ΔΙΚΗΓΟΡΙΚΟΣ ΣΥΛΛΟΓΟΣ ΑΘΗΝΩΝ

ΕΓΧΕΙΡΙΔΙΟ (MANUAL)

ΕΦΑΡΜΟΓΗΣ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ (GDPR) ΓΙΑ ΔΙΚΗΓΟΡΟΥΣΚΑΤΑ ΤΗΝ ΕΝΑΣΚΗΣΗ ΤΟΥ ΔΙΚΗΓΟΡΙΚΟΥ ΛΕΙΤΟΥΡΓΗΜΑΤΟΣ

ΔΣΑ – Οδηγίες εφαρμογής του ΓΚΠΔ*

Από την 25η Μαΐου 2018 ετέθη σε εφαρμογή ο **Γενικός Κανονισμός Προστασίας Δεδομένων [εφεξής ΓΚΠΔ ή Κανονισμός].** Ο Κανονισμός έχει ευρύτατο πεδίο εφαρμογής και, όπως και η προγενέστερη νομοθεσία (διηλ. ο Ν. 2472/97 «*για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα*»), εφαρμόζεται και ως προς την άσκηση του δικηγορικού λειτουργήματος, αφορά διηλ. χωρίς αμφιβολία και στις / τους δικηγόρους.

1. Προϋποθέσεις εφαρμογής ΓΚΠΔ:

Ο Κανονισμός εφαρμόζεται στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, διηλ. σε κάθε πληροφορία που αναφέρεται σε ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο (εν ζωή),

Ως επεξεργασία νοείται 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.

Ο Κανονισμός εφαρμόζεται και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων, τα οποία περιλαμβάνονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Αν και ο μεμονωμένος φάκελος δικογραφίας δεν θεωρείται από μόνος του σύστημα αρχειοθέτησης, το σύνολο των φακέλων δικογραφίας που χειρίζεται και αρχειοθετεί δικηγόρος εμπίπτει στην έννοια του «συστήματος αρχειοθέτησης».

2. Σχέση με το «δικηγορικό απόρρητο»:

Ο Κανονισμός ισχύει πέραν του «δικηγορικού απορρήτου» και εκ παραλλήλου προς αυτό. Οι υποχρεώσεις εμπιστευτικότητας που απορρέουν από την αρχή της ασφάλειας, όπως εξειδικεύονται ιδίως στο άρθρο 32 του Κανονισμού, συρρέουν προς τις ρυθμίσεις του Κώδικα Δεοντολογίας για την εχεμύθεια. Οι υποχρεώσεις εμπιστευτικότητας, όπως και το δικηγορικό απόρρητο, ισχύουν κατά τη διάρκεια, αλλά και μετά από την περαίωση της υποθέσεως ή την ανάκληση της εντολής από τον εντολέα.

---

* Εκπονήθηκε από το Εργαστήριο Νομικής Πληροφορικής της Νομικής Σχολής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών για λογαριασμό του ΔΣΑ

Συντάκτες: Α. Μήτρου, Γ. Γιαννόπουλος, Φ. Παναγοπούλου, Α. Βαρβέρης

3. Προσωπικά δεδομένα στο δικηγορικό γραφείο:

Η / Ο δικηγόρος, με την ιδιότητά του ως Υπευθύνου Επεξεργασίας, επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, είτε μία υπόθεση αφορά και εμπλέκει αμιγώς φυσικά πρόσωπα είτε αφορά νομικά πρόσωπα, καθώς ακόμη και στην τελευταία αυτή περίπτωση το σχετικό αρχείο περιλαμβάνει, σχεδόν ανεξαιρέτως, στοιχεία νομίμων εκπροσώπων, προσώπων που συμμετέχουν στη διοίκηση, συνεργατών κ.α.

Ένα ηλεκτρονικό ή χειρόγραφο έγγραφο δικηγορικού αρχείου περιλαμβάνει -εκτός των προσωπικών δεδομένων που αναφέρονται στους εντολείς- προσωπικά δεδομένα που αναφέρονται σε αντιδίκους, διαμεσολαβητές, μάρτυρες, δικαστικούς λειτουργούς και συνακόλουθα προσωπικά δεδομένα που αναφέρονται σε συνεργαζόμενους δικηγόρους, αντιδίκους δικηγόρους και σε πρόσωπα που σχετίζονται ή απασχολούνται σε φορείς που σχετίζονται με μία υπόθεση (υπαλλήλων σε δημόσιες αρχές, εταιρίες κλπ.).

