΟΡΙΚΟΥ ΓΡΑΦΕΙΟΥ

ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ 2016/679

Ο δικηγόρος, 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 (βλ. συνημμένο excel).

2. Να διαθέτει έντυπο ενημέρωσης των πελατών, σύμφωνα με το άρθρο 13 του Κανονισμού. Δεν οφείλει να λαμβάνει συναίνεση από τους πελάτες του, εκτός αν πρόκειται να κάνει χρήση δεδομένων και για άλλους σκοπούς, πέρα από την τήρηση αρχείου με σκοπό την διεκπεραίωση της εντολής.

2. 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 άλλον δικηγόρο.
>
> <u>Χρόνος άσκησης των δικαιωμάτων: 1 μήνας</u>

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

3. 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).

4. Να λαμβάνει τεχνικά και οργανωτικά μέτρα ασφαλείας δεδομένων, δηλ.:

i. Να κάνει 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 του δικηγορικού γραφείου (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 (δικογράφων, αντίγραφα δικογραφιών κτλ).
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 και δικογράφων.

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 π 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 (δικόγραφα, αντίγραφα δικογραφιών κτλ)

5. Να τηρεί την πολιτική καθαρού γραφείου (Clean desk policy) (βλ. συνημμένο Παράρτημα).

6. Να καταρτίζει συμφωνίες εμπιστευτικότητας με τους συνεργάτες δικηγόρους και ασκουμένους δικηγόρους.

7. Να καταρτίζει συμβάσεις με εκτελούντες την επεξεργασία (δικαστικούς επιμελητές, συμβολαιογράφους κλπ.).

8. Να τηρεί πολιτική ασφαλούς καταστροφής εγγράφων και διαγραφής ψηφιακών δεδομένων.

9. Η ιστοσελίδα του δικηγορικού γραφείου να διαθέτει πολιτική προστασίας δεδομένων και ενημέρωση για cookies (cookies policy).

10. Η αποστολή newsletters του γραφείου πρέπει να διενεργείται με λήψη συγκατάθεσης τύπου double opt-in.

ΠΑΡΑΡΤΗΜΑ: ΠΟΛΙΤΙΚΗ ΚΑΘΑΡΟΥ ΓΡΑΦΕΙΟΥ

1. Πρέπει να διασφαλίζεται ότι όλοι οι φάκελοι δικογραφιών με ευαίσθητες/ εμπιστευτικές πληροφορίες σε έντυπη ή ηλεκτρονική μορφή είναι ασφαλισμένοι στο χώρο εργασίας τους 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 δικογραφιών 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 δικογραφιών 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 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 δίσκοι CDROM, DVD ή USB πρέπει να ασφαλίζονται με κρυπτογράφηση και να παραμένουν σε ασφαλή φύλαξη.