



Οδηγός Εφαρμογής

ΟΔΗΓΙΕΣ ΕΦΑΡΜΟΓΗΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ -
GENERAL DATA PROTECTION REGULATION (GDPR) ΕΕ 2016/679

Contents

1. Εισαγωγή.....	4
2. Δήλωση Συμμόρφωσης του Οργανισμού.....	5
3. Δραστηριότητα του Οργανισμού	6
4. Αρχείο Δραστηριοτήτων Επεξεργασίας.....	7
5. Πληροφόρηση και συγκατάθεση	8
6. Τήρηση και Καταστροφή αρχείων που περιέχουν προσωπικά δεδομένα	12
7. Άσκηση δικαιωμάτων Φυσικών Προσώπων.....	15
8. Διαχείριση Καταγγελιών και Παραπόνων.....	16
9. Παραβίαση προσωπικών δεδομένων.....	17
10. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων.....	18
11. Προστασία της ιδιωτικότητας κατά το σχεδιασμό και εξ ορισμού	19
12. Επιθεωρήσεις και τήρηση συμμόρφωσης.....	20
13. Διαχείριση ιστοτόπων & επικοινωνίας.....	20
13.1 Πολιτική Απορρήτου - Privacy Policy.....	20
13.2 Πολιτική διαχείρισης Cookies.....	21
14. Διαχείριση προμηθευτών - εκτελούντων επεξεργασία.....	21
15. Ασφαλής Χρήση πληροφοριακών συστημάτων	22
15.1 Έλεγχος Πρόσβασης	22
15.2 Ηλεκτρονική Αλληλογραφία	22
15.3 Διαδίκτυο	23
15.4 Φορητές Συσκευές	24
15.5 Άλλες Οδηγίες	25
15.6 Διαχείριση Εγγράφων.....	26
16. Χρήση συστήματος Βιντεοεπιτήρησης.....	27
16.1 Βασικές αρχές.....	27

16.2	Γενικές οδηγίες Χρήσης.....	27
16.3	Τρόπος Διατήρησης Δεδομένων	28
16.4	Διαβίβαση αρχείων	28
16.5	Δικαιώματα που αφορούν την προστασία των προσωπικών δεδομένων	28
16.6	Χρόνος Τήρησης Δεδομένων.....	28
17.	Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) - Data Protection Officer (DPO)	30
18.	Ανθρώπινο δυναμικό.....	32
18.1	Υποψήφιοι εργαζόμενοι.....	32
18.2	Διαχείριση εργαζομένων	33
18.3	Αποχώρηση εργαζομένων	34

1. Εισαγωγή

Η προστασία των προσωπικών δεδομένων και πληροφοριών είναι καίριας σημασίας για τον Οργανισμό προκειμένου να επιτύχει τους στόχους του και να διασφαλίσει την ιδιωτικότητα της ζωής των φυσικών προσώπων που σχετίζονται με τη λειτουργία του.

Ο Οργανισμός είναι υπόχρεος στην τήρηση δεσμεύσεων, οι οποίες αφορούν προστασία των προσωπικών δεδομένων και απορρέουν από:

- Υποχρεώσεις συμμόρφωσης του Οργανισμού με Εθνικές νομοθετικές και κανονιστικές διατάξεις (όπως για παράδειγμα κατευθυντήριες οδηγίες, γνωμοδοτήσεις και αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, κατευθυντήριες οδηγίες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων, αποφάσεις δικαστηρίων, κώδικες δεοντολογίας, κ.λπ.)
- Υποχρεώσεις συμμόρφωσης του Οργανισμού με Ευρωπαϊκές νομοθετικές και κανονιστικές διατάξεις και ιδιαίτερα τον Γενικό Κανονισμό για την προστασία δεδομένων - GDPR
- Υποχρεώσεις που προκύπτουν από τη συνεργασία με άλλες Δημόσιες αρχές (που μπορεί να αποτελούν νομοθετική υποχρέωση, π.χ. εργατική νομοθεσία, ή παροχή στοιχείων σε Δημόσιο Φορέα) στο πλαίσιο των οποίων πραγματοποιείται επεξεργασία δεδομένων φυσικών προσώπων
- Συμβατικές υποχρεώσεις που προέρχονται από τη συνεργασία της με άλλους οργανισμούς σε εθνικό και ευρωπαϊκό επίπεδο
- Απαιτήσεις και υποχρεώσεις των πελατών, προμηθευτών, συνεργατών και εργαζομένων, οι οποίοι συναλλάσσονται με τον Οργανισμό.

Το παρόν εγχειρίδιο περιέχει αναλυτικές οδηγίες εφαρμογής με στόχο την αποτελεσματική τήρηση των υποχρεώσεων του Οργανισμού περί προστασίας των προσωπικών δεδομένων και λαμβάνοντας υπόψη σχετικά πρότυπα και βέλτιστες διεθνείς πρακτικές.

Για την εφαρμογή των οδηγιών εφαρμογής ορίζεται από τη Διοίκηση του Οργανισμού αρμόδιο στέλεχος (εσωτερικό), ο Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ), και ομάδα υποστήριξης του, οι αρμοδιότητες των οποίων περιγράφονται και προσδιορίζονται στην ενότητα 17 του παρόντος.

2. Δήλωση Συμμόρφωσης του Οργανισμού

Δηλώνεται η δέσμευση του Οργανισμού για τη συμμόρφωση με τις εξής απαιτήσεις και πρακτικές προστασίας προσωπικών δεδομένων:

- επεξεργασία των ελάχιστων προσωπικών δεδομένων μόνο όταν είναι απολύτως απαραίτητο για νομικούς και κανονιστικούς σκοπούς ή για έννομους σκοπούς του Οργανισμού
- παροχή διαφανούς πληροφόρησης προς τα φυσικά πρόσωπα για το ποιος επεξεργάζεται τα προσωπικά τους δεδομένα και τον τρόπο επεξεργασίας των προσωπικών δεδομένων
- δίκαιη και νόμιμη επεξεργασία, μόνο σχετικών και απαραίτητων προσωπικών δεδομένων
- τήρηση αρχείου δραστηριοτήτων επεξεργασίας
- επεξεργασία ακριβών και επικαιροποιημένων προσωπικών δεδομένων
- τήρηση μόνο για το χρονικό διάστημα που απαιτείται για νομικούς και κανονιστικούς λόγους και για έννομους σκοπούς του Οργανισμού
- συλλογή, επεξεργασία, διαβίβαση και αποθήκευση προσωπικών δεδομένων με βάση τις βέλτιστες διεθνείς πρακτικές ασφάλειας
- σεβασμός των δικαιωμάτων των φυσικών προσώπων και παροχή των απαραίτητων μέσων διευκόλυνσης για την απρόσκοπτη άσκησή τους
- διενέργεια εκτίμησης αντικτύπου για τις επεξεργασίες που ενδέχεται να επιφέρουν υψηλό κίνδυνο για την ιδιωτικότητα των φυσικών προσώπων
- τήρηση της αρχής προστασίας από το σχεδιασμό και εξ ορισμού (privacy by design and by default) κατά την ανάπτυξη, υλοποίηση και απόσυρση νέων υπηρεσιών
- υιοθέτηση, πιστή εφαρμογή και ένταξη στην καθημερινή λειτουργία του Οργανισμού πολιτικών, διαδικασιών και οδηγιών διαχείρισης προσωπικών δεδομένων
- ευαισθητοποίηση και εκπαίδευση όλου του προσωπικού στα ανωτέρω, ώστε να τηρούνται αποτελεσματικά
- έλεγχος αποτελεσματικής εφαρμογής των πολιτικών, διαδικασιών και οδηγιών διαχείρισης προσωπικών δεδομένων και συνεχής βελτίωσή τους
- αξιοποίηση των εξελίξεων στην τεχνολογία και στην πληροφορική για την πρακτική εφαρμογή των αρχών προστασίας των προσωπικών δεδομένων

3. Δραστηριότητα του Οργανισμού

Η κύρια δραστηριότητα του Οργανισμού είναι: Παροχή υπηρεσιών Ύδρευσης, Αποχέτευσης και Τηλεθέρμανσης

Ωστόσο, στο πλαίσιο των δραστηριοτήτων του, ο Οργανισμός προβαίνει σε επεξεργασία ορισμένων προσωπικών δεδομένων των ακόλουθων κατηγοριών φυσικών προσώπων:

Κατηγορίες Φυσικών Προσώπων	Κατηγορίες Δεδομένων Φυσικών Προσώπων
- Πελάτες (Ύδρευσης, Αποχέτευσης, Τηλεθέρμανσης) - Πολίτες - Συγγενείς πολιτών - Εργαζόμενοι - Υποψήφιοι Εργαζόμενοι - Συγγενείς εργαζομένων (συμπεριλαμβανομένων ανηλίκων) - Εκπαιδευόμενοι (ΤΕΙ, ΕΠΑΣ, ΟΑΕΔ) - Εισηγητές σεμιναρίων - Προμηθευτές - Εργαζόμενοι προμηθευτών	- Μοναδικά αναγνωριστικά (ΑΦΜ, ΑΜΚΑ, ΑΔΤ, ΑΜΑ κ.λπ.) - Βασικά Στοιχεία Φυσικού προσώπου (τηλ., διεύθ., email, ονομ/μο, φύλο κ.λπ.) - Δεδομένα υγείας (π.χ. βεβαιώσεις ασθένειας, αναπηρία, κ.λπ.) - Οικονομικά δεδομένα (π.χ. IBAN, οφειλές, κ.λπ.) - Δεδομένα ποινικού μητρώου (αντίγραφο ποινικού μητρώου, υπεύθυνη δήλωση λευκού ποινικού μητρώου) - Βαθμολογία (μοριοδότηση) - Δεδομένα ασφάλισης (π.χ. ασφαλιστική ενημερότητα) - Δεδομένα σπουδών (π.χ. πτυχία) - Δεδομένα εικόνας (καταγραφή κάμερας) - Βιομετρικά δεδομένα (αναγνώριση προσώπου)

Αναλυτικά όλες οι δραστηριότητες επεξεργασίας αποτυπώνονται στο Αρχείο Δραστηριοτήτων Επεξεργασίας.

4. Αρχείο Δραστηριοτήτων Επεξεργασίας

Με μέριμνα των στελεχών του Οργανισμού και συντονισμό και έγκριση από τον ΥΠΔ, καθορίζονται οι δραστηριότητες που περιλαμβάνουν επεξεργασία προσωπικών δεδομένων και καταρτίζεται το σχετικό Αρχείο δραστηριοτήτων επεξεργασίας λαμβάνοντας υπόψη το Υπόδειγμα Αρχείου Επεξεργασίας Δραστηριοτήτων που έχει εκδώσει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ). Ετησίως ή όταν υπάρχει κάποια κρίσιμη αλλαγή, το Αρχείο δραστηριοτήτων επεξεργασίας επικαιροποιείται από τον ΥΠΔ και κάθε νέα έκδοσή του εγκρίνεται από τη Διοίκηση του Οργανισμού.



5. Πληροφόρηση και συγκατάθεση

Τα φυσικά πρόσωπα, των οποίων τα προσωπικά δεδομένα συλλέγονται ή/ και υφίστανται περαιτέρω επεξεργασία από τον Οργανισμό, ενημερώνονται για τους σκοπούς και τα μέσα επεξεργασίας των προσωπικών τους δεδομένων, λαμβάνοντας πληροφόρηση κατ' ελάχιστον για τα εξής:

- Ταυτότητα και στοιχεία επικοινωνίας του Οργανισμού.
- Ταυτότητα και στοιχεία επικοινωνίας του Υπευθύνου Προστασίας Δεδομένων.
- Σκοπός ή σκοποί επεξεργασίας των προσωπικών δεδομένων.
- Νομιμοποιητική βάση επεξεργασίας των προσωπικών δεδομένων.
- Αποδέκτες ή κατηγορίες αποδεκτών των προσωπικών δεδομένων. Στις περιπτώσεις όπου τα δεδομένα δεν διαβιβάζονται σε τρίτους, αναφέρεται ρητά.
- Χρονικό διάστημα διατήρησης των προσωπικών δεδομένων ή τα κριτήρια που καθορίζουν το εν λόγω διάστημα.
- Αναφορά στη δυνατότητα του φυσικού προσώπου για υποβολή αιτήματος σχετικά με τα ακόλουθα δικαιώματα επί των προσωπικών δεδομένων: πρόσβαση και διόρθωση ή διαγραφή των δεδομένων, περιορισμό της επεξεργασίας ή δικαίωμα εναντίωσης στην επεξεργασία, δικαίωμα στη φορητότητα των δεδομένων, δικαίωμα ανάκλησης της συγκατάθεσης οποτεδήποτε, καθώς και δικαίωμα υποβολής καταγγελίας στην ΑΠΔΠΧ.
- Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων (εφόσον εφαρμοστεί μελλοντικά), συμπεριλαμβανομένης της κατάρτισης προφίλ, και, τουλάχιστον για αυτές τις περιπτώσεις, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.
- Στις περιπτώσεις όπου τα δεδομένα δεν έχουν συλλεχθεί απευθείας από το φυσικό πρόσωπο, επιπρόσθετα των ανωτέρω να παρέχεται ενημέρωση σχετικά με την πηγή άντλησης/ λήψης των δεδομένων και βάσει ποιου πλαισίου.

