Πανελλήνια Ομοσπονδία
Κοινωνικών Συνεταιρισμών
Περιορισμένης Ευθύνης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Υγείας

ΕΚΠΟΝΗΣΗ: CMT Prooptiki CONSULTING MANAGEMENT TRAINING

ΠΑΡΑΔΟΤΕΟ 2.2.2.4

ΟΔΗΓΟΣ ΠΡΟΤΥΠΟΠΟΙΗΜΕΝΩΝ ΔΙΑΔΙΚΑΣΙΩΝ ΕΦΑΡΜΟΓΗΣ ΤΟΥ GDPR

ΥΠΟΕΡΓΟ 2: Δράση 2.2 «Ενίσχυση της επάρκειας και της διοικητικής και διαχειριστικής ικανότητας των Κοι.Σ.Π.Ε.»

ΠΡΑΞΗ:

«Ολοκληρωμένο πρόγραμμα παρέμβασης για την υποστήριξη των Κοινωνικών Συνεταιρισμών (Κοι.Σ.Π.Ε) του αρθ. 12 του Ν.2716/1999 στην κατεύθυνση βελτίωσης της διοικητικής και διαχειριστικής τους ικανότητας»

ΚΩΔΙΚΟΣ:

ΟΠΣ 5041861 στο Επιχειρησιακό Πρόγραμμα «Μεταρρύθμιση Δημόσιου Τομέα 2014-2020»
(Κωδ. Πράξης ΣΑ: 2019ΣΕ49110002)

ΦΟΡΕΑΣ ΥΛΟΠΟΙΗΣΗΣ:

ΠΑΝΕΛΛΗΝΙΑ ΟΜΟΣΠΟΝΔΙΑ Κοι.Σ.Π.Ε.(Π.Ο.Κοι.Σ.Π.Ε.)

Αρ. Πρωτ: 277/ΥΠ1/Π_1/01-10-2020

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Πανελλήνια Ομοσπονδία
Κοινωνικών Συνεταιρισμών
Περιορισμένης Ευθύνης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Υγείας

Ιούλιος, 2022

Το παραδοτέο **2.2.2.4**, αποτελεί μέρος μιας ευρύτερης σειράς εργαλείων και οδηγών προτυποποίησης διαδικασιών, που υλοποίησε η Πανελλήνια Ομοσπονδία Κοινωνικών Συνεταιρισμών Περιορισμένης Ευθύνης (ΠΟΚοιΣΠΕ) στο πλαίσιο του έργου με τίτλο: «Ολοκληρωμένο πρόγραμμα παρέμβασης για την υποστήριξη των Κοινωνικών Συνεταιρισμών Περιορισμένης Ευθύνης (ΚοιΣΠΕ) του αρθρ. 12 του Ν. 2716/1999 στην κατεύθυνση βελτίωσης της διοικητικής και διαχειριστικής τους ικανότητας».

Κύριος σκοπός του έργου, που αναπτύχθηκε σε συνεργασία με τη CMT Prooptiki, είναι η ανάπτυξη, προτυποποίηση και εφαρμογή εργαλείων υποστηριζόμενης απασχόλησης για άτομα με ψυχοκοινωνικά προβλήματα, καθώς και η ενίσχυση της επάρκειας και της διοικητικής και διαχειριστικής ικανότητας των ΚοιΣΠΕ, στο νέο πολλαπλά μεταβαλλόμενο κοινωνικό και οικονομικό πλαίσιο.

Φιλοδοξία του έργου ήταν να αποτελέσει μία πυξίδα στο δρόμο της εργασιακής ένταξης, αφενός για τα άτομα με σοβαρά ψυχοκοινωνικά προβλήματα, που παλεύουν καθημερινά για την κατάκτηση και εμπέδωση του δικαιώματος στην εργασία, αφετέρου για τους ΚοιΣΠΕ, οι οποίοι μέσα στην εικοσαετή τους -πλέον- διαδρομή, επιδιώκουν να ενισχύσουν τις λειτουργίες τους, με σκοπό την ενδυνάμωση του αποκαταστασιακού τους ρόλου και την επίτευξη της βιωσιμότητας τους.

Για την ΠΟΚοιΣΠΕ

Ο Πρόεδρος,
Κουπίδης Σωτήριος

Η Γραμματέας,
Πόλα Νικολάου

ΠΡΟΦΙΛ ΠΟΚΟΙΣΠΕ & ΚΟΙΣΠΕ

Η ΠΟΚοιΣΠΕ αποτελεί Δευτεροβάθμιο Συλλογικό Όργανο των ΚοιΣΠΕ, οι οποίοι είναι Μονάδες Ψυχικής Υγείας με επιχειρηματική δραστηριότητα που εποπτεύονται από το Υπουργείο Υγείας. Θεσπίστηκαν με το άρθρο 12 του Ν.2716/1999 για την «Ανάπτυξη και τον εκσυγχρονισμό των υπηρεσιών ψυχικής υγείας». Επιπρόσθετα στο Ν.4430/2016 για την «Κοινωνική και Αλληλέγγυα Οικονομία» οι ΚοιΣΠΕ θεωρούνται αυτοδίκαια Κοινωνικές Συνεταιριστικές Επιχειρήσεις (ΚοινΣΕπ) Ένταξης.

Αποτελούν μια ιδιαίτερη μορφή Συνεταιρισμών, αφού μέσα από τις παραγωγικές και εμπορικές δραστηριότητες τους, δημιουργούν θέσεις απασχόλησης για άτομα με σοβαρά ψυχοκοινωνικά προβλήματα.

Οι ΚοιΣΠΕ διαδραματίζουν έναν ενεργό και καινοτόμο ρόλο στην κοινωνική ενσωμάτωση – επανένταξη ατόμων με σοβαρά ψυχοκοινωνικά προβλήματα, συμβάλλοντας σημαντικά στην ολοκλήρωση της ψυχιατρικής μεταρρύθμισης στη χώρα μας.

Στην Ελλάδα σήμερα λειτουργούν 32 ΚοιΣΠΕ, ενώ υπάρχουν 3 πρωτοβουλίες σύστασης νέων, και αριθμούν πάνω από 3.400 μέλη συνεταιριστές και 1238 εργαζόμενους, 581 εκ των οποίων είναι εργαζόμενοι - άτομα με σοβαρά ψυχοκοινωνικά προβλήματα. Ο κύκλος εργασιών των ΚοιΣΠΕ κατά το έτος 2022 έφτασε τα 11,38 εκ. ευρώ, καθιστώντας αυτούς μία σημαντική ομάδα αναφοράς του οικοσυστήματος Κοινωνικής Αλληλέγγυας Οικονομίας (ΚΑΛΟ), από την οποία παράχθηκαν οι περισσότερες ώρες εργασίας των ατόμων από ευπαθείς και ευάλωτες κοινωνικά ομάδες.

Οι ΚοιΣΠΕ δραστηριοποιούνται σε ένα πλήθος εμπορικών και παραγωγικών δραστηριοτήτων με βασικούς τομείς δραστηριότητας την παροχή υπηρεσιών καθαριότητας σε δημόσια κτήρια, την εστίαση, τον πρωτογενή τομέα αλλά και τη λειτουργία μικρών καταστημάτων εντός μεγαλύτερων χώρων, όπως για παράδειγμα μικρά καφέ και κυλικεία.

Μάθετε περισσότερα για την ΠΟΚοιΣΠΕ & τους ΚοιΣΠΕ : www.pokoispe.gr ή www.koispesupport.gr.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Πίνακας Περιεχομένων

Εισαγωγή

Κλείνουμε σε λίγο καιρό τέσσερα χρόνια από όταν τέθηκε σε ισχύ ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ε.Ε. (GDPR) και η σημασία του έχει πλέον καταδειχθεί στην πράξη.

Τι είναι ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων?

Στις 27 Απριλίου 2016 υιοθετήθηκε από το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο ο Γενικός Κανονισμός (ΕΕ) 2016/679 για την Προστασία των Δεδομένων, ευρέως γνωστός ως «GDPR» (General Data Protection Regulation), ο οποίος τέθηκε σε εφαρμογή την 25η Μαΐου 2018.

Σύμφωνα με το άρθρο 1 ο κανονισμός θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με το άρθρο 5 του Γενικού Κανονισμού προβλέπονται ορισμένες αρχές βάσει των οποίων θα πρέπει να γίνεται η επεξεργασία των δεδομένων. Οι αρχές αυτές είναι οι εξής:

- Η επεξεργασία των δεδομένων πρέπει να γίνεται με τρόπο σύννομο και θεμιτό και να είναι διαφανής ως προς το υποκείμενο των δεδομένων (αρχή της **νομιμότητας**, της **αντικειμενικότητας** και της **διαφάνειας)**.
- Η επεξεργασία πρέπει να πραγματοποιείται για καθορισμένους, νόμιμους και ρητούς σκοπούς (αρχή του **περιορισμού του σκοπού**).
- Τα υπό επεξεργασία δεδομένα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο απαραίτητο μέτρο για την εξυπηρέτηση των σκοπών της επεξεργασίας (αρχή της **ελαχιστοποίησης των δεδομένων**).
- Τα υπό επεξεργασία δεδομένα πρέπει να είναι ακριβή και να επικαιροποιούνται κατά το αναγκαίο μέτρο. Πρέπει να επιδιώκεται άμεση διαγραφή των δεδομένων εκείνων τα οποία είναι ανακριβή σε σχέση με τους σκοπούς της επεξεργασίας (αρχή της **ακρίβειας**).
- Τα υπό επεξεργασία δεδομένα πρέπει να τηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων τους μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας (αρχή του **περιορισμού της περιόδου αποθήκευσης**).
- Πρέπει να γίνεται χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων προκειμένου να εξασφαλίζεται η επεξεργασία των δεδομένων κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλειά τους (αρχή της **ακεραιότητας** και της **εμπιστευτικότητας**).
- v Τέλος, σε συνέχεια των ανωτέρω υποχρεώσεων που απορρέουν από τις γενικές αρχές του άρθρου 5 του Γενικού Κανονισμού, η παράγραφος 2 του ίδιου άρθρου προβλέπει, περαιτέρω, ότι ο υπεύθυνος επεξεργασίας φέρει ευθύνη και έχει την υποχρέωση να μπορεί να αποδείξει ανά πάσα στιγμή τη συμμόρφωσή του με τις γενικές αρχές της παραγράφου 1 (αρχή της **λογοδοσίας**).

Νομοθετικό Πλαίσιο

Στη νομοθεσία για την προστασία των προσωπικών δεδομένων συγκαταλέγονται ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 (ΓΚΠΔ), ο v. 4624/2019, ο v. 2472/1997 καθώς και ο v. 3471/2006 στον τομέα των ηλεκτρονικών επικοινωνιών.

Ειδικότερα, ο ΓΚΠΔ τέθηκε σε εφαρμογή από τις 25-5-2018, σύμφωνα με το άρθρο 99 παρ. 2 αυτού. Σύμφωνα με το άρθρο 288 της Συνθήκης για τη Λειτουργία της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), ο ΓΚΠΔ έχει άμεση εφαρμογή σε όλα τα κράτη μέλη, τα οποία υποχρεούνται να λάβουν τα αναγκαία μέτρα για την προσαρμογή της εθνικής νομοθεσίας τους.

Με τον ν. 4624/2019 (ΦΕΚ Α΄137), ορίζονται μέτρα εφαρμογής του ΓΚΠΔ και ενσωματώνεται στην εθνική νομοθεσία η Οδηγία (ΕΕ) 2016/680. Ο ν. 2472/1997 καταργήθηκε, εκτός των διατάξεων που αναφέρονται ρητά στο άρθρο 84 του ν. 4624/2019.

Ο ν. 3471/2006, ο οποίος ενσωματώνει την Οδηγία 2002/58/ΕΚ (Οδηγία e-Privacy), όπως έχει τροποποιηθεί με την Οδηγία 2009/136/ΕΚ, αποτελεί συμπλήρωση και εξειδίκευση του θεσμικού πλαισίου της προστασίας των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών.

Χρήσιμοι Ορισμοί:

Απλά Προσωπικά Δεδομένα: είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (πρώην ευαίσθητα δεδομένα)

Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων προβλέπει τις λεγόμενες «ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα» (πρώην «ευαίσθητα προσωπικά δεδομένα») για τις οποίες επιφυλάσσει αυξημένη προστασία. Στις κατηγορίες αυτές ανήκουν δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις φιλοσοφικές ή θρησκευτικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

- **Δεδομένα που αφορούν την υγεία:** δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης

της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

- **Παραβίαση δεδομένων προσωπικού χαρακτήρα»:** η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ` άλλο τρόπο σε επεξεργασία.
- **Υπεύθυνος Επεξεργασίας:** το φυσικό ή νομικό πρόσωπο το οποίο καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των προσωπικών Δεδομένων.
- **Εκτελών την επεξεργασία:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.
- **Επεξεργασία δεδομένων προσωπικού χαρακτήρα:** κάθε πράξη ή σειρά πράξεων που σχετίζεται με δεδομένα 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.
- **Τρίτος:** οποιοδήποτε φυσικό ή νομικό πρόσωπο, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

ΚΕΦΑΛΑΙΟ 1. Η νομική βάση διαχείρισης των προσωπικών δεδομένων στους Κοι.Σ.Π.Ε

Η νομική βάση διαχείρισης των προσωπικών δεδομένων στους Κοι.Σ.Π.Ε

Σκοποί Κοι.Σ.Π.Ε.

Οι Κοινωνικοί Συνεταιρισμοί Περιορισμένης Ευθύνης (Κοι.Σ.Π.Ε.) θεσπίστηκαν με το άρθρο 12 του Ν.2716/1999 του Υπουργείου Υγείας για την «Ανάπτυξη και τον εκσυγχρονισμό των υπηρεσιών ψυχικής υγείας» και αποτελούν μια ιδιαίτερη μορφή συνεταιρισμού, αφού παράλληλα είναι παραγωγικές - εμπορικές μονάδες, αλλά και μονάδες ψυχικής υγείας. Αποστολή των Κοι.Σ.Π.Ε. είναι η κοινωνικοοικονομική ενσωμάτωση και η επαγγελματική ένταξη των Ατόμων με Σοβαρά Ψυχοκοινωνικά Προβλήματα, συμβάλλοντας στη θεραπεία τους και στην κατά το δυνατόν οικονομική τους αυτάρκεια. Οι Κοι.Σ.Π.Ε. είναι νομικά πρόσωπα ιδιωτικού δικαίου με περιορισμένη ευθύνη των μελών τους, έχουν εμπορική ιδιότητα και αποτελούν Μονάδες Ψυχικής Υγείας, οι οποίες εντάσσονται στους Τομείς Ψυχικής Υγείας. Η μέριμνα για την ανάπτυξή τους και η εποπτεία τους ανήκουν στον Υπουργό Υγείας και Πρόνοιας και ασκούνται μέσω της Διεύθυνσης Ψυχικής Υγείας.

Με την θέσπιση των Νόμων για την Κοινωνική & Αλληλέγγυα Οικονομία του 2011 & 2016 οι ΚοιΣΠΕ θεωρήθηκαν αυτοδίκαια Κοινωνικές Συνεταιριστικές Επιχειρήσεις (ΚοινΣΕπ) Ένταξης. Αυτό σημαίνει ότι δύνανται να απασχολούν και άλλες κατηγορίες ευάλωτων ατόμων, όπως αυτά προσδιορίζονται από την παρ. 8 του άρθρου 2 του ν. 4430/2016 (Α` 205), ή και μειονεκτούντες εργαζόμενους. Σύμφωνα με την παρ. 8 του άρθρου 2 του ν. 4430/2016 Ως «ευάλωτες» ορίζονται οι ομάδες εκείνες του πληθυσμού που η ένταξή τους στην κοινωνική και οικονομική ζωή εμποδίζεται από σωματικά και ψυχικά αίτια ή λόγω παραβατικής συμπεριφοράς.

Σύμφωνα με την παρ. 8 του άρθρου 2 του ν. 4430/2016 Ως «ευάλωτες» ορίζονται οι ομάδες εκείνες του πληθυσμού που η ένταξή τους στην κοινωνική και οικονομική ζωή εμποδίζεται από σωματικά και ψυχικά αίτια ή λόγω παραβατικής συμπεριφοράς.

Σε αυτές ανήκουν:

α) τα άτομα με αναπηρία οποιασδήποτε μορφής (σωματική, ψυχική, νοητική, αισθητηριακή),

β) τα άτομα με προβλήματα εξάρτησης από ουσίες ή τα απεξαρτημένα άτομα,

γ) οι ανήλικοι με παραβατική συμπεριφορά, οι φυλακισμένοι/ες και αποφυλακισμένοι/ες.

Ως «ειδικές» ορίζονται οι ομάδες εκείνες του πληθυσμού οι οποίες βρίσκονται σε μειονεκτική θέση ως προς την ομαλή ένταξή τους στην αγορά εργασίας, από οικονομικά, κοινωνικά και πολιτισμικά αίτια. Σε αυτές ανήκουν:

α) τα θύματα ενδοοικογενειακής βίας,

β) τα θύματα παράνομης διακίνησης και εμπορίας αν ανθρώπων,

γ) οι άστεγοι,

δ) τα άτομα που διαβιούν σε συνθήκες φτώχειας,

ε) οι οικονομικοί μετανάστες,

στ) οι πρόσφυγες και οι αιτούντες άσυλο, για όσο εκκρεμεί η εξέταση του αιτήματος χορήγησης ασύλου,

ζ) οι αρχηγοί μονογονεϊκών οικογενειών,

η) τα άτομα με πολιτισμικές ιδιαιτερότητες,

θ) οι μακροχρόνια άνεργοι έως είκοσι πέντε ετών και άνω των πενήντα ετών.

Δεδομένα που συλλέγουν οι Κοι.Σ.Π.Ε: Συλλέγουν τόσο απλά Δεδομένα όσο και ειδικών κατηγοριών Προσωπικά Δεδομένα.

Τα Ειδικών Κατηγοριών Προσωπικά Δεδομένα αφορούν: στη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

Κατά συνέπεια, οι παραπάνω ομάδες δεν αφορούν όλες σε Ειδικών Κατηγοριών Προσωπικά Δεδομένα. Με μια διασταλτική ερμηνεία βέβαια θα μπορούσε κάποιος να ισχυριστεί ότι η γνώση ότι κάποια άτομα ανήκουν σε κάποια από τις παραπάνω κατηγορίες θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και ελευθερίες. Ο ρόλος όμως των Κοι.Σ.Π.Ε. αφορά σε "θεμιτές δραστηριότητες σκοπός των οποίων είναι να επιτρέπουν την άσκηση των θεμελιωδών ελευθεριών".

Δείτε αιτιολογική σκέψη 51 του ΓΚΠΔ «Δεδομένα προσωπικού χαρακτήρα τα οποία είναι εκ φύσεως ιδιαίτερα ευαίσθητα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες χρήζουν ειδικής προστασίας, καθότι το πλαίσιο της επεξεργασίας τους θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες. …… Παρεκκλίσεις από τη γενική απαγόρευση επεξεργασίας δεδομένων προσωπικού χαρακτήρα που υπάγονται στις εν λόγω ειδικές κατηγορίες θα πρέπει να προβλέπονται ρητώς, μεταξύ άλλων, σε περίπτωση ρητής συγκατάθεσης του υποκειμένου των δεδομένων ή όταν πρόκειται για ειδικές ανάγκες, ιδίως όταν η επεξεργασία διενεργείται στο πλαίσιο θεμιτών δραστηριοτήτων ορισμένων ενώσεων ή ιδρυμάτων, σκοπός των οποίων είναι να επιτρέπουν την άσκηση των θεμελιωδών ελευθεριών.»

Το άρθρο 9 παρ. 1 του Γενικού Κανονισμού προβλέπει ότι κατ' αρχήν απαγορεύεται η επεξεργασία των ειδικών κατηγοριών δεδομένων. Κατ' εξαίρεση μόνο επιτρέπεται η επεξεργασία τους για τους λόγους που προβλέπονται στην παρ. 2 του ίδιου άρθρου.

Για να μπορεί ένας οργανισμός να επεξεργαστεί Ειδικών κατηγοριών Προσωπικά Δεδομένα θα πρέπει να ισχύει το παρακάτω:

Λαμβάνοντας υπόψη τα παραπάνω μπορούμε να πούμε ότι:

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται σε μια από τις "νομικές βάσεις", όπως αναφέρονται στο άρθρο 6 §1 του ΓΚΠΔ. Η νόμιμη βάση στην οποία βασίζεται η επεξεργασία κάθε χρήσης των δεδομένων αναφέρεται παρακάτω:

Παροχή Υπηρεσιών – για την επεξεργασία της παροχής των υπηρεσιών, προς τους ωφελουμένους. Άρθρο 6§1(α), το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

6§1(β), η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

6§1(γ), η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

6§1(δ), η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

6§1(στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Επεξεργασία Ειδικών Κατηγοριών Δεδομένων: Σύμφωνα με το άρθρο 9 §1 και 2 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων επιτρέπεται μόνο στις συγκεκριμένες περιπτώσεις που ορίζει ο κανονισμός, ανάμεσα στις οποίες:

άρθ. 9§2(α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

(**Σημείωση 1:** Ενδεχομένως η νομική βάση της συγκατάθεσης να μην είναι ενδεδειγμένη στις περιπτώσεις τόσο λόγω της νομικής ικανότητας των υποκειμένων, όσο και της εργασιακής τους σχέσης με τον Υπεύθυνο Επεξεργασίας.

Σημείωση 2: Στην περίπτωση που η συγκατάθεση πρέπει να ληφθεί για πρόσωπο που δεν έχει δικαιοπρακτική ικανότητα το έντυπο συγκατάθεσης θα πρέπει να υπογράφεται από τον ασκούντα την επιμέλεια, γονέα κ.λπ.)

άρθ. 9§2(β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

άρθ. 9§2(γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί

άρθ. 9§2(η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,

άρθ. 9§2(θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή

άρθ. 9§2(ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Ενέργειες προώθησης του έργου του Κοι.Σ.Π.Ε. - για απάντηση σε ερωτήματα και για ενημέρωση σχετικά με τα νέα και τις υπηρεσίες [Άρθρο 6§1(α) και 6§1(στ) ΓΚΠΔ]

Η συναίνεση σχετικά με την προώθηση του έργου, μπορεί να ανακληθεί οποτεδήποτε, με ισχύ για το μέλλον.

Τήρηση Νομικών Υποχρεώσεων - για τη συμμόρφωση με τις νομικές υποχρεώσεις του Κοι.Σ.Π.Ε. προς τις αστυνομικές, ρυθμιστικές, φορολογικές, λογιστικές, ορκωτούς ελεγκτές, δικαστικές αρχές και υπηρεσίες [Άρθρο 6§1(γ) ΓΚΠΔ]

Η παροχή δεδομένων προσωπικού χαρακτήρα όπως παραπάνω, αποτελεί εκ του νόμου υποχρέωση η οποία εξαρτάται από το συγκεκριμένο αίτημα.

Επιπλέον με δεδομένο ότι οι ωφελούμενοι των Κοι.Σ.Π.Ε. έχουν διττό ρόλο, αφού είναι και εργαζόμενοι αυτών, ιδιαίτερο ενδιαφέρον έχει το άρθρο 27 του Ν.4627/2019 «Επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των σχέσεων απασχόλησης».

1. Δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να υποβάλλονται σε επεξεργασία για σκοπούς της σύμβασης εργασίας, εφόσον είναι απολύτως απαραίτητο για την απόφαση σύναψης σύμβασης εργασίας ή μετά τη σύναψη της σύμβασης εργασίας για την εκτέλεσή της.

2. Στην περίπτωση που η επεξεργασία δεδομένων προσωπικού χαρακτήρα εργαζομένου έχει κατ' εξαίρεση ως νομική βάση τη συγκατάθεσή του, για την κρίση ότι αυτή ήταν αποτέλεσμα ελεύθερης επιλογής, πρέπει να λαμβάνονται υπόψη κυρίως:

α) η υφιστάμενη στη σύμβαση εργασίας εξάρτηση του εργαζομένου και

β) οι περιστάσεις κάτω από τις οποίες χορηγήθηκε η συγκατάθεση. Η συγκατάθεση παρέχεται είτε σε έγγραφη είτε σε ηλεκτρονική μορφή και πρέπει να διακρίνεται σαφώς από τη σύμβαση εργασίας. Ο εργοδότης πρέπει να ενημερώνει τον εργαζόμενο είτε σε έγγραφη είτε σε ηλεκτρονική μορφή σχετικά με τον σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και το δικαίωμά του να ανακαλέσει τη συγκατάθεση σύμφωνα με το άρθρο 7 παράγραφος 3 του ΓΚΠΔ.

3. Κατά παρέκκλιση από το άρθρο 9 παράγραφος 1 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα με την έννοια του άρθρου 9 παράγραφος 1 του ΓΚΠΔ για τους σκοπούς της σύμβασης εργασίας επιτρέπεται, εάν είναι απαραίτητη για την άσκηση των δικαιωμάτων ή την εκπλήρωση νόμιμων υποχρεώσεων που απορρέουν από το εργατικό δίκαιο, το δίκαιο της κοινωνικής ασφάλισης και της κοινωνικής προστασίας και δεν υπάρχει κανένας λόγος να θεωρηθεί ότι το έννομο συμφέρον του υποκειμένου των δεδομένων σε σχέση με την επεξεργασία υπερτερεί. Η παράγραφος 2 ισχύει επίσης για τη συγκατάθεση στην επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα. Η συγκατάθεση πρέπει να αναφέρεται ρητά στα δεδομένα αυτά. Το άρθρο 22 παράγραφος 3 εδάφιο β΄ εφαρμόζεται ανάλογα.

4. Επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων των ειδικών κατηγοριών δεδομένων Προσωπικού Χαρακτήρα των εργαζομένων για τους σκοπούς της σύμβασης εργασίας βάσει συλλογικών συμβάσεων εργασίας. Τα διαπραγματευόμενα μέρη συμμορφώνονται με το άρθρο 88 παράγραφος 2 του ΓΚΠΔ.

5. Ο υπεύθυνος επεξεργασίας λαμβάνει τα ενδεδειγμένα μέτρα για να εξασφαλίσει ότι τηρούνται ιδίως οι αρχές για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που ορίζονται στο άρθρο 5 του ΓΚΠΔ.

6. Οι παράγραφοι 1 έως 5 εφαρμόζονται επίσης, όταν δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένων των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα των εργαζομένων, υπόκεινται σε επεξεργασία, χωρίς αυτά να αποθηκεύονται ή να προορίζονται να αποθηκευτούν σε ένα σύστημα αρχειοθέτησης.

7. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας, είτε είναι δημοσίως προσβάσιμοι είτε μη, επιτρέπεται μόνο εάν είναι απαραίτητη για την προστασία προσώπων και αγαθών. Τα δεδομένα που συλλέγονται μέσω κλειστού κυκλώματος οπτικής καταγραφής δεν επιτρέπεται να χρησιμοποιηθούν ως κριτήριο για την αξιολόγηση της αποδοτικότητας των εργαζομένων. Οι εργαζόμενοι ενημερώνονται εγγράφως, είτε σε γραπτή είτε σε ηλεκτρονική μορφή για την

εγκατάσταση και λειτουργία κλειστού κυκλώματος οπτικής καταγραφής εντός των χώρων εργασίας.

8. Για τους σκοπούς του παρόντος νόμου ως εργαζόμενοι νοούνται οι απασχολούμενοι με οποιαδήποτε σχέση εργασίας ή σύμβαση έργου ή παροχής υπηρεσιών στο δημόσιο και στον ιδιωτικό φορέα, ανεξαρτήτως του κύρους της σύμβασης, οι υποψήφιοι για εργασία και οι πρώην απασχολούμενοι.

ΚΕΦΑΛΑΙΟ 2. Ο ρόλος του DPO και της Αρχής Προστασίας Προσωπικών Δεδομένων

Ο ρόλος του DPO και της Αρχής Προστασίας Προσωπικών Δεδομένων

Ο DPO (Υπεύθυνος Προστασίας Δεδομένων, **ΥΠΔ**) έχει τουλάχιστον τα ακόλουθα καθήκοντα:

Ενημερώνει και συμβουλεύει το Οργανισμό και τους υπαλλήλους που επεξεργάζονται προσωπικά δεδομένα αναφορικά με τις υποχρεώσεις τους που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) και την κείμενη νομοθεσία σχετικά με την προστασία δεδομένων,

Παρακολουθεί τη συμμόρφωση του Οργανισμού με τις διατάξεις του ΓΚΠΔ και την κείμενη νομοθεσία σχετικά με την προστασία δεδομένων και με τις πολιτικές του Οργανισμού σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,

Παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35 του ΓΚΠΔ,

Συνεργάζεται με την εποπτική αρχή, ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία προσωπικών δεδομένων, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36 του ΓΚΠΔ, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Κατά την εκτέλεση των καθηκόντων του, ο ΥΠΔ λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας των δεδομένων.

Ενδεικτικά, ο Υπεύθυνος Προστασίας Δεδομένων:

- παρέχει συμβουλές για τον προσδιορισμό, τη διαχείριση και την επικαιροποίηση των αρχείων δραστηριοτήτων.
- προβαίνει σε εκπαιδεύσεις στελεχών, και προσωπικού του Οργανισμού, ανάλογες με τους σκοπούς και τα μέσα επεξεργασίας προσωπικών δεδομένων, που αυτοί χειρίζονται.
- προβαίνει σε δειγματοληπτικούς εσωτερικούς ελέγχους που αφορούν τη συμμόρφωση των οργανικών μονάδων του Οργανισμού με τις διατάξεις του ΓΚΠΔ, των πολιτικών του Οργανισμού, και της ενωσιακής ή εθνικής νομοθεσίας
- παρέχει τεχνική υποστήριξη στη σύνταξη συμβάσεων ή προσαρτημάτων συμβάσεων του Οργανισμού με το προσωπικό ή τους συνεργάτες αυτού (συμβάσεις

εμπιστευτικότητας), ή, κατά περίπτωση στη σύνταξη συμβάσεων ή προσαρτημάτων συμβάσεων εκτελούντος την επεξεργασία ή από κοινού εκτελούντων την επεξεργασία.
- συμβουλεύει τον Οργανισμό κατά τον σχεδιασμό και ορισμό των τεχνικών και οργανωτικών μέτρων προστασίας.

Υποστηρίζει τεχνικά και νομικά τις ερευνητικές μονάδες και δράσεις του Οργανισμού στα θέματα προστασίας προσωπικών δεδομένων.

Η εταιρεία ή ο οργανισμός σας, είτε είναι υπεύθυνος επεξεργασίας είτε εκτελών την επεξεργασία, οφείλει να διορίσει ΥΠΔ εφόσον οι **βασικές δραστηριότητες που ασκεί** περιλαμβάνουν την επεξεργασία **ευαίσθητων δεδομένων** σε **μεγάλη κλίμακα** ή την **τακτική και συστηματική παρακολούθηση σε μεγάλη κλίμακα** φυσικών προσώπων. Εν προκειμένω, η παρακολούθηση της συμπεριφοράς φυσικών προσώπων περιλαμβάνει όλες τις μορφές ανίχνευσης και κατάρτισης προφίλ στο διαδίκτυο, συμπεριλαμβανομένων των σκοπών της συμπεριφορικής διαφήμισης.

Οι δημόσιες διοικήσεις έχουν πάντα την υποχρέωση να διορίζουν ΥΠΔ (με εξαίρεση τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους ιδιότητα).

Ο ΥΠΔ μπορεί να είναι μέλος του προσωπικού του οργανισμού σας ή μπορεί να είναι εξωτερικός συνεργάτης με βάση σύμβαση παροχής υπηρεσιών. Ο ΥΠΔ μπορεί να είναι φυσικό πρόσωπο ή οργανισμός.

Παραπομπές

- Κατευθυντήριες οδηγίες του ΕΣΠΔ σχετικά με τους υπεύθυνους προστασίας δεδομένων (ΥΠΔ)
- Άρθρα 37, 38, 39 και αιτιολογική σκέψη 97 του ΓΚΠΔ

Η Αρχή Προστασίας Προσωπικών Δεδομένων

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα είναι συνταγματικά κατοχυρωμένη ανεξάρτητη δημόσια Αρχή (άρθρο 9Α του Συντάγματος) που ιδρύθηκε με τον νόμο 2472/1997.

Πλέον, από 29/8/2019, ισχύει ο νόμος 4624/2019 («Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις»). Στον ανωτέρω αναφερόμενο νόμο, τα άρθρα 9 έως και 20 αναφέρονται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (εποπτική αρχή).

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα έχει ως αποστολή της την εποπτεία της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ), του νόμου 4624/2019, του νόμου 3471/2006 και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των αρμοδιοτήτων που της ανατίθενται κάθε φορά.

Ο υπεύθυνος επεξεργασίας και οι εκτελούντες την επεξεργασία υπόκεινται σε κυρώσεις σε περίπτωση παραβίασης των διατάξεων του Γενικού Κανονισμού. Οι εποπτικές Αρχές και συγκεκριμένα στην Ελλάδα η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), δύναται προς τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία να:

- απευθύνει σύσταση ότι σκοπούμενες πράξεις επεξεργασίας είναι πιθανό να παραβαίνουν τον Γενικό Κανονισμό,
- απευθύνει επιπλήξεις όταν πράξεις επεξεργασίας έχουν παραβεί διατάξεις του Γενικού Κανονισμού,
- δίνει εντολή να συμμορφώνονται προς τα αιτήματα του υποκειμένου των δεδομένων για την άσκηση των δικαιωμάτων του σύμφωνα με τον Γενικό Κανονισμό,
- επιβάλει προσωρινό ή οριστικό περιορισμό ή απαγόρευση της επεξεργασίας,
- δίνει εντολή για αναστολή της κυκλοφορίας δεδομένων σε αποδέκτη τρίτη χώρα ή σε διεθνή οργανισμό,
- αποσύρει την πιστοποίηση ή να διατάξει τον οργανισμό πιστοποίησης να αποσύρει ένα εκδοθέν πιστοποιητικό ή να διατάξει τον οργανισμό πιστοποίησης να μην εκδώσει πιστοποίηση, εφόσον οι απαιτήσεις πιστοποίησης δεν πληρούνται ή δεν πληρούνται πλέον,
- επιβάλει διοικητικό πρόστιμο. Τα διοικητικά πρόστιμα δύναται ανάλογα με την κατηγορία των παραβάσεων να ανέλθουν έως τα 20 εκατομμύρια ευρώ ή έως το 4% του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών.

ΚΕΦΑΛΑΙΟ 3. Έντυπα και Διαδικασίες Συμμόρφωσης

3.1 Πολιτική Ιδιωτικότητας

ΟΝΟΜΑΣΙΑ Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.01: ΠΟΛΙΤΙΚΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Η παρούσα Πολιτική Ιδιωτικότητας (εφεξής η "Πολιτική") αφορά στο **.....** (εφεξής "Οργανισμός") και τα δεδομένα προσωπικού χαρακτήρα που τηρεί για φυσικά πρόσωπα.

Ο οργανισμός δεσμεύεται στην προστασία της εμπιστευτικότητας και της ιδιωτικότητας των Δεδομένων Προσωπικού Χαρακτήρα και συμμορφώνεται με τις σχετικές διατάξεις του «Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα», εφεξής «ΓΚΠΔ».

{Εδώ μπορούν να μπουν και λίγα λόγια για το θεσμικό πλαίσιο Λειτουργίας του Οργανισμού}

ΟΡΙΣΜΟΙ

- **Προσωπικά δεδομένα:** είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ.), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.
- **Ευαίσθητα προσωπικά δεδομένα ή ειδικών κατηγοριών:** χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.
- **Δεδομένα που αφορούν την υγεία:** δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.
- **Παραβίαση δεδομένων προσωπικού χαρακτήρα»:** η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ` άλλο τρόπο σε επεξεργασία.
- **Υπεύθυνος Επεξεργασίας:** το φυσικό ή νομικό πρόσωπο το οποίο καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των προσωπικών Δεδομένων.
- **Εκτελών την επεξεργασία:** το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

- **Επεξεργασία δεδομένων προσωπικού χαρακτήρα:** κάθε πράξη ή σειρά πράξεων που σχετίζεται με δεδομένα 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.
- **Τρίτος:** οποιοδήποτε φυσικό ή νομικό πρόσωπο, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα.

ΠΟΙΟΣ ΕΙΝΑΙ Ο ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Ο Οργανισμός ..... είναι ο υπεύθυνος επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, τα οποία επεξεργάζεται στο πλαίσιο της παροχής των υπηρεσιών του.

ΑΝΤΙΚΕΙΜΕΝΟ ΕΠΕΞΕΡΓΑΣΙΑΣ

Αντικείμενο επεξεργασίας είναι τα προσωπικά δεδομένα (ή ειδικών κατηγοριών δεδομένα) των παραληπτών των υπηρεσιών μας (μελών μας) ή και των κηδεμόνων αυτών, των εθελοντών και συνεργατών του Οργανισμού.

ΑΡΧΕΣ ΣΤΙΣ ΟΠΟΙΕΣ ΒΑΣΙΖΟΜΑΣΤΕ

Δεσμευόμαστε να τηρούμε τις παρακάτω αρχές επεξεργασίας προσωπικών Δεδομένων Άρθρο 5 ΓΚΠΔ:

- **Νομιμότητα, αντικειμενικότητα και διαφάνεια** - Τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων.
- **Περιορισμό του σκοπού** - Τα δεδομένα προσωπικού χαρακτήρα τα συλλέγουμε για καθορισμένους, ρητούς και νόμιμους σκοπούς και δεν υποβάλλονται σε περαιτέρω επεξεργασία με τρόπο ασυμβίβαστο με τους σκοπούς αυτούς.
- **Ελαχιστοποίηση δεδομένων** - Τα δεδομένα προσωπικού χαρακτήρα, περιορίζονται σε ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους τα επεξεργαζόμαστε.
- **Ακρίβεια / ποιότητα δεδομένων** - Τα δεδομένα προσωπικού χαρακτήρα φροντίζουμε να είναι να είναι ακριβή και, όπου χρειάζεται, τα επικαιροποιούμε άμεσα.
- **Διατήρηση** - Τα δεδομένα προσωπικού χαρακτήρα τα διατηρούμε όχι περισσότερο από ό,τι είναι απαραίτητο ή απ' ό,τι επιβάλλεται από το Νόμο

- **Ακεραιότητα και εμπιστευτικότητα**– Δεσμευόμαστε για επεξεργασία των προσωπικών δεδομένων με ασφάλεια, ιδίως από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία καταστροφής ή φθοράς, χρησιμοποιώντας κατάλληλα τεχνικά ή οργανωτικά μέτρα.
- **Δεσμευόμαστε και τηρούμε την Αρχή Λογοδοσίας**.

ΣΥΛΛΟΓΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Συλλέγουμε τα προσωπικά δεδομένα στις ακόλουθες περιπτώσεις:

- **Όταν επικοινωνείτε** μαζί μας απ' ευθείας, μέσω του τηλεφωνικού μας κέντρου ή της ιστοσελίδας μας, για να ζητήσετε πληροφορίες για τις υπηρεσίες που προσφέρουμε.
- **Συμπληρώνοντας τα έγγραφα** που απαιτούνται για να γίνετε μέλη μας.
- **Από τα άτομα που σας συνοδεύουν** ή έχουν νόμιμο δικαίωμα να ενεργούν εκ μέρους σας εάν δεν μπορείτε να παράσχετε εσείς τα στοιχεία αυτά.
- **Όταν εγγραφείτε και ζητήσετε** να λαμβάνεται ηλεκτρονική αλληλογραφία ή αλληλογραφία ανακοινώσεων/ειδήσεων του οργανισμού μας.
- **Όταν συμβληθείτε** και χρησιμοποιήσετε τις υπηρεσίες του οργανισμού μας.
- **Όταν συμπληρώσετε** τη φόρμα εθελοντή.
- **Όταν επιλέξετε** να υποστηρίξετε οικονομικά τον οργανισμό.

Τα προσωπικά δεδομένα τα επεξεργαζόμαστε για τους σκοπούς όπως αναλυτικότερα αναφέρονται στη συνέχεια.

Τα δεδομένα συλλέγονται:

- Σε έντυπη μορφή
- Σε ψηφιακή μορφή
- **Σε εικόνα ή video**
- Σε συνδυασμό των παραπάνω

Παρακαλούμε να μας βοηθάτε να τηρούμε ενημερωμένες τις πληροφορίες σας, ενημερώνοντάς μας για τυχόν αλλαγές των δεδομένων σας προσωπικού χαρακτήρα.

ΤΙ ΕΙΔΟΥΣ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ ΣΥΛΛΕΓΟΥΜΕ ΣΧΕΤΙΚΑ ΜΕ ΕΣΑΣ

Οι κάτωθι κατηγορίες δεδομένων σχετικά με εσάς μπορεί να συλλέγονται και να υποβάλλονται σε περαιτέρω επεξεργασία που περιγράφονται στην παρούσα Πολιτική:

- Πληροφορίες Επικοινωνίας (π.χ. Ονοματεπώνυμο, Δ/νση, αριθμ. Τηλεφώνου, email)
- Δεδομένα Υγείας, που είναι απαραίτητα για την εξυπηρέτηση του λήπτη των υπηρεσιών (μέλους)
- Πληροφορίες Πληρωμής (π.χ IBAN/Αρ. Λογαριασμού, επιθυμητός τρόπος πληρωμής)
- Ειδικές κατηγορίες προσωπικών δεδομένων σύμφωνα με το άρθρο 9 & 10 του ΓΚΠΔ.
- Ιστορικό εξυπηρετούμενου (π.χ. ιστορικό υγείας, ποσοστό ικανοποίησης, παράπονα)
- Δεδομένα εφαρμογών / ιστοσελίδων/ μέσων κοινωνικής δικτύωσης (π.χ. cookies)

Στο Παράρτημα 2: "Ενδεικτικές Κατηγορίες Δεδομένων" παρουσιάζονται ενδεικτικά προσωπικά δεδομένα που επεξεργαζόμαστε.

Οι επαγγελματίες υγείας και κοινωνικής φροντίδας που εμπλέκονται στη διαχείριση θεμάτων υγείας μπορούν να έχουν πρόσβαση στο φάκελο υγείας σας εντός του Κέντρου, μόνο για τους σκοπούς που έχουν σαφώς οριστεί. Το λοιπό διοικητικό – οικονομικό προσωπικό που λόγω θέσης, σε εκτέλεση εργασίας τους, απαιτείται να λάβει γνώση των προσωπικών σας δεδομένων (π.χ. για εξυπηρέτησή σας, για υποβολή στοιχείων σε ΕΟΠΠΥ, ΕΦΚΑ κ.λπ.), αυτή θα είναι περιορισμένη και το προσωπικό δεσμεύεται με συμβάσεις **εμπιστευτικότητας** των πληροφοριών που λαμβάνει γνώση.

ΚΑΤΗΓΟΡΙΕΣ ΥΠΟΚΕΙΜΕΝΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Οι κατηγορίες των υποκειμένων περιλαμβάνουν:

- Εξυπηρετούμενους (μέλη)
- Υποψήφιους Εξυπηρετούμενους
- Γονείς / Κηδεμόνες Εξυπηρετούμενων
- Εθελοντές
- Προμηθευτές
- Φυσικά πρόσωπα με την ιδιότητά τους ως εργαζόμενοι, διευθυντές ή εταίροι σε ένα νομικό πρόσωπο.
- Τρίτα πρόσωπα εμπλεκόμενα σε γεγονότα σχετιζόμενα με την παροχή των υπηρεσιών μας.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΣΚΟΠΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ & Η ΝΟΜΙΚΗ ΒΑΣΗ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται σε μια από τις "νομικές βάσεις", όπως αναφέρονται στο άρθρο 6 §1 του ΓΚΠΔ. Η νόμιμη βάση στην οποία βασίζεται η επεξεργασία κάθε χρήσης των δεδομένων αναφέρεται παρακάτω:

Παροχή Υπηρεσιών – για την επεξεργασία της παροχής των υπηρεσιών, προς τους ωφελουμένους. Άρθρο 6§1(α), το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

6§1(β), η επεξεργασία είναι απαραίτητη για την **εκτέλεση σύμβασης** της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

6§1(γ), η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με **έννομη υποχρέωση** του υπευθύνου επεξεργασίας,

6§1(δ), η επεξεργασία είναι απαραίτητη για τη διαφύλαξη **ζωτικού συμφέροντος** του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

6§1(στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των **έννομων συμφερόντων** που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Επεξεργασία Ειδικών Κατηγοριών Δεδομένων: Σύμφωνα με το άρθρο 9 §1 και 2 του ΓΚΠΔ η επεξεργασία ειδικών κατηγοριών δεδομένων επιτρέπεται μόνο στις συγκεκριμένες περιπτώσεις που ορίζει ο κανονισμός, ανάμεσα στις οποίες:

άρθ. 9§2(α) το υποκείμενο των δεδομένων έχει παράσχει **ρητή συγκατάθεση** για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

(**Σημείωση**: *Ενδεχομένως η νομική βάση της συγκατάθεσης να μην είναι ενδεδειγμένη στις περιπτώσεις τόσο λόγω της νομικής ικανότητας των υποκειμένων, όσο και της εργασιακής τους σχέσης με τον Υπεύθυνο Επεξεργασίας*.)

άρθ. 9§2(β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα **του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας**, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

άρθ. 9§2(γ) η επεξεργασία είναι απαραίτητη για την προστασία των **ζωτικών συμφερόντων** του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί

άρθ. 9§2(η) η επεξεργασία είναι απαραίτητη για σκοπούς **προληπτικής ή επαγγελματικής ιατρικής**, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας **ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών** βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,

άρθ. 9§2(θ) η επεξεργασία είναι απαραίτητη για λόγους **δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας**, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή

άρθ. 9§2(ι) η επεξεργασία είναι απαραίτητη για σκοπούς **αρχειοθέτησης** προς το δημόσιο συμφέρον, για σκοπούς **επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς** σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Ενέργειες προώθησης του έργου του Κοι.Σ.Π.Ε. - για απάντηση σε ερωτήματα και για ενημέρωση σχετικά με τα νέα και τις υπηρεσίες [Άρθρο 6§1(α) και 6§1(στ) ΓΚΠΔ]

Η συναίνεση σχετικά με την προώθηση του έργου, μπορεί να ανακληθεί οποτεδήποτε, με ισχύ για το μέλλον.

Τήρηση Νομικών Υποχρεώσεων - για τη συμμόρφωση με τις νομικές υποχρεώσεις του Κοι.Σ.Π.Ε. προς τις αστυνομικές, ρυθμιστικές, φορολογικές, λογιστικές, ορκωτούς ελεγκτές, δικαστικές αρχές και υπηρεσίες [Άρθρο 6§1(γ) ΓΚΠΔ]

Η παροχή δεδομένων προσωπικού χαρακτήρα όπως παραπάνω, αποτελεί εκ του νόμου υποχρέωση η οποία εξαρτάται από το συγκεκριμένο αίτημα.

ΟΙΚΟΝΟΜΙΚΗ ΥΠΟΣΤΗΡΙΞΗ

Ο **Οργανισμός .....** σε περίπτωση οικονομικής υποστήριξης, τηρεί μόνο το ονοματεπώνυμο του δωρητή. Η οικονομική υποστήριξη, γίνεται διαδικτυακά μέσω web-banking, με τη χρήση πιστωτικής ή χρεωστικής κάρτας. Αλλά και με απλές τραπεζικές μεταφορές και με μετρητά. Οι δωρεές καταβάλλονται στους λογαριασμούς που βρίσκονται στον ακόλουθο σύνδεσμο (http://www.....). Τα στοιχεία που τηρεί ο οργανισμός, χρησιμοποιούνται αποκλειστικά από αυτόν, προκειμένου να εκδοθεί αποδεικτικό δωρεάς.

ΠΩΣ ΔΙΑΣΦΑΛΙΖΟΥΜΕ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Διασφαλίζουμε ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία, με την τήρηση πολιτικών και διαδικασιών σύμφωνων με τους σκοπούς επεξεργασίας. Για παράδειγμα, τα ακόλουθα μέτρα ασφαλείας χρησιμοποιούνται για την προστασία των δεδομένων προσωπικού χαρακτήρα κατά αθέμιτης χρήσης ή οποιασδήποτε άλλης μορφής μη εξουσιοδοτημένης επεξεργασίας:

- Η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα περιορίζεται μόνο σε ορισμένο αριθμό εξουσιοδοτημένων προσώπων για τους συγκεκριμένους σκοπούς.
- Το προσωπικό των αρμόδιων τμημάτων που είναι αρμόδιο με τη διαχείριση των προσωπικών δεδομένων, δεσμεύεται με ρήτρες εμπιστευτικότητας έχοντας

διαβαθμισμένη και περιορισμένη πρόσβαση, μόνο στα απαραίτητα για την ολοκλήρωση της παροχής της υπηρεσίας.

- Τα ευαίσθητα δεδομένα αποθηκεύονται σε Η/Υ με εξουσιοδοτημένη πρόσβαση. Επίσης σε έντυπη μορφή κλειδώνονται σε ερμάρια όπου έχουν πρόσβαση μόνο εξουσιοδοτημένα πρόσωπα.
- Επιλέγουμε αξιόπιστους συνεργάτες, οι οποίοι δεσμεύονται εγγράφως σύμφωνα με το άρθρο 28 §4 του ΓΚΠΔ με τις ίδιες υποχρεώσεις όσον αφορά στην προστασία προσωπικών δεδομένων. Διατηρούμε δε το δικαίωμα ελέγχου επί αυτών άρθρο 28 §3 στοιχείο η.
- Τα συστήματα πληροφορικής που χρησιμοποιούνται για την επεξεργασία των δεδομένων είναι τεχνικά απομονωμένα από άλλα συστήματα, προκειμένου να εμποδίζεται η μη εξουσιοδοτημένη πρόσβαση, για παράδειγμα μέσω παράνομης πρόσβασης (hacking).
- Επιπλέον, η πρόσβαση στα εν λόγω συστήματα πληροφορικής παρακολουθείται σε μόνιμη βάση, προκειμένου να εντοπισθεί και αποτραπεί η παράνομη χρήση σε αρχικό στάδιο.

ΓΙΑ ΠΟΣΟ ΧΡΟΝΙΚΟ ΔΙΑΣΤΗΜΑ ΑΠΟΘΗΚΕΥΟΥΜΕ ΤΑ ΔΕΔΟΜΕΝΑ

Αποθηκεύουμε τα δεδομένα προσωπικού χαρακτήρα για όσο χρονικό διάστημα απαιτείται από τον αντίστοιχο σκοπό επεξεργασίας και οποιονδήποτε άλλο επιτρεπόμενο συνδεδεμένο σκοπό. Τα δεδομένα διατηρούνται καθ' όλη τη διάρκεια ισχύος της σύμβασής μας και, μετά τη λήξη αυτής, για όσο χρονικό διάστημα προβλέπεται από την ισχύουσα νομοθεσία.

Πληροφορίες οι οποίες δεν είναι πλέον απαραίτητες, καταστρέφονται με ασφάλεια.

Ειδικά για τα δεδομένα τα οποία επεξεργαζόμαστε βάσει της συγκατάθεσής σας (π.χ. για σκοπούς προώθησης του έργου μας), αυτά τηρούνται από τη λήψη της σχετικής συναίνεσης και έως ότου ανακληθεί αυτή.

Περιορίζουμε την πρόσβαση στα δεδομένα σας στα πρόσωπα που είναι απαραίτητο να τα χρησιμοποιήσουν για το συγκεκριμένο σκοπό.

ΠΟΙΟΙ ΕΙΝΑΙ ΟΙ ΑΠΟΔΕΚΤΕΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Τα δεδομένα προσωπικού χαρακτήρα που συλλέγει ο οργανισμός μας, δεν τα διαβιβάζει σε οποιονδήποτε τρίτο (φυσικό ή νομικό πρόσωπο) για κανένα λόγο, εκτός εάν προβλέπεται από τον νόμο ή ζητείται από τις αρμόδιες αρχές.

Περαιτέρω, εφόσον δικαιολογείται η νομιμότητα της διαβίβασης, τα δεδομένα προσωπικού χαρακτήρα μπορεί να κοινοποιούνται στις ακόλουθες κατηγορίες αποδεκτών:

- Υπάλληλοι μας ή συνεργάτες μας που ενδέχεται να επεξεργάζονται τα δεδομένα σας προσωπικού χαρακτήρα υπό τις οδηγίες μας.

- Όταν για πληρέστερη θεραπεία σας απαιτηθεί η συνεργασία με άλλους φορείς, αφού πρώτα λάβετε γνώση.
- Όταν μια μολυσματική ασθένεια μπορεί να θέσει σε κίνδυνο την ασφάλεια των άλλων.
- Εταιρείες μεταφοράς ή Courier
- Υποκατάστημα του Οργανισμού ή/και συνεργαζόμενους φορείς στο πλαίσιο των αρμοδιοτήτων τους.
- Εξωτερικοί συνεργάτες, οι οποίοι δεσμεύονται εγγράφως σύμφωνα με το άρθρο 28 §4 του ΓΚΠΔ με τις ίδιες υποχρεώσεις όσον αφορά στην προστασία προσωπικών δεδομένων.
- Οποιαδήποτε εποπτική αρχή, όπως απαιτείται από το εκάστοτε ισχύον εποπτικό πλαίσιο.
- Οποιαδήποτε δημόσια ή δικαστική αρχή, εφόσον αυτό επιβάλλεται από το νόμο ή από δικαστική απόφαση π.χ. Δικαστήριο, Φορολογική αρχή, ασφαλιστικά ταμεία κ.λπ.

Παρόλο που η διαβίβαση δεδομένων μέσω του διαδικτύου ή μίας ιστοσελίδας δεν μπορεί να προστατευθεί εγγυημένα από κυβερνοεπιθέσεις (cyberattacks), τόσο εμείς όσο και οι συνεργάτες μας εργαζόμαστε για να διατηρήσουμε φυσικά, ηλεκτρονικά και διαδικαστικά μέτρα ασφαλείας για την προστασία των δεδομένων σας.

ΠΟΥ ΛΑΜΒΑΝΕΙ ΧΩΡΑ Η ΕΠΕΞΕΡΓΑΣΙΑ

Τα προσωπικά δεδομένα των ληπτών των υπηρεσιών μας του προσωπικού και των συνεργατών μας, υποβάλλονται σε επεξεργασία εντός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ).

Στην περίπτωση που απαιτηθεί η διενέργεια έρευνας για την παροχή υπηρεσιών και εκτός του ΕΟΧ τότε αυτό πραγματοποιείται κατόπιν ρητής συγκατάθεσής σας. Άρθρο 49, §4 (α).

ΠΑΡΑΒΙΑΣΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Σε περίπτωση παραβίασης της ασφάλειας και της ακεραιότητας των δεδομένων που βρίσκονται στη διάθεσή μας και αφορούν δεδομένα προσωπικού χαρακτήρα, ο οργανισμός θα λάβει τα ακόλουθα μέτρα:(Σύμφωνα με τα άρθρα 33 και 34 του ΓΚΠΔ):

- Θα εξετάσει και αξιολογήσει τις διαδικασίες εκείνες που απαιτούνται για τον περιορισμό της παραβίασης
- Θα αξιολογήσει τον κίνδυνο και τις επιπτώσεις του στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
- Θα προσπαθήσει να μειώσει όσο το δυνατόν τη ζημιά που έχει προκληθεί ή μπορεί να προκληθεί.
- Θα ειδοποιήσει εντός 72 ωρών από τη γνώση για την παραβίαση, εάν απαιτείται
- Θα αξιολογήσει τις επιπτώσεις στην ιδιωτικότητα και θα λάβει τα κατάλληλα μέτρα για την αποφυγή επανάληψης της παραβίασης.

ΤΑ ΔΙΚΑΙΩΜΑΤΑ ΣΑΣ ΩΣ ΥΠΟΚΕΙΜΕΝΟ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΩΣ ΜΠΟΡΕΙΤΕ ΝΑ ΤΑ ΑΣΚΗΣΕΤΕ

Έχετε δικαίωμα να ζητήσετε πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που σας αφορούν, διόρθωση / διαγραφή των προσωπικών σας δεδομένων, περιορισμό της επεξεργασίας, δικαίωμα να αντιταχθείτε στην επεξεργασία ή/και να ασκήσετε το δικαίωμά σας στη φορητότητα των δεδομένων.

Εάν η επεξεργασία δεδομένων βασίζεται στη συγκατάθεσή σας, μπορείτε να ανακαλέσετε τη συγκατάθεσή σας οποτεδήποτε, με ισχύ για το μέλλον.

Αναλυτικότερα, έχετε το δικαίωμα:

α. **Πρόσβασης**: Δικαίωμα να ενημερωθείτε για την επεξεργασία των Δεδομένων από εμάς, και δικαίωμα πρόσβασης στα δεδομένα.

β. **Διόρθωσης**: Δικαίωμα να ζητήσετε διόρθωση ή συμπλήρωση των δεδομένων σας, αν αυτά είναι ανακριβή ή ελλιπή.

γ. **Διαγραφής**: Δικαίωμα να ζητήσετε τη διαγραφή δεδομένων σας: Αυτό το δικαίωμα μπορούμε να το ικανοποιήσουμε αν:

- Τα δεδομένα δεν είναι πλέον απαραίτητα για τους σκοπούς για τους οποίους συλλέχθηκαν
- Εάν δεν υπάρχει άλλη νομική βάση για επεξεργασία πέραν της συγκατάθεσης.
- Εάν ασκήσετε το δικαίωμα εναντίωσης (δείτε στ κατωτέρω)
- Εάν τα δεδομένα υποβλήθηκαν σε επεξεργασία αντίθετη στις ισχύουσες νομοθετικές διατάξεις
- Εάν τα δεδομένα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση

Διατηρούμε το δικαίωμα άρνησης ικανοποίησης του παραπάνω δικαιώματος εάν η επεξεργασία των δεδομένων είναι απαραίτητη για την τήρηση νομικής μας υποχρέωσης, λόγους δημοσίου συμφέροντος ή τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (άρθρο 17 §3)

δ. **Περιορισμού της επεξεργασίας**: Δικαίωμα να επισημάνετε τα δεδομένα, με στόχο τον περιορισμό επεξεργασίας τους. Για παράδειγμα όταν έχετε αμφισβητήσει την ακρίβεια των προσωπικών σας δεδομένων, για την περίοδο που θα απαιτηθεί για την επαλήθευση.

ε. **Φορητότητας**: Δικαίωμα να λάβετε τα δεδομένα σας σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο καθώς και να ζητήσετε τη διαβίβασή τους, τόσο σε εσάς, όσο και σε άλλο πρόσωπο που θα τα επεξεργαστεί, εάν αυτό είναι εφικτό.

στ. **Εναντίωσης**: Δικαίωμα να αντιτάσσεστε ανά πάσα στιγμή στην επεξεργασία δεδομένων σας, περιλαμβανομένης της κατάρτισης προφίλ, επίσης όταν ο λόγος επεξεργασίας αφορά σε απ' ευθείας εμπορική προώθηση.

Ο οργανισμός θα εξετάσει το αίτημά σας και θα σας απαντήσει εντός ενός μηνός από την παραλαβή του αιτήματος, είτε για την ικανοποίησή του, είτε για τους αντικειμενικούς λόγους που εμποδίζουν την ικανοποίησή του ή, λαμβανομένης της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων, εντός προθεσμίας επιπλέον δύο μηνών. (Άρθρο 12 §3)

Η άσκηση των ανωτέρω δικαιωμάτων σας πραγματοποιείται χωρίς κόστος για εσάς, με την αποστολή σχετικής αίτησης/επιστολής/email στον Υπεύθυνο Επεξεργασίας Δεδομένων.

Για τη διεκπεραίωση οποιουδήποτε από τα παραπάνω δικαιώματα, απαιτείται η ταυτοποίηση, προκειμένου να επιβεβαιώσουμε ότι τα προσωπικά σας δεδομένα προστατεύονται και διατηρούνται ασφαλή.

Στην περίπτωση που δεν είστε ικανοποιημένοι από την χρήση των δεδομένων σας από εμάς ή από την απάντησή μας στην άσκηση των ανωτέρω δικαιωμάτων σας, δικαιούστε να υποβάλετε καταγγελία στην Αρχή Προστασίας Προσωπικών Δεδομένων.

Μπορείτε να ασκήσετε τα παραπάνω δικαιώματά σας, στα στοιχεία επικοινωνίας που αναφέρονται κατωτέρω.

ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ

Για οποιοδήποτε ζήτημα σχετικά με την επεξεργασία των προσωπικών σας δεδομένων και για την άσκηση των παραπάνω δικαιωμάτων σας, μπορείτε να επικοινωνήσετε με τον Οργανισμό . ……., τηλεφωνικά στο +30 ……. (Δευτέρα - Παρασκευή 12:00 - 16:00), με e-mail στη διεύθυνση info@.....org και ταχυδρομικά στη διεύθυνση ……., ΤΚ ……

ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ ΤΗΣ ΑΡΧΗΣ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Τηλέφωνο: +30 21064.75.600, e-mail: contact@dpa.gr και ταχυδρομική διεύθυνση: Λεωφόρος Κηφισίας 1-3, ΤΚ 115 23, Αθήνα.

COOKIES

[Τα Cookies λαμβάνονται υπόψιν εάν η ιστοσελίδα που διατηρείτε κρατά cookies (θα σας το πει αυτό που ανέπτυξε την ιστοσελίδα και τότε πρέπει να βάλετε συγκεκριμένα ποια cookies κρατούνται]

Τα cookies είναι σημαντικά για την αποτελεσματική λειτουργία του διαδικτυακού τόπου www..... και για τη βελτίωση της online εμπειρίας σας.

Τι είναι τα cookies;

Τα cookies είναι μικρά αρχεία κειμένου που περιέχουν πληροφορίες που είναι αποθηκευμένες στο πρόγραμμα περιήγησης ιστού του υπολογιστή σας κατά την περιήγηση στο www……. Αυτά τα cookies μπορούν να καταργηθούν ανά πάσα στιγμή, καθώς μπορείτε να τροποποιήσετε τις ρυθμίσεις του προγράμματος περιήγησης για να απορρίψετε ορισμένα ή όλα τα cookies. Η λειτουργία βοήθειας στα περισσότερα προγράμματα περιήγησης παρέχει πληροφορίες σχετικά με τον τρόπο αποδοχής cookies, την απενεργοποίηση των cookies ή την ειδοποίησή σας κατά τη λήψη ενός νέου cookie.

Οι πληροφορίες που παράγονται από το αρχείο cookies σχετικά με τη χρήση της ιστοσελίδας από εσάς (συμπεριλαμβανομένης και της Διεύθυνσης IP σας) θα διαβιβάζεται στην και θα αποθηκεύεται στην Google, στους servers της.

Εάν δεν αποδεχτείτε τα cookies, ενδέχεται να μην μπορείτε να χρησιμοποιήσετε κάποιες λειτουργίες της Υπηρεσίας μας και σας συνιστούμε να τα αφήσετε ενεργοποιημένα.

Επίσης χρησιμοποιούνται cookies από google analytics και προτείνουμε να ενημερωθείτε από την google για τις πολιτικές απορρήτου που εφαρμόζει.

ΕΠΙΚΟΙΝΩΝΙΑ ΤΟΥ ΕΡΓΟΥ ΜΑΣ - NEWSLETTER

[Σε περίπτωση που αποστέλλετε Newsletter]

Ο επισκέπτης/χρήστης μπορεί να επισκέπτεται τον παρόντα διαδικτυακό τόπο www……. τον οποίο διατηρεί και διαχειρίζεται ο **Οργανισμός …….**, χωρίς να αποκαλύπτει την ταυτότητά του και χωρίς να παρέχει οποιοδήποτε προσωπικό του στοιχείο, με την επιφύλαξη της αποδοχής των σχετικών cookies (βλέπε παραπάνω).

Γενικά, δεν απαιτείται να υποβάλλετε προσωπικά δεδομένα στον οργανισμό διαδικτυακά, αλλά μπορεί να ζητήσουμε από εσάς να παρέχετε ορισμένα προσωπικά δεδομένα προκειμένου να λάβετε πρόσθετες πληροφορίες σχετικά με τις υπηρεσίες μας και τις εκδηλώσεις μας. Ο οργανισμός μπορεί επίσης να ζητά την άδειά σας για ορισμένες χρήσεις των προσωπικών σας δεδομένων και μπορείτε είτε να συναινέσετε ή να αρνηθείτε αυτές τις χρήσεις.

Ωστόσο, προκειμένου ο επισκέπτης/χρήστης να καταστεί αποδέκτης ηλεκτρονικού ενημερωτικού υλικού (πχ. Newsletters) που αποστέλλει ο οργανισμός, ώστε να ενημερώνεται για θέματα της επικαιρότητας και να τύχει στο μέλλον προνομίων από τον οργανισμό δύναται να παρέχει τη ρητή συναίνεσή του αναφορικά με την εγγραφή του στις υπηρεσίες του Διαδικτυακού Τόπου και στην παραχώρηση στον οργανισμό των στοιχείων του. Θα έχετε την δυνατότητα να διαγραφείτε από τον σχετικό κατάλογο παραληπτών, ανακαλώντας την συγκατάθεσή σας, με σχετικό αίτημα προς τον οργανισμό μας. Εάν αποφασίσετε να διαγραφείτε από κάποια υπηρεσία ή επικοινωνία, θα προσπαθήσουμε να διαγράψουμε τα δεδομένα σας το συντομότερο δυνατό, παρόλο που μπορεί να χρειαστούμε ορισμένο χρόνο ή/και πληροφορίες πριν μπορέσουμε να επεξεργαστούμε το αίτημά σας.

Τα προσωπικά στοιχεία που συλλέγονται αποθηκεύονται σε διακομιστές περιορισμένης πρόσβασης που ελέγχονται με κωδικούς πρόσβασης και ο οργανισμός χρησιμοποιεί ειδικές τεχνολογίες και διαδικασίες για να ενισχύσει την προστασία αυτών των πληροφοριών έναντι απώλειας ή κακής χρήσης καθώς και να τις προστατέψει από μη εξουσιοδοτημένη πρόσβαση, κοινοποίηση, τροποποίηση ή καταστροφή. Εντούτοις, αν και ο οργανισμός καταβάλλει κάθε δυνατή προσπάθεια ώστε να προστατευθούν τα ανωτέρω στοιχεία, δεν μπορεί να εγγυηθεί ότι οι ως άνω τεχνολογίες και διαδικασίες δεν θα προσβληθούν ποτέ και κατά οποιοδήποτε τρόπο.

Προς τούτο, εάν υποπέσει στην αντίληψή οποιουδήποτε επισκέπτη/χρήστη οποιαδήποτε παράνομη, κακόβουλη, μη ενδεδειγμένη ή αθέμιτη χρήση δεδομένων προσωπικού χαρακτήρα, τα οποία σχετίζονται με οποιοδήποτε τρόπο με τη χρήση του Διαδικτυακού Τόπου, αναλαμβάνει την υποχρέωση όπως γνωστοποιήσει το γεγονός άμεσα στον οργανισμό.

ΚΩΔΙΚΟΙ ΠΡΟΣΒΑΣΗΣ

Στην περίπτωση που σας δώσουμε (ή έχετε επιλέξει) κωδικό για την πρόσβαση σε ορισμένα τμήματα της ιστοσελίδας μας ή σε οποιαδήποτε άλλη διαδικτυακή πύλη, σε εφαρμογές ή σε υπηρεσίες που προσφέρουμε, είστε υπεύθυνοι να τηρείτε τον εν λόγω κωδικό απόρρητο και να συμμορφώνεστε με κάθε διαδικασία ασφαλείας, για την οποία σας έχουμε ενημερώσει. Σας ζητούμε να μην κοινοποιήσετε τον κωδικό πρόσβασης σε κανένα πρόσωπο.

ΣΥΝΔΕΣΜΟΙ ΣΕ ΆΛΛΟΥΣ ΙΣΤΟΤΟΠΟΥΣ

Η Ιστοσελίδα μας μας μπορεί να περιέχει συνδέσμους προς άλλους ισοτόπους που δεν λειτουργούν από εμάς. Εάν κάνετε κλικ σε ένα σύνδεσμο τρίτου μέρους, θα κατευθυνθείτε στον ιστότοπο αυτού του τρίτου μέρους. Σας συνιστούμε να ελέγξετε την Πολιτική απορρήτου για κάθε ιστότοπο που επισκέπτεστε. Δεν έχουμε έλεγχο και δεν αναλαμβάνουμε καμία ευθύνη για το περιεχόμενο, τις πολιτικές απορρήτου ή τις πρακτικές οποιονδήποτε τοποθεσιών ή υπηρεσιών τρίτου μέρους.

ΕΝΗΜΕΡΩΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Η παρούσα πολιτική αναθεωρείται όταν υπάρχει μια σημαντική αλλαγή. Η αναθεώρηση αυτή θα είναι διαθέσιμη στην ιστοσελίδα μας www.....

ΠΑΡΑΡΤΗΜΑ 1: ΝΟΜΙΚΗ ΒΑΣΗ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ.

Σύμφωνα με το άρθρο 6 του ΓΚΠΔ:

Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:

α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Ευαίσθητα Προσωπικά Δεδομένα:

Άρθρο 9 του ΓΚΠΔ

"Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα"

1. Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

2. Η παράγραφος 1 δεν εφαρμόζεται στις ακόλουθες περιπτώσεις:

α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων,

ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,

ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,

η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,

θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή

ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίου της Ένωσης ή κράτους μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων..

ΠΑΡΑΡΤΗΜΑ 2: ΕΝΔΕΙΚΤΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ

Πληροφορίες Ταυτοποίησης:

- Ονοματεπώνυμο
- Τίτλος (κος/κα)
- Οικογενειακή κατάσταση
- Ημερομηνία γέννησης
- ΑΦΜ
- Αριθμός Δελτίου Ταυτότητας
- ΑΜΚΑ

Πληροφορίες επικοινωνίας:

- Διεύθυνση
- Email
- Αριθμός σταθερού / κινητού τηλεφώνου
- Φαξ

Πληροφορίες Επαγγελματικής Κατάστασης:

- Επάγγελμα
- Εισόδημα (για το προσωπικό)
- Στοιχεία οικονομικής συμπεριφοράς

Πληροφορίες Πληρωμής:

- Αριθμός Τραπεζικού Λογαριασμού / IBAN
- Επιθυμητός τρόπος πληρωμής
- Αριθμός Πιστωτικής/Χρεωστικής Κάρτας

Δεδομένα αναγνώρισης (Ενδεικτικά):

- Αριθμός / κωδικός εξυπηρετούμενου
- Αριθμός συμβολαίου

Επιπλέον προσωπικές πληροφορίες / προτιμήσεις (Ενδεικτικά):

- Άδεια οδήγησης (κατηγορία)
- Επιθυμητός δίαυλος επικοινωνίας

Ειδικές Κατηγορίες Προσωπικών Δεδομένων (Ενδεικτικά):

- Ιατρικό Ιστορικό
- Δεδομένα Υγείας (π.χ. προηγούμενη υγειονομική περίθαλψη)
- Δεδομένα Υγείας προσωπικού (π.χ. άδειες ασθενείας για το προσωπικό)
- ΑΜΚΑ

Ιστορικό μέλους (Ενδεικτικά):

- Βαθμός ικανοποίησης εξυπηρετούμενου ή κηδεμόνα εξυπηρετούμενου (και επιπλέον πληροφορίες από έρευνα ικανοποίησης)
- Ιστορικό παραπόνων

Δεδομένα εφαρμογών / ιστοσελίδων/ μέσων κοινωνικής δικτύωσης:

- Σε περίπτωση που ο χρήστης, μέλος, εθελοντής κ.λπ. έχει εγγραφεί ή συνδεθεί, ενδέχεται να χρησιμοποιεί τα ακόλουθα δεδομένα:
- Επισκεψιμότητα της ιστοσελίδας
- Δεδομένα Cookies (υπό την προϋπόθεση της αποδοχής της πολιτικής cookie)

3.2 Πολιτική Διατήρησης Προσωπικών Δεδομένων

ΟΝΟΜΑΣΙΑ Κοι.Σ.Π.Ε…… ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.02: ΠΟΛΙΤΙΚΗ ΔΙΑΤΗΡΗΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Γενικά

Σύμφωνα με τις διατάξεις του Κανονισμού GDPR, τα προσωπικά δεδομένα πρέπει να διατηρούνται για χρονικό διάστημα που **δεν υπερβαίνει το αναγκαίο, για το σκοπό τον οποίο συλλέχθηκαν**. Με την καταστροφή/διαγραφή των δεδομένων, όταν πλέον δεν χρειάζονται, μειώνουμε τον κίνδυνο να γίνουν ανακριβή, ξεπερασμένα, μη σχετικά ή ακατάλληλα.

Ο Κανονισμός GDPR δεν προβλέπει συγκεκριμένη ελάχιστη ή μέγιστη περίοδο για τη διατήρηση προσωπικών δεδομένων.

Διατήρηση Προσωπικών Δεδομένων

Η διατήρηση προσωπικών δεδομένων για μεγάλο χρονικό διάστημα, μπορεί να προκαλέσει τα ακόλουθα:

- Αυξημένο κίνδυνο, να ξεπεραστεί ο χρόνος διατήρησης των πληροφοριών και οι πληροφορίες αυτές να χρησιμοποιηθούν εις βάρος όλων των ενδιαφερόμενων.
- Τα δεδομένα είναι πιθανό να γίνουν ανακριβή.
- Παρόλο που τα προσωπικά δεδομένα δεν χρειάζονται, πρέπει ακόμα να διατηρούνται με ασφάλεια.
- Η ανταπόκριση στα αιτήματα πρόσβασης των υποκειμένων, για κάθε προσωπικό δεδομένο που διατηρείται, ενδέχεται να είναι πιο δύσκολη και χρονοβόρα, σε περίπτωση που διατηρούνται περισσότερα δεδομένα απ' όσα χρειάζονται.

Για τους παραπάνω λόγους κάθε τμήμα:

- Ανασκοπεί για πόσο διάστημα κρατάει τα προσωπικά δεδομένα.
- Εξετάζει το σκοπό ή τους σκοπούς για τους οποίους κρατάει πληροφορίες, για να αποφασίσει εάν και για πόσο διάστημα θα τα διατηρήσει.
- Διαγράφει με ασφάλεια πληροφορίες που δεν χρειάζονται πλέον.
- Ενημερώνει, αρχειοθετεί, καταστρέφει ή διαγράφει με ασφάλεια τις πληροφορίες, αν έχει περάσει η περίοδος διατήρησης τους.

Κριτήρια καθορισμού χρόνου διατήρησης δεδομένων

Τα προσωπικά δεδομένα θα πρέπει να διατηρηθούν για μεγαλύτερο χρονικό διάστημα σε ορισμένες περιπτώσεις, από ό,τι σε άλλες. Η διάρκεια διατήρησης των προσωπικών δεδομένων θα πρέπει να βασίζεται στις ανάγκες του Οργανισμού.

Απόφαση κάθε φορά λαμβάνεται αξιολογώντας:

- Για ποιο λόγο χρησιμοποιούνται τα δεδομένα.
- Επικρατούσες συνθήκες.
- Νομικές ή κανονιστικές απαιτήσεις.

- Βιομηχανικές ή εμπορικές πρακτικές.

Διατηρούμε τα δεδομένα προσωπικού χαρακτήρα για όσο χρονικό διάστημα απαιτείται από τον αντίστοιχο σκοπό επεξεργασίας και οποιονδήποτε άλλο επιτρεπόμενο συνδεδεμένο σκοπό. Τα δεδομένα διατηρούνται καθ' όλη τη διάρκεια ισχύος της **συμβατικής σχέσης με τα υποκείμενα των δεδομένων** και, μετά τη λήξη αυτής, για όσο χρονικό διάστημα προβλέπεται από την ισχύουσα νομοθεσία ότι είναι δυνατό να εγερθούν αξιώσεις ή, σε περίπτωση έγερσης αξίωσης, έως την αμετάκλητη επίλυση τυχόν διαφοράς.
Στην περίπτωση που τα δεδομένα χρησιμοποιούνται για παραπάνω από έναν σκοπούς, θα τα διατηρούμε έως ότου ο σκοπός με το μακρότερο χρονικό διάστημα λήξει, αλλά θα σταματήσουμε να τα χρησιμοποιούμε για τον σκοπό με το συντομότερο χρονικό διάστημα, μόλις παρέλθει το εν λόγω διάστημα. Δεδομένα που δεν είναι πλέον απαραίτητα, καταστρέφονται ή διαγράφονται με ασφάλεια.

Ειδικά για τα δεδομένα τα οποία επεξεργαζόμαστε βάσει συγκατάθεσης του υποκειμένου(π.χ. για σκοπούς μάρκετινγκ), αυτά τηρούνται από τη λήψη της σχετικής συγκατάθεσης και έως ότου ανακληθεί αυτή.

Περιορίζουμε την πρόσβαση στα δεδομένα σας στα πρόσωπα που είναι απαραίτητο να τα χρησιμοποιήσουν για το συγκεκριμένο σκοπό.

Τέλος Περιόδου Διατήρησης

Η δήλωση ιδιωτικότητας, καθιστά σαφές στους ανθρώπους τι θα συμβεί με τα προσωπικά τους δεδομένα όταν δεν σχετίζονται πλέον μαζί μας.

Το GDPR δεν παρέχει ορισμό για την διαγραφή δεδομένων. Ωστόσο ο όρος διαγραφή μπορεί να ερμηνευθεί ως καταστροφή. Με το φυσικό αρχείο είναι εύκολο να υπάρξει συμμόρφωση, μέσω καταστροφέα εγγράφων. Παρόλα αυτά, σε δεδομένα που διατηρούνται σε ηλεκτρονική μορφή, αυτό μπορεί να είναι πολύ πιο δύσκολο.

Σε κάθε περίπτωση στο αρχείο δραστηριοτήτων του άρθρου 30 καθορίζεται ο χρόνος διατήρησης των προσωπικών δεδομένων.