Επίσης η / ο δικηγόρος / δικηγορικό γραφείο συλλέγει και επεξεργάζεται δεδομένα για τους κάθε φύσεως συνεργάτες του: συνεργάτες δικηγόροι, ασκούμενοι, δικαστικοί επιμελητές, άλλο προσωπικό, προμηθευτές, εξωτερικοί συνεργάτες που παρέχουν υπηρεσίες υποστήριξης κ.α.

4. Βήματα και διαδικασίες συμμόρφωσης

[*Επισημαίνεται ότι το παρόν κείμενο δεν υπεισέρχεται στο ζήτημα της νόμιμης χρήσης προσωπικών δεδομένων ως (νομίμων / παραδεκτών) αποδεικτικών μέσων*]

4.1 Έλεγχος συμμόρφωσης ως προς τις ουσιαστικές απαιτήσεις: Κάθε δικηγόρος ή / και δικηγορικό γραφείο, όπως κάθε Υπεύθυνος Επεξεργασίας (δηλ. το φυσικό ή νομικό πρόσωπο που ορίζει τον σκοπό και τα μέσα επεξεργασίας), οφείλει να ελέγξει τη συμμόρφωσή του με τις απαιτήσεις του Κανονισμού. Οι υποχρεώσεις αυτές αφορούν κατ' αρχήν στις νομιμοποιητικές βάσεις και τις αρχές της επεξεργασίας.

4.2. Βάσεις νομιμότητας: Απαιτείται θεμελίωση της επεξεργασίας των προσωπικών δεδομένων στις νομιμοποιητικές βάσεις που εισάγουν τα άρθρα 6 και 9 ΓΚΠΔ αντίστοιχα. Ειδικότερα πρέπει να αντιμετωπίζονται τα ακόλουθα ερωτήματα:

α) Εξυπηρετεί η επεξεργασία την εκτέλεση σύμβασης μεταξύ του δικηγόρου και του εντολέα του;

β) Έχει ληφθεί συγκατάθεση κατά τα προβλεπόμενα στον Κανονισμό (άρθρο 6, 7 και 9), όταν η επεξεργασία αφορά σκοπούς που δεν εντάσσονται στην εκπλήρωση των αμοιβαίων υποχρεώσεων από τη σύμβαση εντολής;

γ) Υπάρχει υποχρέωση ως προς την επεξεργασία προσωπικών δεδομένων που προβλέπεται σε νόμο;

δ) Μπορεί να υποστηριχθεί η ύπαρξη υπέρτερου εννόμου συμφέροντος του εντολέα ή της/ του δικηγόρου ως προς την επεξεργασία των προσωπικών δεδομένων;

4.3. Αρχή της ελαχιστοποίησης: Πρέπει να πραγματοποιείται έλεγχος της αναγκαιότητας, της καταλληλότητας / προσφορότητας και της υπό στενή έννοια αναλογικότητας. Ο δικηγόρος οφείλει να απαντά το ερώτημα:

Είναι απαραίτητη και σε ποια έκταση η συλλογή και επεξεργασία προσωπικών δεδομένων σε σχέση με τον σκοπό που εξυπηρετούν;

4.4 Ακρίβεια: Πρέπει να αντιμετωπίζεται το ερώτημα:

Είναι τα προσωπικά δεδομένα που τηρούνται ακριβή και επικαιροποιημένα;

4.5 Διατήρηση και διαγραφή: Θα πρέπει να υφίσταται μία στοιχειώδης «πρακτική»/ «πολιτική» ως προς το χρόνο διατήρησης των προσωπικών δεδομένων. Ειδικότερα:

α) Διαγράφονται / καταστρέφονται τα δεδομένα όταν δεν είναι πλέον αναγκαία για την εκπλήρωση των σκοπών για τα οποία συλλέχθηκαν; Υφίσταται πολιτική για τον χρόνο διατήρησης των δεδομένων;

β) Ελέγχεται αν κάποια δεδομένα πρέπει να διατηρηθούν για την εκπλήρωση άλλων νομίμων σκοπών (φορολογικοί έλεγχοι κ.α.);

4.6. Έλεγχος πρόσβασης: Θα πρέπει να υφίσταται πρακτική / πολιτική ως προς το ποιοι (συνεργάτες ή λοιπό προσωπικό) έχουν πρόσβαση στα αρχεία των προσωπικών δεδομένων μέσα σε ένα δικηγορικό γραφείο, ιδίως για συνεργάτες που δεν καλύπτονται από το δικηγορικό απόρρητο.