Στον πίνακα που ακολουθεί φαίνονται οι κατηγορίες των φυσικών προσώπων στα οποία παρέχεται η πληροφόρηση, καθώς και τα χρησιμοποιούμενα ανά περίπτωση μέσα ή/ και έντυπα:

Κατηγορίες φυσικών προσώπων	Έγγραφα ή άλλα μέσα που περιλαμβάνουν το κείμενο πληροφόρησης
Πελάτες	- Αιτήσεις παροχής Ύδρευσης, Αποχέτευσης και Τηλεθέρμανσης - Συμβάσεις παροχής Ύδρευσης, Αποχέτευσης και Τηλεθέρμανσης - Αίτηση ένταξης στο κοινωνικό τιμολόγιο - Έντυπο αντικατάστασης υδρομέτρου - Έντυπο εξουσιοδότησης

Κατηγορίες φυσικών προσώπων	Έγγραφα ή άλλα μέσα που περιλαμβάνουν το κείμενο πληροφόρησης
	- Λογαριασμός (πελάτες Τηλεθέρμανσης)
Ιδιοκτήτες ακινήτων	- Έντυπο προς εκμισθωτές
Εκπαιδευόμενοι	- Αίτηση για πρακτική άσκηση - Ενημερωτικό έντυπο για τα προσωπικά δεδομένα
Εργαζόμενοι	- Παράρτημα Σύμβασης – Προστασία Δεδομένων Προσωπικού Χαρακτήρα - Υπεύθυνη Δήλωση εργαζομένου
Προμηθευτές	- Συμβάσεις

Η παροχή πληροφόρησης από τον Οργανισμό στα φυσικά πρόσωπα είναι συνοπτική, διαφανής, κατανοητή και εύκολα προσβάσιμη, χρησιμοποιώντας σαφή και απλή διατύπωση ακολουθώντας τις παρακάτω αρχές:

- Αποφεύγεται η αναφορά άρθρων και παραγράφων Νομοθεσίας (π.χ. έχετε δικαίωμα πρόσβασης στα προσωπικά σας δεδομένα σύμφωνα με το άρθρο 15 του Ευρωπαϊκού Κανονισμού GDPR) χωρίς πρόσθετη συνοπτική επεξήγηση (όπου είναι εφικτό), δεδομένου ότι πολύ μεγάλο ποσοστό των ατόμων δεν πρόκειται να διαβάσει τον Κανονισμό ή το Νόμο και μπορεί να εκληφθεί ως μη κατανοητή και εύκολα προσβάσιμη πληροφόρηση, και ως ένας τρόπος εκμείευσης της συγκατάθεσης του φυσικού προσώπου χωρίς να είναι βέβαιος στο τι συγκατατίθεται (συνεπώς θα θεωρηθεί ότι η συγκατάθεση δεν δόθηκε εν πλήρει επιγνώσει).
- Η μορφοποίηση είναι τέτοια ώστε το κείμενο πληροφόρησης να είναι άμεσα διακριτό και ορατό στον αναγνώστη. Χρησιμοποιείται έντονη γραφή για κρίσιμες λέξεις ή φράσεις, υπογράμμιση, επαρκής απόσταση μεταξύ γραμμών μιας παραγράφου, επαρκές μέγεθος γραμματοσειράς, χρήση της λέξης «ΠΡΟΣΟΧΗ» σε κόκκινο χρώμα και αρκετά μεγάλο μέγεθος γραμματοσειράς για σημαντικές ενότητες κ.λπ.
- Περιγράφονται λεπτομερώς οι ενέργειες που απαιτούνται από ένα φυσικό πρόσωπο (πελάτης, υποψήφιος για πρόσληψη, κ.λπ.) για να ασκήσει ένα από τα δικαιώματά του αναφορικά με τα προσωπικά δεδομένα, καθώς και τα σημεία και μέσα επικοινωνίας (π.χ. ΥΠΔ, email κ.α.).
- Χρησιμοποιείται διαστρωματική πληροφόρηση (layered privacy notice) ή αναδυόμενα παράθυρα πληροφόρησης (pop-up εμφανίσεις) σε περιπτώσεις ηλεκτρονικής πληροφόρησης, όπου το φυσικό πρόσωπο επιλέγει το σημείο της πληροφόρησης για το οποίο θέλει άμεσα να ενημερωθεί (π.χ. για τους σκοπούς επεξεργασίας) ή ενημερώνεται κατά την αναζήτηση σχετικής πληροφόρησης, αντίστοιχα.
- Χρησιμοποιείται ιεραρχική αποτύπωση (π.χ. bullets, αρίθμηση)

- Χρησιμοποιείται ενεργητική και όχι παθητική φωνή, ενώ αποφεύγονται οι εκφράσεις που οδηγούν σε αμφιβολία, όπως "μπορεί", "είναι πιθανόν", "ίσως".

Εάν τα προσωπικά δεδομένα δεν συλλέγονται άμεσα από το φυσικό πρόσωπο και ο Οργανισμός έχει το ρόλο του Υπεύθυνου Επεξεργασίας, διασφαλίζει ότι τα φυσικά πρόσωπα ενημερώνονται για τα ανωτέρω εντός εύλογης προθεσμίας, η οποία δε θα ξεπερνάει τον ένα μήνα από την συλλογή των δεδομένων και σε κάθε περίπτωση κατά την πρώτη επικοινωνία με το φυσικό πρόσωπο.

Στις περιπτώσεις επεξεργασίας προσωπικών δεδομένων που νομιμοποιητική βάση επεξεργασίας είναι η συγκατάθεση, η λήψη της πραγματοποιείται μέσω όλων των καναλιών επικοινωνίας με τα φυσικά πρόσωπα (έντυπη αίτηση, ηλεκτρονική φόρμα κ.λπ.) λαμβάνοντας τις απαιτήσεις του Κανονισμού ώστε να είναι ελεύθερη και έπειτα από κατάλληλη πληροφόρηση. Το ενημερωτικό κείμενο που παρέχεται στα φυσικά πρόσωπα περιλαμβάνει κατ' ελάχιστον τα εξής:

- Όνομα του Υπεύθυνου Επεξεργασίας και των από κοινού Υπευθύνων (όπου εφαρμόζεται)
- Σκοπός ή σκοποί επεξεργασίας των προσωπικών δεδομένων που συλλέγονται, ανά περίπτωση συγκατάθεσης
- Το είδος των προσωπικών δεδομένων που συλλέγονται στο πλαίσιο του σκοπού επεξεργασίας για τον οποίο ζητείται η συγκατάθεση
- Ενημέρωση για το δικαίωμα ανάκλησης της συγκατάθεσης και τον τρόπο ανάκλησης αυτής
- Πληροφόρηση για την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων (εφόσον εφαρμόζεται ή εφαρμοστεί μελλοντικά), συμπεριλαμβανομένης της κατάρτισης προφίλ, και, τουλάχιστον για αυτές τις περιπτώσεις, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το φυσικό πρόσωπο,
- Γενικές κατηγορίες πιθανών αποδεκτών προσωπικών δεδομένων (π.χ. τράπεζες, άλλες δημόσιες υπηρεσίες, κλπ.). Στην περίπτωση που αποτελεί κρίσιμο προμηθευτή/ συνεργάτη για την παροχή της υπηρεσίας, η πληροφόρηση γίνεται με ονομαστική αναφορά.

Το κείμενο για τη λήψη συγκατάθεσης είναι σαφώς διακριτό από άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση και πληροί τις παρακάτω προϋποθέσεις:

- Η συγκατάθεση γίνεται με σαφή, θετική ενέργεια του φυσικού προσώπου (π.χ. επιλογή τετραγωνιδίου κατά την επίσκεψη της διαδικτυακής ιστοσελίδας, επιλογή επιθυμητών τεχνικών ρυθμίσεων για υπηρεσίες της κοινωνίας των πληροφοριών ή μια δήλωση ή συμπεριφορά που δηλώνει σαφώς, ότι το φυσικό πρόσωπο αποδέχεται την πρόταση επεξεργασίας των προσωπικών του δεδομένων) και όχι στο πλαίσιο γενικών όρων συμβάσεων ή με οποιαδήποτε ένδειξη σιωπηρής απραξίας. Η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν εκλαμβάνονται ως συγκατάθεση.

- Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, δίνεται συγκατάθεση για όλους αυτούς τους σκοπούς ξεχωριστά.
- Η πληροφόρηση που παρέχεται στο πλαίσιο παροχής της συγκατάθεσης μέσω ιστοσελίδας διαφέρει αναλόγως των δυνατοτήτων της ιστοσελίδας. Γίνεται παραπομπή στην Πολιτική Απορρήτου που έχει αναρτηθεί στην ιστοσελίδα ή εναλλακτικά στο link με την εμφάνιση ενός pop-up παραθύρου, στο οποίο θα περιλαμβάνεται η απαραίτητη πληροφόρηση. Κατ' ελάχιστον, η πληροφόρηση υπάρχει στην Πολιτική Απορρήτου του ιστότοπου με παραπομπή σε αυτήν από κάθε άλλο σημείο.
- Ο τρόπος ανάκλησης της συγκατάθεσης του φυσικού προσώπου πραγματοποιείται με την ίδια ευκολία όπως έγινε η αρχική παροχή (π.χ. συμπλήρωση ενός εντύπου, ηλεκτρονική επιλογή ή αποεπιλογή αντίστοιχου κυτίου (checkbox) κ.λπ.) και χωρίς χρέωση του φυσικού προσώπου.
- Γίνεται χρήση διπλής επιβεβαίωσης (double opt-in) της συγκατάθεσης του φυσικού προσώπου.
- Γίνεται λήψη γραπτής συγκατάθεσης σε περίπτωση επεξεργασίας προσωπικών δεδομένων ειδικών κατηγοριών (βιομετρικά δεδομένα), σε περίπτωση απουσίας άλλης νομοποιητικής βάσης (βάσει του άρθρου 9)

Ο Οργανισμός ως Υπεύθυνος Επεξεργασίας φέρει το βάρος απόδειξης της συγκατάθεσης του υποκειμένου για την επεξεργασία των προσωπικών δεδομένων του, γι' αυτό οφείλει να είναι σε θέση να τεκμηριώσει τη λήψη συγκατάθεσης ανά σκοπό επεξεργασίας επικαλούμενη τον τρόπο λήψης αυτής (π.χ. έντυπη φόρμα λήψης συγκατάθεσης, κ.λπ.), αλλά και να αποδείξει ότι η λήψη της έγινε κατόπιν ενημέρωσης του προσώπου.

Ο Οργανισμός τηρεί μητρώα συγκαταθέσεων στα οποία καταγράφονται ο σκοπός επεξεργασίας, το μέσο πληροφόρησης του φυσικού προσώπου, η ημερομηνία παροχής της συγκατάθεσης, ο τρόπος τεκμηρίωσής της (π.χ. ενυπόγραφη φόρμα) και αν είναι σε ισχύ. Επισημαίνεται ότι για την επεξεργασία των προσωπικών δεδομένων ειδικών κατηγοριών (δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και γενετικά δεδομένα, βιομετρικά δεδομένα που υπόκεινται σε επεξεργασία με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό) ο Οργανισμός συλλέγει έγγραφη, ρητή (ξεχωριστή) συγκατάθεση από το φυσικό πρόσωπο.

6. Τήρηση και Καταστροφή αρχείων που περιέχουν προσωπικά δεδομένα

Ο Οργανισμός είναι υπεύθυνος για τον καθορισμό του μέγιστου χρόνου τήρησής των αρχείων που περιέχουν προσωπικά δεδομένα σε ηλεκτρονική ή φυσική μορφή. Ο χρόνος τήρησης προσδιορίζεται με βάση:

- Την υποχρέωση τήρησης των νομικών και κανονιστικών απαιτήσεων σε σχέση με τη διαχείριση προσωπικών δεδομένων
- Τις υποχρεώσεις τήρησης απαιτήσεων τρίτων μερών
- Τις ανάγκες του Οργανισμού στα πλαίσια εκτέλεσης των λειτουργιών του

και αποτυπώνεται σε Πολιτική Αποθήκευσης/ Καταστροφής Φυσικού και Ηλεκτρονικού Αρχείου.