Αρχεία και Δεδομένα

Ο Εκτελών την Επεξεργασία στο αρχείο δραστηριοτήτων (Data Mapping) «GDPR-08 Αρχείο Δραστηριοτήτων» καθορίζει το χρόνο διατήρησης των δεδομένων

3.3. Πολιτική Πρόσβασης Υποκειμένου στα Δεδομένα του

ΟΝΟΜΑΣΙΑ Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.03: ΠΡΟΣΒΑΣΗ ΥΠΟΚΕΙΜΕΝΟΥ ΣΤΑ ΔΕΔΟΜΕΝΑ ΤΟΥ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός & Αποδέκτες Εγγράφου

Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία (Κανονισμός (ΕΕ) 2016/679, άρθρο 15, § 1).

Το δικαίωμα στην πρόσβαση των δεδομένων του υποκειμένου, δίνει την δυνατότητα στα άτομα να αποκτήσουν ένα αντίγραφο των προσωπικών τους δεδομένων, καθώς και άλλες συμπληρωματικές πληροφορίες. Επίσης, βοηθάει τα άτομα να κατανοήσουν, πως και για ποιο λόγο χρησιμοποιούνται τα δεδομένα τους και να ελέγξουν αν αυτό γίνεται σύμφωνα με την νομοθεσία.

Μια Αίτηση Πρόσβασης στα προσωπικά δεδομένα του υποκειμένου, πρέπει να γίνει γραπτώς. Σε γενικές γραμμές, οι προφορικές αιτήσεις για πληροφορίες σχετικά με ένα άτομο δεν είναι έγκυρες.

Σε περίπτωση που ένα επίσημο αίτημα γίνεται προφορικά, σε μέλος του προσωπικού του Οργανισμού, θα πρέπει να ζητηθεί περαιτέρω καθοδήγηση από τον υπεύθυνο προστασίας προσωπικών δεδομένων, ο οποίος θα εξετάσει και θα εγκρίνει τις αιτήσεις.

Μία αίτηση για πρόσβαση στα προσωπικά δεδομένα μπορεί να γίνει με ηλεκτρονικό ταχυδρομείο, φαξ, ταχυδρομείο, εταιρική ιστοσελίδα ή οποιαδήποτε άλλη μέθοδο.

Διεργασίες

Πληροφορίες στις οποίες μπορεί να έχει πρόσβαση το υποκείμενο

Οι πληροφορίες στις οποίες μπορεί να ζητήσει πρόσβαση το υποκείμενο των δεδομένων, αναφέρονται παρακάτω:

α) τους σκοπούς της επεξεργασίας,

β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα

γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινοποιήθηκαν ή πρόκειται να κοινοποιηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα διατηρηθούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

ε) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

στ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,

ζ) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

η) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος εναντίωσης στην εν λόγω επεξεργασία.

Το δικαίωμα διαγραφής μπορεί να ικανοποιηθεί:

- Εάν τα δεδομένα δεν είναι πλέον απαραίτητα για τους σκοπούς που συλλέχθηκαν,
- Εάν υπάρχει άλλη νομική βάση για επεξεργασία πέραν της συγκατάθεσης,
- Εάν ασκηθεί το δικαίωμα εναντίωσης
- Εάν τα δεδομένα υποβλήθηκαν σε επεξεργασία αντίθετη στις ισχύουσες νομοθετικές διατάξεις,
- Εάν τα δεδομένα πρέπει να διαγραφούν ώστε να τηρηθεί νομική υποχρέωση,

Η ανάκληση της συγκατάθεσης του υποκειμένου μπορεί κατά περίπτωση να συνεπάγεται την άμεση διακοπή της παροχής των υπηρεσιών μας, στην περίπτωση που αυτή αποτελεί τη νομική βάση για την επεξεργασία των προσωπικών σας δεδομένων.

Επαλήθευση Ταυτότητας Υποκειμένου

Το μέλος του προσωπικού του Οργανισμού, ή ο υπεύθυνος ασφάλειας πληροφοριών (ΥΑΠ) που θα έρθει σε επαφή, πρέπει να ελέγξει την ταυτότητα κάθε υποκειμένου που κάνει μια αίτηση πρόσβασης, για να εξασφαλίσει ότι οι πληροφορίες δίνονται μόνο στο πρόσωπο που τις δικαιούται. Εάν η ταυτότητα του αιτούντος δεν έχει ήδη παρασχεθεί, το πρόσωπο που λαμβάνει την αίτηση θα πρέπει να επιβεβαιώσει την ταυτοπροσωπία.

Εάν ο αιτών δεν είναι το υποκείμενο των δεδομένων, απαιτείται γραπτή εξουσιοδότηση, που του παρέχει το δικαίωμα να ενεργεί εξ ονόματος και για λογαριασμό του υποκειμένου των δεδομένων.

Άρνηση Απάντησης σε Αιτήματα

Υπάρχουν περιπτώσεις στις οποίες τα υποκείμενα των δεδομένων, δεν έχουν το δικαίωμα πρόσβασης στα προσωπικά τους δεδομένα. Για παράδειγμα:

- Εάν τα δεδομένα φυλάσσονται μόνο για σκοπούς στατιστικής ή έρευνας και τα αποτελέσματα του στατιστικού έργου ή της έρευνας δεν διατίθενται με μορφή που να προσδιορίζει κάποιο από τα άτομα.

- Αιτήσεις που υποβάλλονται για άλλους σκοπούς, που δεν αφορούν προστασία δεδομένων, μπορούν να απορριφθούν.

Διατηρούμε το δικαίωμα άρνησης ικανοποίησης των δικαιωμάτων του υποκειμένου εάν η επεξεργασία των δεδομένων είναι απαραίτητη για την τήρηση νομικής μας υποχρέωσης, για λόγους δημοσίου συμφέροντος ή για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων (άρθρο 17 §3)

Ο οργανισμός θα εξετάσει το αίτημα του υποκειμένου και θα απαντήσει εντός ενός μηνός από την παραλαβή του αιτήματος είτε για την ικανοποίησή του είτε για τους αντικειμενικούς λόγους που εμποδίζουν την ικανοποίησή του ή λαμβανομένης υπ' όψη της πολυπλοκότητας του αιτήματος και του αριθμού των αιτημάτων, εντός προθεσμίας δύο μηνών (άρθρο 12 §3).

Η άσκηση των ανωτέρω δικαιωμάτων πραγματοποιείται χωρίς κόστος για το υποκείμενο, με την αποστολή σχετικής αίτησης / επιστολής / email στον Υπεύθυνο Επεξεργασίας Δεδομένων. Η καταχρηστική άσκηση των παραπάνω δικαιωμάτων (άρθρο 12 §5) μπορεί να επιβάλει την καταβολή εύλογου τέλους.

Σε περίπτωση που ο Υπεύθυνος Ασφάλειας Πληροφοριών ή ο DPO, αρνείται να ικανοποιήσει την αίτηση πρόσβασης στα δεδομένα για λογαριασμό του Οργανισμού, οι λόγοι απόρριψης πρέπει να αναφέρονται γραπτώς. Κάθε άτομο που δεν ικανοποιείται με το αποτέλεσμα της Αίτησης, έχει το δικαίωμα να υποβάλει αίτημα στη Διοίκηση ως Υπεύθυνο Επεξεργασίας αίτημα για να εξετάσει το αποτέλεσμα.

Αρχεία και Δεδομένα

- Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί το αρχείο, «**Πρόσβαση Υποκειμένων στα Δεδομένα τους**». Στο αρχείο φυλάσσεται τα Έντυπα:

→ ΕΝΤΥΠΟ **E.GDPR.03.01** Αίτηση πρόσβασης στην επεξεργασία προσωπικών δεδομένων. Η διάρκεια τήρησης του αρχείου είναι απεριόριστη

3.3.1 Έντυπο «Αίτηση πρόσβασης στην επεξεργασία προσωπικών δεδομένων»

<table>
<tr><td>Κοι.Σ.Π.Ε.....

LOGO</td><td colspan="2">ΕΝΤΥΠΟ Ε.GDPR.03.01: «ΑΙΤΗΣΗ ΠΡΟΣΒΑΣΗΣ ΣΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»</td></tr>
<tr><td>Ονοματεπώνυμο Υποκειμένου</td><td colspan="2">Ημερομηνία Γέννησης Υποκειμένου</td></tr>
<tr><td colspan="2">Διεύθυνση Κατοικίας Υποκειμένου</td><td>ΑΔΤ:</td></tr>
<tr><td>Κινητό Τηλέφωνο Υποκειμένου</td><td colspan="2">Σταθερό Τηλέφωνο Υποκειμένου</td></tr>
<tr><td></td><td colspan="2"></td></tr>
<tr><td colspan="3">Email Υποκειμένου:</td></tr>
<tr><td colspan="3">Παρακαλώ σημειώσατε την ενέργεια που ενδιαφέρεστε να πραγματοποιήσετε:
1. Πρόσβαση: ΝΑΙ □ ΟΧΙ □ 5.Περιορισμού της επεξεργασίας: ΝΑΙ □ ΟΧΙ □
2. Διόρθωση: ΝΑΙ □ ΟΧΙ □ 6. Φορητότητα δεδομένων: ΝΑΙ □ ΟΧΙ □
3. Διαγραφή: ΝΑΙ □ ΟΧΙ □ 7.Εναντίωση: ΝΑΙ □ ΟΧΙ □
4. Λήψη αντιγράφου: ΝΑΙ □ ΟΧΙ □</td></tr>
<tr><td colspan="3">Παρακαλώ αναφέρατε τους λόγους για τους οποίους πραγματοποιείτε το παραπάνω αίτημα:</td></tr>
<tr><td colspan="3">Σε περίπτωση που επιλέξατε να διορθώσετε τα στοιχεία σας, παρακαλώ αναφέρατε τις διορθώσεις που επιθυμείτε να γίνουν:</td></tr>
<tr><td colspan="3">Σε περίπτωση που θέλετε να διαγράψετε δεδομένα, η αίτηση αφορά σε:
Όλα τα δεδομένα □ Ευαίσθητα δεδομένα μόνο □
Άλλο □ (Εάν επιλεγεί, παρακαλώ προσδιορίστε μας όσο το δυνατόν ακριβέστερα τα δεδομένα που επιθυμείτε να διαγραφούν)</td></tr>
<tr><td colspan="3">Τα προσωπικά δεδομένα θα αποσταλούν στο Υποκείμενο ή σε κάποιο Εξουσιοδοτημένο Πρόσωπο;
Στο Υποκείμενο □ Σε εξουσιοδοτημένο πρόσωπο □
(Εάν τα δεδομένα σταλούν σε εξουσιοδοτημένο πρόσωπο, πρέπει να συμπληρωθούν τα ακόλουθα Α και Β στην πίσω σελίδα).</td></tr>
</table>

/0/2022 ΕΚΔΟΣΗ: 1η Σελίδα 2 από 169

Υπογραφή Υποκειμένου _____

Όνομα Υποκειμένου (Ολογράφως) _____
Ημερομηνία _____

Α. Το Υποκείμενο, οφείλει να παρέχει γραπτή εξουσιοδότηση ώστε να αποδοθούν τα δεδομένα της αίτησης στον εκπρόσωπο που έχει ορίσει.

Με το παρόν, εξουσιοδοτώ τον/την _____(συμπληρώστε το όνομα του εκπροσώπου) με Αριθμό Δελτίου Ταυτότητας _____να αιτηθεί εκ μέρους μου επεξεργασία των προσωπικών μου δεδομένων.

Υπογραφή Υποκειμένου _____
Όνομα Υποκειμένου (Ολογράφως) _____

Β. Ο εκπρόσωπος οφείλει να παρέχει γραπτώς τα στοιχεία του ώστε να του αποδοθούν τα δεδομένα της αίτησης που υποβάλλει εκ μέρους του Υποκειμένου.

Ονοματεπώνυμο του εξουσιοδοτημένου προσώπου και διεύθυνση αποστολής των στοιχείων (email ή fax ή ταχυδρομική διεύθυνση – όπου επιπλέον χρεώσεις μπορεί να υπάρξουν)

_____

_____

Υπογραφή Εξουσιοδοτημένου Προσώπου _____
Όνομα Εξουσιοδοτημένου Προσώπου (Ολογράφως) _____
Ημερομηνία _____

Ο οργανισμός θα καταβάλει κάθε προσπάθεια ώστε η αίτηση που υποβάλατε σχετικά με τα προσωπικά σας δεδομένα να εκτελεστεί το συντομότερο δυνατόν, εντός 30 ημερολογιακών ημερών. Παρόλα αυτά, ενόσω επεξεργαζόμαστε το αίτημά σας μη διστάσετε να επικοινωνήσετε στο info@..... για οποιαδήποτε απορία.

/0/2022 ΕΚΔΟΣΗ: 1η Σελίδα 2 από 169

3.4. Πολιτική Διαχείρισης Παραβίασης Δεδομένων

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.04: ΔΙΑΧΕΙΡΙΣΗ ΠΑΡΑΒΙΑΣΗΣ ΔΕΔΟΜΕΝΩΝ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός

Αυτή η διεργασία έχει σχεδιαστεί για να καθορίσει τη διαδικασία διαχείρισης της παραβίασης δεδομένων, και να εξασφαλιστεί ότι:

- Περιστατικά παραβίασης δεδομένων ανιχνεύονται, αναφέρονται και παρακολουθούνται τακτικά.
- Τα περιστατικά αξιολογούνται και αντιμετωπίζονται κατάλληλα.
- Γίνονται ενέργειες για την μείωση των επιπτώσεων μίας παραβίασης.
- Οι σχετικές παραβιάσεις αναφέρονται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, εντός 72 ωρών.
- Πραγματοποιούνται βελτιώσεις για την αποφυγή επανάληψης όμοιων περιστατικών.
- Η εμπειρία αντιμετώπισης του εν λόγω περιστατικού παραβίασης που αποκτήθηκε διαχέεται ευρύτερα εντός του οργανισμού.

Διεργασία

Διαπίστωση Παραβίασης Προσωπικών Δεδομένων / Υποψία Παραβίασης Προσωπικών Δεδομένων

Η παραβίαση των προσωπικών δεδομένων μπορεί να συμβεί για πολλούς λόγους, όπως για παράδειγμα:

- Απώλεια ή κλοπή δεδομένων ή εξοπλισμού στον οποίο αποθηκεύονται δεδομένα, ή μέσω των οποίων είναι δυνατή η πρόσβαση σε αυτά.
- Απώλεια ή κλοπή φυσικού αρχείου.
- Διαδικτυακές επιθέσεις.
- Ακατάλληλοι έλεγχοι πρόσβασης που επιτρέπουν μη εξουσιοδοτημένη/ άσκοπη πρόσβαση στα δεδομένα.
- Αστοχία εξοπλισμού.
- Λανθασμένος ανθρώπινος χειρισμός.
- Απρόβλεπτες συνθήκες, όπως πυρκαγιά ή πλημμύρα.

Όποιος στον οργανισμό παραλάβει καταγγελία είτε μέσω γραπτής είτε ηλεκτρονικής αλληλογραφίας δημιουργεί φάκελο για την υπόθεση και ενημερώνει αμέσως τη Διοίκηση, τον υπεύθυνο ασφαλείας πληροφοριών και τον Υπεύθυνο Προσωπικών Δεδομένων.

Διερεύνηση Περιστατικού

Ανάλογα με το είδος και την σοβαρότητα του περιστατικού, ο οργανισμός θα αξιολογήσει εάν απαιτείται πλήρης διερεύνηση της παραβίασης ή της τυχόν παραβίασης. Όπου απαιτείται, ο οργανισμός θα ορίσει μια κατάλληλη ομάδα έρευνας η οποία θα συντάξει μια πλήρη έκθεση παραβίασης.

Η έρευνα αυτή θα:

α) Καθορίσει την φύση του περιστατικού, τον τύπο και την ένταση των δεδομένων που περιλαμβάνονται και την ταυτότητα των υποκειμένων στα οποία αφορούν τα δεδομένα.

β) Εξετάσει την έκταση της παραβίασης και την ευαισθησία των δεδομένων που αφορά η παραβίαση.

γ) Εκτελέσει μια διαδικασία αξιολόγησης κινδύνου.

δ) Προσδιορίσει τις ενέργειες που πρέπει να εκτελέσει ο Οργανισμός για να περιορίσει την παραβίαση και να ανακτήσει τα δεδομένα που παραβιάσθηκαν.

ε) Αξιολογήσει τον συνεχιζόμενο κίνδυνο και τις απαιτούμενες ενέργειες για την αποτροπή επανάληψης του περιστατικού.

Στην περίπτωση αυτή μπορεί να εκ κινηθεί η διαδικασία «Διορθωτικές Ενέργειες – Προτάσεις Βελτίωσης»

Συντάσσεται δε με ευθύνη του Νομικού Συμβούλου η προβλεπόμενη απάντηση στην αρχή/ φορέα/πελάτη/Υπεύθυνο Επεξεργασίας, λαμβάνοντας υπόψη τα οποιαδήποτε ενδεχομένως χρονικά περιθώρια τίθενται. Σε περίπτωση κλιμάκωσης του θέματος ο χειρισμός συντονίζεται από τον Νομικό Σύμβουλο.

Αναφορά Περιστατικού

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, Είναι ζωτικής σημασίας ότι μόλις εντοπιστεί ή υπάρξει υποψία παραβίασης προσωπικών δεδομένων, ο οργανισμός αναφέρει το περιστατικό αυτό άμεσα στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και το αργότερο εντός 72 ωρών από τη στιγμή που ο οργανισμός αποκτήσει γνώση του γεγονότος, εκτός αν η παραβίαση δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

Προκειμένου να βελτιώσει την κατανόηση των κινδύνων για τα δεδομένα και να τα αντιμετωπίσει πριν συμβεί κάποια παραβίαση, ο ργανισμός, ενθαρρύνει τα άτομα να αναφέρουν αποσοβηθείσες παραβιάσεις (π.χ. περιστατικά που έχουν σχεδόν οδηγήσει σε παραβίαση δεδομένων, και απετράπησαν είτε από επιτυχημένη παρέμβαση είτε από «τύχη»).

Οι αποσοβηθείσες παραβιάσεις αναφέρονται, με την ίδια μορφή και διαδικασία που δομούνται και αναφέρονται οι πραγματικές παραβιάσεις και επισημαίνεται με σαφήνεια ότι το περιστατικό αποτελεί μία αποσοβηθείσα παραβίαση.

Το σύνολο των πληροφοριών που είναι άμεσα διαθέσιμες, πρέπει να συγκεντρωθούν, με σκοπό να συμπληρωθεί η Γνωστοποίηση Περιστατικών Παραβίασης Δεδομένων και να ταχυδρομηθούν ηλεκτρονικά στο **databreach@dpa.gr το συντομότερο δυνατό και μέσα σε 72 ώρες από τη στιγμή που ο οργανισμός θα λάβει γνώση της σχετικής παραβίασης και της αναγνώρισής της**. Η γνωστοποίηση κατ' ελάχιστο:

α) περιγράφει τη φύση της παραβίασης δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα,

β) ανακοινώνει το όνομα και τα στοιχεία επικοινωνίας της Διοίκησης ή άλλου σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες,

γ) περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα,

δ) περιγράφει τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Σε περίπτωση που και εφόσον δεν είναι δυνατόν να παρασχεθούν οι πληροφορίες ταυτόχρονα, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, η Διοίκηση του οργανισμού ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στα υποκείμενα.

Στην ανακοίνωση αυτή περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρθηκαν και στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Δεν απαιτείται ανακοίνωση εάν:

α) ο οργανισμός εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση δεδομένα προσωπικού χαρακτήρα, κυρίως μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση,

β) ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων,

γ) προϋποθέτει δυσανάλογες προσπάθειες. Στην περίπτωση αυτή, γίνεται αντ' αυτής δημόσια ανακοίνωση ή υπάρχει παρόμοιο μέτρο με το οποίο τα υποκείμενα των δεδομένων ενημερώνονται με εξίσου αποτελεσματικό τρόπο.

Οποιαδήποτε αναφορά συνταχθεί θα πρέπει να γίνει με την υποστήριξη και από άλλες ομάδες του οργανισμού συμπεριλαμβανομένων της ομάδας Marketing, των Δημοσίων Σχέσεων και Επικοινωνιών αλλά και του Υπεύθυνου Ασφάλειας Πληροφοριών ή του Υπευθύνου Προστασίας

Δεδομένων (εάν έχει οριστεί). Η αναφορά θα πρέπει να είναι διαθέσιμη στο υποκείμενο κατόπιν αιτήματός του.

Γνωστοποίηση Παραβίασης

Επισκόπηση αρχείου περιστατικών ασφάλειας

Ο Υπεύθυνος Ασφάλειας Πληροφοριών εξετάζει σε τακτά χρονικά διαστήματα, όχι μεγαλύτερα από 6 μήνες, το Αρχείο με τα Περιστατικά παραβίασης που έχουν καταγραφεί από τα στελέχη ή τους συνεργάτες του οργανισμού. Σε περίπτωση διαπιστωθεί η εμφάνιση πολλών αντίστοιχων ή ομοειδών περιστατικών, καταγράφει το γεγονός αυτό σε σχετική αναφορά την οποία προωθεί στη Διοίκηση του οργανισμού, μαζί με τις προτάσεις του για τη λήψη πρόσθετων μέτρων ασφάλειας, και μπορεί να εκκινήσει τη διαδικασία «Διορθωτικές Ενέργειες – Προτάσεις Βελτίωσης»

Η Διοίκηση του οργανισμού αξιολογεί τις προτάσεις, κατά την τακτική ή έκτακτη συνεδρίασή της για την ανασκόπηση της πολιτικής ασφάλειας προσωπικών δεδομένων, και αποφασίζει για τα πρόσθετα μέτρα ασφάλειας που πρέπει να ληφθούν.

Η λήψη πρόσθετων μέτρων ασφάλειας ξεκινά ένα νέο κύκλο αναθεώρησης της Πολιτικής Ασφάλειας του οργανισμού.

Κυρώσεις

Σε περίπτωση που η Διοίκηση του οργανισμού αποφασίσει να κινηθεί νομικά ή να επιβάλει κάποιου είδους κυρώσεις στον υπεύθυνο για την εκδήλωση ενός περιστατικού παραβίασης, ο οργανισμός ακολουθεί τις παρακάτω αρχές:

- Ο οργανισμός, μέσω της εσωτερικής του οργάνωσης για την προστασία των προσωπικών του δεδομένων ή/και με τη συμβολή εξωτερικών συνεργατών διερευνά τα αίτια εκδήλωσης του περιστατικού παραβίασης και επιχειρεί να το τεκμηριώσει κατά το δυνατό πληρέστερα. Στην τεκμηρίωση του περιστατικού περιλαμβάνονται απαραίτητα και αποδεικτικά στοιχεία που αποδίδουν την ευθύνη για την εκδήλωσή του σε κάποιο φυσικό ή νομικό πρόσωπο.
- Η αναλυτική τεκμηρίωση του περιστατικού παραβίασης, μαζί με τα αποδεικτικά στοιχεία, παραδίδονται στους νομικούς συμβούλους/συνεργάτες του οργανισμού.
- Οι νομικοί συνεργάτες του οργανισμού αναλαμβάνουν να κινήσουν τις όποιες νομικές διαδικασίες επιβολής κυρώσεων στον υπεύθυνο εκδήλωσης του περιστατικού, απαιτώντας πιθανώς σχετική αποζημίωση για τη ζημία που προκλήθηκε στον οργανισμό. Όλες οι ενέργειες των νομικών συνεργατών του οργανισμού τελούν υπό την έγκριση της Διοίκησης του οργανισμού.

Αρχεία και Δεδομένα

- Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί το αρχείο, «**Περιστατικά Παραβίασης ή τυχόν Παραβίασης**» όπου τηρούνται οι εκθέσεις των περιστατικών ή τυχόν περιστατικών.

→ ΕΝΤΥΠΟ **E.GDPR.04.01** Αναφορά Περιστατικού / Αδυναμία Ασφάλειας
→ ΕΝΤΥΠΟ **E.GDPR.04.02** Αρχείο Περιστατικών / Αδυναμιών Ασφαλείας

Η διάρκεια τήρησης του αρχείου είναι αόριστη

3.4.1 Έντυπο «Αναφορά Περιστατικού / Αδυναμία Ασφάλειας»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ E.GDPR.04.01: «ΑΝΑΦΟΡΑ ΠΕΡΙΣΤΑΤΙΚΟΥ / ΑΔΥΝΑΜΙΑ ΑΣΦΑΛΕΙΑΣ»**
Στοιχεία στελέχους	
Επώνυμο	
Όνομα	
Θέση στην εταιρεία	
Τηλέφωνο	
Στοιχεία περιστατικού/ αδυναμίας ασφάλειας	
Ημερομηνία	
Ώρα	
Θέμα	
Τύπος	☐ Περιστατικό ασφάλειας ☐ Αδυναμία ασφάλειας
Περιγραφή περιστατικού/ αδυναμίας ασφάλειας	
<Συμπληρώνονται στοιχεία για το περιστατικό (π.χ. συστήματα/ πληροφορία/ πόρους που αφορούσε) και τις επιπτώσεις/ προβλήματα που προκάλεσε>	
Τεκμηρίωση περιστατικού/ αδυναμίας ασφάλειας	
<Παρατίθενται στοιχεία που αποδεικνύουν την πραγματοποίηση του περιστατικού ή/και τις συνέπειές του (εάν υπάρχουν). Αντίστοιχα παρατίθενται στοιχεία για τους κινδύνους που ενδέχεται να εκμεταλλευτούν την αδυναμία ασφάλειας και τις εκτιμώμενες συνέπειές τους.>	

Ονοματεπώνυμο & υπογραφή στελέχους: Ημερομηνία:

Ευρωπαϊκή Ένωση
Επιχειρησιακό Πρόγραμμα
ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020

3.4.2 Έντυπο «Αρχείο Περιστατικών / Αδυναμιών Ασφάλειας»

Α/Α	Ημερομηνία περιστατικού	Ημερομηνία αναφοράς	Σύντομη περιγραφή	Τύπος/ Κατηγορία	Σπουδαιότητα	Ενέργειες επίλυσης	Ημερομηνία επίλυσης	Παρατηρήσεις/ προτάσεις
1.								
2.								
3.								
4.								

3.5 Πολιτική Διαχείρισης Βιογραφικών

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.05: ΔΙΑΧΕΙΡΙΣΗ ΒΙΟΓΡΑΦΙΚΩΝ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός

Σκοπός της διαδικασίας είναι να περιγραφεί ο τρόπος με τον οποίο ο οργανισμός διαχειρίζεται τα βιογραφικά που λαμβάνει από υποψήφιους εργαζόμενους. Τα βιογραφικά σημειώματα περιλαμβάνουν πλήθος προσωπικών δεδομένων και ο οργανισμός τα διαχειρίζεται με ιδιαίτερη προσοχή, λαμβάνοντας όλα τα τεχνικά και οργανωτικά μέτρα για την ασφαλή επεξεργασία και φύλαξή τους.

Διεργασία

Ο οργανισμός δημοσιεύει αγγελίες με τις διαθέσιμες θέσεις εργασίας σε εξειδικευμένους διαδικτυακούς τόπους ανεύρεσης εργασίας, στην ιστοσελίδα της, σε εφημερίδες και σε κάθε πρόσφορο μέσο.

Ο οργανισμός ζητά από τους υποψηφίους εργαζομένους να ενημερώνονται για την πολιτική χειρισμού των προσωπικών τους δεδομένων μέσω του Εντύπου *E.GDPR.05.01 Κείμενο πληροφόρησης υποψηφίων εργαζομένων*, το οποίο είτε δημοσιεύει στο site της είτε αποστέλλει στη Δ/νση Email που οι υποψήφιοι σημειώνουν στο βιογραφικό τους σημείωμα.

Τα βιογραφικά σημειώματα λαμβάνονται σε μια συγκεκριμένη ηλεκτρονική διεύθυνση την οποία διαχειρίζονται ένα ή δύο στελέχη του οργανισμού το πολύ. Σε κάθε υποψήφιο που αποστέλλει βιογραφικό σημείωμα, ο οργανισμός απαντά με προτυποποιημένο κείμενο όπου αναφέρονται κατ' ελάχιστον:

- Τα δικαιώματα του υποψήφιου
- Τα μέτρα ασφάλειας που λαμβάνονται για την προστασία των προσωπικών δεδομένων
- Ο χρόνος τήρησης του βιογραφικού
- Ο τρόπος επικοινωνίας
- Το δικαίωμα υποβολής στον υπεύθυνο επεξεργασίας αίτηση για πρόσβαση, διόρθωση, διαγραφή, περιορισμό, εναντίωση, φορητότητα

Στη συνέχεια τα βιογραφικά σημειώματα αποθηκεύονται στον server του οργανισμού σε σημείο με περιορισμένα δικαιώματα πρόσβασης.

Πρόσβαση στα βιογραφικά σημειώματα έχουν μόνο τα στελέχη της εταιρείας που είναι αρμόδια για την αξιολόγησή τους και την επιλογή του κατάλληλου υποψήφιου.

Το στέλεχος που κάνει την επικοινωνία με τους υποψήφιους, εάν δεν είναι ένα από τα στελέχη του οργανισμού που έχει αποφασιστεί να έχουν πρόσβαση στα βιογραφικά, λαμβάνει μόνο το ονοματεπώνυμο και το τηλέφωνο του υποψήφιου, τα οποία μετά την ολοκλήρωση της επικοινωνίας διαγράφει / καταστρέφει.

Σε περίπτωση που κάποιος υποψήφιος εργαζόμενος αποστείλει βιογραφικό σημείωμα σε άλλο e-mail, το στέλεχος προωθεί το βιογραφικό του στο αρμόδιο προσωπικό και διαγράφει το μήνυμα από τον λογαριασμό ηλεκτρονικού ταχυδρομείου που αρχικά είχε αποσταλεί.

Σε περίπτωση αποστολής βιογραφικού σε έντυπη μορφή, το βιογραφικό καταχωρείται σε κλασέρ σε ερμάριο που κλειδώνει στο χώρο του λογιστηρίου. Και στην περίπτωση των εντύπων, εφαρμόζονται αντίστοιχα τεχνικά και οργανωτικά μέσα, με αυτά που εφαρμόζονται στα βιογραφικά που λαμβάνονται σε ηλεκτρονική μορφή (ενημέρωση του αποστολέα με e-mail ή με τηλεφώνημα, ασφαλής τήρηση κ.λπ.)

Τα Προσωπικά δεδομένα των υποψηφίων εργαζομένων μπορεί να περιλαμβάνουν ενδεικτικά:

Α. Κατά τη διάρκεια της φάσης επιλογής:

- Πληροφορίες που παρέχονται από τον υποψήφιο κι επιτρέπουν την αναγνώριση του υποψήφιου (τίτλος, επώνυμο, όνομα, ημερομηνία και τόπος γέννησης)
- Πληροφορίες που παρέχονται από τον υποψήφιο και αφορούν στοιχεία επικοινωνίας του (διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμός τηλεφώνου, αριθμός κινητού τηλεφώνου, αριθμός φαξ, ταχυδρομική διεύθυνση, χώρα διαμονής, διεύθυνση διαδικτύου).
- Πληροφορίες που παρέχονται από τον υποψήφιο κι έχουν σκοπό την επαλήθευση της συνδρομής των προϋποθέσεων που καθορίζονται στην προκήρυξη της θέσης (αποδεικτικά εκπαίδευσης και κατάρτισης, τίτλοι σπουδών, αποδεικτικά επαγγελματικής πείρας, που περιέχουν πληροφορίες σχετικά με τον τύπο της εργασίας που παρασχέθηκε, τη διάρκεια, τον τύπο της εργασίας, τα καθήκοντα του υποκειμένου των δεδομένων και τις ευθύνες του στην προηγούμενη εργασία, αποδεικτικά γνώσης ξένων γλωσσών, καθώς και δεξιοτήτων που σχετίζονται με τη θέση που έχει προκηρυχθεί).
- Βιογραφικό σημείωμα

Β. Κατά τη φάση πρόσληψης και μετά την πρόσληψη μπορεί να ζητηθούν τα παρακάτω (κατά περίπτωση):

- Διπλώματα, πτυχία, πιστοποιητικά αναφορικά με σπουδές ή κατάρτιση
- Αποδεικτικά προϋπηρεσίας
- Συμβάσεις με προηγούμενους εργοδότες και περιγραφές θέσεων εργασίας
- Πιστοποιητικό ιατρικής επάρκειας
- Ποινικό μητρώο
- Πιστοποιητικό περί εκπληρώσεων στρατολογικών υποχρεώσεων
- Πιστοποιητικό γέννησης

- Πιστοποιητικά που αποδεικνύουν εθνικότητα
- Πιστοποιητικά που αποδεικνύουν οικογενειακή κατάσταση
- Πιστοποιητικό που αποδεικνύει τόπο κατοικίας
- Πιστοποιητικό γέννησης τέκνων
- Δικαστική απόφαση περί λύσεως του γάμου
- Απόφαση διατροφής
- Τραπεζικές πληροφορίες (κωδικοί IBAN και BIC)
- Φορολογικά στοιχεία ΑΦΜ κλπ.

Δεδομένου ότι οι πληροφορίες και τα δεδομένα περιέχονται συχνά σε βιογραφικό σημείωμα, οι υποψήφιοι ενδέχεται να αποκαλύπτουν πρόσθετες πληροφορίες που δεν είναι απαραίτητες για τους σκοπούς της προκήρυξης.

Αρχεία

Ο Υπεύθυνος Προσωπικού τηρεί τα βιογραφικά σημειώματα για όσο χρόνο αναγράφεται στο αρχείο δραστηριοτήτων (Data Mapping).

3.5.1 Έντυπο «Κείμενο Πληροφόρησης Υποψηφίων Εργαζομένων»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ E.GDPR.05.01: «Κείμενο πληροφόρησης υποψηφίων εργαζομένων»**

Τα προσωπικά δεδομένα του βιογραφικού σας σημειώματος που κοινοποιείτε στον Οργανισμό με την επωνυμία «.....» και τον διακριτικό τίτλο «.....» (στο εξής: «οργανισμός» ή «.....»), με έδρα στην ....., ... Αττικής, με τηλέφωνο επικοινωνίας: 210 ....., και e-mail: info@..... θα χρησιμοποιηθούν αποκλειστικά για τον σκοπό ανεύρεσης προσωπικού. Τονίζεται ότι η παροχή των ανωτέρω δεδομένων προσωπικού χαρακτήρα, κρίνεται απαραίτητη για την ολοκλήρωση του ανωτέρω σκοπού, ενώ η νομική βάση στην οποία βασίζεται η εν λόγω επεξεργασία είναι η εκτέλεση σύμβασης και συγκεκριμένα οι ενέργειες κατά το προσυμβατικό στάδιο αυτής (αρ. 6.1β του Γενικού Κανονισμού για την Προστασία Δεδομένων, Κανονισμός [ΕΕ] 2016/679).

Ενημερώνουμε πως για τη χρήση των εν λόγω προσωπικών δεδομένων αποδέκτες θα είναι μόνο το απολύτως απαραίτητο προσωπικό του οργανισμού. Δεσμευόμαστε ότι έχουμε λάβει κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια και την προστασία των δεδομένων σας από κάθε μορφής τυχαία ή αθέμιτη επεξεργασία.

Τα προσωπικά σας δεδομένα αποτελούν αντικείμενο επεξεργασίας μόνο εντός Ελλάδας και ως εκ τούτου δεν διαβιβάζονται σε χώρες εκτός ΕΟΧ. Τα προσωπικά σας δεδομένα θα διαγράφονται μετά από .....

Έχετε δικαίωμα να μας υποβάλετε αίτημα πρόσβασης στα προσωπικά σας δεδομένα, διόρθωσης ανακριβών δεδομένων προσωπικού χαρακτήρα, διαγραφής/ δικαίωμα στη λήθη, φορητότητας των προσωπικών σας δεδομένων και περιορισμού της επεξεργασίας Εάν επιθυμείτε να επικοινωνήσετε για κάθε ζήτημα σχετικό με την επεξεργασία των προσωπικών σας δεδομένων και την άσκηση των δικαιωμάτων σας, μπορείτε να απευθύνεστε στο τηλέφωνο ..... ή στην Δ/νση ..... ή στην δ/νση ηλεκτρονικού ταχυδρομείου .....

Η απάντησή μας στο αίτημά σας θα λάβει χώρα εντός (1) ενός μηνός από τη λήψη του και δε συνεπάγεται κανένα κόστος για εσάς. Η ανωτέρω προθεσμία μπορεί να παραταθεί για χρονικό διάστημα δύο (2) επιπλέον μηνών, λόγω της πολυπλοκότητας ή του αριθμού των αιτημάτων, περίπτωση κατά την οποία θα ενημερωθείτε για την παράταση και τους λόγους αυτής το ταχύτερο δυνατό και το αργότερο εντός μήνα από την παραλαβή του αιτήματος.

Τέλος, έχετε το δικαίωμα να υποβάλλετε καταγγελία στην Αρχή Προστασίας Προσωπικών Δεδομένων (www.dpa.gr) σε περίπτωση που θεωρήσετε ότι η επεξεργασία των προσωπικών σας δεδομένων παραβιάζει τον ισχύον δίκαιο για την προστασία των προσωπικών δεδομένων.

☐ Διάβασα τους ανωτέρω όρους για τη χρήση των προσωπικών μου δεδομένων τους οποίους και κατανοώ.

3.6 Πολιτική Διαχείρισης Συγκατάθεσης Επεξεργασίας Προσωπικών Δεδομένων

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.06: ΑΝΑΚΛΗΣΗ ΣΥΓΚΑΤΑΘΕΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΔ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός

Η διαδικασία αυτή αφορά στο υποκείμενο των δεδομένων που έχει δικαίωμα να ανακαλέσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων.

Η ανάκληση συγκατάθεσης δεν επηρεάζει τη νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση κι έχει πραγματοποιηθεί πριν από την ανάκλησή της.

ΣΗΜΕΙΩΣΗ: Το άρθρο 7 του GDPR σχετικά με τη συγκατάθεση αναφέρει ότι το υποκείμενο των δεδομένων ενημερώνεται πριν από την παροχή της συγκατάθεσής του για το δικαίωμα ανάκλησης της συγκατάθεσής του οποτεδήποτε. Η ανάκληση της συγκατάθεσης δεν θίγει τη νομιμότητα της επεξεργασίας βάσει συγκατάθεσης που βασίστηκε στη συγκατάθεση και πραγματοποιήθηκε πριν από την ανάκλησή της. Η ανάκληση της συγκατάθεσης θα πρέπει να είναι εξίσου εύκολη με την αρχική παροχή της. Η αιτιολογική σκέψη 42 του Κανονισμού GDPR ορίζει ότι η συγκατάθεση δεν πρέπει να θεωρείται ότι χορηγήθηκε ελεύθερα εάν το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συναίνεση χωρίς να ζημιωθεί.

Το δικαίωμα του υποκειμένου των προσωπικών δεδομένων στη λήθη, ισχύει όταν το υποκείμενο των δεδομένων έχει αποσύρει τη συγκατάθεσή του και δεν ισχύουν άλλες προϋποθέσεις νόμιμης επεξεργασίας.