5. Νέες Υποχρεώσεις από τον Κανονισμό: Πότε είναι υπόχρεος η / ο δικηγόρος

5.1. Τήρηση αρχείων επεξεργασίας (άρθρο 30 ΓΚΠΔ): Η τήρηση των αρχείων επεξεργασίας δεν συνιστά σε όλες τις περιπτώσεις υποχρέωση του Υπευθύνου Επεξεργασίας. 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 ή
- η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων κατά το άρθρο 9 παρ. 1 ή
- επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

Θεωρούμε ότι οι - ως άνω διαζευκτικές - προϋποθέσεις συντρέχουν στην περίπτωση της επεξεργασίας που πραγματοποιείται από δικηγόρους ή δικηγορικά γραφεία. Όπως σημειώνει και η Αρχή Προστασίας Δεδομένων

Προσωπικού Χαρακτήρα, η τήρηση των αρχείων αυτών δεν είναι σημαντική μόνο γιατί αποτελεί υποχρέωση από το άρθρο 30 ΓΚΠΔ ως εργαλείο λογοδοσίας, αλλά και γιατί αποτελεί χρήσιμο μέσο για τη σωστή οργάνωση των διαδικασιών χειρισμού των τηρούμενων προσωπικών δεδομένων.

Το ελάχιστο περιεχόμενο του 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 κατά το άρθρο 9 παρ. 1 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 και

ζ) τις προθεσμίες διαγραφής (όπου είναι δυνατό/ προσδιορίσιμο).

Δεν υπάρχει προκαθορισμένος μορφότυπος (format) για το εν λόγω αρχείο. Σημειώνεται, πάντως, ότι η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει δημοσιεύσει σχετικό πρότυπο στην ιστοσελίδα της.

5.2. Εκτίμηση επιπτώσεων (αντικτύπου) της επεξεργασίας (Data protection impact assessment): Η διενέργεια εκτίμησης επιπτώσεων της επεξεργασίας απαιτείται όταν αυτή, σύμφωνα με την αντικειμενική εκτίμηση του Υπευθύνου Επεξεργασίας, 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. Όταν βάσει της διενεργηθείσας εκτίμησης επιπτώσεων και παρά την πρόβλεψη μέτρων προστασίας παραμένει υψηλή επικινδυνότητα της επεξεργασίας, ο υπεύθυνος επεξεργασίας υποχρεούται να προβεί σε προηγούμενη διαβούλευση με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Μία εκτίμηση επιπτώσεων μπορεί να αφορά μια μοναδική επιμέρους πράξη επεξεργασίας ή ένα σύνολο παρόμοιων πράξεων επεξεργασίας.

Σύμφωνα με την αιτιολογική σκέψη 91: «*...η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν θα πρέπει να θεωρείται ότι είναι μεγάλης κλίμακας, εάν η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα ...πελατών δικηγόρου. Στις περιπτώσεις αυτές, η εκτίμηση αντικτύπου της προστασίας δεδομένων δεν θα πρέπει να είναι υποχρεωτική...*». Συνεπώς,

η διενέργεια εκτίμησης επιπτώσεων δεν απαιτείται όταν πρόκειται για μεμονωμένους δικηγόρους. Δεν υπάρχει ασφαλής ερμηνεία αναφορικά με τις δικηγορικές εταιρίες.

Ως εκ τούτου, θα πρέπει να εξετάζεται κατά περίπτωση εάν απαιτείται η διενέργεια τέτοιας εκτίμησης, η οποία κατ' ελάχιστον περιλαμβάνει:

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

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στο άρ. 35 παρ. 1 ΓΚΠΔ και

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας.

6. Υποχρεώσεις διαφάνειας – ενημέρωσης

Σύμφωνα με τα οριζόμενα στον ΓΚΠΔ, η / ο δικηγόρος ως Υπεύθυνος Επεξεργασίας οφείλει να προβαίνει σε ενημέρωση των πελατών του (Υποκειμένων των δεδομένων) αναφορικά με τη συλλογή και επεξεργασία των προσωπικών δεδομένων τους. Η υποχρέωση αυτή υφίσταται ανεξάρτητα από το ποια είναι η βάση νομιμότητας της επεξεργασίας και πρέπει να περιλαμβάνει πληροφόρηση για τα ακόλουθα:

α) τα στοιχεία Υπευθύνου Επεξεργασίας, συμπεριλαμβανομένων των στοιχείων επικοινωνίας,