Οι ενδεικτικοί προβλεπόμενοι ελάχιστοι χρόνοι τήρησης προσωπικών δεδομένων κατά τη νομοθεσία (*με την επιφύλαξη νομοθετικών τροποποιήσεων) είναι:

Αντικείμενο	Ελάχιστος Χρόνος Τήρησης
Γενικές Διατάξεις (ΑΚ 249, 250)	5 ή 20 έτη (ανάλογα με τη φύση των δεδομένων)
Φάκελος Εργαζομένου - μισθολόγια, καταστάσεις μισθοδοσίας, μαγνητικές ταινίες, δισκέτες, Ασφαλιστικό Βιβλιάριο Ασφαλισμένου, Βιβλιάριο Υποχρέωσης Καταβολής Εισφορών, Ανακεφαλαιωτικές Καταστάσεις, Εντολές Ασφάλισης Οικοδόμων (αρ. 6 παρ. 1 ε. Ν. 2972/2001, αρ. 15 παρ.2 Ν. 2972/2001) – όχι λοιπά στοιχεία φακέλου, όπως αξιολογήσεις κλπ.	10ετία, η οποία αρχίζει από την πρώτη ημέρα του επόμενου έτους από εκείνο μέσα στο οποίο παρασχέθηκε η ασφαλιστέα εργασία ή υπηρεσία (χονδρικά 11 έτη)
Φάκελος Εργαζομένου – λοιπά στοιχεία (υπ' αρ. 4/2013 απόφαση ΑΠΔΠΧ)	Για εργαζομένους: πέντε έτη από τη λήξη της εργασιακής σχέσης, Για υποψήφιους εργαζομένους: έξι μήνες από την ολοκλήρωση της διαδικασίας πρόσληψης
Εκπλήρωση φορολογικών υποχρεώσεων πιστωτικών ιδρυμάτων και επενδυτικών σχημάτων, που αφορούν διαβίβαση δεδομένων πελατών τους (αρ. 36 παρ. 3 Ν. 4174/2013)	20ετία για τα δεδομένα που διαβιβάζονται

Αντικείμενο	Ελάχιστος Χρόνος Τήρησης
Βιβλία & Στοιχεία (συνεπώς και συναλλαγές – τιμολόγια/ αρ. 84 παρ. 1, Ν. 2238/1994 και Ν. Ν. 4174/2013)	δετία από το τέλος της χρήσης που αφορούν (χονδρικά 7 έτη – να σημειωθεί ότι υπάρχει πληθώρα υποπεριπτώσεων που θα πρέπει πάντα να ελέγχονται)
Βιντεοεπιτήρηση (άρ. 8 της υπ' αριθμ. 1/2011 Οδηγίας ΑΠΔΠΧ- Ομοίως και το σχέδιο νόμου για την ενσωμάτωση του GDPR, αρ. 5, παρ. 6.)	15 εργάσιμες ημέρες

■ Γενικές διατάξεις

Η συνθηθέστερη παραγραφή, επομένως, και ο χρόνος τήρησης των αντίστοιχων προσωπικών δεδομένων είναι η 5ετία (ΑΚ 250). Παρόλα αυτά κάποιες αξιώσεις που αφορούν τα ίδια δεδομένων παραγράφονται στην 20ετία (ΑΚ 249). Συνεπώς, θα πρέπει να εξετασθεί ανά κατηγορία δεδομένων ο χρόνος τήρησής τους.

■ Παραγραφή ΙΚΑ για εργατικά θέματα

Ο Οργανισμός οφείλει να διατηρεί αντίγραφο της υποβληθείσας ΑΠΔ για χρόνο ίσο με το χρόνο παραγραφής του δικαιώματος του ΙΚΑ-ΕΤΑΜ για τη βεβαίωση των απαιτήσεων του (άρθρο 6 παρ. 1 ε Ν. 2972/2001). Το δικαίωμα του ΙΚΑ-ΕΤΑΜ για τη βεβαίωση σε ευρεία έννοια όλων των χρηματικών απαιτήσεων του, καθώς και των απαιτήσεων των φορέων, κλάδων ή λογαριασμών των οργανισμών κοινωνικής πολιτικής των οποίων τις εισφορές συνεισπράττει το ΙΚΑ-ΕΤΑΜ, **υπόκειται σε δεκαετή παραγραφή**, η οποία αρχίζει από την πρώτη ημέρα του επόμενου έτους από εκείνο μέσα στο οποίο παρασχέθηκε η ασφαλιστέα εργασία ή υπηρεσία (άρθρο 15 παρ. 2 Ν. 2972/2001).

Ο Οργανισμός υποχρεούται και μετά την εφαρμογή της ΑΠΔ να διατηρούν επί δεκαετία τα στοιχεία τα οποία τηρούσαν και υπέβαλαν, κατά τις οικείες διατάξεις, στις υπηρεσίες του ΙΚΑ-ΕΤΑΜ, και τα οποία αντικαθίστανται από την ΑΠΔ (μισθολόγια, καταστάσεις μισθοδοσίας, μαγνητικές ταινίες, δισκέτες, Ασφαλιστικό Βιβλιάριο Ασφαλισμένου, Βιβλιάριο Υποχρέωσης Καταβολής Εισφορών, Ανακεφαλαιωτικές Καταστάσεις) (άρθρο 6 παρ. 2 Ν. 2972/2001).

■ Για φορολογικά στοιχεία

Αρ. 13 παρ. 2 ν.4174/2013:

Τα λογιστικά αρχεία, φορολογικοί ηλεκτρονικοί μηχανισμοί, φορολογικές μνήμες και αρχεία που δημιουργούν οι φορολογικοί ηλεκτρονικοί μηχανισμοί πρέπει να διαφυλάσσονται κατ' ελάχιστον:

- a) για διάστημα πέντε (5) ετών από τη λήξη του αντίστοιχου φορολογικού έτους εντός του οποίου υπάρχει η υποχρέωση υποβολής δήλωσης ή
- b) εφόσον συντρέχουν οι προϋποθέσεις της παραγράφου 2 του άρθρου 36 του Κώδικα, έως ότου παραγραφεί το δικαίωμα έκδοσης από τη Φορολογική Διοίκηση πράξης προσδιορισμού του φόρου, σύμφωνα με τα οριζόμενα στην παράγραφο αυτή ή
- c) έως ότου τελεσιδικήσει η απαίτηση της Φορολογικής Διοίκησης σε συνέχεια διενέργειας φορολογικού ελέγχου ή έως ότου αποσβεστεί ολοσχερώς η απαίτηση λόγω εξόφλησης.

■ **Καταγραφές συναλλαγών (τιμολογίων κλπ.)**

Υπό κανονικές συνθήκες, οι επιχειρήσεις υποχρεούνται σε διαφύλαξη των βιβλίων και στοιχείων τους για έξι χρόνια, σύμφωνα με τις ισχύουσες διατάξεις (αρ. 84 παρ. 1, Ν. 2238/1994 και (Ν. 4174/2013).

■ **Φάκελος εργαζομένου (λουπά δεδομένα)**

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα προτείνει σε Γνωμοδότησή της (4/2013) να προσδιοριστεί ο μέγιστος χρόνος τήρησης, για τους ήδη εργαζόμενους, στα πέντε έτη από τη λήξη της εργασιακής σχέσης.

■ **Βιντεοεπιτήρηση**

Στο αρ. 8 της υπ' αριθμ. 1/2011 Οδηγίας ρυθμίζεται ο χρόνος τήρησης των δεδομένων συστημάτων βιντεοεπιτήρησης, και ορίζεται ότι τα δεδομένα πρέπει να τηρούνται για συγκεκριμένο χρονικό διάστημα ενόψει του επιδιωκόμενου κάθε φορά σκοπού επεξεργασίας. Σε κάθε περίπτωση, εφόσον από τη λήψη εικόνων που αποθηκεύονται ή τη λήψη που γίνεται σε πραγματικό χρόνο δεν προκύπτει επέλευση συμβάντος που εμπίπτει στον επιδιωκόμενο σκοπό, τα δεδομένα πρέπει να καταστρέφονται το αργότερο μέσα σε δεκαπέντε (15) εργάσιμες ημέρες, με την επιφύλαξη ειδικότερων διατάξεων της κείμενης νομοθεσίας που ισχύουν για συγκεκριμένες κατηγορίες υπεύθυνων επεξεργασίας (π.χ. καζίνο) ή αν στην παρούσα Οδηγία ορίζεται διαφορετικά.

Ο Οργανισμός είναι υπεύθυνος να υλοποιεί τη διαγραφή των αρχείων μετά τα προβλεπόμενα χρονικά διαστήματα τήρησης ή να υλοποιεί τα αιτήματα διαγραφής των φυσικών προσώπων, σε περίπτωση που αυτά δεν έρχονται σε αντίθεση με άλλη νομική υποχρέωση του Οργανισμού. Ο τρόπος διαγραφής των αρχείων, αν πρόκειται για φυσικά αρχεία καθημερινής χρήσης είναι η καταστροφή μέσω shredder. Η διαγραφή των ηλεκτρονικών αρχείων, γίνεται από όλα τα σημεία αποθήκευσης (π.χ. από email, τοπικούς φακέλους, servers κ.λπ.) και είναι οριστική διαγραφή (όχι μετακίνηση σε άλλο φάκελο ή απλή διαγραφή στον κάδο ανακύκλωσης), ενώ και η ανωνυμοποίηση των δεδομένων ισοδυναμεί με καταστροφή.

7. Άσκηση δικαιωμάτων Φυσικών Προσώπων

Ο Οργανισμός συγκεντρώνει και αξιολογεί τα αιτήματα των φυσικών προσώπων, σχετικά με την ικανοποίηση των δικαιωμάτων τους (πρόσβαση, διόρθωση, διαγραφή, φορητότητα, περιορισμός της επεξεργασίας, εναντίωση στην επεξεργασία). Τα αιτήματα λαμβάνονται μέσω των μηχανισμών που έχουν τεθεί σε εφαρμογή (π.χ. στην ταχυδρομική διεύθυνση του Οργανισμού, στη διεύθυνση ηλεκτρονικού ταχυδρομείου, στις ηλεκτρονικές φόρμες επικοινωνίας, σε τηλεφωνική γραμμή επικοινωνίας κ.λπ.). Ο Οργανισμός απαντά στα αιτήματα των φυσικών προσώπων δωρεάν και εντός (1) ενός μηνός. Αν χρειαστεί λαμβάνει παράταση άλλων (2) δύο μηνών αφού ενημερώσει τον αιτούντα σχετικά και καταγράφει τους λόγους. Αν τα αιτήματα είναι προδήλως αβάσιμα ή υπερβολικά ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους, ο Οργανισμός μπορεί να επιβάλει την καταβολή εύλογου τέλους ή να αρνηθεί να δώσει συνέχεια στο αίτημα.

Σε κάθε περίπτωση, για να ικανοποιήσει ο Οργανισμός ένα αίτημα, αξιοποιεί τις πληροφορίες που περιλαμβάνονται στο Αρχείο Δραστηριοτήτων Επεξεργασίας.



Τα αιτήματα που είναι σε θέση ο Οργανισμός να ικανοποιήσει, εφόσον από την αρχική αξιολόγηση προκύψουν ότι είναι βάσιμα, αφορούν τα εξής:

- Δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα: ο Οργανισμός παρέχει στο φυσικό πρόσωπο την πληροφόρηση που αιτείται, σχετικά με την επεξεργασία των προσωπικών του δεδομένων, όπως σκοποί επεξεργασίας, κατηγορίες δεδομένων, χρόνοι τήρησης, αποδέκτες, τα δικαιώματά του κ.λπ. Επίσης, είναι σε θέση να παρέχει δωρεάν στο φυσικό πρόσωπο ένα αντίγραφο των προσωπικών του δεδομένων αν το αιτηθεί, σε ηλεκτρονική μορφή, εφόσον τηρούνται ηλεκτρονικά. Κάθε φυσικό πρόσωπο λαμβάνει αντίγραφο των δικών του και μόνο δεδομένων προσωπικού χαρακτήρα και όχι τρίτων.
- Δικαίωμα διόρθωσης, δικαίωμα διαγραφής και δικαίωμα αναστολής ή διακοπής της επεξεργασίας των δεδομένων: Ο Οργανισμός εκτελεί τις σχετικές ενέργειες (διαγραφή, διόρθωση, παύση ή αναστολή της επεξεργασίας). Ενημερώνει άμεσα οποιονδήποτε επεξεργάζεται τα προσωπικά δεδομένα του φυσικού προσώπου που υπέβαλλε το αίτημα, είτε ανήκει στο προσωπικό του Οργανισμού, είτε είναι εξωτερικός συνεργάτης ή άλλη τρίτη οντότητα που έχει λάβει από τον Οργανισμό τα προσωπικά δεδομένα του φυσικού προσώπου, ώστε να προβεί στις αντίστοιχες ενέργειες.