Ευθύνες

Υπεύθυνος Επεξεργασίας

Ως υπεύθυνη επεξεργασίας δεδομένων, του οργανισμού, ευθύνεται βάσει του GDPR για τη διαχείριση της ανάκλησης συγκατάθεσης από το υποκείμενο των δεδομένων βάσει συμβουλών από τον υπεύθυνο προστασίας δεδομένων.**Διαδικασίες**

Ανάκληση συγκατάθεσης για επεξεργασία προσωπικών δεδομένων

Το υποκείμενο των δεδομένων ανακαλεί τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων, συμπληρώνοντας το έντυπο E.GDPR.06.01 «Ανάκληση συγκατάθεσης επεξεργασίας προσωπικών δεδομένων».

Ανάκληση συγκατάθεσης για επεξεργασία προσωπικών δεδομένων για πολλούς σκοπούς. Όταν η επεξεργασία έχει πολλαπλούς σκοπούς, η ανάκληση της συγκατάθεσης πρέπει να γίνει διακριτά για κάθε σκοπό που επιθυμεί το υποκείμενο, όπως καταγράφεται στο έντυπο ανάκλησης συγκατάθεσης επεξεργασίας προσωπικών δεδομένων.

Διακοπή δραστηριοτήτων που βασίζονται στη συγκατάθεση

Οι δραστηριότητες επεξεργασίας που βασίζονται στη συγκατάθεση διακόπτονται σύμφωνα με τη σχετική διαδικασία όπου λαμβάνει χώρα η επεξεργασία. Ο Υπεύθυνος Προστασίας Δεδομένων θα ενημερώσει τον υπεύθυνο επεξεργασίας σχετικά με αυτήν την αλλαγή, ώστε να μπορεί να διακοπεί η επεξεργασία.

Ανάκληση γονικής συγκατάθεσης

Ταυτοποίηση γονικής μέριμνας

Ο οργανισμός λαμβάνει μέτρα για την ταυτοποίηση του ασκούντος τη γονική μέριμνα συγκεκριμένου παιδιού για λογαριασμό και στο όνομα του οποίου εκείνος απέσυρε τη συγκατάθεση.

Διακοπή δραστηριοτήτων βασισμένων στην συγκατάθεση

Οι δραστηριότητες επεξεργασίας που βασίζονται στη συγκατάθεση διακόπτονται σύμφωνα με την παρούσα διαδικασία.

Αρχεία και Δεδομένα

- Ο Υπεύθυνος εκτέλεσης κάθε δραστηριότητας τηρεί το αρχείο, «**Ανακλήσεις Συγκατάθεσης**» όπου τηρούνται τα σχετικά έντυπα ανάκλησης συγκατάθεσης. Η διάρκεια τήρησης του αρχείου είναι αόριστη.

3.6.1 Έντυπο «Αίτηση Ανάκλησης Συγκατάθεσης Επεξεργασίας Προσωπικών Δεδομένων»

/0/2022 ΕΚΔΟΣΗ: 1η Σελίδα 1 από 2

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ E.GDPR.06.01: «ΑΙΤΗΣΗ ΑΝΑΚΛΗΣΗΣ ΣΥΓΚΑΤΑΘΕΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»**

Ο/Η _____ (Ονοματεπώνυμο Υποκειμένου) με Αριθμό Δελτίου Ταυτότητας _____δηλώνω υπεύθυνα πως ανακαλώ τη συγκατάθεσή μου όσον αφορά στην επεξεργασία των προσωπικών μου δεδομένων από τον οργανισμό. Ο οργανισμός «ΧΧΧ» δεν έχει πλέον τη συγκατάθεσή μου προκειμένου να επεξεργάζεται τα προσωπικά μου δεδομένα για το σκοπό:

_____

_____

(περιγράψτε το σκοπό για τον οποίο θα χρησιμοποιούνταν τα προσωπικά σας δεδομένα), η οποία είχε προηγουμένως δοθεί).

Υπογραφή Υποκειμένου: _____

Ημερομηνία: _____

Σε περίπτωση που το υποκείμενο είναι ανήλικο, ο γονέας καλείται να συμπληρώσει ως ασκών τη γονική μέριμνα για το εν λόγω υποκείμενο τα κάτωθι:

Υπογραφή Γονέα: _____

Αριθμός Δελτίου Ταυτότητας: _____

Ημερομηνία: _____

Κατάσταση Αιτήματος: ΕΓΚΡΙΝΕΤΑΙ □ ΑΠΟΡΡΙΠΤΕΤΑΙ □

Σε περίπτωση απόρριψης να συμπληρωθεί:

Ο λόγος απόρριψης όπως αυτή κρίθηκε απαραίτητη από τον Υπεύθυνο Προστασίας Δεδομένων του οργανισμού είναι:

_____

_____

Ο Υπεύθυνος: _____

Υπογραφή: _____

Ημερομηνία: _____

□ Εστάλη ενημέρωση στο Υποκείμενο

Ονοματεπώνυμο: _____

Υπογραφή: _____

3.7 Μεθοδολογία Εκτίμησης Αντίκτυπου Προστασίας Δεδομένων

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.07: ΜΕΘΟΔΟΛΟΓΙΑ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΕΑΠΔ)

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Γενικά

Ο ΓΚΠΔ στο άρθρο 35 ορίζει «*Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.*»

Κατά συνέπεια όταν αυτό κρίνεται απαραίτητο, η διενέργεια ΕΑΠΔ είναι νομικά υποχρεωτική. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που είναι απαραίτητο να διαθέτουν ΕΑΠΔ.

Επίσης το άρθρο 25 του ΓΚΠΔ ορίζει ότι, πρέπει να υφίσταται εγκεκριμένος μηχανισμός προστασίας των προσωπικών δεδομένων ήδη από το σχεδιασμό και εξ' ορισμού.

Σκοπός & αποδέκτες του παρόντος εγγράφου

Σκοπός του παρόντος εγγράφου είναι η περιγραφή της μεθοδολογίας διενέργειας Εκτίμησης Αντικτύπου σχετικά με την Προστασία των Δεδομένων (ΕΑΠΔ) που εφαρμόζει ο οργανισμός και ο προσδιορισμός της τιμής του μέγιστου αποδεκτού επιπέδου επικινδυνότητας.

Ο σκοπός της ΕΑΠΔ είναι να επισημάνει στον οργανισμό τους κινδύνους ιδιωτικότητας που σχετίζονται με ένα έργο που βρίσκεται σε εξέλιξη ή πρόκειται να αναληφθεί, ή/και με υφιστάμενες διαδικασίες που εμπεριέχουν επεξεργασία ΠΔ.

Η ΕΑΠΔ μπορεί να αφορά σε περισσότερες από μία διαδικασίες ή έργα στην περίπτωση που η δομή και το περιεχόμενο της επεξεργασίας επιτρέπει την συγκεκριμένη ομαδοποίηση, για λόγους διευκόλυνσης και οικονομίας.

Στη συνέχεια του παρόντος εγγράφου ο όρος «έργο» νοείται ότι περιλαμβάνει και τις υφιστάμενες ή νέες διαδικασίες που αφορούν σε επεξεργασία ΠΔ.

Το βασικό παραδοτέο της ΕΑΠΔ είναι μια αναφορά που περιγράφει λεπτομερώς τις επιπτώσεις που εντοπίστηκαν και τις λύσεις ή τις ενέργειες που προτείνονται για την αντιμετώπιση τους.

Η ΕΑΠΔ πρέπει να ξεκινήσει παράλληλα με το σχεδιασμό του έργου -εάν δεν βρίσκεται σε εξέλιξη- έτσι ώστε να εκτιμηθούν και να εντοπιστούν οι κίνδυνοι για παραβίαση της ιδιωτικότητας πριν την εφαρμογή του.

Η μεθοδολογία της διενέργειας Εκτίμησης Αντικτύπου έχει εφαρμογή στο σύνολο των πόρων του οργανισμού που εμπίπτουν στο πεδίο εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων.

Ποια είναι τα βασικά επιδιωκόμενα αποτελέσματα:

- καθορισμός των δυνητικών επιπτώσεων και κινδύνων του έργου επί των προσωπικών δεδομένων.
- καθορισμός των επιπτώσεων αυτών αφού ληφθούν υπόψη όλα τα ενδιαφερόμενα μέρη (π.χ. υποκείμενα δεδομένων, κοινωνία, ΑΠΔΠΧ, κ.λπ.).
- κατανόηση της αποδοχής του έργου και των χαρακτηριστικών του από τις εταιρείες και τους ανθρώπους που θα επηρεαστούν από αυτό.
- διαχείριση του κινδύνου των προσωπικών δεδομένων και άλλων κινδύνων για την ιδιωτικότητα και τα σχετικά δικαιώματα κι ελευθερίες των φυσικών προσώπων, με τον εντοπισμό και την αξιολόγηση λιγότερο επεμβατικών εναλλακτικών λύσεων.
- εντοπισμός τρόπων με τους οποίους μπορούν να αποφευχθούν οι αρνητικές επιπτώσεις στην ιδιωτικότητα.
- στα σημεία όπου είναι αναπόφευκτες οι αρνητικές επιπτώσεις στην ιδιωτικότητα, σαφήνεια ως προς την επιχειρησιακή ανάγκη που τις δικαιολογεί.
- τεκμηρίωση των αποτελεσμάτων.

Αποδέκτες του παρόντος εγγράφου είναι όλα τα στελέχη (ή και συνεργάτες) του οργανισμού που συμμετέχουν στη διαδικασία Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων.

Μεθοδολογία Εκτίμησης Αντικτύπου Προστασίας Δεδομένων & διαχείρισης επικινδυνότητας

Γιατί πρέπει να υλοποιηθεί ΕΑΠΔ;

Πέραν των νομικών υποχρεώσεων, τα ζητήματα ιδιωτικού απορρήτου που δεν αντιμετωπίζονται σωστά μπορεί να επηρεάσουν την εμπιστοσύνη στον οργανισμό και να υπονομεύσουν την επιτυχία του έργου. Ένα μεγάλο μέρος της επιτυχίας ενός έργου εξαρτάται από το κατά πόσον πληρούνται οι απαιτήσεις της νομοθεσίας για την προστασία της ιδιωτικότητας. Είναι προς το συμφέρον του οργανισμού λοιπόν να προβεί στη διενέργεια ΕΑΠΔ για έργα που χειρίζονται προσωπικά δεδομένα.

Τα οφέλη της ΕΑΠΔ περιλαμβάνουν:

- την εξασφάλιση ότι το έργο συμμορφώνεται με το κανονιστικό πλαίσιο περί προστασίας προσωπικών δεδομένων.
- την προβολή των αξιών του οργανισμού και της κοινότητας γύρω από την ιδιωτικότητα και τα προσωπικά δεδομένα στο σχεδιασμό του έργου

- τη μείωση του μελλοντικού κόστους όσον αφορά στο χρόνο διαχείρισης, στο νομικό κόστος και στην πιθανή αρνητική δημοσιότητα, εξετάζοντας θέματα ιδιωτικότητας και προστασίας προσωπικών δεδομένων εγκαίρως σε ένα έργο
- τον προσδιορισμό στρατηγικών για την επίτευξη των στόχων του έργου χωρίς να επηρεάζεται η ιδιωτικότητα
- την διαβεβαίωση των ενδιαφερόμενων ότι το έργο έχει σχεδιαστεί με γνώμονα την προστασία της ιδιωτικότητας
- την ευαισθητοποίηση της κοινότητας και την αποδοχή του έργου μέσω δημόσιας διαβούλευσης εάν απαιτείται.

Πότε χρονικά πρέπει να εκκινηθεί μια διαδικασία ΕΑΠΔ

Για να είναι αποτελεσματική, μια ΕΑΠΔ πρέπει να αποτελεί αναπόσπαστο μέρος της διαδικασίας σχεδιασμού του έργου.

Θα πρέπει να αναληφθεί έγκαιρα ώστε να δύναται να επηρεάσει το σχεδιασμό του έργου ή, εάν υπάρχουν σημαντικές αρνητικές επιπτώσεις στην ιδιωτικότητα, να επανεξετάσει τη συνέχιση ενός έργου. Μια ΕΑΠΔ λειτουργεί πιο αποτελεσματικά όταν ενημερώνεται και συμβάλλει στη διαμόρφωση της εξέλιξης του έργου, διασφαλίζοντας ότι η ιδιωτικότητα και η προστασία αυτής και των προσωπικών δεδομένων λαμβάνεται υπόψη σε όλη τη διάρκεια ζωής του έργου.

Επίσης, η συνεπής και έγκαιρη χρήση μιας ΕΑΠΔ διασφαλίζει ότι όλοι οι αρμόδιοι υπάλληλοι εξετάζουν τα θέματα ιδιωτικότητας από τα αρχικά στάδια ενός έργου.

Θα πρέπει να επανεξετάζεται και να ενημερώνεται όταν υπάρχουν αλλαγές στο σχεδιασμό του έργου. Εάν υπάρξουν ουσιαστικές αλλαγές στον τρόπο χειρισμού των προσωπικών δεδομένων ή αλλαγές σε ένα υπάρχον έργο, τότε ίσως χρειαστεί να γίνει επαναξιολόγηση στο σύνολο της ΕΑΠΔ. Επίσης σε κάθε φάση του κύκλου ζωής ενός έργου θα πρέπει να λαμβάνονται υπόψη τα θέματα ιδιωτικότητας.

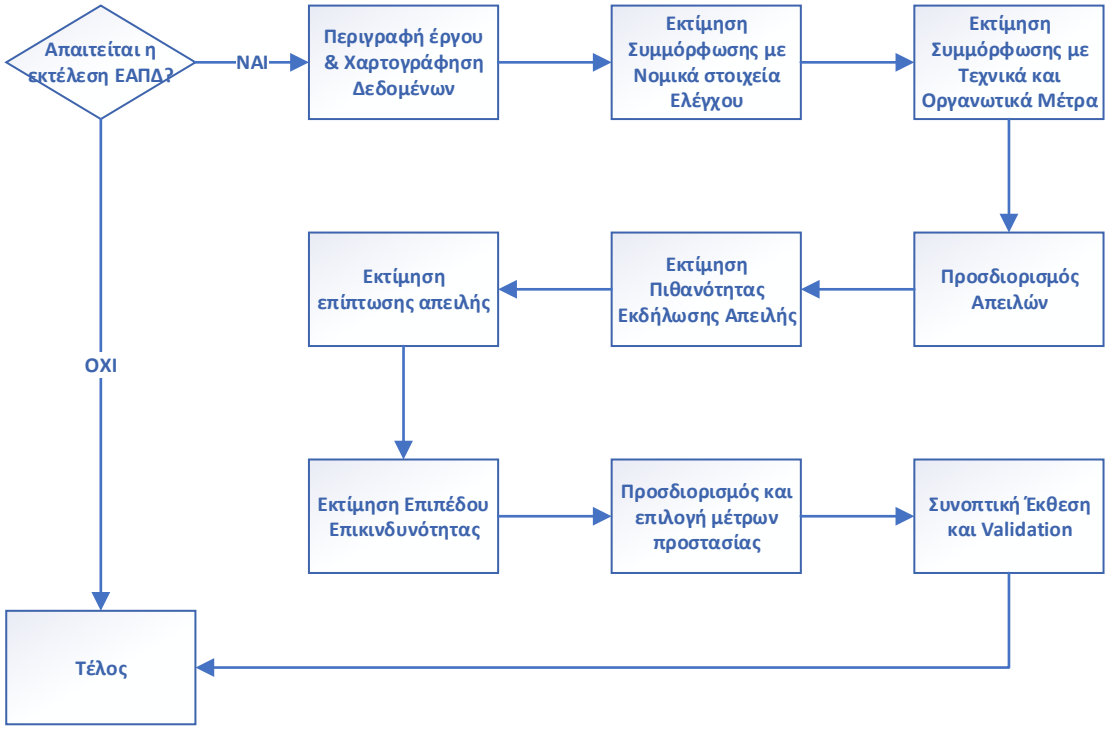
Μεθοδολογία - Εισαγωγή

Η Εκτίμηση Αντικτύπου Προστασίας Δεδομένων έχει ως στόχο την ανάδειξη των κινδύνων για τα προσωπικά δεδομένα, το μέγεθος των κινδύνων αυτών, και τις πιθανές επιπτώσεις στην ασφάλεια των Προσωπικών Δεδομένων. Αποτέλεσμα αυτής της διαδικασίας είναι η ταξινόμηση των κινδύνων με ορθολογικά κριτήρια, όπως το μέγεθος της ζημίας που θα προκύψει από την παραβίαση της ασφάλειας των προσωπικών δεδομένων και η πιθανότητα να προκύψει τέτοια παραβίαση. Έτσι είναι δυνατή η επιλογή αντιμέτρων που είναι συμβατά με την αξία των προσωπικών δεδομένων που θα προστατεύουν καθώς και η ιεράρχηση της υλοποίησης των αντιμέτρων αυτών.

Η ΕΑΠΔ θα πρέπει να διεξάγεται από μέλη της ομάδας του έργου, που γνωρίζουν και έχουν κατανοήσει τόσο το αντικείμενο του έργου όσο και την ίδια τη διαδικασία.

Ο οργανσιμός έχει υιοθετήσει και χρησιμοποιεί μια μεθοδολογία ανάλυσης επικινδυνότητας που βασίζεται σε διεθνή πρότυπα και πρακτικές των οποίων οι αναφορές παρουσιάζονται στο τέλος του παρόντος.

Η μεθοδολογία ΕΑΠΔ παρουσιάζεται στο σχήμα που ακολουθεί.



Εικόνα 1: Μεθοδολογία ΕΑΠΔ

Βήμα 1: Καθορισμός εάν απαιτείται η εκτέλεση ΕΑΠΔ

Το πρώτο βήμα της μεθοδολογίας επιβάλλει να καθοριστεί εάν η διενέργεια της ΕΑΠΔ είναι απαραίτητη για κάθε έργο, στο οποίο πρόκειται να πραγματοποιηθεί ή πραγματοποιείται επεξεργασία προσωπικών δεδομένων. Η διενέργεια ΕΑΠΔ δεν είναι απαραίτητη σε όλα τα έργα

Το άρθρο 35 του ΓΚΠΔ απαιτεί να διεξάγεται ΕΑΠΔ, όταν η επεξεργασία που πραγματοποιείται είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Οι Αρχές Προστασίας Προσωπικών Δεδομένων (Εποπτικές Αρχές) συστήνουν να διεξάγεται ΕΑΠΔ όποτε πραγματοποιείται επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων ή οποιαδήποτε άλλη δραστηριότητα που μπορεί να επηρεάσει το απόρρητο και την ασφάλεια των προσωπικών δεδομένων.

Ο οργανισμός είναι υπεύθυνός για τα προσωπικά δεδομένα που συλλέγει, ακόμη και όταν αυτά διατηρούνται από εξωτερικούς παρόχους υπηρεσιών ή εργολάβους.

Η διαδικασία αποτίμησης επικινδυνότητας ενεργοποιείται στις εξής περιπτώσεις:

- Όταν συντελούνται σημαντικές αλλαγές στην οργανωτική δομή, στη λειτουργία ή/και τους πληροφοριακούς πόρους του οργανισμού που εμπίπτουν στο πεδίο εφαρμογής της Ασφάλειας των Προσωπικών Δεδομένων.
- Όταν εκδηλώνεται μεγάλος αριθμός περιστατικών παραβίασης της ασφάλειας, ιδιαίτερα με επαναλαμβανόμενο χαρακτήρα.
- Όταν σημειώνεται καίριο πλήγμα στην ασφάλεια των πληροφοριών ή μεγάλης έκτασης καταστροφές.
- Όποτε το κρίνει η Διοίκηση ή/και ο Υπεύθυνος της Διεργασίας που αφορούν τα προσωπικά δεδομένα ή/και ο Υπεύθυνος Προστασίας Δεδομένων .

Επίσης εκτελείται αποτίμηση επικινδυνότητας σε τακτή βάση, τουλάχιστον μία φορά ανά έτος, σε συνδυασμό με την ανασκόπηση της ΕΑΠΔ.

Αναλυτικά τα κριτήρια παρουσιάζονται στην αναφορά [10] στο τέλος του παρόντος.

Βήμα 2: Περιγραφή Έργου και Χαρτογράφηση Δεδομένων (Data map)

Μια ΕΑΠΔ βασίζεται σε μια ευρεία περιγραφή της επεξεργασίας που πραγματοποιείται στο πλαίσιο του έργου, όπως:

- σκοποί της επεξεργασίας
- πώς οι σκοποί ταιριάζουν με τους ευρύτερους στόχους
- το πεδίο εφαρμογής και το εύρος της επεξεργασίας
- οποιαδήποτε σύνδεση με υπάρχοντα προγράμματα ή άλλα έργα
- ποιος είναι υπεύθυνος για την επεξεργασία
- χρονοδιάγραμμα λήψης αποφάσεων που θα επηρεάσει το σχεδιασμό του έργου
- ορισμένα από τα βασικά στοιχεία ιδιωτικού απορρήτου - για παράδειγμα, την έκταση και τον τύπο των δεδομένων που θα συλλέγονται, τον τρόπο με τον οποίο πρέπει να αντιμετωπιστεί το επίπεδο της ασφάλειας και τον τρόπο με τον οποίο θα τύχουν επεξεργασίας τα προσωπικά δεδομένα.

Η περιγραφή του έργου θα πρέπει να παραμείνει σχετικά σύντομη και δεν πρέπει να περιλαμβάνει ανάλυση των επιπτώσεων στην ιδιωτικότητα. Αυτές οι πληροφορίες είναι σημαντικές καθώς παρέχουν το πλαίσιο για την ΕΑΠΔ.

Οι πληροφορίες που πρέπει να συλλεχθούν σε αυτή τη φάση περιλαμβάνουν:

- Υπεύθυνος Επεξεργασίας: Το φυσικό πρόσωπο που έχει την ευθύνη έναντι του νόμου για την επεξεργασία του αρχείου για λογαριασμό του οργανισμού.
- Εκτελών την Επεξεργασία: Το μέλος/μέλη του προσωπικού που επεξεργάζονται τα προσωπικά δεδομένα του αρχείου.
- Ποιοι έχουν πρόσβαση στα δεδομένα: Αναφέρονται τα μέλη του προσωπικού που έχουν πρόσβαση στα δεδομένα χωρίς όμως να τα επεξεργάζονται
- Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα: Ποιες κατηγορίες προσωπικών δεδομένων περιλαμβάνονται στο εν λόγω αρχείο (π.χ. ονοματεπώνυμο, ΑΦΜ, κλπ. ή δημογραφικά δεδομένα, φορολογικά δεδομένα κλπ., απλά ή ειδικών κατηγοριών)
- Τρόπος Συλλογής Δεδομένων: ο τρόπος που συλλέγονται τα δεδομένα, π.χ. από τα ίδια τα υποκείμενα, από τρίτους, από συνεργάτες μέσω προωθητικών ενεργειών κλπ.
- Αποθήκευση Δεδομένων (πως / που): Με ποιο τρόπο αποθηκεύονται τα ΠΔ και σε ποιο σημείο (αφορά έντυπα και ηλεκτρονικά ΠΔ)
- Πληροφοριακά Συστήματα στα οποία καταχωρούνται: Σε ποιες εφαρμογές καταχωρίζονται (π.χ. εφαρμογή μισθοδοσίας)
- Σκοπός επεξεργασίας: Για ποιο λόγο γίνεται η συλλογή και επεξεργασία των ΠΔ (π.χ. εκτέλεση μισθοδοσίας)
- Νόμιμη βάση επεξεργασίας: Σε ποια άρθρα του κανονισμού 6 ή 9 βασίζεται η κάθε επεξεργασία.
- Κατηγορίες Υποκειμένων: Ποιους αφορούν τα προσωπικά δεδομένα που περιλαμβάνονται στο αρχείο που αναλύεται (π.χ. προσωπικό)
- Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα: Οι κατηγορίες προσωπικών δεδομένων που τηρούνται στο αρχείο
- Κατηγορίες αποδεκτών προσωπικών δεδομένων: Σε ποιους καταλήγουν τα ΠΔ για περαιτέρω επεξεργασία.
- Διαβίβαση σε Τρίτες Χώρες: Αναφέρεται εάν γίνεται διαβίβαση προσωπικών δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης
- Προβλεπόμενη Περίοδος Διαγραφής: Ποιος είναι ο κύκλος ζωής τους, δηλαδή μετά από πόσο χρονικό διάστημα θεωρείται ότι δεν εξυπηρετούν το σκοπό της επεξεργασίας, οπότε και διαγράφονται.
- Τρόπος Διαγραφής / καταστροφής: Αναφέρεται ο τρόπος με τον οποίο καταστρέφονται τα προσωπικά δεδομένα
- Μέτρα Φυσικής Ασφάλειας: Ποια μέτρα λαμβάνει ο οργανισμός για τη φυσική ασφάλεια του αρχείου ΠΔ που αναλύεται.
- Τεχνικά Μέτρα Ασφάλειας (ΙΤ): Ποια τεχνικά μέτρα λαμβάνει ο οργανισμός για την ΙΤ ασφάλεια του αρχείου ΠΔ που αναλύεται.

- Ενημέρωση στα Υποκείμενα δεδομένων: Πως ενημερώνονται τα υποκείμενα των δεδομένων για την τήρηση και επεξεργασία τους.

Βήμα 3: Εκτίμηση Συμμόρφωσης με τα Νομικά Σημεία Ελέγχου του ΓΚΠΔ

Στον ΓΚΠΔ γίνεται εκτενής αναφορά στα νομικά σημεία τα οποία στα οποία θα πρέπει να δώσει ιδιαίτερη σημασία ο οργανισμός προκειμένου να συμμορφωθεί με τον κανονισμό.

Αυτά περιλαμβάνουν σε γενικές γραμμές τις Θεμελιώδεις αρχές επεξεργασίας Προσωπικών Δεδομένων, τη νόμιμη βάση επεξεργασίας, τα δικαιώματα των υποκειμένων, τις σχέσεις των υπευθύνων και εκτελούντων την επεξεργασία, τη μεταφορά δεδομένων εκτός χωρών του Ευρωπαϊκού Οικονομικού Χώρου, θέματα πληροφόρησης και ενημέρωσης του προσωπικού και των υποκειμένων κ.λπ.

Αυτά τα θέματα θα πρέπει να εξεταστούν ως προς τη συμμόρφωση του οργανισμού με αυτά.

Βήμα 4: Εκτίμηση Συμμόρφωσης με Τεχνικά και Οργανωτικά Μέτρα Ελέγχου Ασφάλειας

Ο ΓΚΠΔ στο άρθρο 32 παρ.1 αναφέρει μόνο ότι προκειμένου να μειωθεί το επίπεδο κινδύνου, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τους σκοπούς επεξεργασίας κ.λπ. θα πρέπει να εφαρμοστούν τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων». Επιβάλλεται λοιπόν να προσδιοριστούν τα Τεχνικά και Οργανωτικά μέτρα που θα εξεταστούν ως προς την ασφάλειά τους και τους κινδύνους που διατρέχουν. Ο Κανονισμός απαιτεί κατά περίπτωση τουλάχιστον τα ακόλουθα μέτρα:

- Ψευδωνυμοποίηση και ανωνυμοποίηση των δεδομένων προσωπικού χαρακτήρα
- Τη διασφάλιση της ακεραιότητας, της διαθεσιμότητας και αξιοπιστίας των συστημάτων
- Τη δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση συμβάντος.
- Διαδικασία για τακτική δοκιμή εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων.

Επιπλέον θα πρέπει να ελεγχθούν οι παρακάτω πληροφοριακοί πόροι του οργανισμού που αφορούν στη συγκεκριμένη επεξεργασία της οποίας πρέπει να εκτιμηθεί και μετριαστεί ο κίνδυνος:

- Δεδομένα (σε ηλεκτρονική ή έντυπη μορφή)
- Πληροφοριακά συστήματα

- Εξοπλισμός (εξυπηρετητές, υπολογιστές, μέσα αποθήκευσης, εκτυπωτές κλπ.)
- Τηλεπικοινωνιακές υποδομές
- Υλικοτεχνική υποδομή (κτιριακές εγκαταστάσεις, computer rooms κλπ.)
- Ανθρώπινο δυναμικό (στελεχιακό δυναμικό ή και συνεργάτες με πρόσβαση σε πληροφοριακούς πόρους)

Η αναγνώριση των τεχνικών και οργανωτικών μέτρων που απαιτούνται ώστε να μειωθεί ο κίνδυνος διαρροής προσωπικών δεδομένων και στέρησης των δικαιωμάτων και ελευθεριών των φυσικών προσώπων, αποτελεί ουσιαστικά το πεδίο εφαρμογής της ΕΑΠΔ.

Γενικές κατηγορίες θεματικών περιοχών που πρέπει να εξεταστούν σύμφωνα με το ISO27002:2013 είναι:

- Πολιτικές Ασφάλειας
- Οργάνωση της Ασφάλειας των πληροφοριών
- Ασφάλεια ανθρωπίνων πόρων
- Διαχείριση πληροφοριακών πόρων
- Έλεγχος πρόσβασης
- Φυσική και περιβαλλοντική ασφάλεια
- Ασφάλεια λειτουργιών
- Ασφάλεια Επικοινωνιών
- Προμήθεια ανάπτυξη και συντήρηση συστημάτων
- Σχέσεις με προμηθευτές
- Διαχείριση περιστατικών ασφαλείας πληροφοριών
- Ασφάλεια πληροφοριών κατά τη διαχείριση επιχειρησιακής συνέχειας
- Συμμόρφωση

Βήμα 5: Προσδιορισμός των απειλών

Ως απειλή λογίζεται κάθε παράγων που εκούσια ή ακούσια ελλοχεύει για την εκμετάλλευση κάποιων αδυναμιών/ κενών στην ασφάλεια του οργανισμού και των πληροφοριακών του πόρων. Οι παράγοντες εκείνοι που προκαλούν την εκδήλωση μιας απειλής μπορούν να καταταγούν –γενικά– σε τρεις κατηγορίες:

- Φυσικές απειλές, π.χ. πλημμύρα, σεισμός, πυρκαγιά
- Απειλές από τον ανθρώπινο παράγοντα, ακούσιες (π.χ. λανθασμένη εισαγωγή στοιχείων στο πληροφοριακό σύστημα, 'άνοιγμα' αρχείων μολυσμένων με ιούς) ή εκούσιες (π.χ. επιθέσεις από χάκερς, υποκλοπή στοιχείων, απάτη, κλοπή)
- Περιβαλλοντικές απειλές, π.χ. παρατεταμένη απώλεια ηλεκτρικής ισχύος, υψηλό επίπεδο μόλυνσης

Αποτέλεσμα της εκτέλεσης αυτού του βήματος είναι ο προσδιορισμός των απειλών παραβίασης της ασφάλειας των πόρων.

Βήμα 6: Εκτίμηση της πιθανότητας εκδήλωσης απειλής

Σε αυτό το βήμα της μεθοδολογίας ανάλυσης επικινδυνότητας εκτιμάται η πιθανότητα εκδήλωσης κάθε απειλής που προσδιορίστηκε στο προηγούμενο βήμα.

Κατά την εκτίμηση της πιθανότητας όπου μία απειλή θα εκμεταλλευθεί επιτυχώς ένα κενό/ αδυναμία στο συνολικό πλαίσιο ασφάλειας πρέπει να ληφθούν υπόψη διάφορες παράμετροι όπως:

- το κίνητρο και οι δυνατότητες του επιχειρούντος την παραβίαση
- η φύση του κενού/ αδυναμίας του πλαισίου ασφάλειας
- η εκδήλωση (και η συχνότητα εκδήλωσης) αντίστοιχων απειλών κατά το παρελθόν

Η πιθανότητα εκδήλωσης μιας απειλής μπορεί να λάβει πέντε (5) τιμές: Πολύ Υψηλή, Υψηλή, Μέση, Χαμηλή και Πολύ Χαμηλή. Η εκτίμηση της πιθανότητας εκδήλωσης μιας απειλής γίνεται σύμφωνα με τον πίνακα που ακολουθεί.

Τιμή	Πιθανότητα εκδήλωσης απειλής	Περιγραφή
1	Πολύ χαμηλή: Σχεδόν απίθανο να εκδηλωθεί	<= 1 επεισόδιο ανά 10 έτη
2	Χαμηλή: Μικρή πιθανότητα να εκδηλωθεί	~ 1 επεισόδιο ανά 3 έτη
3	Μέση: Εκδηλώνεται περιστασιακά	~ 1 επεισόδιο ανά έτος
4	Υψηλή: Συχνή / επανειλημμένη εκδήλωση	~ 1 επεισόδιο ανά 3 μήνες
5	Πολύ Υψηλή: Σχεδόν βέβαιο ότι θα εκδηλωθεί	~ 1 επεισόδιο / μήνα

Βήμα 7: Εκτίμηση της επίπτωσης απειλής

Αντίστοιχα με το προηγούμενο βήμα της μεθοδολογίας, σε αυτό το βήμα, και για κάθε απειλή που προσδιορίστηκε, εκτιμάται το μέγεθος της ζημίας (επίπτωση) που θα προκύψει από ενδεχόμενο γεγονός παραβίασης της ασφάλειας κάποιου πληροφοριακού πόρου του οργανισμού και κατ' επέκταση των προσωπικών δεδομένων των υποκειμένων.

Η εκδήλωση μιας απειλής και η επιτυχημένη παραβίαση της ασφάλειας μπορεί να έχουν σημαντικές επιπτώσεις στη λειτουργία του οργανισμού. Οι επιπτώσεις αυτές αφορούν στην αποτυχία διασφάλισης των βασικών στόχων ασφάλειας:

- Απώλεια εμπιστευτικότητας: Η μη εξουσιοδοτημένη αποκάλυψη εμπιστευτικών πληροφοριών του οργανισμού μπορεί να οδηγήσει σε πλήγμα του κύρους και της δημόσιας εικόνας του οργανισμού, σε παραβίαση της νομοθεσίας περί προστασίας προσωπικών δεδομένων/ πνευματικών δικαιωμάτων κ.ο.κ.
- Απώλεια ακεραιότητας: Η ακεραιότητα ενός συστήματος ή μιας ομάδας δεδομένων παραβιάζεται όταν το σύστημα ή τα δεδομένα υπόκεινται σε μη εξουσιοδοτημένες αλλαγές, εκούσιες ή ακούσιες. Η παραβίαση της ακεραιότητας μπορεί να οδηγήσει σε ανακριβή και λανθασμένα δεδομένα, καθώς και σε εσφαλμένες αποφάσεις που

λαμβάνονται βάσει των δεδομένων αυτών. Γενικά, η απώλεια της ακεραιότητας πλήττει σε μεγάλο βαθμό την αξιοπιστία του συστήματος και των δεδομένων.

- Απώλεια διαθεσιμότητας: Η μη διαθεσιμότητα ενός συστήματος ή η αδυναμία πρόσβασης σε δεδομένα οδηγεί σε απώλεια παραγωγικού χρόνου των χρηστών και μπορεί να πλήξει σημαντικά τη λειτουργία του οργανισμού.

Για την εκτίμηση των επιπτώσεων της επιτυχούς εκδήλωσης μιας απειλής χρησιμοποιείται επίσης μία κλίμακα πέντε (5) τιμών: Πολύ Υψηλή, Υψηλή, Μέση, Χαμηλή και Πολύ Χαμηλή. Η αντιστοίχιση των επιπτώσεων κάθε απειλής στις τιμές αυτές γίνεται βάσει του πίνακα που ακολουθεί.

Τιμή	**Επίπτωση απειλής**	**Περιγραφή**
1	Πολύ χαμηλή	Καμία πρακτική επίπτωση
2	Χαμηλή	Τα υποκείμενα των δεδομένων είτε δεν θα επηρεαστούν είτε ενδέχεται να αντιμετωπίσουν πολύ μικρές δυσκολίες, οι οποίες θα ξεπεραστούν χωρίς κανένα πρόβλημα. Μικρές συνέπειες στο επίπεδο ασφάλειας (λογισμικό, δεδομένα, υποδομές, ανθρώπινοι πόροι) και εν γένει τη λειτουργία του φορέα. Στις επιπτώσεις που εντάσσονται σε αυτό το επίπεδο περιλαμβάνονται: • Απώλεια χαμηλής αξίας στοιχείων της υλικοτεχνικής και τεχνολογικής υποδομής ή άλλων άυλων πόρων του φορέα • Μικρή απώλεια χρόνου των στελεχών σε γραφειοκρατικές διατυπώσεις • Απώλεια χρόνου για τη διαμόρφωση δεδομένων κάποιου. • Λήψη ανεπιθύμητων μηνυμάτων (π.χ. spam) • Λήψη μηνυμάτων στοχοθετημένης διαφήμισης για κοινά καταναλωτικά προϊόντα. • Απλή ενόχληση από πληροφορίες που ζητήθηκαν ή ελήφθησαν • Φόβος απώλειας ελέγχου των δεδομένων κάποιου χωρίς να συμβαίνει πραγματικά
3	Μέση	Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές δυσκολίες, τις οποίες όμως θα μπορέσουν να ξεπεράσουν. Δυσμενείς αλλά όχι καταστροφικές συνέπειες στο επίπεδο ασφάλειας (υλικό, λογισμικό, δεδομένα, υποδομές, ανθρώπινοι πόροι) και εν γένει τη λειτουργία του φορέα. Στις επιπτώσεις που εντάσσονται σε αυτό το επίπεδο περιλαμβάνονται: • Η επίτευξη πλήγματος στο κύρος και τη δημόσια εικόνα του φορέα • Απρόβλεπτες πληρωμές (π.χ. πρόστιμα που επιβλήθηκαν εσφαλμένα) • Χαμένες ευκαιρίες (π.χ. ακύρωση ταξιδιού, τερματισμός λογαριασμού στο διαδίκτυο), παραλαβή μηνυμάτων που ενδέχεται να βλάψουν το υποκείμενο • Αύξηση κόστους (π.χ. τιμές ασφαλιστηρίων συμβολαίων) • Επεξεργασία εσφαλμένων δεδομένων με παράλληλη δημιουργία δυσλειτουργιών (π.χ. σε πελάτες) • Στοχοθετημένη διαφήμιση σε άτομο που ήθελε να διατηρήσει το θέμα εμπιστευτικό (π.χ. διαφήμιση εγκυμοσύνης, θεραπεία με φάρμακα)

		• Αίσθημα εισβολής στην ιδιωτική ζωή χωρίς ανεπανόρθωτες ζημιές • Εκφοβισμός στα κοινωνικά δίκτυα
4	Υψηλή	Τα υποκείμενα των δεδομένων μπορεί να αντιμετωπίζουν σημαντικές συνέπειες, οι οποίες θα μπορούν να ξεπεραστούν αν και με πραγματικές και σοβαρές δυσκολίες. Εξαιρετικά δυσμενείς συνέπειες στο επίπεδο ασφάλειας (υλικό, λογισμικό, δεδομένα, υποδομές, ανθρώπινοι πόροι) και εν γένει τη λειτουργία του φορέα. Στις επιπτώσεις που εντάσσονται σε αυτό το επίπεδο περιλαμβάνονται: • Η απώλεια ιδιαίτερα υψηλής αξίας στοιχείων της υλικοτεχνικής και τεχνολογικής υποδομής ή άλλων σημαντικών άυλων πόρων του φορέα • Η επίτευξη πλήγματος στο κύρος και τη δημόσια εικόνα του φορέα • Οικονομικές δυσκολίες μη προσωρινές (π.χ. υποχρέωση λήψης δανείου) Απαγόρευση κατοχής τραπεζικών λογαριασμών. • Μοναδικές και μη επαναλαμβανόμενες χαμένες ευκαιρίες (π.χ. στεγαστικό δάνειο, άρνηση σπουδών, απασχόληση, απαγόρευση εξέτασης) • Απώλεια απασχόλησης • Διάσταση ή διαζύγιο • Οικονομική ζημιά ως αποτέλεσμα απάτης (π.χ. μετά από phishing) • Απώλεια δεδομένων πελατών • Αίσθηση εισβολής στην ιδιωτική ζωή με μη αναστρέψιμες ζημιές. • Αίσθημα παραβίασης θεμελιωδών δικαιωμάτων (π.χ. διακρίσεις, ελευθερία έκφρασης) • Θύμα εκβιασμού, μπούλινγκ.
5	**Πολύ Υψηλή**	Τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές ή ακόμη και μη αναστρέψιμες συνέπειες, τις οποίες δεν μπορούν να ξεπεράσουν. Καταστροφικές συνέπειες για τη λειτουργία του φορέα. Στις επιπτώσεις που εντάσσονται σε αυτό το επίπεδο περιλαμβάνονται: • Εκτεταμένες καταστροφές της υλικοτεχνικής και τεχνολογικής υποδομής του φορέα • Η παρατεταμένη αδυναμία λειτουργίας του φορέα • Η επίτευξη καθοριστικού πλήγματος στο κύρος και τη δημόσια εικόνα του φορέα, το οποίο μπορεί να οδηγήσει στον τερματισμό της λειτουργίας του • Μακροχρόνιες ή μόνιμες σωματικές ασθένειες (π.χ. παραβίαση των αντενδείξεων) • Χρηματοοικονομικός κίνδυνος • Αδυναμία εργασίας • Απώλεια αποδεικτικών στοιχείων στο πλαίσιο δικαστικών διενέξεων • Απώλεια πρόσβασης σε ζωτικής σημασίας υποδομές (νερό, ηλεκτρική ενέργεια) • Ποινικές διώξεις και ποινές • Αλλαγή διοικητικής κατάστασης ή/και νομικής αυτονομίας.