β) τη βάση νομιμότητας της επεξεργασίας (π.χ. για την εκτέλεση εντολής),

γ) τον σκοπό και το είδος της επεξεργασίας,

δ) τις κατηγορίες των Υποκειμένων των δεδομένων,

ε) το χρονικό διάστημα τήρησης των δεδομένων ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

στ) ενημέρωση για πιθανούς αποδέκτες των δεδομένων: ενημέρωση για το εάν λαμβάνει χώρα διαβίβαση δεδομένων σε τρίτους (εφόσον είναι απαραίτητο για εκπλήρωση της εντολής: όπως η διαβίβαση δεδομένων σε πληρεξούσιο δικηγόρο αντιδίκου, αντίδικο, δικαστήρια, δημόσιες αρχές κ.α.),

ζ) ενημέρωση για διαβιβάσεις προσωπικών δεδομένων σε άλλη χώρα - με επισήμανση εάν πρόκειται για τρίτη (εκτός ΕΕ, ΕΟΧ) χώρα,

η) ενημέρωση για τα δικαιώματα των Υποκειμένων.

Τα δικαιώματα που οφείλει να ικανοποιήσει ο / η δικηγόρος εντός ενός (1) μηνός είναι τα εξής:

i) **Δικαίωμα πρόσβασης:** Το Υποκείμενο των δεδομένων δικαιούται να γνωρίζει αν τα δεδομένα υφίστανται επεξεργασία, με ποιο τρόπο και για ποιο σκοπό.

ii) **Δικαίωμα διόρθωσης – επικαιροποίησης:** Το Υποκείμενο των δεδομένων δικαιούται να ζητήσει τη διόρθωση ανακριβών / ελλιπών δεδομένων.

iii) **Δικαίωμα διαγραφής** (δικαίωμα στη λήθη): Το Υποκείμενο των δεδομένων δικαιούται να ζητήσει τη διαγραφή μετά από το πέρας της εντολής, εφ' όσον τα δεδομένα δεν είναι απαραίτητα και εφ' όσον δεν επιβάλλεται τήρηση εκ του νόμου.

iv) **Δικαίωμα περιορισμού της επεξεργασίας.**

v) **Δικαίωμα εναντίωσης στην επεξεργασία.**

[Στα δικαιώματα συμπεριλαμβάνεται και το δικαίωμα φορητότητας, το οποίο θεωρούμε ότι καλύπτεται από την υποχρέωση της / του δικηγόρου να διαβιβάζει τον φάκελο εκ του Κώδικα (και ηλεκτρονικά). Επίσης, το δικαίωμα να μην υπόκειται το Υποκείμενο των δεδομένων σε απόφαση που έχει ληφθεί με αυτοματοποιημένο τρόπο, αλλά λόγω των προϋποθέσεων εφαρμογής και των σχετικών εξαιρέσεων πιθανολογείται ότι δεν θα συντρέχει περίπτωση εφαρμογής στο πλαίσιο της σχέσης δικηγόρου / δικηγορικού γραφείου και εντολέα].

θ) Ενημέρωση για τον τρόπο άσκησης των δικαιωμάτων και τη διατύπωση αιτημάτων και παραπόνων στην /στον δικηγόρο / δικηγορικό γραφείο.

ι) Ενημέρωση για το δικαίωμα ανάκλησης της συγκατάθεσης, εφόσον η επεξεργασία των προσωπικών δεδομένων βασίζεται σε συγκατάθεση.

ια) Ενημέρωση για το δικαίωμα της καταγγελίας στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, εγγράφως (Κηφισίας 1-3, Τ.Κ. 115 23, Αθήνα) ή ηλεκτρονικά (www.dpa.gr) μετά από την υποβολή παραπόνου στον υπεύθυνο επεξεργασίας ή τον υπεύθυνο προστασίας (DPO).

Οι πληροφορίες αυτές είναι σκόπιμο να περιλαμβάνονται και σε ιστοσελίδα/ δικτυακό τόπο που ενδεχομένως διατηρεί η/ο δικηγόρος/το δικηγορικό γραφείο.

7. Σύναψη συμβάσεων με Εκτελούντες την Επεξεργασία

Όταν αναθέτουμε σε τρίτους την επεξεργασία προσωπικών δεδομένων για λογαριασμό μας αυτοί χαρακτηρίζονται ως Εκτελούντες την Επεξεργασία.