- Δικαίωμα ανάκλησης συγκατάθεσης: Το φυσικό πρόσωπο μπορεί να ανακαλεί τη συγκατάθεσή του συνολικά ή/ και τμηματικά κατά τον χρόνο που επιθυμεί και με την ίδια ευκολία με την οποία αρχικά έδωσε τη συγκατάθεσή του.
- Δικαίωμα στη φορητότητα: Ο Οργανισμός παρέχει στο φυσικό πρόσωπο τα προσωπικά του δεδομένα που έχει ο ίδιος δώσει σε αυτήν, σε ηλεκτρονικό αρχείο κατάλληλης μορφής. Εφόσον το φυσικό πρόσωπο το επιθυμεί, η Οργανισμός διαβιβάζει τα δεδομένα σε άλλο οργανισμό ή ιδιωτική εταιρεία που θα της υποδειχθεί, σε περίπτωση που αυτό είναι τεχνικά εφικτό (εφαρμογή μόνο στην περίπτωση που υπάρξει μελλοντικά μια ιδιωτική εταιρεία η οποία να παρέχει τις ίδιες υπηρεσίες με τον Οργανισμό).

8. Διαχείριση Καταγγελιών και Παραπόνων

Ο Οργανισμός ενημερώνει το φυσικό πρόσωπο για τη δυνατότητα υποβολής καταγγελίας εις βάρος της στην Εποπτική Αρχή, τόσο κατά την πληροφόρηση όσο και κατά την αδυναμία εξυπηρέτησης αιτήματός του.

Σε περίπτωση λήψης καταγγελίας από την Εποπτική Αρχή ή ενός παραπόνου από φυσικό πρόσωπο, που αφορά τα προσωπικά του δεδομένα που επεξεργάζεται ο Οργανισμός, διερευνάται άμεσα η καταγγελία ή το παράπονο και ο ΥΠΔ συντονίζει τη διαχείριση της υπόθεσης έως την ολοκλήρωσή της. Οι καταγγελίες καταγράφονται σε ένα μητρώο καταγγελιών, στο οποίο περιλαμβάνονται όλες οι λεπτομέρειες που σχετίζονται με αυτήν (π.χ. τι αφορά, ημερομηνία υποβολής, αποτέλεσμα καταγγελία κ.λπ.).

Για την υποβολή καταγγελίας έχουν εκδοθεί υποδείγματα καταγγελιών από την ΑΠΔΠΧ, τα οποία μπορούν να βρεθούν στο παρακάτω link:

http://www.dpa.gr/portal/page?_pageid=33,211532&_dad=portal&_schema=PORTAL



9. Παραβίαση προσωπικών δεδομένων

Σε περίπτωση εντοπισμού παραβίασης προσωπικών δεδομένων ο Οργανισμός αξιολογεί το περιστατικό σε συνεργασία με τον ΥΠΔ και τη Διοίκηση και τυχόν άλλους εμπλεκόμενους (IT, Προμηθευτές, κ.λπ.), και εξετάζει εάν απαιτείται γνωστοποίηση της παραβίασης στην ΑΠΔΠΧ. Ο Οργανισμός προχωράει σε γνωστοποίηση παραβίασης στην ΑΠΔΠΧ όταν η παραβίαση ενδέχεται να προκαλέσει κίνδυνο στα δικαιώματα και τις ελευθερίες των προσώπων τα οποία αφορά το περιστατικό. Επιπλέον, ο Οργανισμός ενημερώνει και τα φυσικά πρόσωπα αν κριθεί απαραίτητο (όταν ενδέχεται να υπάρξει υψηλός κίνδυνος για τα φυσικά πρόσωπα από την παραβίαση, π.χ. παραβίαση προσωπικών δεδομένων ειδικών κατηγοριών ή οικονομικών δεδομένων), για το περιστατικό παραβίασης προσωπικών δεδομένων και για τα μέτρα που θα πρέπει να λάβουν.

Ενδεικτικά αναφέρονται τα παρακάτω παραδείγματα:

Παραβίαση	Γνωστοποίηση στην ΑΠΔΠΧ	Ενημέρωση φυσικών προσώπων
Παραβίαση προσωπικών δεδομένων που είναι δημόσια διαθέσιμα και δεν ενδέχεται να επιφέρουν κίνδυνο για τα φυσικά πρόσωπα.	Δεν απαιτείται γνωστοποίηση προς την ΑΠΔΠΧ.	Δεν απαιτείται ενημέρωση των φυσικών προσώπων.
Παραβίαση εμπιστευτικότητας προσωπικών δεδομένων που είναι ασφαλώς κρυπτογραφημένα.	Απαιτείται γνωστοποίηση προς την ΑΠΔΠΧ.	Δεν απαιτείται ενημέρωση των φυσικών προσώπων.
Παραβίαση ακεραιότητας ή διαθεσιμότητας δεδομένων που ήταν ασφαλώς κρυπτογραφημένα.	Απαιτείται γνωστοποίηση προς την ΑΠΔΠΧ.	Ενδεχομένως να απαιτείται γνωστοποίηση προς τα φυσικά πρόσωπα (π.χ. αν τα προσωπικά δεδομένα ήταν ειδικών κατηγοριών ή οικονομικά δεδομένα).

Ο Οργανισμός τηρεί μητρώο παραβιάσεων προσωπικών δεδομένων. Επίσης, για την γνωστοποίηση της παραβίασης χρησιμοποιείται το «Έντυπο Γνωστοποίησης» που έχει εκδοθεί από την ΑΠΔΠΧ το οποίο μπορεί να βρεθεί στο παρακάτω link:

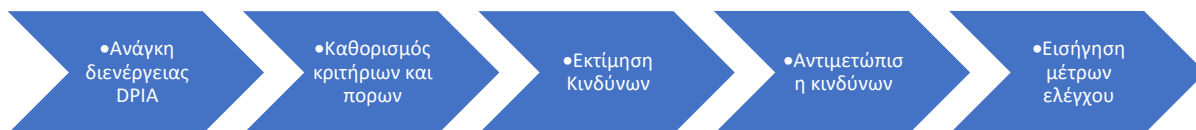
http://www.dpa.gr/portal/page?_pageid=33,211142&_dad=portal&_schema=PORTAL



10. Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

Ο Οργανισμός δεν έχει προχωρήσει στη διενέργεια εκτίμησης αντικτύπου για τους υφιστάμενους σκοπούς επεξεργασίας. Η απόφασή της τεκμηριώνεται γραπτώς από τη Διοίκηση και τον ΥΠΔ. Ωστόσο, έχει θέσει τα παρακάτω κριτήρια για την αξιολόγηση ανάγκης διενέργειας μελέτης εκτίμησης αντικτύπου σε νέες πράξεις επεξεργασίας: η χρήση νέων τεχνολογιών ή η εισαγωγή ή μεταβολής υπηρεσίας στην οποία πραγματοποιείται επεξεργασία προσωπικών δεδομένων:

- η λήψη απόφασης για την έναρξη επεξεργασίας προσωπικών δεδομένων ειδικών κατηγοριών,
- αλλαγές στο νομικό και κανονιστικό πλαίσιο σε σχέση με την επεξεργασία προσωπικών δεδομένων,
- επέκταση των επιχειρησιακών δραστηριοτήτων του Οργανισμού,
- σχετική εντολή από εποπτική ή κρατική αρχή,
- συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών των φυσικών προσώπων με αυτοματοποιημένη επεξεργασία,
- μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών,
- συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.



11. Προστασία της ιδιωτικότητας κατά το σχεδιασμό και εξ ορισμού

Ο Οργανισμός λαμβάνει υπόψη του, τις βάσεις που θέτει ο Ευρωπαϊκός Κανονισμός GDPR για την προστασία των προσωπικών δεδομένων και τον μετριασμό των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων κατά τη διαδικασία σχεδιασμού νέων δραστηριοτήτων (π.χ. σχεδιασμό νέων συστημάτων, προϊόντων και υπηρεσιών) και τις σχετικές με το θέμα απόψεις του Ευρωπαίου Επόπτη Προστασίας Δεδομένων, ώστε να λαμβάνονται υπόψιν προβλέψεις για την προστασία των δεδομένων προσωπικού χαρακτήρα:

A. από το σχεδιασμό:

1. Το αποτέλεσμα ενός έργου σχεδιασμού της επεξεργασίας, περιλαμβάνει την προστασία των δεδομένων και των δικαιωμάτων των φυσικών προσώπων σε όλο τον κύκλο ζωής του έργου, δηλαδή από τη φάση του σχεδιασμού έως και την ολοκλήρωση της επιχειρησιακής φάσης (επεξεργασία και διακοπή αυτής). Οι απαιτήσεις αυτές αποτυπώνονται στις προδιαγραφές του έργου.
2. Η προσέγγιση διαχείρισης κινδύνου για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων γίνεται με την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, λαμβάνοντας υπόψη τις διαθέσιμες τεχνολογίες και το κόστος εφαρμογής τους τόσο από σκοπιάς επιχειρηματικής πρακτικής και φιλοσοφίας όσο και από άποψη εκτίμησης του ρίσκου της έναντι και του εκτιμώμενου κόστους υλοποίησης (cost benefit analysis) και των απαιτήσεων του Κανονισμού.
3. Ο συνεχής έλεγχος της καταλληλότητας και αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων για την επίτευξη των βασικών αρχών επεξεργασίας (π.χ. αρχή της ακεραιότητας και εμπιστευτικότητας, αρχή της λογοδοσίας κ.λπ.).
4. Την ολοκληρωμένη προσέγγιση της ενσωμάτωσης των απαιτήσεων σε όλη την επεξεργασία, περιλαμβάνοντας και μέσα τα οποία θεωρούνται «εξωτερικά» της επεξεργασίας, όπως κείμενα πληροφόρησης γι' αυτήν.

B. εξ ορισμού:

1. Επεξεργασία μόνο των ελάχιστων απαιτητών προσωπικών δεδομένων για τον οριζόμενο σκοπό επεξεργασίας βάσει και των νομικών απαιτήσεων και τη διαφανή πληροφόρηση προς τα φυσικά πρόσωπα.
2. Ορισμός του εύρους των προσωπικών δεδομένων που συλλέγονται, της περιόδου αποθήκευσης και της προσβασιμότητας σε αυτά, με την ιδιαιτερότητα της εξ' ορισμού διασφάλισης ότι τα δεδομένα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων.

Τέλος, επιλέγει συνεργάτες-εκτελούντες την επεξεργασία που εφαρμόζουν και συμμορφώνονται με τα παραπάνω.

12. Επιθεωρήσεις και τήρηση συμμόρφωσης

Ο Οργανισμός διενεργεί ετησίως εσωτερικές επιθεωρήσεις αναφορικά με τις εφαρμοζόμενες πρακτικές, διαδικασίες, οδηγίες, κ.λπ., για την επεξεργασία των προσωπικών δεδομένων. Στόχος είναι ο εντοπισμός αποκλίσεων από τα όσα έχουν γνωστοποιηθεί στο προσωπικό του Οργανισμού και έχει θέσει ως υποχρεωτικά η Διοίκηση.

Η Διοίκηση του Οργανισμού ανασκοπεί τα θέματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα ετησίως ή/ και εκτάκτως, εφόσον πρόκειται για επείγουσες/ κρίσιμες περιπτώσεις που ενδέχεται να επηρεάσουν σε μεγάλο βαθμό τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό GDPR. Τα θέματα όπου ενδεικτικά περιλαμβάνονται στη θεματολογία των συμβουλίων ανασκόπησης αφορούν τα εξής:

- αποτελέσματα εσωτερικών επιθεωρήσεων
- κίνδυνοι που εντοπίστηκαν και αφορούν τη διαχείριση των δεδομένων προσωπικού χαρακτήρα,
- πρόοδος ή/ και αποτελέσματα δράσεων υλοποίησης/ τροποποίησης συστημάτων πληροφορικής και επικοινωνιών
- αποτελέσματα επιθεωρήσεων από εξωτερικούς φορείς (π.χ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
- αποτελέσματα διαχείρισης παραπόνων και καταγγελιών φυσικών προσώπων, αναφορικά με τη διαχείριση των προσωπικών τους δεδομένων
- περιστατικά παραβίασης της ασφάλειας των δεδομένων προσωπικού χαρακτήρα και αποτελέσματα ενεργειών που εκτελέστηκαν στο πλαίσιο γνωστοποίησής τους στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,
- απόψεις των φυσικών προσώπων.