Βήμα 8: Εκτίμηση του επιπέδου επικινδυνότητας

Έχοντας προσδιορίσει τις απειλές, τις πιθανότητες εκδήλωσής τους, καθώς και τις επιπτώσεις τους αντίστοιχα, σε αυτό το στάδιο υπολογίζεται το επίπεδο επικινδυνότητας που κρύβει η ενδεχόμενη επιτυχής εκδήλωση μιας απειλής. Η εκτίμηση του επιπέδου επικινδυνότητας προκύπτει ως συνάρτηση της πιθανότητας εκδήλωσης μιας απειλής και της σοβαρότητας των επιπτώσεών της στη λειτουργία, κύρος, εικόνα κλπ.

[*Επίπεδο επικινδυνότητας*] = [*Πιθανότητα εκδήλωσης απειλής*] x [*Επίπτωση απειλής*]

Συνεπώς, το επίπεδο επικινδυνότητας λαμβάνει τιμές 1-25.

Επίπεδο επικινδυνότητας		**ΠΙΘΑΝΟΤΗΤΑ**				
		Πολύ χαμηλή (1)	Χαμηλή (2)	Μέση (3)	Υψηλή (4)	Πολύ υψηλή (5)
ΕΠΙΠΤΩΣΗ	Πολύ χαμηλή (1)	1	2	3	4	5
	Χαμηλή (2)	2	4	6	8	10
	Μέση (3)	3	6	9	12	15
	Υψηλή (4)	4	8	12	16	20
	Πολύ υψηλή (5)	5	10	15	20	25

Το επίπεδο επικινδυνότητας μιας απειλής ορίζεται στον επόμενο πίνακα:

HRN (Hazard Rating Number)	**Επίπεδο Επικινδυνότητας**	**Περιγραφή**
HRN <=4	**Αποδεκτό**	Για απειλή με χαμηλό / πολύ χαμηλό επίπεδο επικινδυνότητας, τα στελέχη που είναι υπεύθυνα για την ασφάλεια των πληροφοριών μπορούν να αποφασίσουν απλά να αποδεχθούν την ύπαρξη της συγκεκριμένης απειλής.
4 < HRN <= 9	**Ανεκτό**	Εάν το επίπεδο επικινδυνότητας μιας απειλής είναι μέσο, είναι καλό να ληφθούν πρόσθετα μέτρα ασφαλείας. Ωστόσο, σε αυτή την περίπτωση, ο σχεδιασμός και η υλοποίηση των διορθωτικών μέτρων μπορούν να γίνουν σε ένα εύλογο χρονικό διάστημα από τον εντοπισμό της ανάγκης.

HRN >= 10	**Μη αποδεκτό**	Εάν μία απειλή εκτιμηθεί ότι παρουσιάζει υψηλή / πολύ υψηλή επικινδυνότητα, υπάρχει άμεση και επιτακτική ανάγκη για τη λήψη μέτρων αντιμετώπισής της.

Βήμα 9: Προσδιορισμός και επιλογή μέτρων προστασίας

Σε αυτό το στάδιο της μεθοδολογίας, προσδιορίζονται, για όσες απειλές έχουν επίπεδο επικινδυνότητας που υπερβαίνει τη μέγιστη επιτρεπόμενη τιμή, τα μέτρα προστασίας που πρέπει να υλοποιηθούν προκειμένου να αντιμετωπιστούν αποτελεσματικά οι κίνδυνοι που αναγνωρίστηκαν.

Όποτε ο υπεύθυνος επεξεργασίας δεν μπορεί να βρει επαρκή μέτρα για τη μείωση των κινδύνων σε αποδεκτό επίπεδο (δηλαδή οι υπολειπόμενοι κίνδυνοι παραμένουν υψηλοί) απαιτείται διαβούλευση με την εποπτική αρχή.

Επιπλέον, ο υπεύθυνος επεξεργασίας θα πρέπει να διαβουλεύεται με την εποπτική αρχή οποτεδήποτε το δίκαιο του κράτους μέλους απαιτεί από τους υπευθύνους επεξεργασίας να διαβουλεύονται και/ή να λαμβάνουν προηγούμενη έγκριση από την εποπτική αρχή σε σχέση με την επεξεργασία από υπεύθυνο επεξεργασίας για την εκτέλεση καθήκοντος που ασκείται από τον εν λόγω υπεύθυνο προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία (άρθρο 36 §5 του ΓΚΠΔ).

Θα πρέπει, ωστόσο, να αναφερθεί ότι ανεξαρτήτως του κατά πόσον απαιτείται ή όχι διαβούλευση με την εποπτική αρχή βάσει του επιπέδου του υπολειπόμενου κινδύνου, οι υποχρεώσεις τήρησης αρχείου της ΕΑΠΔ και επικαιροποίησης της ΕΑΠΔ σε εύθετο χρόνο παραμένουν.

Βήμα 10: Συνοπτική έκθεση και Validation

Στο τέλος δημιουργείται μια συνοπτική έκθεση με τα κύρια στοιχεία της Αξιολόγησης Αντικτύπου των Προσωπικών Δεδομένων και δημιουργείται επίσης η Δήλωση Εφαρμογής (Statement of Applicability) των κριτηρίων της WP 29 (Δείτε το Παράρτημα 1).

Υπευθυνότητες και Ρόλοι

Υπεύθυνος Επεξεργασίας

Ο οργανισμός, ως υπεύθυνος επεξεργασίας, είναι υπεύθυνη για τη συμμόρφωση με το ισχύον κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων. Ο οργανισμός θα λάβει το σύνολο των προσηκόντων μέτρων με σκοπό τη διασφάλιση της ιδιωτικότητας ήδη από το

σχεδιασμό της επεξεργασίας και την προστασία των υποκειμένων των δικαιωμάτων σύμφωνα με το νόμο.

Χρήστες Δεδομένων

Το σύνολο των εργαζόμενων και συνεργατών του οργανισμού, υποχρεούνται να συμμορφώνονται με το ισχύον κανονιστικό πλαίσιο για την προστασία των προσωπικών δεδομένων και την πολιτική ιδιωτικότητας. Στην περίπτωση κατά την οποία εντοπίζεται θέμα ή ερώτημα σχετικό με την προστασία των προσωπικών δεδομένων, αυτό πρέπει να τεθεί υπόψιν του υπεύθυνου προστασίας δεδομένων ή/και των Υπευθύνων Έργων.

Υπεύθυνοι Έργων (Project Managers) ή Υπεύθυνοι Διαδικασιών

Οι Υπεύθυνοι Έργων ή Διαδικασιών, υποχρεούνται να διασφαλίσουν για ότι όλα τα έργα /προγράμματα ή διαδικασίες, στα οποία πραγματοποιείται ή ενδέχεται να πραγματοποιηθεί συλλογή ή/και επεξεργασία προσωπικών δεδομένων θα μελετηθεί η ανάγκη διενέργειας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων. Στην περίπτωση αυτή η διενέργεια εκτίμησης αντικτύπου θα πραγματοποιείται καθ'όλη τη διάρκεια του έργου/προγράμματος ή αλλαγών στην εκτέλεση της διαδικασίας.

Οι Υπεύθυνοι Έργων / Προγραμμάτων ή διαδικασιών πρέπει να διασφαλίσουν ότι έχουν συμβουλευθεί τον Υπεύθυνο Προστασίας Δεδομένων για τα θέματα που αφορούν στην προστασία των προσωπικών δεδομένων.
Στην περίπτωση που η ΕΑΠΔ αφορά σε περισσότερα του ενός έργα, απαιτείται συνεργασία των εμπλεκόμενων υπεύθυνων επεξεργασίας και σαφής κατανομή των υποχρεώσεών τους για την αντιμετώπιση των κινδύνων.

Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων

Ο υπεύθυνος ασφαλείας πληροφοριακών συστημάτων πρέπει να έχει, τουλάχιστον, την επίβλεψη και τον έλεγχο της εφαρμογής της πολιτικής ασφαλείας και των μέτρων ασφαλείας, να ελέγχει τη συμμόρφωση και να αναπτύσσει καλές πρακτικές για την προστασία των προσωπικών δεδομένων. Θα πρέπει να διασφαλίζει ότι όπου υπάρχει επεξεργασία προσωπικών δεδομένων, έχουν αναγνωριστεί οι πόροι για την επεξεργασία και έχουν ανατεθεί σε συγκεκριμένα άτομα.

Υπεύθυνος Προστασίας Δεδομένων

Ο Υπεύθυνος Προσωπικών Δεδομένων (DPO), βοηθά τον Υπεύθυνο Επεξεργασίας βάσει της συμβουλευτικής του Ιδιότητας. Δεν είναι καθήκον του να ξεκινήσει την DPIA, ή να την αναλάβει εξ' ολοκλήρου από μόνος του.
Ως εκ τούτου αυτός ο οποίος πρέπει να οριστεί Υπεύθυνος της διαδικασίας εκπόνησης DPIA πρέπει να είναι ο «Υπεύθυνος» (Owner) της Διαδικασίας ή του Project που πρόκειται να υλοποιηθεί.

Αναφορές:

[1] ISO 27005:2011 Information technology -- Security techniques -- Information security risk management

[2] ISO 27002:2013 Information technology -- Security techniques – Code of practice for information security controls

[3] ISO 31000:2009 Risk Management – Principles and Guidelines

[4] ISO 31010:2009 Risk Management – Risk assessment techniques

[5] NIST SP 800-30 (Rev.1): "Guide for Conducting Risk Assessments".

[6] Privacy Impact Assessment (PIA), CNIL, Feb 2018 ed.

[7] Conducting PIA code of Practice, ICO, 2014

[8] Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248 αναθ. 01 Εκδόθηκαν στις 4 Απριλίου 2017 , Όπως τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 4 Οκτωβρίου 2017

[9] Standard Data Protection Model v.1.0-trial version 2016: https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf.

[10] Κριτήρια ενεργοποίησης ΕΑΠΔ: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/)

[11] Felix Bieker, Michael Friedewald, Marit Hansen, Hannah Obersteller, and Martin Rost, "A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation", Springer International Publishing Switzerland, pp. 21–37, 2016.

[12] Βασίλης Ζορκάδης, «Εκτίμηση Αντικτύπου στην προστασία Δεδομένων», Δ/ντής Γραμματείας ΑΠΔΠΧ.

Παράρτημα 1 : Κριτήρια για μια αποδεκτή ΕΑΠΔ

Η ομάδα εργασίας του άρθρου 29 προτείνει τα ακόλουθα κριτήρια, τα οποία οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιούν για να αξιολογούν κατά πόσο μια ΕΑΠΔ ή μια μεθοδολογία διενέργειας ΕΑΠΔ είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον ΓΚΠΔ:		Βήμα Διαδικασίας
Παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας [άρθρο 35§7α]: • λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτ. σκέψη 90) • καταγράφονται τα είδη δεδομένων προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος διατήρησης των δεδομένων προσωπικού χαρακτήρα • παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας • προσδιορίζονται οι πόροι στους οποίους εναποτίθενται τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων) • λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 §8)	√	Περιγραφή Έργου και Χαρτογράφηση Δεδομένων (Data map)
Εκτιμώνται η αναγκαιότητα και η αναλογικότητα [άρθρο 35 §7β] και καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον κανονισμό [άρθρο 35 § 7δ και αιτιολογική σκέψη 90], λαμβάνοντας υπόψη: τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει: • καθορισμένων, ρητών και νόμιμων σκοπών [άρθρο 5 §1β)]· • της νομιμότητας της επεξεργασίας (άρθρο 6)· • κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων [άρθρο 5 §1γ)]· • της περιορισμένης διάρκειας αποθήκευσης [άρθρο 5 §1ε)]· μέτρα που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων: • πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14): • δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρθρα 15 και 20)· • δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)· • δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)· σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)·	√	Εκτίμηση Συμμόρφωσης με τα Νομικά Σημεία Ελέγχου του ΓΚΠΔ

διασφαλίζονται οι περιστάσεις που περιβάλλουν τη διεθνή διαβίβαση ή τις διεθνείς διαβιβάσεις (Κεφάλαιο V)·		
Αναγνωρίζονται, αναλύονται και αξιολογούνται οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων [άρθρο 35 §7γ)]: • έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (πρβλ. αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων: • έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)· • εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων • εξακριβώνονται απειλές που θα μπορούσαν να επιφέρουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων· • εκτιμώνται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90)· • καθορίζονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (άρθρο 35 §7δ) και αιτιολογική σκέψη 90)	√	Εκτίμηση Συμμόρφωσης με Τεχνικά και Οργανωτικά Μέτρα Ελέγχου Ασφάλειας, Προσδιορισμός Απειλών, Εκτίμηση Πιθανότητας εκδήλωσης απειλής, Εκτίμηση Επίπτωσης Απειλής, Εκτίμηση Επικινδυνότητας, Προσδιορισμός και Επιλογή Μέτρων προστασίας
Συμμετέχουν τα ενδιαφερόμενα μέρη: • ζητείται η γνώμη του ΥΠΔ (άρθρο 35 §2) • ζητείται η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους, όταν ενδείκνυται (άρθρο 35 §9) • προηγούμενη διαβούλευση (άρθρο 36)	√	Συνοπτική έκθεση και Επικύρωση (Validation)

Παράρτημα 2: <u>Πλαίσιο απαραίτητων τυπικών κριτηρίων πληρότητας της μελέτης εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ)</u>
<u>(αρ. 35 παρ. 2 και 7-9 του ΓΚΠΔ, κριτήρια των κατευθυντήριων γραμμών για την εκτίμηση αντικτύπου WP248)</u>

Έγγραφο της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα με τίτλο «ESSENTIAL_STANDARD_CRITERIA_DPIA.doc»

3.7.1 Έντυπο «Εργαλείο Εκτίμησης Αντικτύπου Προστασίας Δεδομένων»

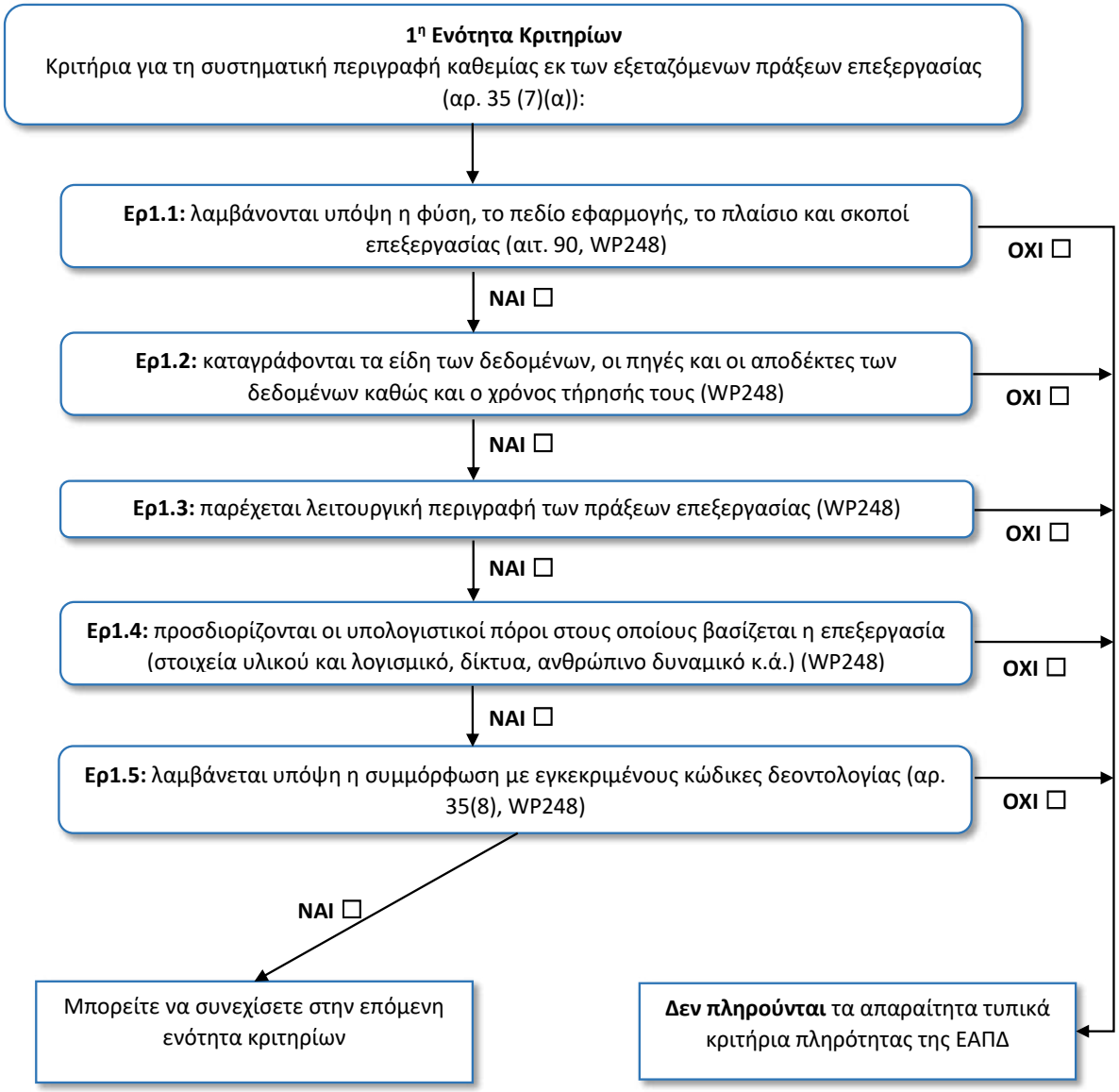
ΟΝΟΜΑ ΟΡΓΑΝΙΣΜΟΥ:									
Τεκμηρίωση και Περίληψη από τον Υπεύθυνο Διεργασίας									
Την ../../…. Ο Υπεύθυνος της διεργασίας …….. του Οργανισμού παρουσιάζει την ακόλουθη σύνοψη σχετικά με τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων και την παρούσα Εκτίμηση Αντικτύπου: Χρησιμοποιούμε σύστημα επιτήρησης για τον σκοπό της προστασίας προσώπων και αγαθών. Η επεξεργασία είναι απαραίτητη για σκοπούς εννόμων συμφερόντων που επιδιώκουμε ως υπεύθυνος επεξεργασίας (άρθρο 6 παρ. 1. στ ΓΚΠΔ). Στόχος της ΧΧΧ είναι να παρέχει εξατομικευμένη ιατρική ακριβείας καθώς και η παραγωγή υψηλής Έρευνας. Για το σκοπό αυτό είναι απαραίτητη η απρόσκοπτη και αδιάλειπτη λειτουργία του Υπολογιστικού εξοπλισμού του Ιδρύματος. Φαινόμενα κλοπών ή καταστροφών του ανωτέρω εξοπλισμού δημιουργούν ανυπέρβλητα εμπόδια στην επίτευξη των στόχων του. Το έννομο συμφέρον μας συνίσταται στην ανάγκη να προστατεύσουμε τον χώρο μας και τα αγαθά που ευρίσκονται σε αυτόν από παράνομες πράξεις, όπως ενδεικτικά από κλοπές. Η χρήση του συστήματος βιντεοεπιτήρησης έχει κριθεί απαραίτητη λόγω του μεγάλου κι εναλλασσόμενου αριθμού προσώπων, που επισκέπτονται τις εγκαταστάσεις, της ειδικής φύσεως δεδομένων που τηρούνται στην εταιρεία (γενετικό και βιολογικό υλικό), της αξίας του Υπολογιστικού εξοπλισμού της εταιρείας. [Υπογραφή]									
Τεκμηρίωση από τον Data Protection Officer									
Την ../../…. Ο Υπεύθυνος Προσωπικών Δεδομένων του Οργανισμού εξέφρασε την ακόλουθη γνώμη σχετικά με τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων και την παρούσα Εκτίμηση Αντικτύπου: Η διενέργειας εκτίμησης αντικτύπου (Data protection impact assessment- DPIA), είναι ένα σημαντικό μέτρο προστασίας των υποκειμένων των δεδομένων από «υψηλούς κινδύνους» και ένα εξίσου σημαντικό μέτρο συμμόρφωσης του Ιδρύματος προς τις διατάξεις του ΓΚΠΔ. Πρόκειται για ένα μέτρο πλήρως ενταγμένο στην ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξορισμού (Privacy by design / Privacy by default), σύμφωνα με τα οριζόμενα στις διατάξεις του άρθρου 25 του ΓΚΔΠ. Λαμβάνοντας υπόψιν ότι: 1. Στα καθήκοντα του DPO συμπεριλαμβάνεται η διατύπωση γνώμης σχετικά με την προστασία των δεδομένων των υποκειμένων κατά τη διενέργεια DPIA. 2. Στα καθήκοντα του DPO συμπεριλαμβάνεται η παρακολούθηση της συμμόρφωσης του υπευθύνου επεξεργασίας ως ένα μέτρο ενίσχυσης της συμμόρφωσης προς τις διατάξεις									

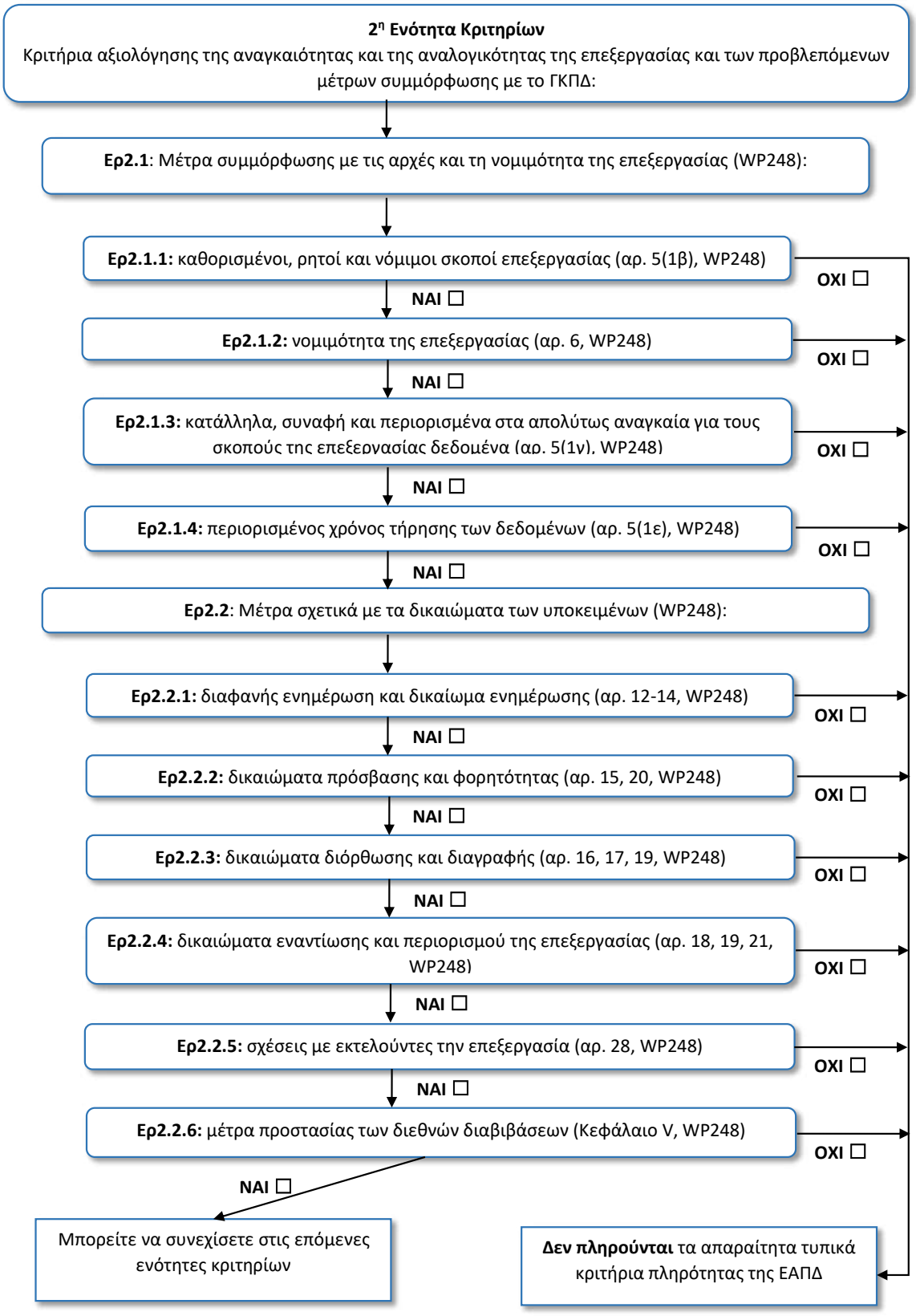
του ΓΚΔΠ 3. Ο ΓΚΠΔ θεσπίζει ρητά την εμπλοκή του DPO στη διενέργεια DPIA, σε δύο διατάξεις: (α) στο άρθρο 35 παρ. 2 θεσπίζεται ρητά η υποχρέωση για τον υπεύθυνο επεξεργασίας να ζητεί τη γνώμη του DPO, εφόσον αυτός έχει οριστεί, κατά τη διενέργεια DPIA σχετικά με την προστασία δεδομένων και (β) στο άρθρο 39 παρ. 2 θεσπίζεται ρητά, ανάμεσα στα καθήκοντα του DPO, και εκείνο του να «παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και [να] παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35» Συμφωνούμε με την DPIA η οποία έχει εκπονηθεί και θα πρέπει να τηρείται απαρέγκλιτα απαραίτητα δε θα πρέπει τακτικά να ανασκοπείται η εφαρμογή της. [Υπογραφή]
Επικύρωση από τον Νόμιμο Εκπρόσωπο
Την ../../…. Ο Νόμιμος Εκπρόσωπος της εταιρείας επικυρώνει την Εκτίμηση Αντικτύπου Προσωπικών Δεδομένων της διεργασίας .....υπό την ιδιότητά του ως Υπεύθυνος Επεξεργασίας: [Υπογραφή]

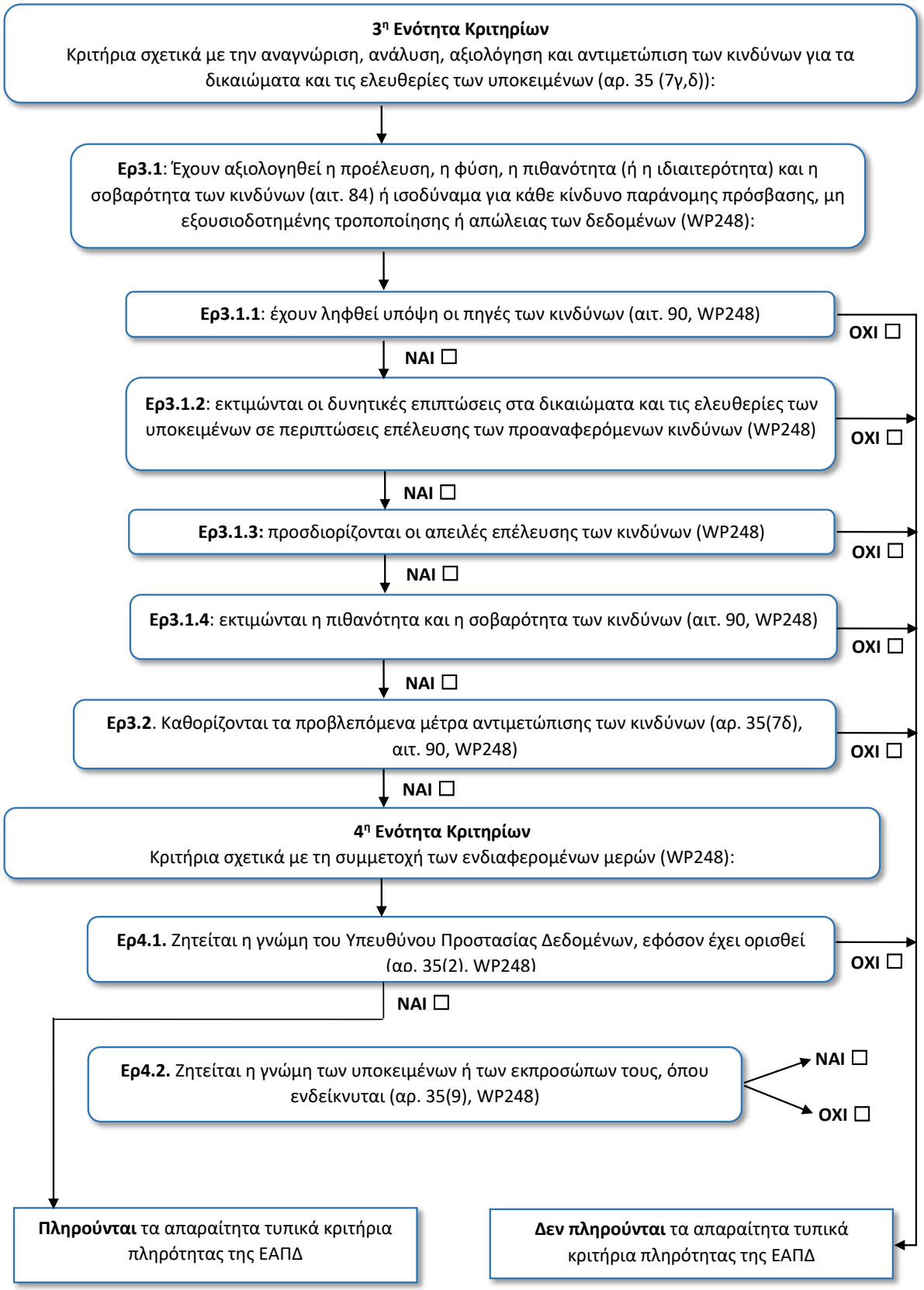
3.7.2 Έντυπο «Essential Standard Criteria – DPIA»

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα **Κηφισίας 1-3, Αμπελόκηποι, ΤΚ 115 23 Αθήνα** **Τηλ.:210 6475 600, Fax:210 6475628**	**http:// www.dpa.gr** **Email: contact@dpa.gr**

Πλαίσιο απαραίτητων τυπικών κριτηρίων πληρότητας της μελέτης εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ)
(αρ. 35 παρ. 2 και 7-9 του ΓΚΠΔ, κριτήρια των κατευθυντήριων γραμμών για την εκτίμηση αντικτύπου WP248)




2η Ενότητα Κριτηρίων
Κριτήρια αξιολόγησης της αναγκαιότητας και της αναλογικότητας της επεξεργασίας και των προβλεπόμενων μέτρων συμμόρφωσης με το ΓΚΠΔ:
Ερ2.1: Μέτρα συμμόρφωσης με τις αρχές και τη νομιμότητα της επεξεργασίας (WP248):
Ερ2.1.1: καθορισμένοι, ρητοί και νόμιμοι σκοποί επεξεργασίας (αρ. 5(1β), WP248)
Ερ2.1.2: νομιμότητα της επεξεργασίας (αρ. 6, WP248)
Ερ2.1.3: κατάλληλα, συναφή και περιορισμένα στα απολύτως αναγκαία για τους σκοπούς της επεξερνασίας δεδομένα (αρ. 5(1ν), WP248)
Ερ2.1.4: περιορισμένος χρόνος τήρησης των δεδομένων (αρ. 5(1ε), WP248)
Ερ2.2: Μέτρα σχετικά με τα δικαιώματα των υποκειμένων (WP248):
Ερ2.2.1: διαφανής ενημέρωση και δικαίωμα ενημέρωσης (αρ. 12-14, WP248)
Ερ2.2.2: δικαιώματα πρόσβασης και φορητότητας (αρ. 15, 20, WP248)
Ερ2.2.3: δικαιώματα διόρθωσης και διαγραφής (αρ. 16, 17, 19, WP248)
Ερ2.2.4: δικαιώματα εναντίωσης και περιορισμού της επεξεργασίας (αρ. 18, 19, 21, WP248)
Ερ2.2.5: σχέσεις με εκτελούντες την επεξεργασία (αρ. 28, WP248)
Ερ2.2.6: μέτρα προστασίας των διεθνών διαβιβάσεων (Κεφάλαιο V, WP248)
ΝΑΙ ☐
ΟΧΙ ☐
Μπορείτε να συνεχίσετε στις επόμενες ενότητες κριτηρίων
Δεν πληρούνται τα απαραίτητα τυπικά κριτήρια πληρότητας της ΕΑΠΔ


3η Ενότητα Κριτηρίων
Κριτήρια σχετικά με την αναγνώριση, ανάλυση, αξιολόγηση και αντιμετώπιση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων (αρ. 35 (7γ,δ)):
Ερ3.1: Έχουν αξιολογηθεί η προέλευση, η φύση, η πιθανότητα (ή η ιδιαιτερότητα) και η σοβαρότητα των κινδύνων (αιτ. 84) ή ισοδύναμα για κάθε κίνδυνο παράνομης πρόσβασης, μη εξουσιοδοτημένης τροποποίησης ή απώλειας των δεδομένων (WP248):
Ερ3.1.1: έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτ. 90, WP248)
ΟΧΙ ☐
ΝΑΙ ☐
Ερ3.1.2: εκτιμώνται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων σε περιπτώσεις επέλευσης των προαναφερόμενων κινδύνων (WP248)
ΟΧΙ ☐
ΝΑΙ ☐
Ερ3.1.3: προσδιορίζονται οι απειλές επέλευσης των κινδύνων (WP248)
ΟΧΙ ☐
ΝΑΙ ☐
Ερ3.1.4: εκτιμώνται η πιθανότητα και η σοβαρότητα των κινδύνων (αιτ. 90, WP248)
ΟΧΙ ☐
ΝΑΙ ☐
Ερ3.2. Καθορίζονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (αρ. 35(7δ), αιτ. 90, WP248)
ΟΧΙ ☐
ΝΑΙ ☐
4η Ενότητα Κριτηρίων
Κριτήρια σχετικά με τη συμμετοχή των ενδιαφερομένων μερών (WP248):
Ερ4.1. Ζητείται η γνώμη του Υπευθύνου Προστασίας Δεδομένων, εφόσον έχει ορισθεί (αρ. 35(2), WP248)
ΟΧΙ ☐
ΝΑΙ ☐
Ερ4.2. Ζητείται η γνώμη των υποκειμένων ή των εκπροσώπων τους, όπου ενδείκνυται (αρ. 35(9), WP248)
ΝΑΙ ☐
ΟΧΙ ☐
Πληρούνται τα απαραίτητα τυπικά κριτήρια πληρότητας της ΕΑΠΔ
Δεν πληρούνται τα απαραίτητα τυπικά κριτήρια πληρότητας της ΕΑΠΔ

3.8 Πολιτική Χαρτογράφησης Δεδομένων - Αρχείο Δραστηριοτήτων

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.08: ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός

Σκοπός της διαδικασίας είναι η περιγραφή της δημιουργίας και τήρησης του αρχείου δραστηριοτήτων από τον οργανισμό.

Η τήρηση του αρχείου δραστηριοτήτων είναι απαίτηση από τον Γενικό Κανονισμό Προστασίας Δεδομένων – GDPR 679/2016, άρθρο 30 §1.

Οι εργασίες δημιουργίας του αρχείου δεδομένων, αφορούν στην οργανωμένη συλλογή των απαιτούμενων πληροφοριών προκειμένου να χαρτογραφηθεί η ροή δεδομένων του οργανισμού. Η διαδικασία αυτή θα βοηθήσει τα στελέχη του οργανισμού να κατανοήσουν, αλλά και να συμμορφωθούν με τις απαιτήσεις του Κανονισμού και περιλαμβάνει:

- **καταγραφή των προσωπικών δεδομένων** που τηρεί, επεξεργάζεται και μεταβιβάζει ο οργανισμός,
- **ταξινόμηση και κατηγοριοποίηση δεδομένων** – περιπτώσεις ευαίσθητων προσωπικών δεδομένων, που παρουσιάζουν αυστηρότερες απαιτήσεις,
- **χαρτογράφηση δεδομένων** - προσδιορισμός του προσωπικού που έχει πρόσβαση στα προσωπικά δεδομένα, διαφύλαξη της ασφάλειας των δεδομένων, επαρκής εκπαίδευση του προσωπικού. Επιπλέον θα προσδιορίσει σημεία στις διαδικασίες του οργανισμού όπου τα δεδομένα μεταφέρονται σε άλλη, εκτελών την επεξεργασία οργανισμό,
- **αξιολόγηση των κινδύνων** – εκτίμηση πιθανών κινδύνων που συνδέονται με τις αρχές του GDPR, π.χ. δυνατότητες για μείωση του όγκου των δεδομένων.