Τέτοιες περιπτώσεις μπορεί να είναι διάφορα φυσικά πρόσωπα (εκτός του προσωπικού του γραφείου) ή εταιρίες που παρέχουν υπηρεσίες: συμβολαιογράφοι, λογιστές / λογιστικά γραφεία, δικαστικοί επιμελητές, υπηρεσίες ταχυδρομείου, υπηρεσίες συντήρησης / υποστήριξης λογισμικού κ.α. Οι Εκτελούντες βαρύνονται με την υποχρέωση να τηρούν τις οδηγίες του δικηγόρου/ δικηγορικού γραφείου ως προς την επεξεργασία προσωπικών δεδομένων αλλά και να τηρούν τις εκ του άρθρου 28 του Κανονισμού υποχρεώσεις. Οι υποχρεώσεις αυτές πρέπει να εξειδικεύονται και να αποτυπώνονται σε αμοιβαία δεσμευτικό κείμενο (σύμβαση Εκτελούντος την Επεξεργασία).

8. Μέτρα ασφαλείας

Η / Ο δικηγόρος / το δικηγορικό γραφείο ως Υπεύθυνος Επεξεργασίας υποχρεούται να λαμβάνει τεχνικά και οργανωτικά μέτρα ασφάλειας των προσωπικών δεδομένων που συλλέγει, τηρεί, χρησιμοποιεί κ.λπ. ώστε να τα προστατεύσει, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση/ ανακοίνωση σε ή πρόσβαση από μη δικαιούμενα προς τούτο πρόσωπα.

Η λήψη τεχνικών και οργανωτικών μέτρων είναι νομική υποχρέωση και η μη συμμόρφωση ελέγχεται και επισύρει την επιβολή κυρώσεων.

Πολλά από αυτά τα μέτρα είναι αναγκαίο να λαμβάνονται για τη γενικότερη προστασία των πληροφοριακών συστημάτων και των πληροφοριών που τηρούνται σε ένα γραφείο και την αντιμετώπιση σχετικών απειλών και κινδύνων (προστασία από κακόβουλο λογισμικό, ιούς, επιθέσεις σε πληροφοριακά συστήματα, φθορά δεδομένων κ.α.).

Το άρθρο 32 του Κανονισμού παραθέτει ενδεικτικά ορισμένα μέτρα προστασίας (κρυπτογράφηση κ.α.) αλλά σε κάθε περίπτωση η / ο δικηγόρος/ δικηγορικό γραφείο πρέπει να δίνει ιδιαίτερη βάση σε:

α) Δέσμευση των συνεργατών με ρήτρες εμπιστευτικότητας / εχεμύθειας – αυτό έχει ιδιαίτερη σημασία για τους συνεργάτες ενός γραφείου που δεν δεσμεύονται από το «δικηγορικό απόρρητο».

β) Προσδιορισμός και περιορισμός και καταγραφή των προσώπων που έχουν (φυσική ή ηλεκτρονική) πρόσβαση σε βάσεις δεδομένων, προσωπικά δεδομένα, αρχεία κ.α.

γ) Διαβαθμισμένη πρόσβαση στην πληροφορία με αντίστοιχη τεκμηρίωση (πολιτική πρόσβασης).

δ) Λήψη μέτρων ασφαλούς τήρησης και ελέγχου πρόσβασης ιδίως όταν πρόκειται για αρχεία με δικόγραφα, αντίγραφα δικογραφιών.

ε) Πολιτική φυσικής ασφάλειας των χώρων του γραφείου και πολιτική «καθαρού γραφείου» («κλείδωμα φακέλων», κλείδωμα υπολογιστών, προστασία εκτυπώσεων κ.α.).

στ) Πολιτική ασφαλούς καταστροφής/ διαγραφής προσωπικών δεδομένων (Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει εκδώσει στο παρελθόν την Οδηγία 1/2005, η οποία εξακολουθεί να ισχύει ως προς τις βασικές επιταγές της).

ζ) Προστασία και ασφαλή χρήση ισχυρών κωδικών / συνθηματικών.

η) Προστασία και ασφαλή χρήση και φύλαξη των συσκευών αποθήκευσης δεδομένων, ιδίως των φορητών όπως, εξωτερικούς δίσκους, usb κ.α.

θ) Χρήση σύγχρονων λειτουργικών συστημάτων και λογισμικού προστασίας από ιούς και κακόβουλο λογισμικό (firewall).

ι) Τήρηση εφεδρικών αντιγράφων ασφαλείας (back-up) σε τακτά χρονικά διαστήματα με χρήση κρυπτογράφησης.

ια) Πολιτικές χρήσης φορητών και αφαιρούμενων συσκευών και τεχνικά μέτρα για την ορθή χρήση τους.