Η ανασκόπηση των ανωτέρω καταλήγει σε αποφάσεις με γνώμονα τη συνεχή βελτίωση των διαδικασιών, πολιτικών, υποδομών κ.λπ., που εφαρμόζονται με σκοπό την προστασία των δεδομένων προσωπικού χαρακτήρα για το σύνολο των φυσικών προσώπων, καθώς και τη συμμόρφωση με τον Ευρωπαϊκό Κανονισμό GDPR και την σχετική Ελληνική Νομοθεσία.

13. Διαχείριση ιστοτόπων & επικοινωνίας

13.1 Πολιτική Απορρήτου - Privacy Policy

Ο Οργανισμός είναι υπεύθυνος για την ανάρτηση Πολιτικής Απορρήτου (Privacy Policy) στον ιστότοπό του, σε εμφανές σημείο που είναι προσβάσιμο ανά πάσα στιγμή κατά την πλοήγηση των χρηστών (π.χ. στο footer κάθε ιστότοπου). Στην Πολιτική Απορρήτου δεσμεύεται πλήρως για την προστασία των προσωπικών δεδομένων των επισκεπτών και χρηστών των ιστοσελίδων της, σύμφωνα με όλους τους σχετικούς κανονισμούς και νόμους της Ευρωπαϊκής Ένωσης (ΕΕ) και της Ελλάδας σχετικά με την προστασία των δεδομένων και ιδιαίτερα με τον Γενικό

Κανονισμό για την Προστασία των Προσωπικών Δεδομένων 2016/679/ΕΕ - General Data Protection Regulation (GDPR). Η εν λόγω Πολιτική Απορρήτου επικαιροποιείται όποτε αυτό κρίνεται αναγκαίο.

13.2 Πολιτική διαχείρισης Cookies

Ο Οργανισμός είναι υπεύθυνος για την ανάρτηση της Πολιτικής διαχείρισης Cookies στην ίδια ή σε ξεχωριστή σελίδα με την Πολιτική Απορρήτου. Η Πολιτική διαχείρισης Cookies ενημερώνει τους χρήστες του ιστοτόπου για τις πρακτικές που ακολουθούνται για τη διαχείριση των cookies με διακριτό τρόπο, ανά κατηγορία cookies. Η εν λόγω Πολιτική επικαιροποιείται όποτε αυτό κρίνεται αναγκαίο.

14. Διαχείριση προμηθευτών - εκτελούντων επεξεργασία

Ο Οργανισμός είναι υπεύθυνος για την τήρηση καταλόγου τρίτων μερών που εκτελούν επεξεργασία προσωπικών δεδομένων εκ μέρους της. Ανασκοπεί περιοδικά τις σχετικές συμβάσεις οι οποίες περιλαμβάνουν ανά περίπτωση όρους για τα ακόλουθα:

1	Η επεξεργασία των προσωπικών δεδομένων γίνεται μόνο βάσει οδηγιών και κατευθύνσεων του Οργανισμού και μόνο για τους σκοπούς που έχει ορίσει αυτός.
2	Λίστα των τεχνικών και οργανωτικών μέτρων που λαμβάνει το εκάστοτε τρίτο μέρος (εκτελών την επεξεργασία) για τη διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των πληροφοριών.
3	Όροι εχεμύθειας/ τήρησης εμπιστευτικότητας, με τους οποίους δεσμεύονται και οι υπάλληλοι του τρίτου μέρους (εκτελών την επεξεργασία) που επεξεργάζονται προσωπικά δεδομένα.
4	Το τρίτο μέρος που επεξεργάζεται δεδομένα για λογαριασμό του Οργανισμού δεν επιτρέπεται να αναθέσει μέρος ή συνολικά τις εργασίες επεξεργασίας σε τρίτο, χωρίς προηγούμενη γραπτή άδεια από τον Οργανισμό.
5	Τα προσωπικά δεδομένα που έχει το τρίτο μέρος (εκτελών την επεξεργασία) στην κατοχή του, θα πρέπει να διαγράφονται ή να παραδίδονται στην οργανισμός κατά τη λήξη της συνεργασίας μαζί της.
6	Σε περίπτωση ενός συμβάντος παραβίασης προσωπικών δεδομένων το οποίο γίνεται αντιληπτό από το τρίτο μέρος που εκτελεί την επεξεργασία (εκτελών την επεξεργασία), θα πρέπει να ενημερώνει άμεσα τον Οργανισμό με λεπτομέρειες για τη φύση του περιστατικού, πιθανές αιτίες, όγκο δεδομένων και φυσικών προσώπων που επηρεάζονται, μέτρα που ελήφθησαν ή θα ληφθούν κ.λπ. Πιο συγκεκριμένα, καθορίζεται ο τρόπος ενημέρωσης για τη γνωστοποίηση και το χρονικό διάστημα εντός του οποίου είναι απαραίτητο να ενημερώνεται ο Οργανισμός.
7	Το τρίτο μέρος (εκτελών την επεξεργασία) θέτει στη διάθεση του Οργανισμού κάθε πληροφορία προς απόδειξη της συμμόρφωσης της με τον Ευρωπαϊκό Κανονισμό GDPR. Παράλληλα, επιτρέπει και διευκολύνει τους ελέγχους από τον Οργανισμό ή άλλον ελεγκτή εντεταλμένο από τον Οργανισμό.
8	Το τρίτο μέρος (εκτελών την επεξεργασία) επικουρεί τον Οργανισμό με τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εκπλήρωση της υποχρέωσής του να απαντά σε αιτήματα άσκησης δικαιωμάτων του υποκειμένου των δεδομένων/φυσικού προσώπου.

Επιπρόσθετα, εκτός από τις υφιστάμενες συμβάσεις, οι παραπάνω όροι διασφαλίζονται και σε κάθε νέα σύμβαση.

Σε περίπτωση που κάποιος κύριος προμηθευτής συνεργάζεται με υπο-προμηθευτές ή υπεργολάβους, ενημερώσει προηγουμένως σχετικά τον Οργανισμό.

15. Ασφαλής Χρήση πληροφοριακών συστημάτων

Το σύνολο των εργαζομένων του Οργανισμού που είναι χρήστες πληροφοριακών συστημάτων ακολουθεί τις κάτωθι οδηγίες κατά την πρόσβαση και τη χρήση των συστημάτων, τη χρήση ηλεκτρονικής αλληλογραφίας και διαδικτύου και τη χρήση φορητών συσκευών, με σκοπό την Ασφάλεια των Πληροφοριών και την Προστασία των Προσωπικών Δεδομένων.

15.1 Έλεγχος Πρόσβασης

- Οι χρήστες ακολουθούν τους παρακάτω κανόνες για τη δημιουργία ασφαλών κωδικών πρόσβασης, συγκεκριμένα οι κωδικοί πρόσβασης:
 - Έχουν μήκος τουλάχιστον 8 χαρακτήρων.
 - Έχουν τουλάχιστον ένα χαρακτήρα από τρεις εκ των τεσσάρων ακόλουθων κατηγοριών:
 - Κεφαλαία γράμματα
 - Μικρά γράμματα
 - Αριθμοί
 - Ειδικοί χαρακτήρες (` ~ ! @ # \$ % ^ & * () - _ = + [{] } \ | ; : ' " < , > . / ? € £)
 - Αλλάζουν υποχρεωτικά σε περιοδική βάση (ενδεικτικά αναφέρεται βάσει καλών πρακτικών κάθε 90 ημέρες). Στα συστήματα τα οποία δεν μπορεί να επιβληθεί αλλαγή κωδικών πρόσβασης μέσω πολιτικής, οι χρήστες είναι υπεύθυνοι για την έγκαιρη αλλαγή κωδικού.
 - Είναι διαφορετικοί από τους τελευταίους τέσσερις που έχουν χρησιμοποιήσει.
 - Δεν περιλαμβάνουν προσωπικά στοιχεία του χρήστη.
 - Δε συμπίπτουν με κωδικούς που χρησιμοποιούν για προσωπικές χρήσεις εκτός Οργανισμού.
- Οι χρήστες γνωρίζουν ότι οι κωδικοί πρόσβασης είναι αυστηρά προσωπικοί, και δεν πρέπει να κοινοποιούνται σε τρίτους και αποτελούν ευθύνη του κάθε εργαζομένου να διατηρούνται μυστικοί. Σε καμία περίπτωση δεν επιτρέπεται η αποστολή των αναγνωριστικών πρόσβασης (username – password) στα πληροφοριακά συστήματα του Οργανισμού μέσω email.
- Οι κωδικοί πρόσβασης δεν επιτρέπεται να φυλάσσονται σε έντυπη μορφή και ειδικά σε έγγραφα και σημειώματα (post-it) τα οποία βρίσκονται σε κοινή θέα στην περιοχή γύρω από το σταθμό εργασίας.
- Οι χρήστες θα πρέπει να κλειδώνουν τους υπολογιστές όταν απομακρύνονται από τη θέση εργασίας τους.

15.2 Ηλεκτρονική Αλληλογραφία

- Οι χρήστες κρυπτογραφούν τα αρχεία με εμπιστευτικές ή απόρρητες πληροφορίες τα οποία διακινούνται με email.

- Οι χρήστες δεν ανοίγουν συνημμένα αρχεία, πατούν συνδέσμους (links) σε e-mails ή απαντούν σε e-mails όταν:
 - Ο αποστολέας είναι άγνωστος
 - Το όνομα του αποστολέα διαφέρει από την ηλεκτρονική του διεύθυνση.
 - Το κείμενο του μηνύματος έχει πολλά ορθογραφικά/ συντακτικά/ εκφραστικά λάθη.
 - Το μήνυμα φαινομενικά προέρχεται από παρόχους οικονομικών ή και άλλων υπηρεσιών και ζητούνται αναγνωριστικά, οικονομικά ή οποιαδήποτε άλλα προσωπικά στοιχεία των χρηστών.
 - Το email έχει αποσταλεί σε πολλαπλούς μη φανερούς παραλήπτες (undisclosed recipients – batch email).

Περιπτώσεις λήψης email με προαναφερόμενα χαρακτηριστικά αναφέρονται στον Υπεύθυνο Ασφάλειας Πληροφοριών.

- Δεν επιτρέπεται το «άνοιγμα» εκτελέσιμων αρχείων που επισυνάπτονται σε email.
- Για την αποφυγή επιθέσεων phishing με χρήση ίδιου ή παρόμοιου domain name, ακολουθούνται οι εξής οδηγίες:
 - Στην περίπτωση email αίτησης πληρωμών ή αλλαγής οικονομικών στοιχείων από συνεργάτες, η ταυτότητα του αποστολέα και η εγκυρότητα του email θα πρέπει να επιβεβαιώνεται με τηλεφωνική κλήση στον αποστολέα/ συνεργάτη.
 - Η ανταλλαγή emails που περιέχουν εμπιστευτικές ή απόρρητες πληροφορίες του Οργανισμού, θα πρέπει να γίνεται χρησιμοποιώντας τον επίσημο κατάλογο ηλεκτρονικών διευθύνσεων του Οργανισμού. Συνιστάται η αποφυγή χρήσης απαντητικών μηνυμάτων σε αυτές τις περιπτώσεις.
- Σε περίπτωση που υπάρχει υποψία ότι ένα e-mail περιέχει ιό, ενημερώνεται άμεσα ο Υπεύθυνος Ασφάλειας Πληροφοριών.
- Δεν πρέπει να αποστέλλονται video ή εικόνες και γενικότερα μεγάλου μεγέθους αρχεία μέσω του ηλεκτρονικού ταχυδρομείου, καθώς δημιουργείται συμφόρηση και καθυστέρηση στο δίκτυο.
- Οι χρήστες δεν θα πρέπει να χρησιμοποιούν την επαγγελματική διεύθυνση ηλεκτρονικού ταχυδρομείου για την εγγραφή τους σε ηλεκτρονικές υπηρεσίες εξωτερικών παρόχων ή να τη γνωστοποιούν σε σελίδες κοινωνικής δικτύωσης.

15.3 Διαδίκτυο

Το διαδίκτυο (Internet) μπορεί να χρησιμοποιηθεί για τη σύνδεση σε οποιοδήποτε ιστότοπο (Web site) απαιτείται για επαγγελματικούς λόγους, στο πλαίσιο της εργασίας κάθε χρήστη. Επιπλέον:

- Δεν επιτρέπεται η χρήση του διαδικτύου για πρόσβαση σε ιστοσελίδες με ρατσιστικό, πορνογραφικό ή οποιουδήποτε άλλο παράνομο, μη αποδεκτό και επιβλαβές περιεχόμενο.