Υποχρέωση τήρησης του αρχείου

Υπόχρεοι τήρησης του αρχείου είναι εταιρείες/οργανισμοί που ενεργούν ως υπεύθυνοι επεξεργασίας ή ως εκτελούντες την επεξεργασία. Η απαίτηση τήρησης αυτού δεν ισχύει για εταιρείες/οργανισμούς που απασχολούν λιγότερα από 250 άτομα, εκτός εάν 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 (άρθρο 9 §1 π.χ. δεδομένα για την υγεία). ή αφορά σε επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

Διαδικασία

Πληροφορίες που πρέπει να τηρούνται

Το Αρχείο Δραστηριοτήτων πρέπει να περιλαμβάνει τουλάχιστον τις εξής πληροφορίες:

- Την περιγραφή της κάθε δραστηριότητας του οργανισμού
- Τη νομική βάση της επεξεργασίας
- Τα στοιχεία του υπεύθυνου ή/και του εκτελούντος την επεξεργασία
- Το σκοπό της επεξεργασίας
- Τις κατηγορίες των υποκειμένων των δεδομένων

- Τις κατηγορίες των προσωπικών δεδομένων
- Τις κατηγορίες των αποδεκτών των προσωπικών δεδομένων
- Τη διαβίβαση σε τρίτες χώρα/ διεθνή οργανισμό (όπου συντρέχει)
- Την προθεσμία τήρησης και τον τρόπο διαγραφής των δεδομένων
- Τα τεχνικά και οργανωτικά μέτρα ασφάλειας

Συμπλήρωση εντύπου

Για κάθε αρχείο δραστηριότητας επεξεργασίας, συμπληρώνεται ένα έντυπο Ε.08.01 «Αρχείο Δραστηριοτήτων – Data Mapping», ή Εναλλακτικά το αρχείο Excel: Αρχείο_Δραστηριοτήτων_Επεξεργασίας_vX,X_IDNA Genomics

το οποίο περιέχει τουλάχιστον τα παρακάτω στοιχεία:

- **Αρχείο (Δραστηριότητα Επεξεργασίας).** Ονομασία αρχείου για την συγκεκριμένη δραστηριότητα.
- **Υπεύθυνος Επεξεργασίας (Ιδιότητα).** Υπεύθυνος επεξεργασίας είναι ο Νόμιμος Εκπρόσωπος.
- **Εκτελών την επεξεργασία.** Τα μέλη του προσωπικού που επεξεργάζονται τα προσωπικά δεδομένα του αρχείου.
- **Ποιοι έχουν πρόσβαση στα δεδομένα.** Αναφέρονται τα μέλη του προσωπικού ή τρίτοι που έχουν πρόσβαση στα δεδομένα χωρίς απαραίτητα να τα επεξεργάζονται.
- **Τρόπος Συλλογής Δεδομένων.** Ο τρόπος που συλλέγονται τα δεδομένα, π.χ. από τα ίδια τα υποκείμενα, από συνεργαζόμενους τρίτους ή μέσω προωθητικών ενεργειών κλπ.
- **Αποθήκευση Δεδομένων (πως / που).** Με ποιο τρόπο αποθηκεύονται τα ΠΔ και σε ποιο σημείο (αφορά έντυπα και ηλεκτρονικά ΠΔ)
- **Πληροφοριακά Συστήματα στα οποία καταχωρούνται.** Σε ποιες εφαρμογές καταχωρίζονται (π.χ. εφαρμογή μισθοδοσίας)
- **Σκοπός επεξεργασίας.** Για ποιο λόγο γίνεται η συλλογή και επεξεργασία των ΠΔ (π.χ. εκτέλεση μισθοδοσίας)
- **Νόμιμη Βάση Επεξεργασίας.** Καταγράφεται η νόμιμη βάση επεξεργασίας σύμφωνα τουλάχιστον με τα άρθρο 6 ή/και 9 του ΓΚΠΔ
- **Τρόπος απόδειξης συγκατάθεσης** (εφόσον η βάση για τη νομιμότητα είναι η συγκατάθεση)
- **Κατηγορίες Υποκειμένων.** Ποιους αφορούν τα προσωπικά δεδομένα που περιλαμβάνονται στο αρχείο που αναλύεται (π.χ. προσωπικό επιχείρησης, ασθενείς, πελάτες κ.λπ.)
- **Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα.** Ποιες κατηγορίες προσωπικών δεδομένων περιλαμβάνονται στο εν λόγω αρχείο (π.χ. ονοματεπώνυμο, ΑΦΜ, κλπ. ή δημογραφικά δεδομένα, φορολογικά δεδομένα κλπ, δεδομένα ειδικών κατηγοριών όπως δεδομένα υγείας, γενετικά και βιομετρικά δεδομένα.)

- **Κατηγορίες αποδεκτών προσωπικών δεδομένων.** Σε ποιους καταλήγουν τα ΠΔ για περαιτέρω επεξεργασία.
- **Διαβίβαση σε Τρίτες Χώρες.** Αναφέρεται εάν γίνεται διαβίβαση προσωπικών δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης (Εάν ναι να αναφέρεται η Νομική Βάση για τη διαβίβαση (σύμφωνα με άρθρα 45-49 του Κανονισμού))
- **Προβλεπόμενη Περίοδος Διαγραφής.** Ποιος είναι ο κύκλος ζωής τους, δηλαδή μετά από πόσο χρονικό διάστημα θεωρείται ότι δεν εξυπηρετούν το σκοπό της επεξεργασίας, οπότε και διαγράφονται
- **Τρόπος Διαγραφής / καταστροφής.** Αναφέρεται ο τρόπος με τον οποίο καταστρέφονται τα προσωπικά δεδομένα (φυσικής και ηλεκτρονικής μορφής)
- **Μέτρα Φυσικής Ασφάλειας.** Ποια μέτρα λαμβάνει η επιχείρηση για τη φυσική ασφάλεια του αρχείου ΠΔ που αναλύεται
- **Τεχνικά Μέτρα Ασφάλειας (ΙΤ).** Ποια τεχνικά μέτρα λαμβάνει η επιχείρηση για την ΙΤ ασφάλεια του αρχείου ΠΔ που αναλύεται
- Πραγματοποιείται **αυτοματοποιημένη λήψη αποφάσεων**, συμπεριλαμβανομένου προφίλ; (εάν έχει εφαρμογή)
- **Απαιτείται η διενέργεια εκτίμησης αντικτύπου** στην προστασία προσωπικών δεδομένων (ΕΑΠΔ);
- **Έχει λάβει χώρα περιστατικό παραβίασης** δεδομένων προσωπικού χαρακτήρα; Εάν ναι που είναι καταχωρημένο (σε ποιο αρχείο)
- **Ενημέρωση στα Υποκείμενα δεδομένων.** Πως ενημερώνονται τα υποκείμενα των δεδομένων για την τήρηση και επεξεργασία τους

Επικαιροποίηση εντύπου

Κατά τακτά χρονικά διαστήματα ανάλογα με τις αλλαγές οι οποίες επέρχονται στον τρόπο ή τους εμπλεκόμενους επεξεργασίας των προσωπικών δεδομένων, ο υπεύθυνος κάθε δραστηριότητας ανασκοπεί και επικαιροποιεί τα περιεχόμενα του εντύπου Ε.08.01 «Αρχείο Δραστηριοτήτων – Data Mapping».

Αρχεία και Δεδομένα

Ο Υπεύθυνος εκτέλεσης κάθε δραστηριότητας τηρεί τα έντυπα Ε.08.01 «Αρχείο Δραστηριοτήτων – Data Mapping» ή Excel:

Αρχείο_Δραστηριοτήτων_Επεξεργασίας_vX,X_IDNA Genomics

Η διάρκεια τήρησης του αρχείου είναι αόριστη.

3.8.1 Έντυπο «Αρχείο Δραστηριοτήτων»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ Ε.GDPR.08.01: «ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ – DATA MAPPING»**

Αρχείο(Δραστηριότητα Επεξεργασίας)		Ημερομηνία: ΧΧ/ΧΧ/ΧΧΧΧ Έκδοση: Χη
Υπεύθυνος Επεξεργασίας (Ιδιότητα)		
Τομέας Δραστηριότητας		
Νόμιμος εκπρόσωπος		
Μονάδα		
Υπεύθυνος αρχείου δραστηριότητας (Όνομα και στοιχεία επικοινωνίας)		
Από κοινού υπεύθυνος επεξεργασίας Όνομα και στοιχεία επικοινωνίας Σύμβαση άρθρου 26 (link)		
Εκτελών την επεξεργασία Όνομα και στοιχεία επικοινωνίας, Σύμβαση άρθρου 28 (link)		
Υπεύθυνος Προστασίας Δεδομένων		
Ποιοι έχουν πρόσβαση στα δεδομένα		
Τρόπος Συλλογής Δεδομένων (Πηγές των δεδομένων)		
Αποθήκευση Δεδομένων (πως / που / τύπος δεδομένων)		
Πληροφοριακά Συστήματα στα οποία καταχωρούνται		

Σκοπός επεξεργασίας	
Νόμιμη Βάση Επεξεργασίας	
Τρόπος απόδειξης συγκατάθεσης (εφόσον βάση για τη νομιμότητα είναι η συγκατάθεση)	
Κατηγορίες Υποκειμένων Δεδομένων	
Κατηγορίες Δεδομένων Προσωπικού Χαρακτήρα	
Κατηγορίες αποδεκτών προσωπικών δεδομένων	
Διαβίβαση Δεδομένων σε Τρίτη χώρα; (Εάν Ναι σε ποια;)	
Προβλεπόμενη περίοδος διαγραφής	
Τρόπος διαγραφής / καταστροφής	
Μέτρα Φυσικής Ασφάλειας	
Τεχνικά Μέτρα Ασφάλειας (IT) (link στην πολιτική ασφάλειας πληροφοριακών συστημάτων)	
Ενημέρωση στα Υποκείμενα δεδομένων (Πως γίνεται;)	
Απαιτείται διενέργεια εκτίμησης αντικτύπου (ΕΑΠΔ)?	
Εάν Ναι (στο παραπάνω) σε ποιο Στάδιο βρίσκεται η ΕΑΠΔ Link	
Έχει λάβει χώρα ποτέ περιστατικό παραβίασης ΔΠΧ; (Εάν ναι δώστε περισσότερα στοιχεία) (link σε αρχείο καταγραφής παραβίασης)	

3.9 Πολιτική Διαχείρισης Συμβάσεων

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.09: ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΣΕΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός

Αυτή η πολιτική έχει σχεδιαστεί για να καθορίσει τη διαδικασία διαχείρισης των Συμβάσεων που αφορούν στην Εμπιστευτικότητα αλλά και τη διαχείριση Προσωπικών Δεδομένων από τις διάφορες κατηγορίες συνεργατών του Υπευθύνου Επεξεργασίας όπως:

- Προσωπικό
- Συνεργάτες
- Εκτελούντες την Επεξεργασία βάσει του άρθρου 28 του Γενικού Κανονισμού Προστασίας Δεδομένων.

Δεδομένου ότι ο Υπεύθυνος Επεξεργασίας έχει ορίσει τους σκοπούς επεξεργασίας που διενεργεί κατά την κείμενη νομοθεσία, δεσμεύεται να ενεργεί σύμφωνα με τις αρχές που διέπουν την επεξεργασία κατά τον Γενικό Κανονισμό Προστασίας Δεδομένων, να προστατεύει και να σέβεται τα δικαιώματα των υποκειμένων.

Στο πλαίσιο της κανονιστικής συμμόρφωσης με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων της ΕΕ 2016/679 (ΓΚΠΔ) και της Εθνικής Νομοθεσίας, οι συνεργάτες του Υπευθύνου Επεξεργασίας θα πρέπει να δεσμεύονται με σύμβαση για την επεξεργασία των προσωπικών δεδομένων των υποκειμένων.

Πολιτική

Κάθε φορά που ο Υπεύθυνος Επεξεργασίας χρησιμοποιεί έναν εκτελούντα την Επεξεργασία θα πρέπει να υπάρχει μία υπογεγραμμένη σύμβαση (ή άλλο ισοδύναμο έγγραφο).

Η σύμβαση είναι σημαντική και για τα δύο μέρη γιατί καθορίζει τις ευθύνες και υποχρεώσεις τους.

Το άρθρο 28 του ΓΚΠΔ καθορίζει τι πρέπει να συμπεριληφθεί στη σύμβαση.

Εάν ένας εκτελών την επεξεργασία χρησιμοποιεί άλλον Οργανισμό, (δηλ. υπο-εκτελούντα την επεξεργασία), για να βοηθήσει στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για έναν Υπεύθυνο Επεξεργασίας πρέπει επίσης να έχει συνάψει γραπτή σύμβαση με τον υπο-εκτελούντα την επεξεργασία.

Τι πρέπει να περιληφθεί στη σύμβαση:

- Το αντικείμενο και η διάρκεια της επεξεργασίας
- Η φύση και ο σκοπός επεξεργασίας
- Το είδος των δεδομένων προσωπικού χαρακτήρα και οι κατηγορίες των υποκειμένων των δεδομένων
- Οι υποχρεώσεις και τα δικαιώματα του υπεύθυνου επεξεργασίας.

Οι συμβάσεις πρέπει επίσης να περιλαμβάνουν ειδικούς όρους όπως:

- Επεξεργασία πραγματοποιείται μόνο κατόπιν τεκμηριωμένων οδηγιών του Υπευθύνου Επεξεργασίας
- Εμπιστευτικότητα. Διασφάλιση αυτής με συμβατικά κείμενα ή κανονιστικούς όρους
- Κατάλληλα Οργανωτικά μέτρα ασφαλείας
- Τα δικαιώματα των υποκειμένων
- Υποχρέωση συνδρομής Εκτελούντος την Επεξεργασία προς τον Υπεύθυνο Επεξεργασίας από τους υπεργολάβους.
- Υποχρέωση συνδρομής Εκτελούντος την Επεξεργασία σε Επιθεωρήσεις και Ελέγχους
- Συνδρομή από τον υπεργολάβο για τη διενέργεια Διενέργειας Εκτίμησης Αντικτύπου (DPIA)
- Υποχρέωση επιστροφής ή διαγραφής των δεδομένων με τη λήξη της συνεργασίας.
- Διαβίβαση δεδομένων σε τρίτες χώρες.(εφόσον εφαρμόζεται)

Οι Υπεύθυνοι επεξεργασίας πρέπει να χρησιμοποιούν εκτελούντες οι οποίοι δίνουν σαφείς εγγυήσεις για τα τεχνικά και οργανωτικά μέτρα που μπορούν να λάβουν για την προστασία των δικαιωμάτων των υποκειμένων.

Οι Υπεύθυνοι επεξεργασίας είναι κυρίως υπεύθυνοι για τη συνολική συμμόρφωση με τον ΓΚΠΔ και για την απόδειξη της συμμόρφωσης. Αν αυτό δεν επιτευχθεί, ενδέχεται να είναι υπεύθυνοι για την καταβολή αποζημιώσεων σε δικαστικές διενέξεις ή να υπόκεινται σε πρόστιμα ή άλλες κυρώσεις.

Ένας Εκτελών την επεξεργασία δεν μπορεί να εμπλέξει υπηρεσίες υπο-εκτελούντα την επεξεργασία χωρίς προηγούμενη εξουσιοδότηση του Υπευθύνου επεξεργασίας. Εάν δοθεί η εξουσιοδότηση τότε ο εκτελών μπορεί να συνάψει σύμβαση με υπο-εκτελούντα (υπεργολάβο). Οι εκτελούντες την επεξεργασία παραμένουν υπεύθυνοι έναντι του Υπευθύνου την επεξεργασία για τη συμμόρφωση των υπεργολάβων τους.

Προκειμένου να καλυφθούν οι παραπάνω απαιτήσεις, αναπτύχθηκαν τα παρακάτω **σχέδια συμβάσεων**:

1. ΠΡΟΣΑΡΤΗΜΑ ΣΤΗΝ ΑΠΟ …/…/…… ΣΥΜΒΑΣΗ ΕΡΓΑΣΙΑΣ ΣΥΜΦΩΝΗΤΙΚΟ ΓΙΑ ΤΗΝ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

   (Υπογράφεται μεταξύ **του οργανισμού** και **προσωπικού** του συνδεόμενου με σύμβαση εργασίας ορισμένου ή αορίστου χρόνου)

2. ΠΡΟΣΑΡΤΗΜΑ: ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΗΝ ΑΠΟ……/201. ΣΥΜΒΑΣΗ («Κύρια Σύμβαση») ΜΕΤΑΞΥ **του οργανισμού** ΚΑΙ Τ……(«ο Συνεργάτης») ΜΕ ΑΝΤΙΚΕΙΜΕΝΟ ……..

(Υπογράφεται μεταξύ **του οργανισμού** και **συνεργατών**, φυσικών ή νομικών συνδεόμενων με **τον οργανισμό** με συμβάσεις παροχής υπηρεσιών ή έργου, οι οποίοι δεν έχουν την ιδιότητα του εκτελούντος την επεξεργασία)

3. Χρησιμοποιείται για τους εργαζόμενους είτε το a. είτε το Κείμενο ενημέρωσης b μαζί με το σχέδιο σύμβασης c
    a. ΠΡΟΣΑΡΤΗΜΑ: ΣΤΗΝ ΑΠΟ……/201. ΣΥΜΒΑΣΗ («Κύρια Σύμβαση») ΜΕΤΑΞΥ **του οργανισμού** ΚΑΙ τ……. ΕΚΤΕΛΟΥΝΤΟΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ
    b. Ενημέρωση για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα Εργαζομένων
    c. ΙΔΙΩΤΙΚΟ ΣΥΜΦΩΝΗΤΙΚΟ ΤΗΡΗΣΗΣ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑΣ (Confidentiality Agreement)

    (Υπογράφεται μεταξύ **του οργανισμού** και **συνεργατών**, φυσικών ή νομικών προσώπων συνδεόμενων με τον **οργανισμό** με συμβάσεις παροχής υπηρεσιών ή έργου, **οι οποίοι έχουν την ιδιότητα του εκτελούντος την επεξεργασία**)

4. Θα πρέπει να σημειωθεί ότι πέραν των ανωτέρω σχεδίων συμβάσεων – προσαρτημάτων ενδέχεται να προκύψει η ανάγκη κατάρτισης και περαιτέρω προσαρτημάτων που αφορούν στα προσωπικά δεδομένα. Ειδική περίπτωση αποτελεί αυτή της **από κοινού επεξεργασίας προσωπικών δεδομένων** μεταξύ υπευθύνων επεξεργασίας. Στην προκειμένη περίπτωση υπογράφεται **του οργανισμού** και φυσικών ή νομικών προσώπων σύμβαση που καθορίζει από κοινού τους σκοπούς και τα μέσα της επεξεργασίας. Τα παραπάνω προσαρτήματα - συντάσσονται αφού μελετηθεί η κάθε περίπτωση χωριστά.

Αρχεία και Δεδομένα

Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί το αρχείο, «**Αρχείο Συμβάσεων Επεξεργασίας Προσωπικών Δεδομένων**» όπου τηρούνται οι αντίστοιχες Συμβάσεις, και καταγράφονται στο αρχείο ***E-GDPR-09-01 «Μητρώο Εκτελούντων την Επεξεργασία»*** Η διάρκεια τήρησης του αρχείου αναφέρεται στα αρχεία δραστηριοτήτων.

3.9.1 Έντυπο «Μητρώο Εκτελούντων την Επεξεργασία»

Α/Α	Οργανωτική Μονάδα σχετική με την επεξεργασία	Επωνυμία Τρίτου μέρους (Εκτελούντος την Επεξεργασία ή Υποεκτελούντος την Επεξεργασία)	Στοιχεία επικοινωνίας Τρίτου μέρους (Εκτελούντος την Επεξεργασία ή Υποεκτελούντος την Επεξεργασία)	Ρόλος Τρίτου μέρους (Εκτελούντος την Επεξεργασία ή Υποεκτελούντος την Επεξεργασία)	Στοιχεία επικοινωνίας DPO Τρίτου μέρους (Εκτελούντος την Επεξεργασία ή Υποεκτελούντος την Επεξεργασία)	Σύνδεσμος (Link) στη σύμβαση	Status σύμβασης	Αντικείμενο σύμβασης/Κατηγορίες επεξεργασίας	Γλώσσα σύμβασης	Τοποθεσία εκτελούντος (ΕΕ, ΕΟΧ, εκτός ΕΟΧ)	Επωνυμία Εγκεκριμένων υπεργολάβων/ υπο-εκτελούντων του τρίτου μέρους από την Εταιρεία	Στοιχεία επικοινωνίας υπεργολάβων/υπο-εκτελούντων του τρίτου μέρους από την Εταιρεία
1				Εκτελών			Ενεργή		Ελληνικά			
2				Εκτελών			Ανενεργή		Αγγλικά			

3.9.2 Προσάρτημα Σύμβασης «Εκτελούντος την Επεξεργασία»

ΣΥΜΦΩΝΗΤΙΚΟ ΠΕΡΙ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΜΕΤΑΞΥ ΤΗΣ «.....» ΩΣ ΥΠΕΥΘΥΝΟΥ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΤΟΥ ΣΥΝΕΡΓΑΤΗ ..... ΩΣ ΕΚΤΕΛΟΥΝΤΟΣ ΕΠΕΞΕΡΓΑΣΙΑ

ΠΡΟΣΑΡΤΗΜΑ ΣΤΗΝ ΑΠΟ ..... ΣΥΜΒΑΣΗ

Τόπος ..../.../202..

Στο πλαίσιο κανονιστικής συμμόρφωσης με τις απαιτήσεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων της ΕΕ 2016/679 (ΓΚΠΔ) και της Εθνικής Νομοθεσίας, όπως εκάστοτε ισχύει, το παρόν συμφωνητικό ενσωματώνεται ως Προσάρτημα στην από ..... σύμβαση παροχής υπηρεσιών (ΑΝΤΙΚΕΙΜΕΝΟ ΑΥΤΗΣ) (εφεξής η «κύρια σύμβαση») μεταξύ:

α) αφενός μεν της εταιρίας «.....» και το διακριτικό τίτλο «.....», που εδρεύει στην ..... Αττικής, ..., με Α.Φ.Μ. ....., Δ.Ο.Υ. .....όπως νόμιμα εκπροσωπείται, (στο εξής ο «Υπεύθυνος Επεξεργασίας» - ΥΕ) και

β) αφετέρου της εταιρίας με την επωνυμία..... Δ/νση ..... με ΑΦΜ ..... ΔΟΥ ....., όπως νόμιμα εκπροσωπείται (στο εξής ο «Εκτελών Επεξεργασία» - ΕτΕ).

ΟΡΙΣΜΟΙ:

Προσωπικά δεδομένα: είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα άτομο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο) στο οποίο αναφέρονται τα δεδομένα ονομάζεται υποκείμενο των δεδομένων.

Επεξεργασία δεδομένων προσωπικού χαρακτήρα: κάθε πράξη ή σειρά πράξεων που σχετίζεται με δεδομένα 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.

Υπεύθυνος Επεξεργασίας: το φυσικό ή νομικό πρόσωπο το οποίο καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας των προσωπικών Δεδομένων.

Εκτελών την επεξεργασία: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας.

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

ΠΡΟΟΙΜΙΟ

Δεδομένου ότι ο Υπεύθυνος Επεξεργασίας έχει ορίσει τους σκοπούς επεξεργασίας που διενεργεί κατά την κείμενη νομοθεσία, δεσμεύεται να ενεργεί σύμφωνα με τις αρχές που διέπουν την επεξεργασία κατά τον Γενικό Κανονισμό Προστασίας Δεδομένων, να προστατεύει και να σέβεται τα δικαιώματα του υποκειμένου. Αναλυτικότερα, η Πολιτική Ιδιωτικότητας του Υπεύθυνου Επεξεργασίας έχει δημοσιευτεί στην ιστοσελίδα του https://.....com/.

Δεδομένου ότι μεταξύ των εδώ συμβαλλομένων έχει υπογραφεί η από ..... σύμβαση παροχής υπηρεσιών ....., δυνάμει ή εξ' αφορμής της οποίας ο Εκτελών την Επεξεργασία αποκτά ή ενδέχεται να αποκτήσει πρόσβαση και να επεξεργαστεί προσωπικά δεδομένα που τηρεί ο Υπεύθυνος Επεξεργασίας.

Δεδομένου ότι βάσει του άρθρου 28 του ΓΚΠΔ απαιτείται να συναφθεί το παρόν συμφωνητικό, συνημμένο υπ' αριθ. 1 του οποίου αποτελεί το Παράρτημα στοιχείων Επεξεργασίας Δεδομένων.

Δια του παρόντος συμφωνήθηκαν και έγιναν αποδεκτά τα ακόλουθα:

ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ – ΥΠΟΧΡΕΩΣΕΙΣ ΕΤΕ

1. Ο ΕτΕ θα συμμορφώνεται πλήρως με τις προβλέψεις του Γενικού Κανονισμού Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ) ΕΕ 2016/679, όπως αυτός ενσωματώνεται στο εθνικό δίκαιο και εκάστοτε ισχύει, και θα εφαρμόζει τις αρχές προστασίας προσωπικών δεδομένων, όπως ενδεικτικά τις αρχές νομιμότητας, αντικειμενικότητας και διαφάνειας, ακεραιότητας, εμπιστευτικότητας, λογοδοσίας.
2. Ο ΕτΕ επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας.
3. Ο ΕτΕ θα επεξεργάζεται τα προσωπικά δεδομένα ως Εμπιστευτικές Πληροφορίες. Η επεξεργασία δε, περιορίζεται στο βαθμό που απαιτείται για την προσήκουσα εκπλήρωση της κύριας σύμβασης.
4. Ο ΕτΕ υποχρεούται να τηρεί μυστικούς τους όρους και τις συμφωνίες του παρόντος, καθώς και κάθε πληροφορία ή εμπορικά και επαγγελματικά μυστικά

του ΥΕ, που θα περιέλθουν σε γνώση του από την εκτέλεση της μεταξύ τους κύριας σύμβασης, και οφείλει να μην αποκαλύπτει τέτοιες πληροφορίες σε τρίτους.

5. Ο ΕτΕ δεσμεύεται και εγγυάται ότι θα λάβει κάθε πρόσφορο μέτρο προκειμένου το προσωπικό του και κάθε συνεργαζόμενος με αυτόν ή καθ' οιονδήποτε τρόπο αναμειγνυόμενος άμεσα ή έμμεσα με την εκτέλεση του παρόντος, θα τηρούν την υποχρέωση εχεμύθειας προς τον ΥΕ και παράλληλα δεσμεύεται ότι τα προαναφερόμενα άτομα τελούν σε πλήρη γνώση των υποχρεώσεων του ΕτΕ που απορρέουν από το παρόν και ότι αναλαμβάνουν **τις ίδιες υποχρεώσεις** όπως αυτές ορίζονται στο παρόν.

6. Ο ΕτΕ συνδράμει τον ΥΕ στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36 του ΓΚΠΔ, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία

7. Ο ΕτΕ κατ' επιλογή του ΥΕ, διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον ΥΕ μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός εάν το δίκαιο της Ένωσης ή του κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα.

ΥΠΕΡΓΟΛΑΒΟΣ

8. Οι τυχόν υπεργολάβοι του ΕτΕ μπορούν να αναλάβουν έργο, υπηρεσία, εντολή που αφορούν στην κύρια σύμβαση, μόνο μετά από προηγούμενη άδεια του ΥΕ. Σε περίπτωση μη παροχής της ανωτέρω άδειας εκ μέρους του Υε, απαγορεύεται οποιαδήποτε ανάθεση έργου, υπηρεσίας, εντολής από τον ΕτΕ σε υπεργολάβο.

9. Κατά την περίπτωση στην οποία έχει συμφωνηθεί εγγράφως η επεξεργασία από υπεργολάβο, ο ΕτΕ υποχρεούται στη σύναψη συμφωνητικού μεταξύ του και του υπεργολάβου, το οποίο θα διασφαλίζει ότι ο υπεργολάβος θα υποκαθίσταται στο σύνολο των δικαιωμάτων και υποχρεώσεων του ΕτΕ.

10. Η εκτέλεση επεξεργασίας από υπεργολάβο -για τον οποίο έχει συμφωνήσει ο ΥΕ- δεν ασκεί καμία επιρροή επί της ευθύνης του ΕτΕ για πράξεις ή παραλείψεις του υπεργολάβου σε σχέση με τον ΕτΕ στο πλαίσιο της εκτέλεσης του παρόντος.

ΥΠΟΚΕΙΜΕΝΑ ΔΕΔΟΜΕΝΩΝ

11. Ο ΥΕ υποχρεούται να παρέχει στα υποκείμενα των δεδομένων πληροφόρηση αναφορικά με την επεξεργασία προσωπικών δεδομένων, όπως επίσης αναφορικά με την εξασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων, σύμφωνα με το ισχύον νομοθετικό πλαίσιο (ειδικότερα αναφορικά με τα δικαιώματα πρόσβασης, φορητότητας, διόρθωσης και διαγραφής).

12. Σε εκτέλεση της υποχρέωσης της ανωτέρω παραγράφου, ο ΕτΕ θα παρέχει στον ΥΕ το σύνολο των αιτουμένων πληροφοριών, ή θα προβαίνει στην παροχή, τροποποίηση ή διαγραφή των προσωπικών δεδομένων αναλόγως του σχετικού αιτήματος του υποκειμένου των προσωπικών δεδομένων προς τον ΥΕ.

ΑΣΦΑΛΕΙΑ

13. Ο ΕτΕ δηλώνει ρητώς και εγγυάται ότι δεν θα προβαίνει σε επεξεργασία, συλλογή, αποθήκευση, χρήση, διαβίβαση ή κάθε άλλη μορφή διάθεσης δεδομένων προσωπικού χαρακτήρα με οποιονδήποτε τρόπο πέραν των σκοπών που έχει ορίσει ο ΥΕ.

14. Ο ΕτΕ δηλώνει ρητώς ότι στο πλαίσιο των αρχών της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας, θα λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την ασφάλεια των προσωπικών δεδομένων, καθώς και για την προστασία τους από τυχαία ή αθέμιτη καταστροφή, απώλεια, αλλοίωση, απαγορευμένη διάδοση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

15. Ο ΕτΕ οφείλει να τηρεί κατάλληλα αρχεία για κάθε επεξεργασία προσωπικών Δεδομένων, όπως Αρχεία Δραστηριοτήτων, σύμφωνα με το άρθρο 30 του ΓΚΠΔ.

16. Ο ΕτΕ δεσμεύεται να σεβαστεί την Πολιτική Ιδιωτικότητας του ΥΕ, καθώς και το Σύστημα Πολιτικής Ασφάλειας Πληροφοριών του ΥΕ, τα οποία έχουν έλθει σε γνώση του.

17. Ο ΕτΕ δεσμεύεται να προσαρμοστεί στις συνολικές κανονιστικές απαιτήσεις του ΓΚΠΔ (συμμόρφωση προς διεθνή πρότυπα ασφάλειας, δημιουργία μητρώου επεξεργασιών και πολιτικών διαχείρισης δεδομένων, ορισμός Υπευθύνου Προστασίας Δεδομένων, εφόσον απαιτείται κλπ.), καθώς και να αποδέχεται ελέγχους συμμόρφωσης (compliance audits) από τον ΥΕ μετά από προηγούμενη έγγραφη ενημέρωση ενός (1) μηνός.

ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ

18. Απαγορεύεται καταρχήν η διαβίβαση προσωπικών δεδομένων που ο ΕτΕ κατέχει, συλλέγει ή επεξεργάζεται κατά την παροχή των υπηρεσιών στο πλαίσιο της κύριας σύμβασης ή επ' ευκαιρία αυτής.

19. Ο ΕτΕ μπορεί να προβεί σε αποκάλυψη/διαβίβαση πληροφοριών μόνο:
    1.1. όταν υποχρεούται σε αυτό εκ του νόμου ενώπιον δημοσίων αρχών, οι οποίες μπορεί να τις απαιτήσουν νομίμως. Στην περίπτωση αυτή, εάν δεν υπάρχει άλλο νομικό κώλυμα, ο ΕτΕ οφείλει να ενημερώσει εντός 24 ωρών τον ΥΕ για την υποχρέωσή του αυτή.
    1.2. σε υπεργολάβο ή φορέα που συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ όταν διαθέτει ρητή έγγραφη έγκριση του ΥΕ.

ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΛΛΑΔΑΣ

20. Ο ΕτΕ οφείλει να μην επεξεργάζεται Προσωπικά Δεδομένα εκτός του Ευρωπαϊκού Οικονομικού Χώρου χωρίς την προηγούμενη έγγραφη συγκατάθεση του ΥΕ και, όπου παρέχεται η συγκατάθεση αυτή σε μια τέτοια διαβίβαση, να συμμορφώνεται με τις διατάξεις του παρόντος άρθρου και των Τυποποιημένων Συμβατικών Ρητρών.

ΑΝΑΦΟΡΑ ΠΕΡΙΣΤΑΤΙΚΩΝ ΑΣΦΑΛΕΙΑΣ

21. Ο ΕτΕ οφείλει: i) να ενημερώσει τον ΥΕ αμέσως μόλις αντιληφθεί την εμφάνιση οποιουδήποτε περιστατικού που επέφερε ή είναι λογικά πιθανό να επιφέρει παραβίαση της ασφάλειας, συμπεριλαμβανομένης οποιασδήποτε τυχαίας ή παράνομης απώλειας, κλοπής, διαγραφής, αποκάλυψης ή παραποίησης Προσωπικών Δεδομένων ή/ και οποιασδήποτε μη εξουσιοδοτημένης χρήσης ή πρόσβασης σε Προσωπικά Δεδομένα (εφεξής το «Περιστατικό Ασφαλείας»), ii) να παρέχει κάθε συνεργασία και πληροφόρηση που θα ζητηθεί από τον ΥΕ, σε σχέση με το Περιστατικό Ασφαλείας, το συντομότερο δυνατόν και σε κάθε περίπτωση εντός 24 ωρών από την λήψη γνώσης του Περιστατικού Ασφαλείας, συμπεριλαμβάνοντας:
    1.1. όλες τις λεπτομέρειες του Περιστατικού Ασφαλείας, συμπεριλαμβανομένων των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών Υποκειμένων Δεδομένων,

1.2. πλήρη στοιχεία των Προσωπικών Δεδομένων που τέθηκαν σε κίνδυνο, συμπεριλαμβανομένων των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών αρχείων Προσωπικών Δεδομένων,

1.3. όπου αυτό είναι γνωστό, λεπτομέρειες των πιθανών συνεπειών του Περιστατικού Ασφαλείας,

1.4. πλήρεις λεπτομέρειες σχετικά με τον τρόπο, με τον οποίο διερευνάται το Περιστατικό Ασφαλείας, καθώς και μέτρα για τη μείωση και την αποκατάσταση που έχουν ήδη τεθεί σε εφαρμογή και πρέπει να τεθούν σε εφαρμογή.

ΝΟΜΙΚΗ ΕΥΘΥΝΗ ΕΚΤΕΛΟΥΝΤΟΣ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ

22. Ο ΕτΕ ευθύνεται πλήρως έναντι του ΥΕ και υποχρεούται να τον αποζημιώσει πλήρως για κάθε θετική ή αποθετική ζημία που του προκάλεσε με πράξεις ή παραλείψεις του, είτε εκ δόλου είτε εξ αμελείας.

1. Στην ως άνω περίπτωση, ο ΕτΕ υποχρεούται να καλύψει, ενδεικτικά και όχι περιοριστικά, τυχόν διοικητικά πρόστιμα που επιβλήθηκαν εξαιτίας του στον ΥΕ μετά από ελέγχους των Εποπτικών Αρχών, αποζημιώσεις που ο ΥΕ τυχόν κατέβαλε μετά από αγωγές πελατών ή τρίτων, την αξία απολεσθέντων δεδομένων, το κόστος από τυχόν αναστολή εργασιών, το κόστος από απώλεια φήμης ή περιουσίας, την ηθική βλάβη, καθώς και όποια άλλη βλάβη τυχόν ο ΥΕ υπέστη στο πλαίσιο της κύριας σύμβασης ή επ' ευκαιρία αυτής, εκτός αν αποδείξει ότι η ευθύνη βαρύνει αποκλειστικά τον ΥΕ, οπότε ο ΕτΕ απαλλάσσεται.

2. Ο ΥΕ δικαιούται σε περίπτωση παραβιάσεως των υποχρεώσεων που απορρέουν από την παρούσα σε καταγγελία της κύριας σύμβασης ακόμα και χωρίς την καταβολή αποζημιώσεως.

ΔΙΑΡΚΕΙΑ ΤΗΣ ΣΥΜΒΑΣΗΣ

23. Η παρούσα ισχύει καθ' όλη τη διάρκεια ισχύος της κύριας σύμβασης μεταξύ ΥΕ και ΕτΕ, οι δε απορρέουσες υποχρεώσεις και δικαιώματα θα συνεχίσουν να ισχύουν και μετά την καθ' οιονδήποτε τρόπο λύση ή λήξη αυτής.

24. Κατά τη λήξη μη λύση της κύριας σύμβασης με οποιονδήποτε τρόπο, ο ΕτΕ υποχρεούται να επιστρέψει στον ΥΕ οποιοδήποτε υλικό έχει στην κατοχή του και έχει αποκτήσει κατά την παροχή ή επ' αφορμή παροχής των υπηρεσιών του, καθώς και σημειώσεις ή υπομνήματα και άλλα έγγραφα ή μέσα μαγνητικής αποτύπωσης που ανήκουν ή αφορούν στον ΥΕ, ιδιαίτερα όσα περιέχουν Εμπιστευτικές Πληροφορίες και Δεδομένα Προσωπικού Χαρακτήρα.

Η παρούσα συνετάχθη σε δύο (2) πρωτότυπα και κάθε μέρος, αφού τα υπέγραψε, έλαβε από ένα.

ΟΙ ΣΥΜΒΑΛΛΟΜΕΝΟΙ

ΥΠΕΥΘΥΝΟΣ ΕΠΕΞΕΡΓΑΣΙΑΣ **ΕΚΤΕΛΩΝ ΕΠΕΞΕΡΓΑΣΙΑ**

ΣΥΝΗΜΜΕΝΟ 1

Παράρτημα Στοιχείων Επεξεργασίας Δεδομένων

Το Παράρτημα αποτελεί μέρος του Προσαρτήματος και πρέπει να συμπληρωθεί από τα μέρη

Υπεύθυνος Επεξεργασίας

……..

Εκτελών την Επεξεργασία

Ο εκτελών την επεξεργασία είναι:

……

……

Φύση, σκοπός και αντικείμενο Επεξεργασίας (εάν δεν προβλέπονται στην κύρια σύμβαση)

……

Υποκείμενα των Δεδομένων

Τα Προσωπικά Δεδομένα που υπόκεινται σε επεξεργασία αφορούν τις ακόλουθες κατηγορίες υποκειμένων των δεδομένων (παρακαλούμε διευκρινίστε):

1. Εργαζόμενοι (Ενδεικτικά)
2. Ασθενείς (Ενδεικτικά)

Κατηγορίες Δεδομένων

Τα Προσωπικά Δεδομένα που υπόκεινται σε επεξεργασία αφορούν τις ακόλουθες κατηγορίες δεδομένων (παρακαλούμε διευκρινίστε):

1. Στοιχεία Επικοινωνίας και Ταυτότητας (Ενδεικτικά)
2. Στοιχεία μισθολογικής κατάστασης (Ενδεικτικά)

Ειδικές Κατηγορίες Δεδομένων (εφόσον απαιτείται)

Τα Προσωπικά Δεδομένα που υπόκεινται σε επεξεργασία αφορούν τις ακόλουθες ειδικές κατηγορίες δεδομένων (παρακαλούμε διευκρινίστε):

3.9.3 Προσάρτημα Σύμβασης «Εξωτερικού Συνεργάτη»

ΠΡΟΣΑΡΤΗΜΑ
ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ
ΣΤΗΝ ΑΠΟ……/201. ΣΥΜΒΑΣΗ («Κύρια Σύμβαση»)
ΜΕΤΑΞΥ ΤΗΣ «……» με δ.τ.
«……» ΚΑΙ Τ……(«ο Συνεργάτης») ΜΕ
ΑΝΤΙΚΕΙΜΕΝΟ ……

Στο πλαίσιο εκτέλεσης της κύριας σύμβασης, αλλά και σύμφωνα με τις υποχρεώσεις που απορρέουν από τον νόμο, ο Συνεργάτης υποχρεούται να τηρεί εχεμύθεια σχετικά με όλες τις εμπιστευτικές πληροφορίες της «ΧΧΧ» που έρχονται σε γνώση του κατά την παροχή ή με αφορμή την παροχή των υπηρεσιών του προς την «ΧΧΧ».