- Οι χρήστες δεν πρέπει να πατούν πάνω σε διαφημίσεις, banners προσφορών και γενικότερα σε pop-ups παράθυρα.
- Οι χρήστες δεν πρέπει να ανοίγουν κάθε είδους αρχείο προερχόμενου από το διαδίκτυο χωρίς να έχει προηγηθεί σάρωση από αντικό λογισμικό.
- Απαγορεύεται η δημιουργία λογαριασμών σε online υπηρεσίες ή/ και κοινωνικά μέσα δικτύωσης (social media) όπως gmail, facebook κ.λπ. με τα ίδια αναγνωριστικά (user name ή / και password) που χρησιμοποιούνται ήδη για πρόσβασή σε πληροφοριακούς πόρους του Οργανισμού (υπολογιστές, laptops, servers κ.α.).
- Απαγορεύεται η χρήση της δυνατότητας πρόσβασης στο διαδίκτυο για απόκτηση παράνομης πρόσβασης σε άλλο υπολογιστικό σύστημα ή υπηρεσία.
- Απαγορεύεται η αντιγραφή αρχείων και προγραμμάτων μη επαγγελματικού περιεχομένου μέσω του διαδικτύου.
- Δεν επιτρέπεται η χρήση υπηρεσιών live streaming, πάρα μόνο κατόπιν έγκρισης από τη Διοίκηση του Οργανισμού.

15.4 Φορητές Συσκευές

Οι χρήστες φορητών συσκευών ακολουθούν τις παρακάτω οδηγίες:

- Δεν αφήνουν ανεπιτήρητες τις φορητές συσκευές σε δημόσιους χώρους.
- Κατά τη χρήση των συσκευών σε δημόσιους χώρους είναι ιδιαίτερως προσεκτικοί ώστε να μην είναι εύκολη η ανάγνωση πληροφοριών από την οθόνη της συσκευής.
- Μεταφέρουν τους φορητούς υπολογιστές (laptop, tablet) στην ειδική τσάντα μεταφοράς και όχι ακάλυπτα ή σε τσάντα που δεν παρέχει προστασία σε περίπτωση πτώσης ή κρούσης.
- Δεν επιτρέπουν τη χρήση των laptop, των tablet ή των smartphone σε πρόσωπα εκτός Οργανισμού.
- Δε συνδέονται με υπηρεσίες του Οργανισμού χωρίς τη χρήση πρωτοκόλλων Ασφαλείας ή μηχανισμών VPN. Σε περίπτωση απομακρυσμένης διασύνδεσης, αυτή θα πρέπει να μένει ενεργή μόνο για όσο χρόνο απαιτείται για την ολοκλήρωση της εργασίας. Δεν εισάγουν κωδικούς πρόσβασης ενώ είναι συνδεδεμένοι σε δημόσια/ μη-ασφαλή ασύρματα δίκτυα.
- Δεν προσπαθούν να απενεργοποιήσουν οποιαδήποτε εφαρμογή ή άλλο μέτρο ασφάλειας που έχει εφαρμοστεί στη συσκευή από το προσωπικό του Οργανισμού (π.χ. antivirus, κλείδωμα BIOS, τοπικό firewall κ.λπ.)
- Σε περίπτωση απώλειας ή κλοπής φορητής συσκευής, οι χρήστες ενημερώνουν άμεσα τον Υπεύθυνο Ασφάλειας Πληροφοριών.

15.5 Άλλες Οδηγίες

- Οι χρήστες χρησιμοποιούν τους πόρους και τις προσφερόμενες υπηρεσίες του Οργανισμού, όπως ηλεκτρονική αλληλογραφία (e-mail), πρόσβαση στο διαδίκτυο, φορητά υπολογιστικά μέσα, κ.λπ. μόνο στο πλαίσιο της εργασίας τους.
- Η επιφάνεια εργασίας των υπολογιστών δεν θα πρέπει να δίνει πληροφορίες σε έναν τρίτο για το αντικείμενο και τα έργα με τα οποία ασχολείται ο χρήστης.
- Οι χρήστες δεν επιτρέπεται να εγκαθιστούν προγράμματα λογισμικού πέρα από αυτά που είναι ήδη εγκατεστημένα σε κάθε υπολογιστική μονάδα.
- Οι χρήστες δεν επιτρέπεται να επιχειρούν πρόσβαση σε πληροφορίες και συστήματα για τα οποία δεν έχουν λάβει την απαραίτητη εξουσιοδότηση.
- Οι χρήστες δεν επιτρέπεται να μεταφέρουν πληροφορίες του Οργανισμού, χωρίς την προηγούμενη έγκριση από τον Προϊστάμενο του τμήματός τους. Σε περίπτωση μεταφοράς μεγάλων αρχείων δεν επιτρέπεται η χρήση δωρεάν εκδόσεων online file sharing συστημάτων (wetransfer, dropbox).
- Δεν επιτρέπεται η χρήση εφαρμογών (ftp, p2p κ.α.) για την δικτυακή μεταφορά με τις οποίες ο χρήστης μπορεί να μεταφέρει αρχεία από δικτυακούς τόπους στην υπολογιστική του μονάδα, εκτός αν έχει σχετική άδεια από τον Υπεύθυνο Ασφάλειας Πληροφοριών.
- Δεν επιτρέπεται η χρήση εφαρμογών για την ανίχνευση δικτυακών πληροφοριών (network scanning, port scanning κ.λπ.), τόσο για πληροφοριακές υποδομές του Οργανισμού (intranet) όσο και εκτός (internet).
- Κατά την αποθήκευση πληροφοριών σε φορητά μέσα αποθήκευσης, και σε περίπτωση που η πληροφορία έχει διαβάθμιση «Απόρρητη» ή «Εμπιστευτική», τα αποθηκευτικά μέσα θα πρέπει να κρυπτογραφούνται.
- Η αποθήκευση αρχείων με προσωπικά δεδομένα φυσικών προσώπων σε προσωπικούς υπολογιστές ή σε κοινόχρηστους φακέλους γίνεται μόνο για την εκτέλεση επιχειρησιακών δραστηριοτήτων που δεν μπορούν να υλοποιηθούν μέσω των κύριων εφαρμογών του Οργανισμού και μόνο για το χρονικό διάστημα που απαιτείται για την ολοκλήρωση των εν λόγω δραστηριοτήτων.
- Δεν επιτρέπεται το άνοιγμα και η χρήση αρχείων αποθηκευμένων σε φορητά αποθηκευτικά μέσα (USB, CD κ.λπ.) αν δεν έχει προηγηθεί σάρωσή τους με το αντικό λογισμικό που είναι εγκατεστημένο στην υπολογιστική μονάδα.
- Δεν επιτρέπεται το «άνοιγμα» εκτελέσιμων αρχείων από εξωτερικά/φορητά αποθηκευτικά μέσα.
- Οι χρήστες οφείλουν να αναφέρουν άμεσα κάθε συμβάν ή περιστατικό Ασφάλειας Πληροφοριών ή άλλη αδυναμία ασφάλειας στον Υπεύθυνο Ασφάλειας Πληροφοριών.

- Απαγορεύεται η με οποιοδήποτε τρόπο κοινοποίηση ή γνωστοποίηση σε τρίτους, εκτός Οργανισμού, πληροφορικών σχετικά με τα συστήματα της, τις υποδομές της ή/ και τα μέτρα ασφάλειας που εφαρμόζονται.
- Οι χρήστες οφείλουν να συνεργάζονται με τους διαχειριστές συστημάτων προκειμένου να διερευνάται η πηγή και ο τρόπος εγκατάστασης κακόβουλου λογισμικού σε περίπτωση ανίχνευσής του στις υπολογιστικές τους μονάδες.

15.6 Διαχείριση Εγγράφων

- Οι χρήστες δεν αφήνουν έγγραφα πάνω στη θέση εργασίας, κατά την απομάκρυνσή τους από τους σταθμούς εργασίας για μεγάλο χρονικό διάστημα ή στο τέλος της ημέρας.
- Οι εκτυπώσεις εγγράφων γίνονται μόνο για την εκτέλεση εργασιών όπου χρειάζονται έντυπα μέσα.
- Στην περίπτωση εκτύπωσης ή φωτοτύπησης εγγράφων, οι χρήστες απομακρύνουν άμεσα τα πρωτότυπα και εκτυπωμένα έγγραφα από τα μηχανήματα, ειδικά όταν πρόκειται για έγγραφα με εμπιστευτικές ή απόρρητες πληροφορίες.
- Τα έγγραφα με διαβάθμιση «απόρρητο» ή/και «εμπιστευτικό» αποθηκεύονται σε κλειδωμένα ντουλάπια ή συρτάρια. Οι χρήστες που έχουν πρόσβαση σε αυτά, κρατούν τα κλειδιά σε ασφαλές σημείο, το οποίο και δεν πρέπει να γνωστοποιείται σε άλλους χρήστες. Τα ντουλάπια και συρτάρια αποθήκευσης, καθώς και το σημείο φύλαξης των κλειδιών, θα πρέπει να ελέγχονται.
- Η αποστολή εγγράφων γίνεται πάντα σε σφραγισμένο φάκελο με την επωνυμία του Οργανισμού. Στην περίπτωση εγγράφων με εμπιστευτικές ή απόρρητες πληροφορίες, χρησιμοποιείται υπηρεσία courier ή συστημένη αλληλογραφία.
- Οι χρήστες καταστρέφουν όλα τα εκτυπωμένα έγγραφα και αντίγραφα, μετά το πέρας της χρήσης τους, και εφόσον δεν απαιτείται η φύλαξή τους. Στην περίπτωση εγγράφων με απόρρητες ή εμπιστευτικές πληροφορίες, αυτά καταστρέφονται χρησιμοποιώντας καταστροφέα εγγράφων (shredder).

16. Χρήση συστήματος Βιντεοεπιτήρησης

16.1 Βασικές αρχές

Ακολουθούν οι βασικές αρχές που διέπουν την λειτουργία του συστήματος βιντεοεπιτήρησης:

- Αποκλειστικός σκοπός της εγκατάστασης κλειστού κυκλώματος τηλεόρασης είναι η διαφύλαξη προσώπων και αγαθών.
- Σε εμφανές σημείο πριν την είσοδο στο χώρο όπου γίνεται βιντεοεπιτήρηση, αναρτάται σχετική/-ές ενημερωτική/-ες πινακίδα/-ες. Η πινακίδα παρέχει ενημέρωση κατ' ελάχιστον για τα εξής:
 - Σκοπός (ως ανωτέρω)
 - Ύπαρξη δικαιωμάτων πρόσβασης, διαγραφής, περιορισμού και εναντίωσης στην επεξεργασία και τρόπος άσκησής τους
 - Στοιχεία επικοινωνίας με ΥΠΔ
- απαγορεύεται:
 - η καταγραφή ήχου
 - η απεικόνιση δημοσίων χώρων (παράπλευροι οδοί, πεζοδρόμια, είσοδοι γειτονικών κατοικιών, περαστικοί, στάσεις λεωφορείου, δημόσιος δρόμος, πινακίδες διερχομένων αυτοκινήτων)
 - η απεικόνιση άλλων ιδιωτικών χώρων

16.2 Γενικές οδηγίες Χρήσης

Γενικότερα στον χώρο εργασίας ισχύουν τα κάτωθι:

- Το σύστημα βιντεοεπιτήρησης δεν χρησιμοποιείται για την επιτήρηση των εργαζομένων εντός των χώρων εργασίας.
- Απαγορεύεται η βιντεοεπιτήρηση σε αίθουσες γραφείων ή διαδρόμων του χώρου εργασίας και σε χώρους που οι εργαζόμενοι έχουν αυξημένες προσδοκίες για την ιδιωτικότητά τους, όπως τουαλέτες και προθάλαμοι τουαλετών, μπάνια, αποδυτήρια και χώροι ανάπαυσης.
- Επιτρέπεται η βιντεοεπιτήρηση μόνον, εφόσον οι κάμερες εστιάζουν στα αγαθά που προστατεύονται, όπως στα ταμεία, κ.λπ.
- Επιτρέπεται η λήψη εικόνας εφόσον περιορίζεται στην επιτήρηση της πόρτας και λαμβάνει τη λιγότερη δυνατή εικόνα από κοινόχρηστους χώρους, όπως σκάλα, διάδρομο και ασανσέρ.

Για την περίπτωση που οι κάμερες λαμβάνουν εικόνα τότε, ακόμα και αν δεν καταγράψουν/αποθηκεύουν δεδομένα, συντελείται επεξεργασία προσωπικών δεδομένων (έστω και πιο ήπιας μορφής σε σχέση με την καταγραφή), οπότε ισχύουν όλα τα ανωτέρω σχετικά με τις προϋποθέσεις νομιμότητας.

16.3 Τρόπος Διατήρησης Δεδομένων

Ο Οργανισμός διασφαλίζει την ασφάλεια αναφορικά με:

- την μετάδοση: Μέσω ασφαλών καναλιών, προστατευμένων από cyber επιθέσεις.
- την πρόσβαση: Ο χώρος όπου υπάρχουν οι οθόνες παρακολούθησης και τα δεδομένα είναι κλειστός και μη προσβάσιμος σε τρίτους παρά μόνο στον Υπεύθυνο Επεξεργασίας.
- την αποθήκευση: Το σύστημα καταγραφής είναι σε θέση να προσδιορίσει ποιος έχει δει, διαγράψει, αντιγράψει ή τροποποιήσει οποιαδήποτε παρακολούθηση, βίντεο, πλάνο.

16.4 Διαβίβαση αρχείων

Επιτρέπεται να διαβιβάζονται τα τηρούμενα αρχεία μόνο κατόπιν συγκατάθεσης των ατόμων που απεικονίζονται σε αυτά.

Εξαίρεση :

- Όταν αρμόδιες δικαστικές, εισαγγελικές και αστυνομικές αρχές ζητούν νομίμως δεδομένα κατά την άσκηση των καθηκόντων τους.
- Κατά το σχέδιο του εφαρμοστικού νόμου, ο οποίος δεν έχει ακόμα ψηφισθεί, η διαβίβαση επιτρέπεται και χωρίς συγκατάθεση μετά από ειδικά αιτιολογημένη αίτηση τρίτου, όταν τα δεδομένα είναι αναγκαίο να χρησιμοποιηθούν ως αποδεικτικά στοιχεία για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή μιας αξιόποινης πράξης και μπορούν να συνεισφέρουν στη διερεύνηση των πραγματικών περιστατικών ή στην αναγνώριση των δραστών.

16.5 Δικαιώματα που αφορούν την προστασία των προσωπικών δεδομένων

Το υποκείμενο αναφορικά με την προστασία των προσωπικών του δεδομένων μπορεί να ασκήσει τα δικαιώματα πρόσβασης, διαγραφής, περιορισμού και εναντίωσης της επεξεργασίας προς τον Υπεύθυνο Επεξεργασίας (το φυσικό ή νομικό πρόσωπο που φέρει την ευθύνη για την εγκατάσταση του συστήματος βιντεοεπιτήρησης).

Σε περίπτωση που το υποκείμενο δεν λάβει απάντηση εντός της προβλεπόμενης προθεσμίας (ενός μηνός με – υπό προϋποθέσεις – παράταση δύο μηνών) ή η απάντηση που λάβει δεν ήταν ικανοποιητική ή το ζήτημα του δεν έχει επιλυθεί, μπορεί να απευθυνθεί στην ΑΠΔΠΧ (www.dpa.gr), ενώ πάντα διατηρεί τη δυνατότητα άσκησης δικαστικής προσφυγής.

16.6 Χρόνος Τήρησης Δεδομένων

Τα δεδομένα τηρούνται για τον μικρότερο δυνατό χρόνο. Εφόσον από τη λήψη εικόνων δεν προκύπτει επέλευση συμβάντος, όπως κλοπή, ληστεία, ξυλοδαρμός, τα δεδομένα καταστρέφονται το αργότερο μέσα σε δεκαπέντε (15) εργάσιμες ημέρες.

Σε περίπτωση συμβάντος σε βάρος του προσώπου ή των αγαθών του Υπευθύνου Επεξεργασίας, επιτρέπεται να τηρούνται οι εικόνες στις οποίες έχει καταγραφεί το συγκεκριμένο συμβάν σε χωριστό αρχείο για 30 ημέρες. Εάν το συμβάν αφορά τρίτον, ο Υπεύθυνος Επεξεργασίας επιτρέπεται να τηρεί τις εικόνες για 3 μήνες.

Εάν αυτά περιλαμβάνουν κάποιο συμβάν που έχει διαδραματιστεί, αυτά αντιγράφονται σε ξεχωριστό αρχείο το οποίο μπορεί να διατηρηθεί το πολύ για 30 ημέρες. Αν η εν λόγω καταγραφή αφορά τρίτο πρόσωπο, μπορεί να διατηρηθεί για 3 μήνες. Μετά την πάροδο του ανωτέρω χρονικού διαστήματος ο Υπεύθυνος Επεξεργασίας μπορεί να τηρεί τα δεδομένα για μεγαλύτερο συγκεκριμένο χρονικό διάστημα μόνο σε εξαιρετικές περιπτώσεις όπου το συμβάν χρήζει περαιτέρω διερεύνησης. Στην περίπτωση αυτή ο Υπεύθυνος Επεξεργασίας ενημερώνει την ΑΠΔΠΧ για το αναγκαίο χρονικό διάστημα τήρησης των εν λόγω λήψεων.

17. Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ) - Data Protection Officer (DPO)

Ο Οργανισμός έχει αποφασίσει να ανατεθεί ο ρόλος του ΥΠΔ σε στέλεχος του Οργανισμού, η θέση του οποίου δεν έρχεται σε σύγκρουση συμφερόντων με το ρόλο του ΥΠΔ. Ο ρόλος του έχει καθοριστεί εγγράφως και περιλαμβάνει τα ακόλουθα:

- Ενημερώνει και συμβουλεύει τη Διοίκηση του Οργανισμού και τους υπαλλήλους του αναφορικά με τις υποχρεώσεις τους που απορρέουν από τον Ευρωπαϊκό Κανονισμό GDPR και την ενδεχόμενη σχετική Ελληνική Νομοθεσία αναφορικά με την προστασία προσωπικών δεδομένων.
- Παρακολουθεί τη συμμόρφωση του Οργανισμού με τον Ευρωπαϊκό Κανονισμό GDPR, τη σχετική Ελληνική Νομοθεσία και με τις πολιτικές και διαδικασίες του Οργανισμού σε σχέση με την προστασία των προσωπικών δεδομένων, τουλάχιστον μέσω της διενέργειας (από τον ίδιο, άλλα στελέχη του Οργανισμού ή εξωτερικούς συνεργάτες) εσωτερικών επιθεωρήσεων.
- Φροντίζει για την ευαισθητοποίηση και την κατάρτιση των υπαλλήλων που επεξεργάζονται προσωπικά δεδομένα και αναθέτει σχετικές αρμοδιότητες.
- Παρέχει συμβουλές όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των προσωπικών δεδομένων (DPIA) και παρακολουθεί την υλοποίησή της σύμφωνα με όσα ορίζει ο Ευρωπαϊκός Κανονισμός GDPR.
- Είναι ο υπεύθυνος επικοινωνίας με την ΑΠΔΠΧ για τα ζητήματα που σχετίζονται με την επεξεργασία προσωπικών δεδομένων.
- Είναι ο υπεύθυνος επικοινωνίας και σημείο επαφής με τα φυσικά πρόσωπα (πελάτες, εργαζόμενοι, κλπ.) σε δεύτερο επίπεδο και φροντίζει μέσω κατάλληλης εκπαίδευσης για την ορθή επικοινωνία σε πρώτο επίπεδο από τα αρμόδια στελέχη του Οργανισμού.
- Παρακολουθεί τις εξελίξεις στο θεσμικό και κανονιστικό πλαίσιο των προσωπικών δεδομένων (νόμοι, αποφάσεις δικαστηρίων, συστάσεις ΑΠΔΠΧ, οδηγίες European Data Protection Board, κ.α.) και φροντίζει για την ενσωμάτωσή τους στην καθημερινή λειτουργία του Οργανισμού.

Παράλληλα, ο ΥΠΔ έχει την ευθύνη της παρακολούθησης της ομαλής λειτουργίας των κάτωθι:

- Διασφάλιση της ακρίβειας και ορθότητας των δεδομένων, καθώς και της διαγραφής τους όταν αυτό απαιτείται, βάσει των οριζόμενων στον Ευρωπαϊκό Κανονισμό GDPR και την ενδεχόμενη σχετική Ελληνική Νομοθεσία
- Κατάρτιση και εφαρμογή της Πολιτικής Διαχείρισης Δεδομένων Προσωπικού Χαρακτήρα του Οργανισμού, καθώς και άλλων επιμέρους πολιτικών, διαδικασιών, οδηγιών κ.λπ.
- Επικαιροποίηση του Αρχείου Δραστηριοτήτων Επεξεργασίας του Οργανισμού.

Η Διοίκηση του Οργανισμού διασφαλίζει ότι ο ΥΠΔ:

- Συμμετέχει εγκαίρως σε όλες τις αποφάσεις που σχετίζονται με την προστασία των προσωπικών δεδομένων.
- Υποστηρίζεται με τους κατάλληλους πόρους, υλικούς και ανθρώπινους, για την εκτέλεση των καθηκόντων του, καθώς και με πόρους που απαιτούνται για τη διατήρηση της τεχνογνωσίας του στο θέμα της διαχείρισης προσωπικών δεδομένων και ιδιωτικότητας.
- Υποστηρίζεται από ομάδα η οποία αποτελείται από στελέχη διαφορετικών πεδίων εξειδίκευσης (πληροφορικής, νομικής, ανάπτυξης επιχειρησιακής δραστηριότητας, εσωτερικού ελέγχου, αξιολόγησης κινδύνων κ.λπ.) και η οποία του παρέχει τις πληροφορίες που χρειάζεται στο πλαίσιο των αρμοδιοτήτων του.
- Διαθέτει επαρκή χρόνο για να εκπληρώνει τα καθήκοντά του. Σε περίπτωση που ο ρόλος του ΥΠΔ δεν θα ανατεθεί υπό μορφή πλήρους απασχόλησης, αποτελεί καλή πρακτική ο προσδιορισμός του ποσοστού του χρόνου που απαιτείται για την εκτέλεση των καθηκόντων του (εντός χρονικής περιόδου ικανής για εξαγωγή συμπερασμάτων), ώστε να ληφθούν οι σχετικές αποφάσεις για τις ανάγκες λειτουργίας του ρόλου και τους απαιτούμενους πόρους.
- Η Διοίκηση του Οργανισμού κατά την επιλογή του ΥΠΔ και σε συνεχή βάση εξασφαλίζει ότι δεν υπάρχει σύγκρουση συμφερόντων μεταξύ του ρόλου του ΥΠΔ και τυχόν άλλου ρόλου του. Η σύγκρουση προκύπτει αν οι αρμοδιότητες του άλλου ρόλου επιτρέπουν να λαμβάνει αποφάσεις σχετικά με το σκοπό και τα μέσα επεξεργασίας των προσωπικών δεδομένων. Για την εξασφάλιση της μη σύγκρουσης συμφερόντων, η Διοίκηση λαμβάνει υπόψη της τη σχετική οδηγία του WP 29 και παρακολουθεί σχετικές συστάσεις της ΑΠΔΠΧ.

Τα στοιχεία επικοινωνίας του ΥΠΔ δημοσιεύονται και διαβιβάζονται στην ΑΠΔΠΧ μέσω του εντύπου «**Ορισμός Υπευθύνου Προστασίας Δεδομένων**» που έχει εκδοθεί από την Αρχή, το οποίο μπορεί να βρεθεί στο παρακάτω link:

http://www.dpa.gr/portal/page?_pageid=33,211475&_dad=portal&_schema=PORTAL

18. Ανθρώπινο δυναμικό

18.1 Υποψήφιοι εργαζόμενοι

Στα έντυπα μέσω των οποίων ζητούνται προσωπικά δεδομένα από υποψήφιους εργαζομένους (σπουδαστές, φοιτητές) σημειώνονται τα πεδία που η συμπλήρωσή τους είναι υποχρεωτική. Τα πεδία που θα επισημαίνονται ως υποχρεωτικά είναι τα ελάχιστα δυνατά για το σκοπό της εκάστοτε επεξεργασίας.

Κατά την υποβολή αίτησης πρόσληψης στο Πρωτόκολλο, οι υποψήφιοι εργαζόμενοι ενημερώνονται με τα παραπάνω υποχρεωτικά στοιχεία αλλά και το χρόνο τήρησης των δεδομένων (μοναδικά αναγνωριστικά, βαθμολογία, κ.λπ.) για την επεξεργασία που πραγματοποιείται στο πλαίσιο της κάλυψης της θέσης εργασίας και ενόψει εκτέλεσης σύμβασης με τον υποψήφιο εργαζόμενο.

Με το πέρας του χρόνου τήρησης των δεδομένων για τον οποίο έχει ενημερωθεί ο υποψήφιος εργαζόμενος τα δεδομένα διαγράφονται από τον Οργανισμό και τηρείται αποδεικτικό καταστροφής τους.