Ο Συνεργάτης, στο πλαίσιο της κύριας σύμβασης του με την «ΧΧΧ», έχει τη δυνατότητα πρόσβασης και διακίνησης ιδιαίτερα ευαίσθητων πληροφοριών σχετικών με την δραστηριότητα της «ΧΧΧ». Συγκεκριμένα, ο Συνεργάτης βρίσκεται σε θέση να λαμβάνει γνώση και έχει δυνατότητα πρόσβασης και διακίνησης πληροφοριών που σχετίζονται με εμπιστευτικές πληροφορίες, μεταξύ των οποίων περιλαμβάνονται και δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων, η προστασία των οποίων εμπίπτει στο πεδίο εφαρμογής του Γενικού Κανονισμού ΕΕ 679/2016, καθώς και των λοιπών κανονισμών και νόμων που εκάστοτε ισχύουν για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Για αυτό τον λόγο, αμφότερα τα μέρη κρίνουν απαραίτητο όπως προβούν στη σύναψη της παρούσας ιδιαίτερης συμφωνίας σχετικά με τις υποχρεώσεις του Συνεργάτη σε σχέση με τις εμπιστευτικές πληροφορίες της «ΧΧΧ» ή των δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων της «ΧΧΧ», των συναλλασσόμενων με αυτήν καθώς και των χρηστών των υπηρεσιών της, στα οποία τυχόν έχει πρόσβαση ή των οποίων λαμβάνει γνώση ή/και διακινεί.

Ο Συνεργάτης δηλώνει ότι κατανοεί τη σημασία που έχει για την «ΧΧΧ» η εχεμύθεια και η σωστή διαχείριση των κατά τα ανωτέρω Εμπιστευτικών Πληροφοριών και δεδομένων προσωπικού χαρακτήρα.

ΟΡΙΣΜΟΙ

Εμπιστευτική Πληροφορία: θεωρείται οποιαδήποτε πληροφορία ή δεδομένο, που έρχεται σε γνώση του Συνεργάτη είτε με έγγραφο, είτε προφορικά είτε με ηλεκτρονικό ή με οποιονδήποτε τρόπο, κατά τη διάρκεια της παροχής των υπηρεσιών του ή επ' ευκαιρία και με

αφορμή αυτήν, και αφορά είτε την «ΧΧΧ» είτε τα στελέχη αυτής είτε τους συναλλασσόμενους με αυτήν καθώς και τους χρήστες των υπηρεσιών της (φυσικά ή νομικά πρόσωπα).

Ο Συνεργάτης υποχρεούται να θεωρεί ως εμπιστευτική οποιαδήποτε πληροφορία, σύμφωνα με τα ανωτέρω, ανεξαρτήτως σοβαρότητας ή μη αυτής. Ως εμπιστευτικές θεωρούνται ενδεικτικά κι όχι περιοριστικά οι κάτωθι πληροφορίες για την «ΧΧΧ»: τα επιχειρησιακά του σχέδια, οι συναλλαγές, η υπογραφή συμβάσεων κάθε φύσεως, η οικονομική κατάσταση της «ΧΧΧ», οι τεχνικές γνώσεις, το know – how, οι πληροφορίες σχετικά με το προσωπικό της «ΧΧΧ», σχετικά με τους προμηθευτές της «ΧΧΧ», τους όρους διενέργειας των προμηθειών, τον αριθμό, τα ονόματα και τις σχέσεις της «ΧΧΧ» με συναλλασσόμενους με αυτήν ή με τους χρήστες των υπηρεσιών της, τις διαπραγματεύσεις για συναλλαγές της «ΧΧΧ» ή την πρόσληψη προσωπικού κ.λ.π.

Εμπιστευτική πληροφορία, τέλος, χαρακτηρίζεται κάθε πληροφορία, της οποίας η διαρροή ενδέχεται να βλάψει τα συμφέροντα και τη φήμη της «ΧΧΧ» ή του προσωπικού της ή τα δικαιώματα τρίτων συναλλασσόμενων με την «ΧΧΧ» ή χρηστών των υπηρεσιών της. Τέλος εμπιστευτική πληροφορία χαρακτηρίζονται και τα προσωπικά δεδομένα (βλέπε κατωτέρω).

Μία εμπιστευτική κατά τα ανωτέρω πληροφορία παύει να θεωρείται εμπιστευτική από τη στιγμή που η «ΧΧΧ» προβαίνει και στον βαθμό που προβαίνει σε επίσημη ανακοίνωσή της, η ρύθμιση αυτή ωστόσο δεν ισχύει όσον αφορά στα προσωπικά δεδομένα (βλέπε κατωτέρω).

Προσωπικά Δεδομένα : είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα φυσικό πρόσωπο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο), στο οποίο αναφέρονται τα δεδομένα, ονομάζεται υποκείμενο των δεδομένων.

Ευαίσθητα Προσωπικά Δεδομένα ή ειδικών κατηγοριών: χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια, στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα παραπάνω δεδομένα τυχόν εργαζομένων, ή συνεργατών ή συναλλασσόμενων με την «ΧΧΧ», καθώς και των χρηστών των υπηρεσιών της, όπως αυτά καθορίζονται από τον Γενικό Κανονισμό ΕΕ 2016/679 (όπως αυτός θα ενσωματωθεί στο εθνικό δίκαιο περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα), θεωρούνται εμπιστευτικές πληροφορίες για την «ΧΧΧ».

ΥΠΟΧΡΕΩΣΕΙΣ ΣΥΝΕΡΓΑΤΗ

1.α. Υποχρέωση διαχείρισης της εμπιστευτικής πληροφορίας με ιδιαίτερη επιμέλεια
Ο Συνεργάτης υποχρεούται να διαχειρίζεται κάθε Εμπιστευτική Πληροφορία με απόλυτη εχεμύθεια, λαμβάνοντας με ιδιαίτερη επιμέλεια κάθε αναγκαίο μέτρο για την προστασία της (ενδεικτικά την αποθήκευσή της σε κλειδωμένο χώρο ή αν η αποθήκευση γίνεται ηλεκτρονικά με ειδικό κωδικό) και να μην παρέχει πρόσβαση σε κανένα πρόσωπο που δεν είναι ειδικά εξουσιοδοτημένο.
Ο Συνεργάτης υποχρεούται να χρησιμοποιεί την Εμπιστευτική Πληροφορία αποκλειστικά και μόνο για τον σκοπό που αυτή αποκαλύφθηκε σε αυτόν και στον βαθμό που είναι αναγκαίο για την εκτέλεση της κύριας σύμβασης.

Απαγορεύεται στον Συνεργάτη να προβαίνει σε εμπορική χρήση της εμπιστευτικής πληροφορίας ή να την χρησιμοποιεί προς όφελός του.

Απαγορεύεται στο Συνεργάτη να αντιγράφει ή να φωτοτυπεί ή να εξάγει την Εμπιστευτική Πληροφορία ή τμήμα αυτής, χωρίς ειδική άδεια της «ΧΧΧ», εκτός αν αυτό είναι απολύτως απαραίτητο για την εκπλήρωση του σκοπού για τον οποίο του αποκαλύφθηκε η Εμπιστευτική Πληροφορία.

Ο Συνεργάτης θα χρησιμοποιήσει τυχόν λογισμικό που θα του παραχωρηθεί για την παροχή των υπηρεσιών του και σε καμία περίπτωση δεν θα το χρησιμοποιήσει για την μεταφορά δεδομένων ή γενικότερα στοιχείων που αποτελούν περιουσιακό στοιχείο της «ΧΧΧ» εκτός της «ΧΧΧ» ή εκτός συστημάτων της «ΧΧΧ» και χωρίς την πρότερη έγγραφη έγκρισή της.

Διευκρινίζεται ότι η εχεμύθεια και εμπιστευτικότητα στη διαχείριση της πληροφορίας πρέπει να τηρείται όχι μόνο προς πρόσωπα τρίτα με την «ΧΧΧ», αλλά και προς πρόσωπα εντός της «ΧΧΧ» που δεν είναι εξουσιοδοτημένα να έχουν πρόσβαση στην Εμπιστευτική Πληροφορία.

Σε περίπτωση που ο Συνεργάτης υποχρεωθεί από δικαστική ή αστυνομική αρχή να αποκαλύψει σύμφωνα με το νόμο την Εμπιστευτική Πληροφορία, υποχρεούται όπως ενημερώσει εκ των προτέρων και σε κάθε περίπτωση την επομένη εργάσιμη ημέρα την «ΧΧΧ», εκτός κι αν αυτό απαγορεύεται βάσει διατάξεως νόμου.

1.β. Υποχρεώσεις αναφορικά με προσωπικό και συνεργάτες

Ο Συνεργάτης υποχρεούται να ενημερώνει το προσωπικό ή τους προστηθέντες του, τους συνεργάτες ή/και και υπεργολάβους του, στους οποίους έχει αναθέσει την εκτέλεση των υποχρεώσεών του που προκύπτουν από την κύρια σύμβαση, σχετικά με τις υποχρεώσεις που απορρέουν από το παρόν, και να προβεί στο σύνολο των αναγκαίων κατά την κρίση του μέτρων με σκοπό τη διασφάλιση από τα πρόσωπα αυτά των όρων του παρόντος.

1.γ. Επιπρόσθετες υποχρεώσεις για τα προσωπικά δεδομένα

Ο Συνεργάτης δεσμεύεται να σεβαστεί την Πολιτική Ιδιωτικότητας της «ΧΧΧ», καθώς και το Σύστημα Ασφάλειας Πληροφοριών αυτής, τα οποία έχουν έλθει σε γνώση του, υποχρεούται, δε, να ενημερώσει άμεσα την «ΧΧΧ» για τυχόν εκ μέρους του αντιρρήσεις ή επιφυλάξεις του αναφορικά με την εφαρμογή τους.

Ο Συνεργάτης δεσμεύεται να μην προβαίνει σε καμία επεξεργασία προσωπικών δεδομένων χωρίς προηγούμενη εντολή της «ΧΧΧ».

Ο Συνεργάτης οφείλει: i) να ενημερώσει την «ΧΧΧ» αμέσως μόλις αντιληφθεί την εμφάνιση οποιουδήποτε περιστατικού που επέφερε ή είναι λογικά πιθανό να επιφέρει παραβίαση της ασφάλειας, συμπεριλαμβανομένης οποιασδήποτε τυχαίας ή παράνομης απώλειας, κλοπής, διαγραφής, αποκάλυψης ή παραποίησης Προσωπικών Δεδομένων ή/ και οποιασδήποτε μη εξουσιοδοτημένης χρήσης ή πρόσβασης σε Προσωπικά Δεδομένα (εφεξής το «Περιστατικό Ασφαλείας»), ii) να παρέχει κάθε συνεργασία και πληροφόρηση που θα ζητηθεί από την «ΧΧΧ» σε σχέση με το Περιστατικό Ασφαλείας το συντομότερο δυνατόν και σε κάθε περίπτωση εντός 24 ωρών από την γνώση του Περιστατικού Ασφαλείας, συμπεριλαμβάνοντας:

- όλες τις λεπτομέρειες του Περιστατικού Ασφαλείας, συμπεριλαμβανομένων των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών Υποκειμένων Δεδομένων,
- πλήρη στοιχεία των Προσωπικών Δεδομένων που τέθηκαν σε κίνδυνο, συμπεριλαμβανομένων των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών αρχείων Προσωπικών Δεδομένων,
- όπου αυτό είναι γνωστό, λεπτομέρειες των πιθανών συνεπειών του Περιστατικού Ασφαλείας,
- πλήρεις λεπτομέρειες σχετικά με τον τρόπο, με τον οποίο διερευνάται το Περιστατικό Ασφαλείας, καθώς και μέτρα για τη μείωση και την αποκατάσταση που έχουν ήδη τεθεί σε εφαρμογή ή πρέπει να τεθούν σε εφαρμογή.

1.δ. Επέκταση Εχεμύθειας

Λόγω της κοινής συστέγασης, διαχείρισης και διοίκησης με τη μονοπρόσωπη ανώνυμη εταιρεία με την επωνυμία «ΧΧΧ» και τη «ΧΧΧ», όλες οι υποχρεώσεις του εργαζομένου που αναφέρονται στην παρούσα σύμβαση εφαρμόζονται και στις παραπάνω εταιρείες. Ειδικότερα, ο

εργαζόμενος υποχρεούται να θεωρεί και να αντιμετωπίζει οποιαδήποτε πληροφορία περιέρχεται σε γνώση του και αφορά τις προαναφερόμενες εταιρείες, ως Εμπιστευτικές Πληροφορίες σύμφωνα με τους ορισμούς της παρούσας σύμβασης, αναλαμβάνοντας τις ίδιες υποχρεώσεις και δεσμεύσεις, ιδίως ως προς την υποχρέωση εχεμύθειας εν σχέση με αυτές.

2. Υποχρεώσεις μετά τη λήξη της κύριας σύμβασης

Κατά τη λήξη της κύριας σύμβασης με οποιοδήποτε τρόπο, ο Συνεργάτης υποχρεούται να επιστρέψει στην «ΧΧΧ» οποιοδήποτε υλικό έχει στην κατοχή του και έχει αποκτήσει κατά την παροχή ή επ' αφορμή παροχής των υπηρεσιών του, καθώς και σημειώσεις ή υπομνήματα και άλλα έγγραφα ή μέσα μαγνητικής αποτύπωσης που ανήκουν ή αφορούν την «ΧΧΧ», ιδιαίτερα όσα περιέχουν Εμπιστευτικές Πληροφορίες και Δεδομένα Προσωπικού Χαρακτήρα.

ΕΥΘΥΝΗ ΣΥΝΕΡΓΑΤΗ

Σε περίπτωση παραβίασης κάποιας από τις υποχρεώσεις που ο Συνεργάτης αναλαμβάνει δια της παρούσας, υποχρεούται σε πλήρη αποζημίωση κάθε θετικής και αποθετικής ζημίας της «ΧΧΧ», καθώς και όλων των φυσικών ή νομικών προσώπων που τυχόν έχουν υποστεί βλάβη από την παραβίαση αυτή.

Η «ΧΧΧ», δικαιούται, σε περίπτωση παραβιάσεως των υποχρεώσεων που απορρέουν από την παρούσα, σε καταγγελία της κύριας σύμβασης με το Συνεργάτη, ακόμα και χωρίς την καταβολή αποζημιώσεως.

ΔΙΑΡΚΕΙΑ

Το παρόν προσάρτημα ισχύει καθ' όλη τη διάρκεια ισχύος της κύριας σύμβασης καθώς και κάθε νόμιμης παράτασης αυτής.

ΟΙ ΣΥΜΒΑΛΛΟΜΕΝΟΙ

ΓΙΑ ΤΗΝ ΧΧΧ **ΓΙΑ ΤΟΝ ΣΥΝΕΡΓΑΤΗ**

Προσάρτημα εμπιστευτικότητας για συμβάσεις που *πρόκειται να υπογραφούν:*

Προσάρτημα με τίτλο «Εμπιστευτικότητα πληροφοριών και προσωπικών δεδομένων» συνυπογράφεται από τα μέρη, επισυνάπτεται στην κύρια σύμβαση και αποτελεί αναπόσπαστο τμήμα αυτής.

3.9.4 Προσάρτημα Σύμβασης «Εργαζομένου»

ΠΡΟΣΑΡΤΗΜΑ ΣΤΗΝ ΑΠΟ .../.../.....ΣΥΜΒΑΣΗ ΕΡΓΑΣΙΑΣ ΣΥΜΦΩΝΗΤΙΚΟ ΓΙΑ ΤΗΝ ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Στη.....σήμερα την ..... μεταξύ των κάτωθι συμβαλλόμενων:

1. αφενός μεν της εταιρίας «.....» και το διακριτικό τίτλο «.....», που εδρεύει στην .....Αττικής, ..., με Α.Φ.Μ. ....., Δ.Ο.Υ. ..... που εκπροσωπείται νόμιμα από την κα. ....., και

2. του/της ..... από την άλλη πλευρά, εργαζόμενου/ης στην ..... που κατοικεί στην .....επί της οδού.....) εφεξής καλούμενου χάριν συντομίας «εργαζόμενος»,

συμφωνούνται και συνομολογούνται τα κάτωθι:

ΠΡΟΟΙΜΙΟ

Ο εργαζόμενος συνδέεται με την **XXX** με την από ..... σύμβαση εργασίας. Σύμφωνα με την εν λόγω σύμβαση, αλλά και σύμφωνα με τις υποχρεώσεις που απορρέουν από τον νόμο, ο εργαζόμενος υποχρεούται να τηρεί εχεμύθεια σχετικά με όλες τις εμπιστευτικές πληροφορίες της **XXX** που έρχονται σε γνώση του κατά την παροχή ή με αφορμή την παροχή των υπηρεσιών του προς την **XXX** και για την εκπλήρωση των καθηκόντων που του έχουν ανατεθεί.

Ο εργαζόμενος, στο πλαίσιο της σχέσης εργασίας του με την **XXX**, έχει τη δυνατότητα πρόσβασης και διακίνησης ιδιαίτερα ευαίσθητων πληροφοριών σχετικών με την δραστηριότητα της **XXX**. Συγκεκριμένα, ο εργαζόμενος βρίσκεται σε θέση να λαμβάνει γνώση και έχει δυνατότητα πρόσβασης και διακίνησης πληροφοριών που σχετίζονται με εμπιστευτικές πληροφορίες, μεταξύ των οποίων περιλαμβάνονται και δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων, η προστασία των οποίων εμπίπτει στο πεδίο εφαρμογής του Γενικού Κανονισμού ΕΕ 679/2016, καθώς και των λοιπών κανονισμών και νόμων που εκάστοτε ισχύουν για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Για αυτό τον λόγο, αμφότερα τα μέρη κρίνουν απαραίτητο όπως προβούν στη σύναψη της παρούσας ιδιαίτερης συμφωνίας σχετικά με τις υποχρεώσεις του εργαζόμενου σε σχέση με τις εμπιστευτικές πληροφορίες της **XXX** ή των δεδομένων προσωπικού χαρακτήρα φυσικών προσώπων της **XXX**, των συναλλασσόμενων με αυτή καθώς και των χρηστών των υπηρεσιών της, στα οποία τυχόν έχει πρόσβαση ή των οποίων λαμβάνει γνώση ή/και διακινεί.

Ο εργαζόμενος δηλώνει ότι κατανοεί τη σημασία που έχει για την **XXX** η εχεμύθεια και η σωστή διαχείριση των κατά τα ανωτέρω Εμπιστευτικών Πληροφοριών και δεδομένων προσωπικού χαρακτήρα.

ΟΡΙΣΜΟΙ

Εμπιστευτική Πληροφορία: θεωρείται οποιαδήποτε πληροφορία ή δεδομένο, που έρχεται σε γνώση του εργαζόμενου είτε με έγγραφο, είτε προφορικά είτε με ηλεκτρονικό ή με οποιονδήποτε τρόπο, κατά τη διάρκεια της παροχής των υπηρεσιών του ή επ' ευκαιρία και με αφορμή αυτήν, και αφορά είτε την XXX είτε τα στελέχη αυτής είτε τους συναλλασσόμενους με αυτή καθώς και τους χρήστες των υπηρεσιών της (φυσικά ή νομικά πρόσωπα).

Ο εργαζόμενος υποχρεούται να θεωρεί ως εμπιστευτική οποιαδήποτε πληροφορία, σύμφωνα με τα ανωτέρω, ανεξαρτήτως σοβαρότητας ή μη αυτής. Ως εμπιστευτικές θεωρούνται ενδεικτικά κι όχι περιοριστικά οι κάτωθι πληροφορίες για την **XXX**: τα επιχειρησιακά της σχέδια, οι συναλλαγές, η υπογραφή συμβάσεων κάθε φύσεως, η οικονομική κατάσταση της **XXX**, οι τεχνικές γνώσεις, το know – how, οι πληροφορίες σχετικά με το προσωπικό της **XXX**, σχετικά με τους προμηθευτές της **XXX**, τους όρους διενέργειας των προμηθειών, τον αριθμό, τα ονόματα και τις σχέσεις της **XXX** με συναλλασσόμενους με αυτήν ή με τους χρήστες των υπηρεσιών της, τις διαπραγματεύσεις για συναλλαγές της **XXX** ή την πρόσληψη προσωπικού κ.λ.π.

Εμπιστευτική πληροφορία, τέλος, χαρακτηρίζεται κάθε πληροφορία, της οποίας η διαρροή ενδέχεται να βλάψει τα συμφέροντα και τη φήμη της **XXX** ή του προσωπικού της ή τα δικαιώματα τρίτων συναλλασσόμενων με την **XXX** ή χρηστών των υπηρεσιών της. Τέλος εμπιστευτική πληροφορία χαρακτηρίζονται και τα προσωπικά δεδομένα (βλέπε κατωτέρω).
Μία εμπιστευτική κατά τα ανωτέρω πληροφορία παύει να θεωρείται εμπιστευτική από τη στιγμή που η **XXX** προβαίνει και στον βαθμό που προβαίνει σε επίσημη ανακοίνωσή της, η ρύθμιση αυτή ωστόσο δεν ισχύει όσον αφορά στα προσωπικά δεδομένα (βλέπε κατωτέρω).

Προσωπικά Δεδομένα : είναι κάθε πληροφορία που αναφέρεται σε και περιγράφει ένα φυσικό πρόσωπο, όπως: στοιχεία αναγνώρισης (ονοματεπώνυμο, ηλικία, κατοικία, επάγγελμα, οικογενειακή κατάσταση κλπ.), φυσικά χαρακτηριστικά, εκπαίδευση, εργασία (προϋπηρεσία, εργασιακή συμπεριφορά κλπ), οικονομική κατάσταση (έσοδα, περιουσιακά στοιχεία, οικονομική συμπεριφορά), ενδιαφέροντα, δραστηριότητες, συνήθειες. Το άτομο (φυσικό πρόσωπο), στο οποίο αναφέρονται τα δεδομένα, ονομάζεται υποκείμενο των δεδομένων.

Ευαίσθητα Προσωπικά Δεδομένα ή ειδικών κατηγοριών: χαρακτηρίζονται τα προσωπικά δεδομένα ενός ατόμου που αναφέρονται στη φυλετική ή εθνική του προέλευση, στα πολιτικά του φρονήματα, στις θρησκευτικές ή φιλοσοφικές του πεποιθήσεις, στη συμμετοχή του σε συνδικαλιστική οργάνωση, στην υγεία του, στην κοινωνική του πρόνοια,

στην ερωτική του ζωή, τις ποινικές διώξεις και καταδίκες του, καθώς και στη συμμετοχή του σε συναφείς με τα ανωτέρω ενώσεις προσώπων.

Τα παραπάνω δεδομένα τυχόν εργαζομένων, ή συνεργατών ή συναλλασσόμενων με την **XXX**, καθώς και των χρηστών των υπηρεσιών του, όπως αυτά καθορίζονται από τον Γενικό Κανονισμό ΕΕ 2016/679 (όπως αυτός θα ενσωματωθεί στο εθνικό δίκαιο περί προστασίας του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα), θεωρούνται εμπιστευτικές πληροφορίες για την **XXX**.

ΥΠΟΧΡΕΩΣΕΙΣ ΕΡΓΑΖΟΜΕΝΟΥ

1.α. Υποχρέωση διαχείρισης της εμπιστευτικής πληροφορίας με ιδιαίτερη επιμέλεια

Ο εργαζόμενος υποχρεούται να διαχειρίζεται κάθε Εμπιστευτική Πληροφορία με απόλυτη εχεμύθεια, λαμβάνοντας με ιδιαίτερη επιμέλεια κάθε αναγκαίο μέτρο για την προστασία της (ενδεικτικά την αποθήκευσή της σε κλειδωμένο χώρο ή αν η αποθήκευση γίνεται ηλεκτρονικά με ειδικό κωδικό) και να μην παρέχει πρόσβαση σε κανένα πρόσωπο που δεν είναι ειδικά εξουσιοδοτημένο.

Ο εργαζόμενος υποχρεούται να χρησιμοποιεί την Εμπιστευτική Πληροφορία αποκλειστικά και μόνο για τον σκοπό που αυτή αποκαλύφθηκε σε αυτόν και στον βαθμό που είναι αναγκαίο για την εκτέλεση της κύριας σύμβασης.

Απαγορεύεται στον εργαζόμενο να προβαίνει σε εμπορική χρήση της εμπιστευτικής πληροφορίας ή να την χρησιμοποιεί προς όφελός του.

Απαγορεύεται στον εργαζόμενο να αντιγράφει ή να φωτοτυπεί ή να εξάγει την Εμπιστευτική Πληροφορία ή τμήμα αυτής, χωρίς ειδική άδεια της **XXX**, εκτός αν αυτό είναι απολύτως απαραίτητο για την εκπλήρωση του σκοπού για τον οποίο του αποκαλύφθηκε η Εμπιστευτική Πληροφορία ή για την εκπλήρωση των καθηκόντων που του έχουν ανατεθεί στο πλαίσιο της εργασιακής του σχέσης με την **XXX**.

Ο εργαζόμενος θα χρησιμοποιήσει τυχόν λογισμικό που θα του παραχωρηθεί για την παροχή των υπηρεσιών του και σε καμία περίπτωση δεν θα το χρησιμοποιήσει για την μεταφορά δεδομένων ή γενικότερα στοιχείων που αποτελούν περιουσιακό στοιχείο της **XXX** εκτός της **XXX** ή εκτός συστημάτων της **XXX** και χωρίς την πρότερη έγγραφη έγκρισή της.

Διευκρινίζεται ότι η εχεμύθεια και εμπιστευτικότητα στη διαχείριση της πληροφορίας πρέπει να τηρείται όχι μόνο προς πρόσωπα τρίτα με την **XXX**, αλλά και προς πρόσωπα εντός της **XXX** που δεν είναι εξουσιοδοτημένα να έχουν πρόσβαση στην Εμπιστευτική Πληροφορία.

Σε περίπτωση που ο εργαζόμενος υποχρεωθεί από δικαστική ή αστυνομική αρχή να αποκαλύψει σύμφωνα με το νόμο την Εμπιστευτική Πληροφορία, υποχρεούται όπως ενημερώσει εκ των προτέρων και σε κάθε περίπτωση την επομένη εργάσιμη ημέρα την **XXX**, εκτός κι αν αυτό απαγορεύεται βάσει διατάξεως νόμου.

1.β. Επιπρόσθετες υποχρεώσεις για τα προσωπικά δεδομένα

Ο εργαζόμενος δεσμεύεται να σεβαστεί την Πολιτική Ιδιωτικότητας της **XXX**, καθώς και το Σύστημα Ασφάλειας Πληροφοριών αυτής, τα οποία έχουν έλθει σε γνώση του, υποχρεούται, δε, να ενημερώσει άμεσα την **XXX** για τυχόν εκ μέρους του αντιρρήσεις ή επιφυλάξεις του αναφορικά με την εφαρμογή τους.

Ο εργαζόμενος δεσμεύεται να μην προβαίνει σε καμία επεξεργασία προσωπικών δεδομένων χωρίς προηγούμενη εντολή της **XXX**, εκτός εάν η επεξεργασία αυτή εμπίπτει στα καθήκοντα που του έχουν ανατεθεί στο πλαίσιο της εργασιακής του σχέσης με την **XXX**.

Ο εργαζόμενος οφείλει: i) να ενημερώσει την **XXX** αμέσως μόλις αντιληφθεί την εμφάνιση οποιουδήποτε περιστατικού που επέφερε ή είναι λογικά πιθανό να επιφέρει παραβίαση της ασφάλειας, συμπεριλαμβανομένης οποιασδήποτε τυχαίας ή παράνομης απώλειας, κλοπής, διαγραφής, αποκάλυψης ή παραποίησης Προσωπικών Δεδομένων ή/ και οποιασδήποτε μη εξουσιοδοτημένης χρήσης ή πρόσβασης σε Προσωπικά Δεδομένα (εφεξής το «Περιστατικό Ασφαλείας»), ii) να παρέχει κάθε συνεργασία και πληροφόρηση που θα ζητηθεί από την **XXX** σε σχέση με το Περιστατικό Ασφαλείας το συντομότερο δυνατόν και σε κάθε περίπτωση εντός 24 ωρών από την γνώση του Περιστατικού Ασφαλείας, συμπεριλαμβάνοντας:

- όλες τις λεπτομέρειες του Περιστατικού Ασφαλείας, συμπεριλαμβανομένων των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών Υποκειμένων Δεδομένων,
- πλήρη στοιχεία των Προσωπικών Δεδομένων που τέθηκαν σε κίνδυνο, συμπεριλαμβανομένων των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών αρχείων Προσωπικών Δεδομένων,
- όπου αυτό είναι γνωστό, λεπτομέρειες των πιθανών συνεπειών του Περιστατικού Ασφαλείας,
- πλήρεις λεπτομέρειες σχετικά με τον τρόπο, με τον οποίο διερευνάται το Περιστατικό Ασφαλείας, καθώς και μέτρα για τη μείωση και την αποκατάσταση που έχουν ήδη τεθεί σε εφαρμογή ή πρέπει να τεθούν σε εφαρμογή.

1.γ. Επέκταση Εχεμύθειας

Λόγω της κοινής συστέγασης, διαχείρισης και διοίκησης με τη μονοπρόσωπη ανώνυμη εταιρεία με την επωνυμία «ΧΧΧ» και τη «ΧΧΧ», όλες οι υποχρεώσεις του εργαζομένου που αναφέρονται στην παρούσα σύμβαση εφαρμόζονται και στις παραπάνω εταιρείες. Ειδικότερα, ο εργαζόμενος υποχρεούται να θεωρεί και να αντιμετωπίζει οποιαδήποτε πληροφορία περιέρχεται σε γνώση του και αφορά τις προαναφερόμενες εταιρείες, ως Εμπιστευτικές Πληροφορίες σύμφωνα με τους ορισμούς της παρούσας σύμβασης, αναλαμβάνοντας τις ίδιες υποχρεώσεις και δεσμεύσεις, ιδίως ως προς την υποχρέωση εχεμύθειας εν σχέση με αυτές.

2. Υποχρεώσεις μετά τη λήξη της σύμβασης εργασίας

Κατά τη λήξη της εργασιακής σχέσης με οποιοδήποτε τρόπο, ο εργαζόμενος υποχρεούται να επιστρέψει στην **XXX** οποιοδήποτε υλικό έχει στην κατοχή του και έχει αποκτήσει κατά την παροχή ή επ' αφορμή παροχής των υπηρεσιών του, καθώς και σημειώσεις ή υπομνήματα και άλλα έγγραφα ή μέσα μαγνητικής αποτύπωσης που ανήκουν ή αφορούν την **XXX**, ιδιαίτερα όσα περιέχουν Εμπιστευτικές Πληροφορίες και Δεδομένα Προσωπικού Χαρακτήρα.

ΕΥΘΥΝΗ ΕΡΓΑΖΟΜΕΝΟΥ

Σε περίπτωση παραβίασης κάποιας από τις υποχρεώσεις που ο εργαζόμενος αναλαμβάνει δια της παρούσας, υποχρεούται σε πλήρη αποζημίωση κάθε θετικής και αποθετικής ζημίας της **XXX**, καθώς και όλων των φυσικών ή νομικών προσώπων που τυχόν έχουν υποστεί βλάβη από την παραβίαση αυτή.

Η **XXX**, δικαιούται, σε περίπτωση παραβιάσεως των υποχρεώσεων που απορρέουν από την παρούσα, σε καταγγελία της σύμβασης εργασίας με τον εργαζόμενο ακόμα και χωρίς την καταβολή αποζημιώσεως.

ΔΙΑΡΚΕΙΑ ΣΥΜΦΩΝΗΤΙΚΟΥ

Το παρόν διαρκεί για όσο χρόνο διαρκεί η μεταξύ της **XXX** και του εργαζόμενου σύμβασης εργασίας.

Η παρούσα συνετάχθη σε δύο (2) πρωτότυπα και κάθε μέρος, αφού τα υπέγραψε, έλαβε από ένα.

ΟΙ ΣΥΜΒΑΛΛΟΜΕΝΟΙ

ΓΙΑ ΤΟΝ **ΓΙΑ ΤΟΝ ΕΡΓΑΖΟΜΕΝΟ**

3.10 Πολιτική Συγκατάθεσης

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GDPR.10: ΠΟΛΙΤΙΚΗ ΣΥΓΚΑΤΑΘΕΣΗΣ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Σκοπός

Αυτή η πολιτική έχει σχεδιαστεί για να παρέχει κατευθύνσεις για τη διαχείριση των Συγκαταθέσεων.

Δεδομένου ότι ο Υπεύθυνος Επεξεργασίας ορίζει τους σκοπούς επεξεργασίας που διενεργεί κατά την κείμενη νομοθεσία, δεσμεύεται να ενεργεί σύμφωνα με τις αρχές που διέπουν την επεξεργασία κατά τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ 2016/679 (ΓΚΠΔ), να προστατεύει και να σέβεται τα δικαιώματα των υποκειμένων.

Μία σημαντική νόμιμη βάση επεξεργασίας των προσωπικών δεδομένων (άρθρο 6 του ΓΚΠΔ) αλλά και των ειδικών κατηγοριών Δεδομένων (άρθρο 9 του ΓΚΠΔ) είναι η συγκατάθεση, λεπτομέρειες για την οποία θα δοθούν στη συνέχεια.

Πολιτική

Γενικά

- Η παροχή συγκατάθεσης/συναίνεσης του υποκειμένου για επεξεργασία των προσωπικών του δεδομένων αποτελεί μία από τις νόμιμες βάσεις επεξεργασίας τόσο των απλών όσο και των δεδομένων ειδικών κατηγοριών (άρθρα 6 και 9 του ΓΚΠΔ).
- Η ρητή συγκατάθεση μπορεί να νομιμοποιήσει
    - την επεξεργασία δεδομένων **ειδικών** κατηγοριών
    - τη λήψη **αυτοματοποιημένων** αποφάσεων καθώς και
    - τη διαβίβαση των προσωπικών δεδομένων προς **τρίτες χώρες** και διεθνείς οργανισμούς.
- Ο Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) θέτει **αυστηρές προϋποθέσεις** για την λήψη **έγκυρης** συγκατάθεσης του υποκειμένου των δεδομένων από τον υπεύθυνο επεξεργασίας. Σε πολλές όμως περιπτώσεις, η συγκατάθεση ***δεν είναι απαραίτητη***. Η προσφυγή στη νόμιμη βάση της συγκατάθεσης προτείνεται ***μόνο σε περίπτωση κατά την οποία δεν υπάρχει κάποια άλλη νόμιμη βάση για την επεξεργασία των δεδομένων***.
- Πρακτικές και έντυπα λήψης συγκατάθεσης θα πρέπει να είναι σύμφωνα με τις διατάξεις του ΓΚΠΔ, ενώ ενδέχεται πρακτικές κι έντυπα που ίσχυαν πριν από τη θέση σε ισχύ του ΓΚΠΔ να έχουν ανάγκη επικαιροποίησης και συμμόρφωσης με τις προϋποθέσεις που θέτει ο ΓΚΠΔ.
- Η ρητή συγκατάθεση απαιτεί πολύ σαφή και συγκεκριμένη δήλωση συναίνεσης.
- Οι δημόσιες αρχές και οι εργοδότες θα χρειαστεί να λάβουν πρόσθετη μέριμνα για να αποδείξουν ότι η συναίνεση των πολιτών και των εργαζομένων παρέχεται ελεύθερα και

πρέπει να αποδεικνύεται ότι η συναίνεση αυτή δεν έχει ληφθεί υπό πίεση λόγω της σαφούς ανισότητας μεταξύ υπεύθυνου επεξεργασίας και υποκειμένου των δεδομένων.

Τι πρέπει να προσέχουμε όταν ζητάμε συγκατάθεση/συναίνεση

- Έχουμε ελέγξει ότι η συγκατάθεση είναι η πιο κατάλληλη νόμιμη βάση για την επεξεργασία.
- Ζητάμε από τους ανθρώπους να προβούν σε ενεργητική και θετική επιλογή (Opt-in).
- Ενημερώνουμε τα άτομα ότι μπορούν να ανακαλέσουν τη συγκατάθεσή τους και δίνουμε τη δυνατότητα αυτή (Opt-out).
- Η συγκατάθεση πρέπει να ενημερώνει το υποκείμενο των δεδομένων αναφορικά με το **όνομα του υπεύθυνου της επεξεργασίας,** τους **σκοπούς** της επεξεργασίας και να δίνεται ελεύθερα.
- Έχουμε διατυπώσει το κείμενο της συγκατάθεσης/συναίνεσης ξεχωριστά και σαφώς διακριτά από άλλα θέματα, όπως από όρους και προϋποθέσεις σε κάποια σύμβαση.
- Δεν χρησιμοποιούμε κουτιά που έχουν επισημανθεί προηγουμένως ή οποιανδήποτε άλλη μέθοδο από την οποία να προκύπτει ή να τεκμαίρεται η συγκατάθεση του υποκειμένου.
- Χρησιμοποιούμε σαφή, απλή γλώσσα που είναι εύκολο να κατανοηθεί.
- Διευκρινίζουμε γιατί θέλουμε τα δεδομένα και τι θα κάνουμε με αυτά, περιγράφουμε δηλαδή σαφώς το σκοπό επεξεργασίας.
- Δίνουμε διακριτές επιλογές για να λάβουμε διακριτές συγκαταθέσεις για **διαφορετικούς** σκοπούς και τύπους επεξεργασίας.
- Αποφεύγουμε να χρησιμοποιούμε τη συγκατάθεση ως προϋπόθεση για την παροχή μιας υπηρεσίας όταν υπάρχουν εναλλακτικές νόμιμες βάσεις επεξεργασίας.
- Εάν προσφέρουμε ηλεκτρονικές υπηρεσίες απευθείας σε παιδιά, ζητάμε τη συγκατάθεσή τους μόνο αν διαθέτουμε μέτρα επαλήθευσης της ηλικίας (και μέτρα λήψης γονικής συναίνεσης για τα μικρότερα παιδιά).
- *Η ακατάλληλη ή άκυρη συγκατάθεση ενέχει τον κίνδυνο της καταστροφής της εμπιστοσύνης των υποκειμένων των δεδομένων προς τον οργανισμό, την καταστροφή της φήμης του οργανισμού, αλλά και την πιθανότητα επιβολής εις βάρος του οργανισμού μεγάλων προστίμων.*

Πώς πρέπει να αποκτήσουμε, καταγράψουμε τη συγκατάθεση

Το κείμενο του εντύπου συγκατάθεσης πρέπει να είναι σαφές, περιεκτικό και διακριτό από άλλους όρους και προϋποθέσεις κι εύκολο στην κατανόηση. Περιλαμβάνει:

- το όνομα του οργανισμού σας.