Στην περίπτωση όπου σύμφωνα με τα παραπάνω διαπιστωθεί αναντιστοιχία στα στοιχεία του υποψήφιου εργαζομένου, ο Οργανισμός απευθύνεται στον υποψήφιο εργαζόμενο για παροχή διευκρινήσεων ώστε να διασφαλιστεί η ακριβής και δίκαιη επεξεργασία των στοιχείων του.

Ο Οργανισμός έχει διασφαλίσει την τήρηση των προσωπικών δεδομένων που αφορούν υποψήφιους εργαζομένους για χρονικό διάστημα όχι μεγαλύτερο από εκείνο που ο κάθε υποψήφιος έχει ενημερωθεί. Το διάστημα αυτό προσδιορίζεται στην Πολιτική Αποθήκευσης/Καταστροφής Φυσικού και Ηλεκτρονικού Αρχείου. Μετά το πέρας του εν λόγω χρονικού διαστήματος τα προσωπικά δεδομένα διαγράφονται και τηρείται αποδεικτικό καταστροφής τους.

Τα προσωπικά δεδομένα των υποψήφιων εργαζομένων τηρούνται για τον ελάχιστο δυνατό χρόνο για τον οποίο είναι απαραίτητα στο πλαίσιο του σκοπού επεξεργασίας για τον οποίο συλλέχθηκαν και με βάση την Πολιτική Αποθήκευσης/Καταστροφής Φυσικού και Ηλεκτρονικού Αρχείου.

Παράλληλα με την σύμβαση εργασίας, οι εργαζόμενοι λαμβάνουν και υπογράφουν ενημερωτικό έντυπο το οποίο περιλαμβάνει αναφορές στον Ευρωπαϊκό Κανονισμό GDPR ή/ και το οποίο θα τροποποιηθεί κατάλληλα σε ενδεχόμενη νέα Ελληνική Νομοθεσία που θα αντικαταστήσει την υφιστάμενη. Στο ενημερωτικό αυτό έντυπο συνυπολογίζονται κατ' ελάχιστον:

- Τα προσωπικά δεδομένα που συλλέγονται (π.χ. στοιχεία εκπαίδευσης, στοιχεία κατοικίας κ.λπ.)
- Οι σκοποί επεξεργασίας τους (π.χ. έκδοση μισθοδοσίας, αξιολόγηση)
- Οι χρόνοι διατήρησης των δεδομένων αυτών
- Τυχόν αποδέκτες των δεδομένων καθώς και οι σκοποί επεξεργασίας αυτών (π.χ. Διαύγεια, φορείς εκπαίδευσης, κ.λπ.)

- Ενημέρωση σχετικά με την ικανοποίηση των δικαιωμάτων του εργαζομένου (π.χ. πρόσβαση στον φάκελό του, διόρθωση στοιχείων, δικαίωμα καταγγελίας κ.λπ.)

Ακόμη, περιλαμβάνεται πρόβλεψη για την καταστροφή του δελτίου υγείας εργαζομένου μετά τη λήξη της εργασιακής σχέσης, εφόσον δεν υπάρχει άλλη νομοθετική απαίτηση που υποχρεώνει τον Οργανισμό να το τηρήσει.

18.2 Διαχείριση εργαζομένων

Οι εργαζόμενοι πληροφορούνται από τον Οργανισμό για την παρουσία, τη χρήση και το σκοπό οποιουδήποτε εξοπλισμού ανίχνευσης ή/και οποιασδήποτε συσκευής που ενεργοποιείται όσον αφορά τους σταθμούς εργασίας τους, όπως και για οποιαδήποτε κακή χρήση ηλεκτρονικών επικοινωνιών που ανιχνεύεται (ηλεκτρονικό ταχυδρομείο ή Διαδίκτυο) κατά τη διάρκεια παροχής της εργασίας τους.

Η πρόθεση του Οργανισμού για αυτεπάγγελτη εξακρίβωση δεδομένων των εργαζομένων (π.χ. επαγγελματικών προσόντων ή εργασιακής εμπειρίας σε προηγούμενους εργοδότες) δηλώνεται επίσης ρητά. Η διαδικασία εξακρίβωσης είναι διαφανής και οι εργαζόμενοι ενημερώνονται για τις πληροφορίες που πρόκειται να εξακριβωθούν, καθώς και για τα μέσα και τις πηγές των οποίων ο Οργανισμός θα κάνει χρήση με σκοπό την εξακρίβωση.

Οι εργαζόμενοι λαμβάνουν γνώση για τυχόν τροποποιήσεις του κανονισμού χρήσης επικοινωνιακών μέσων και μέσων ηλεκτρονικής επεξεργασίας μέσω μίας ειδοποίησης με αποστολή e-mail για τυχόν αλλαγές στα σχετικά αναρτημένα έγγραφα στο intranet του Οργανισμού.

Τα προσωπικά δεδομένα των εργαζομένων τηρούνται με ασφαλή τρόπο σε όλες τις μορφές τους. Η τήρηση δεδομένων που είναι σε έγχαρτη μορφή πραγματοποιείται σε φωριαμούς που κλειδώνουν. Αντίστοιχα, τα δεδομένα των εργαζομένων που είναι σε ψηφιακή μορφή είναι προσβάσιμα με τη χρήση κωδικού. Αποκλειστικά τα άτομα με την κατάλληλη εξουσιοδότησή έχουν πρόσβαση στα δεδομένα του προσωπικού και μόνο για συγκεκριμένους σκοπούς επεξεργασίας.

Η συλλογή δεδομένων ειδικών κατηγοριών για σκοπούς παρακολούθησης παροχής ίσων ευκαιριών (π.χ. αναπηρίες) πραγματοποιείται αποκλειστικά για τους σκοπούς αυτούς. Για την επεξεργασία των συγκεκριμένων στοιχείων, όπου είναι εφικτό, γίνεται χρήση ανωνυμοποιημένων στοιχείων με τρόπο ώστε να μην είναι δυνατή η ταυτοποίηση συγκεκριμένων εργαζομένων.

Τα προσωπικά δεδομένα που αφορούν την υγεία των εργαζομένων, λόγω της φύσης τους (δεδομένα ειδικών κατηγοριών) και των συνεπειών που μπορεί να έχει η αποκάλυψή τους, συλλέγονται μόνο εφόσον αυτό είναι απολύτως απαραίτητο για έναν από τους παρακάτω λόγους:

- για την αξιολόγηση της καταλληλότητας του εργαζομένου ή του υποψήφιου για μια συγκεκριμένη θέση ή εργασία, παρούσα ή μελλοντική,
- για την εκπλήρωση των υποχρεώσεων του εργοδότη για υγιεινή και ασφάλεια της εργασίας,
- για τη θεμελίωση των δικαιωμάτων των εργαζομένων.

Η συλλογή των δεδομένων υγείας γίνεται από τον Ιατρό Εργασίας ο οποίος θα είναι και ο μοναδικός που θα έχει πρόσβαση σε αυτά.

Τα δεδομένα υγείας των εργαζομένων καταχωρούνται και διατηρούνται χωριστά από τα άλλα δεδομένα (σύμφωνα με την οδηγία της ΑΠΔΠΧ Αρ. 115/2001) και μόνο για το απαιτούμενο χρονικό διάστημα. Ειδικότερα, τα δεδομένα υγείας που συλλέγονται με σκοπό την αξιολόγηση της ικανότητας ενός υποψηφίου διαγράφονται αμέσως μετά την εκπλήρωση του σκοπού. Σε περίπτωση ανάγκης τήρησης στο φάκελο του εργαζομένου μια βεβαίωση ιατρού αναφορικά με την καταλληλότητα, αυτή πραγματοποιείται μόνο εφόσον δεν αναφέρονται στοιχεία σχετικά με την υγεία του εργαζομένου.

Τα δικαιολογητικά αναρρωτικών αδειών προσκομίζονται από τους εργαζόμενους σε κλειστό φάκελο και πρόσβαση στο περιεχόμενο έχει μόνο το Τμήμα Διοίκησης & Εκπαίδευσης του Οργανισμού, με σκοπό να διαπιστώσει τη νομιμότητα λήψης της αναρρωτικής αδείας. Επίσης, εφόσον είναι εφικτό και δεν υπάρχει άλλη νομοθετική υποχρέωση, τα δικαιολογητικά αυτά καταστρέφονται μετά την εκπλήρωση του σκοπού (έλεγχος, πληρωμή εργαζομένου κ.λπ.), ιδιαίτερα σε περίπτωση όπου γίνεται αναφορά στην πάθηση του εργαζομένου.

Ο εργαζόμενος λαμβάνει ενημέρωση σχετικά με τον τρόπο αξιολόγησής του, τα κριτήρια με τα οποία πραγματοποιείται, τη βαθμολογία και τους εκτελούντες την επεξεργασία αυτή. Εν συνεχεία, λαμβάνει γνώση των αποτελεσμάτων ή/και να παίρνει μέρος στη διαδικασία αυτή. Επίσης, πληροφορείται για τους σκοπούς χρήσης των δεδομένων αυτών (π.χ. προαγωγή, επιπλέον εκπαίδευση κ.λπ.) καθώς και για τους τρόπους και χρόνους αποθήκευσής τους.

Ο Οργανισμός εξασφαλίζει ότι τα δεδομένα των εργαζομένων της τα οποία τηρεί είναι ακριβή. Για τον σκοπό αυτό εξετάζει τρόπους μέσω των οποίων θα τα ενημερώνει είτε λόγω μεταβολής των στοιχείων του εργαζομένου, είτε στο πλαίσιο περιοδικής επισκόπησής τους στο πλαίσιο καταγεγραμμένης διαδικασίας.

18.3 Αποχώρηση εργαζομένων

Ο Οργανισμός τηρεί τα άκρως απαραίτητα δεδομένα μετά την αποχώρηση ενός εργαζομένου (απόλυση, παραίτηση κλπ.), π.χ. ημερομηνίες αναγγελιών πρόσληψης/ αποχώρησης και αντικείμενο εργασίας, και τεκμηριώνει τον σκοπό (π.χ. δημιουργία βεβαίωσης εργασίας μετά από αίτημα του πρώην εργαζομένου), ενώ ο χρόνος τήρησης έχει συμπεριληφθεί και στην Πολιτική Αποθήκευσης/ Καταστροφής Φυσικού και Ηλεκτρονικού Αρχείου.

Επιπρόσθετα, ελέγχονται οι υφιστάμενοι αρχειοθετημένοι φάκελοι πρώην εργαζομένων για να καταστραφούν όσα αρχεία δεν απαιτούνται (π.χ. αποτελέσματα αξιολογήσεων).

Τα προσωπικά δεδομένα τηρούνται για τον ελάχιστο δυνατό χρόνο για τον οποίο είναι απαραίτητα στο πλαίσιο ομαλής λειτουργίας μιας σύμβασης ή συμφωνητικού, καθώς και στο πλαίσιο Νομοθετικών και Κανονιστικών υποχρεώσεων, και μόνο όσα δεδομένα είναι άκρως απαραίτητα. Όταν πλέον τα δεδομένα δεν είναι απαραίτητα τα έγγραφα και αρχεία που τα περιλαμβάνουν, είτε έντυπης είτε ηλεκτρονικής μορφής, διαγράφονται.

Οι χρόνοι τήρησης και καταστροφής των αρχείων έχουν οριστεί ανά κατηγορία ή είδος αρχείων, καθώς ανάλογα με το σκοπό επεξεργασίας και τις νομοθετικές απαιτήσεις εμφανίζονται διαφοροποιήσεις.

Οι υπάλληλοι ενημερώνονται κατά την αποχώρησή τους από τον Οργανισμό, σχετικά με την επεξεργασία των προσωπικών τους δεδομένων που προτίθεται να κάνει ο Οργανισμός, όπως για παράδειγμα την τήρηση των άκρως απαραίτητων δεδομένων για να είναι εφικτή η παραγωγή βεβαίωσης μετά από πιθανή μελλοντική αίτηση, ή την τήρηση ορισμένων δεδομένων βάσει τυχόν νομοθετικής απαίτησης (με αναφορά στην νομοθεσία αυτή). Επιπλέον, ενημερώνονται για το δικαίωμα φορητότητας των προσωπικών τους δεδομένων, ενώ τους παρέχονται τα προσωπικά δεδομένα του φακέλου τους που τηρούνται σε ηλεκτρονική μορφή (η φορητότητα αφορά ιατρικά δεδομένα ή δεδομένα που προσκόμισε ο ίδιος ο εργαζόμενος στον Οργανισμό (π.χ. βιογραφικά σημειώματα, στοιχεία προϋπηρεσίας κ.λπ.).