- γιατί θέλετε τα δεδομένα?
- τι θα κάνετε με αυτά? και
- αναφορά στη δυνατότητα των ατόμων να ανακαλούν τη συγκατάθεσή τους ανά πάσα στιγμή.

Όπου είναι δυνατόν, δώστε ***διακριτές*** επιλογές συγκατάθεσης για ***διαφορετικούς σκοπούς*** και διαφορετικούς τύπους επεξεργασίας.

Διατηρήστε αρχεία για να αποδείξετε τη λήψη συγκατάθεσης από τα υποκείμενα των δεδομένων- ποιος συμφώνησε, πότε, πώς και το περιεχόμενο της ενημέρωσής τους.

Διαχείριση συγκατάθεσης / συναίνεσης

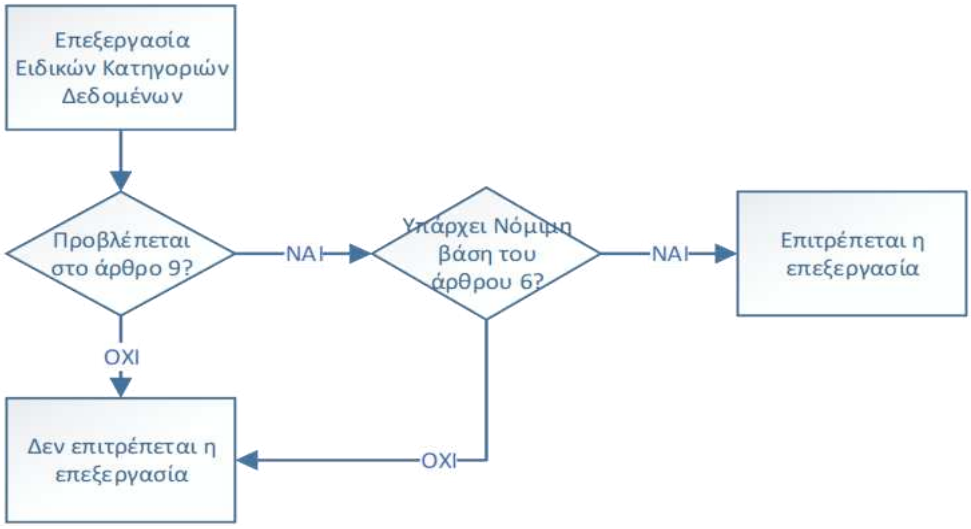
- ***Αναθεωρούμε*** σε τακτά χρονικά διαστήματα συναινέσεις/συγκαταθέσεις και τα κείμενά τους για να ελέγξουμε ότι η σχέση μεταξύ του υπεύθυνου επεξεργασίας, η επεξεργασία και οι σκοποί της δεν έχουν αλλάξει. Να λάβετε υπόψη τις αναθεωρήσεις αυτές στην Ανασκόπηση από τη Διοίκηση.
- ***Επικαιροποιούμε*** τα έντυπα συγκατάθεσης και τα αναπροσαρμόζουμε αν υπάρξει κάποια αλλαγή.
- Διευκολύνουμε τα άτομα να ανακαλέσουν τη συγκατάθεσή τους οποιαδήποτε στιγμή και τους ενημερώνουμε πώς να το κάνουν (δείτε και σχετική διαδικασία).
- Δεν υπάρχει καθορισμένη προθεσμία για την παροχή και λήψη συγκατάθεσης. Η διάρκεια μιας ληφθείσας συγκατάθεσης εξαρτάται από το πλαίσιο του σκοπού της επεξεργασίας.

Ειδικών Κατηγοριών Προσωπικά Δεδομένα

Κατ' αρχήν ***απαγορεύεται*** η επεξεργασία τους.
Εκ φύσεως είναι ιδιαίτερα ευαίσθητα δεδομένα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες και χρήζουν ειδικής προστασίας.
Πότε **επιτρέπεται** η Επεξεργασία Ειδικών Κατηγοριών Δεδομένων?

- Θα πρέπει να υπάρχει μία εκ των προϋποθέσεων του **άρθρου 9 ΚΑΙ**
- Νόμιμη βάση επεξεργασίας βάσει του **άρθρου 6**.

Δηλαδή θα πρέπει να ισχύει:



Μία από τις Νόμιμες βάσεις επεξεργασίας ειδικών κατηγοριών Προσωπικών Δεδομένων του άρθρου 9 είναι όταν υπάρχει ***Συγκατάθεση***.

- το άτομο την δίνει ελεύθερα
- είναι σε θέση να επιλέξει κατά πόσο ενδιαφέρεται για τις συγκεκριμένες υπηρεσίες που προσφέρονται
- δεν διατρέχει τον κίνδυνο εξαπάτησης, εκφοβισμού, εξαναγκασμού ή σημαντικών αρνητικών επιπτώσεων εάν δεν συγκατατεθεί π.χ. οποιοδήποτε οικονομικό κόστος
- ο υπεύθυνος επεξεργασίας ***πρέπει να αποδείξει*** ότι το άτομο έδωσε τη συγκατάθεσή του
- Μπορεί να ανακληθεί ανά πάσα στιγμή

Στην περίπτωση που η συγκατάθεση πρέπει να ληφθεί για πρόσωπο που δεν έχει δικαιοπρακτική ικανότητα το έντυπο **E.GDPR.10.01: «ΕΝΤΥΠΟ ΣΥΓΚΑΤΑΘΕΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»** θα πρέπει να υπογράφεται από τον ασκούντα την επιμέλεια, γονέα κ.λπ.

Συγκατάθεση και διαφημιστικά Ηλεκτρονικά Μηνύματα

Για να αποστέλλονται διαφημιστικά emails, η **συγκατάθεση** είναι μια μόνο προϋπόθεση και **όχι η μόνη**. Με την ePrivacy (2002/58/ΕΚ με τις τροποποιήσεις με την 2009/136/ΕΚ) οδηγία υπάρχει και το *soft opt-in*, που δίνει την ευχέρεια στις επιχειρήσεις να διαφημίζουν στους πελάτες τους χωρίς συγκατάθεση, αρκεί:

α) να πήραν το email **νομίμως** στο πλαίσιο πώλησης ή άλλης παρόμοιας συναλλαγής,

β) να είχαν ενημερώσει **εκείνη τη στιγμή** (τη στιγμή της συλλογής του email) ότι θα χρησιμοποιήσουν το email και για διαφήμιση,

γ) να διαφημίζουν **παρόμοια** προϊόντα και

δ) να δίνουν δυνατότητα **δωρεάν** και **εύκολης διαγραφής** σε κάθε μήνυμα.

(Από δημοσίευμα του Δρ.Γεωργίου Ρουσόπουλου)

Θεωρούμε ότι πρέπει αυτούσια να αναφερθούν οι §3 & 4 του άρθρου 11 του Ν.3471/2006 που αναφέρεται σε «***Μη ζητηθείσα επικοινωνία***»

«3. Τα στοιχεία επαφής ηλεκτρονικού ταχυδρομείου που αποκτήθηκαν νομίμως, στο πλαίσιο της πώλησης προϊόντων ή υπηρεσιών ή άλλης συναλλαγής, μπορούν να χρησιμοποιούνται για την απευθείας προώθηση παρόμοιων προϊόντων ή υπηρεσιών του προμηθευτή ή για την εξυπηρέτηση παρόμοιων σκοπών, ακόμη και όταν ο αποδέκτης του μηνύματος δεν έχει δώσει εκ των προτέρων τη συγκατάθεσή του, υπό την προϋπόθεση ότι του παρέχεται κατά τρόπο σαφή και ευδιάκριτο η δυνατότητα να αντιτάσσεται, με εύκολο τρόπο και δωρεάν, στη συλλογή και χρησιμοποίηση των ηλεκτρονικών του στοιχείων, και αυτό σε κάθε μήνυμα σε περίπτωση που ο χρήστης αρχικά δεν είχε διαφωνήσει σε αυτή τη χρήση.
4. Απαγορεύεται η αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, που έχουν σκοπό την άμεση εμπορική προώθηση προϊόντων και υπηρεσιών, όταν δεν αναφέρεται ευδιάκριτα και σαφώς η ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, καθώς επίσης και η έγκυρη διεύθυνση στην οποία ο αποδέκτης του μηνύματος μπορεί να ζητεί τον τερματισμό της επικοινωνίας.»

Σχέδιο Εντύπου Συγκατάθεσης

Ένα σχέδιο Εντύπου Συγκατάθεσης αποτελεί το ***Έντυπο Ε.GDPR.10.01.Συγκατάθεση Επεξεργασίας Προσωπικών Δεδομένων»***, το οποίο πρέπει να αρχειοθετείται στο σχετικό αρχείο.

Το έντυπο αυτό μπορεί να τροποποιείται ανάλογα το σκοπό/ούς ή τον τύπο επεξεργασίας των προσωπικών δεδομένων.

Αρχεία και Δεδομένα

Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί το έντυπο αρχείο, «**Αρχείο Συγκαταθέσεων / Συναινέσεων**» όπου τηρούνται τα αντίστοιχα έντυπα συγκαταθέσεων των υποκειμένων.
Εάν η συγκατάθεση δεν είναι έγγραφη θα πρέπει να:
Διατηρούμε αρχείο για το πότε και πώς έχουμε λάβει τη συγκατάθεση του ατόμου.
Φροντίζουμε να καταγράψουμε ακριβώς τι ενημέρωση έχει γίνει στα υποκείμενα κατά τη στιγμή λήψης της συγκατάθεσης.
Η διάρκεια τήρησης του αρχείου είναι όσο διαρκεί ο αντίστοιχος σκοπός και η σχέση με το υποκείμενο.

Σχετικές διατάξεις του ΓΚΠΔ - Βλ. Άρθρο 4 παράγραφος 11, άρθρο 6 παράγραφος 1 στοιχείο α) 7, άρθρο 8, άρθρο 9 παράγραφος 2 στοιχείο α) και αιτιολογικές σκέψεις 32, 38, 40, 42, 43, 171.

3.10.1 Έντυπο «Συγκατάθεσης Επεξεργασίας Προσωπικών Δεδομένων»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ E.GDPR.10.01: «ΕΝΤΥΠΟ ΣΥΓΚΑΤΑΘΕΣΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ»**

Ο κάτωθι υπογράφων/ουσα, δηλώνω ότι έχω ενημερωθεί και συγκατατίθεμαι στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από την ....., σύμφωνα με τις διατάξεις του Γενικού Κανονισμού Προσωπικών Δεδομένων (ΓΚΠΔ/ΕΕ 679/2016) μεταξύ των οποίων και των ειδικών κατηγοριών δεδομένων.

Ενημέρωση αναφορικά με τον τρόπο με τον οποίο επεξεργαζόμαστε τα δεδομένα σας, αναγράφονται λεπτομερώς στη σχετική Πολιτική Ιδιωτικότητας του οργανισμού μας, η οποία έχει αναρτηθεί και βρίσκεται στη διάθεσή σας, στην ιστοσελίδα μας www.....gr
Μπορείτε να προβείτε στη συγκατάθεση με τη συμπλήρωση του αντίστοιχου τετραγώνου.
Ειδικότερα:

Σκοπός 1: .....

- Συμφωνώ ότι μπορείτε να συλλέξετε, επεξεργαστείτε, γνωστοποιήσετε και να διαβιβάσετε τα προσωπικά μου δεδομένα, καθώς επίσης, δεδομένα υγείας μου και λοιπά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα, με σκοπό την .....

□ Συναινώ □ Δεν Συναινώ

Σκοπός 2: .....

- Συμφωνώ ότι μπορείτε να συλλέξετε και επεξεργαστείτε, τα προσωπικά μου δεδομένα, καθώς επίσης, δεδομένα υγείας μου και λοιπά ειδικών κατηγοριών δεδομένα προσωπικού χαρακτήρα, με σκοπό ..... Επιπλέον μπορείτε να γνωστοποιείτε και να διαβιβάζετε, αυτά τα προσωπικά δεδομένα, σε συνεργαζόμενα με εσάς ή με την ..... φυσικά ή νομικά πρόσωπα (όπως ενδεικτικά, ...), με σκοπό την παροχή των υπηρεσιών ..... που προβλέπονται από τη σύμβαση, συμπεριλαμβανομένης .....

□ Συναινώ □ Δεν Συναινώ

Σκοπός 3: Ενημέρωση για παρεχόμενες υπηρεσίες και προϊόντα

- Συμφωνώ ότι μπορείτε να συλλέξετε, επεξεργαστείτε, γνωστοποιήσετε και διαβιβάσετε τα προσωπικά μου δεδομένα, για την ενημέρωσή μου σχετικά με νέα του οργανισμού σας, τις παρεχόμενες από εσάς υπηρεσίες, τη διεξαγωγή έρευνας ικανοποίησης πελατών καθώς επίσης και προώθηση σχετικού επικοινωνιακού υλικού.
-

□ Συναινώ □ Δεν Συναινώ

Ημερομηνία: _____

Ονοματεπώνυμο: _____

Email: _____

Υπογραφή: _____

Σημ: Για εξαρτώμενο μέλος κάτω των 18 ετών υπογράφει ο Κηδεμόνας αναφέροντας τα στοιχεία του και τα στοιχεία του εξαρτώμενου μέλους.

3.11 Πολιτική CCTV

ΔΗΛΩΣΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΓΙΑ
ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

ΜΕΣΩ ΣΥΣΤΗΜΑΤΟΣ ΒΙΝΤΕΟΕΠΙΤΗΡΗΣΗΣ

Το παρόν αποσκοπεί στην ενημέρωση των εργαζομένων του οργανισμού και των συνεργαζομένων ή/και συνδεδεμένων με αυτή που φιλοξενούνται στους χώρους και εγκαταστάσεις της και των επισκεπτών της/τους για την ύπαρξη και λειτουργία συστήματος βιντεοεπιτήρησης μέσω καμερών κλειστού κυκλώματος τηλεόρασης (CCTV), το σκοπό της ύπαρξης και λειτουργίας αυτής, καθώς και τα μέτρα ασφαλείας που λαμβάνονται από τον οργανισμό για την προστασία των δεδομένων προσωπικού χαρακτήρα των εργαζομένων και τα δικαιώματα των τελευταίων σε σχέση με τα δεδομένα αυτά.

1. Υπεύθυνος Επεξεργασίας

Για οποιοδήποτε ζήτημα σχετικά με την επεξεργασία των προσωπικών σας δεδομένων και για την άσκηση των δικαιωμάτων σας, μπορείτε να επικοινωνήσετε με τον Οργανισμό, τηλεφωνικά στο +30 XXXXXXXXX (Δευτέρα - Παρασκευή 10:00 - 15:00), με e-mail: dpo@..... και ταχυδρομικά στη διεύθυνση: .....

2. Σκοπός Επεξεργασίας και Νομική Βάση

Χρησιμοποιούμε σύστημα επιτήρησης για τον σκοπό της προστασίας προσώπων και αγαθών. Η επεξεργασία είναι απαραίτητη για σκοπούς εννόμων συμφερόντων που επιδιώκουμε ως υπεύθυνος επεξεργασίας (άρθρο 6 παρ. 1. στ ΓΚΠΔ).

3. Ανάλυση Εννόμων Συμφερόντων

Το έννομο συμφέρον μας συνίσταται στην ανάγκη να προστατεύσουμε τον χώρο μας και τα αγαθά που ευρίσκονται σε αυτόν από παράνομες πράξεις, όπως ενδεικτικά από κλοπές. Το ίδιο ισχύει και για την ασφάλεια της ζωής, της σωματικής ακεραιότητας, της υγείας καθώς και της περιουσίας του προσωπικού μας και τρίτων συνεργατών, χρηστών των υπηρεσιών μας, επισκεπτών, που νομίμως ευρίσκονται στον επιτηρούμενο χώρο. Ο οργανισμός φυλάσσεται επί 24ώρου βάσεως από εταιρεία φύλαξης, ενώ για την είσοδο και έξοδο του κτιρίου καθώς και στις εισόδους των εργαστηρίων υπάρχει σύστημα access control για το μόνιμο προσωπικό και έλεγχος εισόδου για τους επισκέπτες, τους χρήστες υπηρεσιών και τους συνεργάτες μας. Η χρήση του συστήματος βιντεοεπιτήρησης έχει κριθεί απαραίτητη λόγω του μεγάλου κι εναλλασσόμενου αριθμού προσώπων, που επισκέπτονται τις εγκαταστάσεις μας, της ειδικής φύσεως δεδομένων που τηρούμε και της αξίας του εξοπλισμού μας του οποίου η απρόσκοπτη και αδιάλειπτη λειτουργία του είναι απαραίτητη. Φαινόμενα κλοπών ή καταστροφών του

ανωτέρω εξοπλισμού δημιουργούν ανυπέρβλητα εμπόδια στην επίτευξη των στόχων μας. Η ανάγκη λειτουργίας συστήματος βιντεοεπιτήρησης επιτείνεται από την ιδιαιτερότητα των εγκαταστάσεων, και το μέγεθος του χώρου που πρέπει να προστατευθεί. Τα λοιπά μέσα επιτήρησης και ασφάλειας δεν κρίνονται κατά τα ανωτέρω επαρκή, σε σχέση με τα προστατευτέα αγαθά.

4. Δεδομένα που συλλέγονται

Συλλέγουμε μόνο δεδομένα εικόνας και περιορίζουμε τη λήψη σε χώρους που αξιολογήσαμε ότι υπάρχει αυξημένη πιθανότητα τέλεσης παράνομων πράξεων π.χ. εισόδους στις εγκαταστάσεις, περιβάλλοντα χώρο, διαδρόμους, χώρους εργαστηρίων, χωρίς να εστιάζουμε σε χώρους όπου ενδέχεται να περιορίζεται υπέρμετρα η ιδιωτική ζωή των προσώπων των οποίων λαμβάνεται η εικόνα, περιλαμβανομένου του δικαιώματός τους στον σεβασμό των δεδομένων προσωπικού χαρακτήρα. Οι κάμερες καταγράφουν 24 ώρες την ημέρα και 7 ημέρες την εβδομάδα. Οι κάμερες **δεν** βιντεοσκοπούν χώρους εργασίας.

5. Αποδέκτες

Το τηρούμενο υλικό είναι προσβάσιμο μόνο από το αρμόδιο / εξουσιοδοτημένο προσωπικό μας που είναι επιφορτισμένο με την ασφάλεια του χώρου. Το υλικό αυτό δεν διαβιβάζεται σε τρίτους, με εξαίρεση τις ακόλουθες περιπτώσεις: α) προς τις αρμόδιες δικαστικές, εισαγγελικές και αστυνομικές αρχές όταν περιλαμβάνει στοιχεία απαραίτητα για τη διερεύνηση μιας αξιόποινης πράξης, η οποία αφορά πρόσωπα ή αγαθά του υπευθύνου επεξεργασίας, β) προς τις αρμόδιες δικαστικές, εισαγγελικές και αστυνομικές αρχές όταν ζητούν δεδομένα, νομίμως, κατά την άσκηση των καθηκόντων τους, και γ) προς το θύμα ή τον δράστη μιας αξιόποινης πράξης, όταν πρόκειται για δεδομένα τα οποία ενδέχεται να αποτελούν αποδεικτικά στοιχεία της πράξης.

6. Επεξεργασία Δεδομένων-Χρόνος Τήρησης

Οι κάμερες συνδέονται απευθείας με καταγραφικά όπου αποθηκεύεται το υλικό. Η βιντεοεπιτήρηση δεν γίνεται σε πραγματικό χρόνο.

Τηρούμε τα δεδομένα για επτά (7) ημέρες, μετά την πάροδο των οποίων διαγράφονται αυτόματα. Σε περίπτωση που στο διάστημα αυτό διαπιστώσουμε κάποιο περιστατικό, απομονώνουμε τμήμα του βίντεο και το τηρούμε έως και έναν (1) μήνα ακόμα, με σκοπό τη διερεύνηση του περιστατικού και την έναρξη νομικών διαδικασιών για την υπεράσπιση των εννόμων συμφερόντων μας, ενώ αν το περιστατικό αφορά τρίτους θα τηρήσουμε το βίντεο έως και τρεις (3) μήνες ακόμα.

7. Ποια είναι τα δικαιώματά σας και πώς μπορείτε να τα ασκήσετε;

Τα υποκείμενα των δεδομένων έχουν τα εξής δικαιώματα:

- Δικαίωμα πρόσβασης: έχετε δικαίωμα να μάθετε αν επεξεργαζόμαστε την εικόνα σας και, εφόσον αυτό ισχύει, να λάβετε αντίγραφο αυτής.
- Δικαίωμα περιορισμού: έχετε δικαίωμα να μας ζητήσετε να περιορίσουμε την επεξεργασία, όπως για παράδειγμα να μη διαγράψουμε δεδομένα τα οποία θεωρείτε απαραίτητα για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων.
- Δικαίωμα εναντίωσης: έχετε δικαίωμα να αντιταχθείτε στην επεξεργασία.
- Δικαίωμα διαγραφής: έχετε δικαίωμα να ζητήσετε να διαγράψουμε δεδομένα σας.

Μπορείτε να ασκήσετε τα δικαιώματά σας στέλνοντας e-mail στη διεύθυνση dpo@..... ή επιστολή στην ταχυδρομική μας διεύθυνση ή καταθέτοντάς μας οι ίδιοι το αίτημα αυτοπροσώπως. Για να εξετάσουμε ένα αίτημα που σχετίζεται με την εικόνα σας, θα πρέπει να μας προσδιορίσετε πότε περίπου βρεθήκατε στην εμβέλεια των καμερών και να μας δώσετε μια εικόνα σας, ώστε να μας διευκολύνει στον εντοπισμό των δικών σας δεδομένων και στην απόκρυψη των δεδομένων τρίτων εικονιζόμενων προσώπων.

Εναλλακτικά, σας δίνουμε τη δυνατότητα να προσέλθετε στις εγκαταστάσεις μας για να σας επιδείξουμε τις εικόνες στις οποίες εμφανίζεστε. Επισημαίνουμε επίσης ότι η άσκηση δικαιώματος εναντίωσης ή διαγραφής δεν συνεπάγεται την άμεση διαγραφή δεδομένων ή την τροποποίηση της επεξεργασίας. Σε κάθε περίπτωση θα σας απαντήσουμε αναλυτικά το συντομότερο δυνατόν, εντός των προθεσμιών που ορίζει ο ΓΚΠΔ.

8. Δικαίωμα Υποβολής Καταγγελίας

Σε περίπτωση που θεωρείτε ότι η επεξεργασία των δεδομένων που σας αφορούν παραβαίνει τον Κανονισμό (ΕΕ) 2016/679, έχετε δικαίωμα να υποβάλετε καταγγελία σε εποπτική αρχή. Αρμόδια εποπτική αρχή για την Ελλάδα είναι η Αρχή Προστασίας Δεδομένων, Κηφισίας 1-3, 115 23, Αθήνα, https://www.dpa.gr/, τηλ. 2106475600.

3.12 Διαδικασία Διορθωτικών Ενεργειών

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ

ΓΚΠΔ 2016/679 (GDPR)

GEN-04: ΔΙΟΡΘΩΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ & ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. Αποτύπωση Διεργασίας

1.1. Διορθωτικές Ενέργειες

Οι Διορθωτικές ενέργειες αποσκοπούν στην αποφυγή της επανάληψης διαπιστωθέντων μη συμμορφώσεων, συνεισφέροντας με αυτόν τον τρόπο στην διεργασία της συνεχούς βελτίωσης των επιδόσεων και της αποτελεσματικότητας του οργανισμού. Έναρξη λήψης Διορθωτικών Μέτρων πραγματοποιείται για προβλήματα που προέρχονται από:

- το Σύστημα Συμμόρφωσης
- Καθημερινή χρήση Διεργασιών και Πολιτικών του Συστήματος
- Επιθεωρήσεις Πελατών, Φορέων ή Αρχών
- Αποτελέσματα Εσωτερικών Επιθεωρήσεων
- Αποτελέσματα Ανασκοπήσεων του Συστήματος
- Αποτελέσματα Αυτό-αξιολόγησης
- Μη τήρηση της σχετικής νομοθεσίας και κανονισμών.
- την Επεξεργασία Προσωπικών & Ειδικών κατηγοριών (Ευαίσθητων) Προσωπικών Δεδομένων
- Περιστατικά Παραβίασης Δεδομένων
- Αδυναμία ανταπόκρισης σε αιτήματα υποκειμένων
- Αδυναμία τήρησης Μέτρων Ασφάλειας
- Παράπονα υποκειμένων
- Άσκηση Δικαιωμάτων Υποκειμένων
- Συγκαταθέσεις και σκοποί επεξεργασίας
- Διατήρηση αρχείων και δεδομένων
- Συνεργασία με Προμηθευτές

Η ανάλυση και παρακολούθηση των πρωταρχικών αιτίων των «μη συμμορφώσεων» διενεργείται συστηματικά από τον Υπεύθυνο Ασφάλειας Πληροφοριών. Τα συμπεράσματα και οι αιτίες καταγράφονται στο Έντυπο E.GEN.04.01 «Διορθωτικές Ενέργειες & Προτάσεις Βελτίωσης» και παρουσιάζονται συγκεντρωτικά και ειδικότερα κατά την διεξαγωγή της ανασκόπησης του συστήματος συμμόρφωσης.

1.2. Υλοποίηση Διορθωτικών Ενεργειών

Από τη στιγμή που έχει εντοπιστεί κάποιο πρόβλημα, ή πρόβλημα που πιθανόν να εμφανιστεί, όλα τα στελέχη έχουν την δυνατότητα να εισηγηθούν ενέργειες αντιμετώπισης. Η πρόταση αυτή, καταγεγραμμένη στο Έντυπο E.GEN.04.01 «Διορθωτικές Ενέργειες & Προτάσεις Βελτίωσης», προωθείται στον Υπεύθυνο Ασφάλειας Πληροφοριών, ο οποίος, σε συνεργασία με τους Υπεύθυνους των εμπλεκόμενων διαδικασιών/πολιτικών:

- διερευνά το εμφανιζόμενο πρόβλημα, μη συμμόρφωση, ή πρόταση,

- αναλύει και καταγράφει τις πιθανές αιτίες εμφάνισης και
- καθορίζει τις απαιτούμενες ενέργειες αντιμετώπισης, τον υπεύθυνο υλοποίησης και την ημερομηνία αποπεράτωσης των ενεργειών.

Σε περίπτωση που απαιτηθεί, για την υλοποίηση των ενεργειών μπορεί να ζητηθεί η έγκριση της Διοίκησης του οργανισμού.

Σημειώνεται ότι:

- η διεξοδική και προσεκτική ανάλυση του προβλήματος συνήθως οδηγεί στη λήψη των σωστών μέτρων αντιμετώπισης
- μπορεί να καθοριστεί συγκεκριμένη ομάδα έργου για την αντιμετώπιση του προβλήματος και την υλοποίηση των Διορθωτικών Μέτρων.

Ο υπεύθυνος που ορίζεται για την υλοποίηση, λαμβάνει αντίγραφο του Εντύπου και πραγματοποιεί την διορθωτική ενέργεια.

Με την ολοκλήρωση της υλοποίησης, ενημερώνεται ο Υπεύθυνο Ασφάλειας Πληροφοριών, ο οποίος φέρει την ευθύνη ελέγχου της αποτελεσματικότητας των ενεργειών που πραγματοποιήθηκαν.

Ο έλεγχος αυτός γίνεται είτε άμεσα είτε κατά την διεξαγωγή της αμέσως επόμενης Εσωτερικής Επιθεώρησης και συμπληρώνεται το σχετικό πεδίο του Εντύπου.

Αν για την υλοποίηση της διορθωτικής ενέργειας απαιτείται αλλαγή γραπτής διαδικασίας ή σύνταξη / έκδοση νέας, ο Υπεύθυνο Ασφάλειας Πληροφοριών συντονίζει τις ενέργειες σύμφωνα με όσα ορίζονται στη GEN-05 «Έλεγχος Εγγράφων & Αρχείων του συστήματος».

1.3. Προτάσεις Βελτίωσης

Προτάσεις για βελτίωση οποιωνδήποτε ενεργειών ή διαδικασιών με σκοπό την αύξηση του επιπέδου ασφάλειας των πληροφοριών του οργανισμού μπορούν να υποβάλουν όλα τα στελέχη.

Οι Προτάσεις διατυπώνονται στο Έντυπο E.GEN.04.01 «Διορθωτικές Ενέργειες & Προτάσεις Βελτίωσης», και προωθούνται στον Υπεύθυνο Συμμόρφωσης, ο οποίος, σε συνεργασία με τους υπεύθυνους των εμπλεκόμενων διεργασιών / πολιτικών, προχωρά στην αξιολόγηση της Πρότασης και την απόφαση υλοποίησής της ή όχι.

Σε περίπτωση που απαιτηθεί, για την υλοποίηση των ενεργειών μπορεί να ζητηθεί η έγκριση της Διοίκησης.

Από τη στιγμή που η Πρόταση Βελτίωσης έχει αποφασιστεί να υλοποιηθεί ισοδυναμεί με Διορθωτική Ενέργεια και ακολουθούνται τα βήματα που αναφέρονται στην Παράγραφο 1.2 «Υλοποίηση Διορθωτικών Ενεργειών».

2. Εισερχόμενα

Εισερχόμενα Από πού το λαμβάνω (πηγές) Τρόπος λήψης Παρατηρήσεις

Ανάγκη για διορθωτική / πρόταση βελτίωσης που προκύπτει (όχι περιοριστικά) από §1.1. Όλοι οι εργαζόμενοι Προφορικά, Γραπτώς, Email

3. Στοιχεία που απαιτούνται για την ορθή υλοποίηση της διεργασίας

Νόμοι / Κανονισμοί, Πρότυπα:

- Νομοθεσία
- Πρότυπα, Κανονισμοί

Πόροι:

- Hardware, software H/Y

Έλεγχοι σε κρίσιμα σημεία

- Έλεγχοι αναγκαιότητας τροποποιήσεων στο σύστημα Συμμόρφωσης με τη συμπλήρωση του εντύπου E.GEN.04.01

4. Εξερχόμενα

Εξερχόμενο Πού το δίνω (αποδέκτες) Τρόπος παράδοσης Παρατηρήσεις

Υλοποίηση Διορθωτικής / Βελτίωσης Υπεύθυνος πολιτικής - Διεργασίας / Υπεύθυνο Ασφάλειας Πληροφοριών / Υπεύθυνος Ασφάλειας Δεδομένων / Γραπτώς, Email

5. Αρχεία και Δεδομένα

Ο Υπεύθυνο Ασφάλειας Πληροφοριών τηρεί το αρχείο, «Αρχείο Διορθωτικών Ενέργειων & Προτάσεων Βελτίωσης» με όλα τα έντυπα E.GEN.04.01 «Διορθωτικές Ενέργειες & Προτάσεις Βελτίωσης».

3.12.1 Έντυπο «Διορθωτικές Ενέργειες – Προτάσεις Βελτίωσης»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ Ε.GEN.04.01: «ΔΙΟΡΘΩΤΙΚΕΣ ΕΝΕΡΓΕΙΕΣ / ΠΡΟΤΑΣΕΙΣ ΒΕΛΤΙΩΣΗΣ»**

Α/Α : | **Διεργασία:**

Ημ/νία:

➢ **Συμπληρώστε Κατάλληλα**

Διορθωτική Ενέργεια:		**Πρόταση Βελτίωσης:**		**Εσωτερική Επιθεώρηση:**	
Εξωτερική Επιθεώρηση:		**Αποτέλεσμα Ανασκόπησης:**		**Μη συμμόρφωση:**	
Παράπονο Πελάτη:		**Άλλη Περίπτωση:**			

➢ **Περιγραφή Προβλήματος / Πρότασης**

Υπ. Συμπλήρωσης:

➢ **Πιθανές Αιτίες - Διερεύνηση & Αξιολόγηση**

Υπ. Συμπλήρωσης:

➢ **Απόφαση - Επόμενες Ενέργειες**

Α/Α	**Περιγραφή Ενέργειας**	**Υπεύθυνος Υλοποίησης/ Υπογραφή**	**Ημ/νια Ολοκλήρωσης**

Υπ. Συμπλήρωσης:

ΕΛΕΓΧΟΣ ΥΛΟΠΟΙΗΣΗΣ ΕΝΕΡΓΕΙΩΝ - FOLLOW UP ACTION

Έγιναν οι Απαιτούμενες Ενέργειες ;	**ΝΑΙ** £	**ΟΧΙ** £	**Λήψη Νέων Μέτρων:**	
Κρίνονται Αποτελεσματικές ;	**ΝΑΙ** £	**ΟΧΙ** £		

Παρατηρήσεις:

Ο Υπ. Ελέγχου:		**Ημ/νια:**

3.13 Διαδικασία Ικανότητες & Ευαισθητοποίηση Προσωπικού

Κοι.Σ.Π.Ε..... ***LOGO***

ΣΥΣΤΗΜΑ ΣΥΜΜΟΡΦΩΣΗΣ ΜΕ ΤΟΝ ΓΚΠΔ 2016/679 (GDPR)

GEN-06: «ΙΚΑΝΟΤΗΤΕΣ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΠΡΟΣΩΠΙΚΟΥ»

	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	**ΥΠΟΓΡΑΦΗ**
Υπεύθυνος Σύνταξης:		
Υπεύθυνος Έγκρισης:		

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. Αποτύπωση Διεργασίας

Ο οργανισμός υιοθετεί κατάλληλες Διαδικασίες/Πολιτικές ώστε να διασφαλίζεται ότι όλο το προσωπικό, είναι επαρκώς καταρτισμένο και διαθέτει σε διαρκή βάση τις αναγκαίες γνώσεις, για την αποτελεσματική παροχή των υπηρεσιών προς τους πελάτες και για την ασφάλεια των πληροφοριών.
Η διαδικασία παρουσιάζεται και περιγράφεται αναλυτικά παρακάτω:

1.1 Ενέργειες Εσωτερικής Εκπαίδευσης & Αξιολόγησης

Κατά την πρόσληψη νέων εργαζόμενων και πριν την οριστική ανάθεση των καθηκόντων εργασίας τους, πραγματοποιείται εσωτερική εκπαίδευση, σε θέματα που σχετίζονται με:

- τους κανόνες λειτουργίας του οργανισμού,
- τις διαδικασίες που εφαρμόζονται στη συγκεκριμένη θέση εργασίας για την οποία προορίζονται,
- τις διαδικασίες και πολιτικές που εφαρμόζονται για την Ασφάλεια των Προσωπικών Δεδομένων,
- τα εφαρμοζόμενο σύστημα για την Ασφάλεια των Προσωπικών Δεδομένων.

Οι πληροφορίες εκπαίδευσης καταχωρούνται στο Έντυπο E.GEN.06.01. «Παρουσιολόγιο» Εκπαίδευσης, όπου καταχωρούνται οι συμμετέχοντες, οι πληροφορίες εκπαίδευσης και η υπογραφή τους.
Επιπρόσθετα, όλες οι εκπαιδεύσεις στις οποίες οι εργαζόμενοι συμμετέχουν καταχωρούνται στο Έντυπο E.GEN.06.03 Καρτέλα Εκπαίδευσης Προσωπικού.
Ο Υπεύθυνος Εκπαίδευσης αξιολογεί την προσφερόμενη εκπαίδευση ώστε να μπορεί να δει τι θα ωφελούσε τους εργαζομένους. Η αξιολόγηση λαμβάνει χώρα μετά την ολοκλήρωση της εκπαίδευσης σε τρία επίπεδα, «Πολύ καλή», «καλή», «μέτρια». Στην περίπτωση του χαρακτηρισμού «μέτρια» αξιολογείται εάν θα πρέπει να επαναληφθεί η εκπαίδευση.
Η αξιολόγηση καταγράφεται στο Έντυπο E.GEN.06.02. «Προγραμματισμός Εκπαίδευσης».

1.2 Ενέργειες Εξωτερικής Εκπαίδευσης

Οι ενέργειες Εξωτερικής Εκπαίδευσης που υλοποιούνται είναι:

i. Προγραμματισμένες - σύμφωνα με το Πρόγραμμα Εσωτερικών και Εξωτερικών Εκπαιδεύσεων, το οποίο καταρτίζει η Διοίκηση με τον Υπεύθυνο Ασφάλειας Πληροφοριών

ii. Έκτακτες - που μπορεί να προκύψουν:

- ύστερα από απαίτηση της Διοίκησης
- ύστερα από απαίτηση συνεργατών του οργανισμού

Στο τέλος κάθε εκπαίδευσης ακολουθεί η αξιολόγηση του εκπαιδευτικού προγράμματος με χρήση του αντίστοιχου εντύπου.

Το είδος αυτών των εκπαιδεύσεων, τα διάφορα στοιχεία τους και οι αξιολογήσεις των εκπαιδεύσεων καταγράφονται στα αρχεία ηλεκτρονικής ή/ και έντυπης μορφής που διατηρεί ο Υπεύθυνος. Στα αρχεία της εκπαίδευσης καταχωρούνται οι σχετικές βεβαιώσεις παρακολούθησης (training certificates) καθώς και τα πιστοποιητικά γνώσεων.

2. Εισερχόμενα

- Αιτήματα Εκπαίδευσης
- Προγραμματισμός Εκπαίδευσης

3. Εξερχόμενα

- Κάλυψη αναγκών οργανισμού
- Προγραμματισμός Εκπαίδευσης
- Αξιολόγηση εκπαιδευτικού προγράμματος

4. Αρχεία και Δεδομένα

Οι εκπαιδεύσεις των εργαζομένων αρχειοθετούνται από τον ΥΑΠ στο Αρχείο «Εκπαίδευση – Στοιχεία Εργαζομένων», με τα παρακάτω έγγραφα:

- Έντυπο Ε.GEN.06.01. «Παρουσιολόγιο εκπαίδευσης»
- Έντυπο Ε.GEN.06.02. «Προγραμματισμός Εκπαίδευσης»
- Έντυπο Ε.GEN.06.03. «Καρτέλα Εκπαίδευσης Προσωπικού»
- Βιογραφικά, πτυχία, σχετικές Βεβαιώσεις παρακολούθησης, πιστοποιητικά εργαζομένων
- Υλικό των διαφόρων εκπαιδευτικών προγραμμάτων

3.13.1 Έντυπο «Παρουσιολόγιο Εκπαίδευσης»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ Ε.GEN.06.01. «ΠΑΡΟΥΣΙΟΛΟΓΙΟ ΕΚΠΑΙΔΕΥΣΗΣ»**

Ημερομηνία / Περίοδος: | **Διάρκεια:**

ΘΕΜΑΤΙΚΗ ΕΝΟΤΗΤΑ:

ΥΠΕΥΘΥΝΟΣ ΕΚΠΑΙΔΕΥΣΗΣ:

Α/Α	**ΣΥΜΜΕΤΕΧΟΝΤΕΣ**	**Θέση**	**Υπογραφή**
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
Επιχειρησιακό Πρόγραμμα
ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

3.13.2 Έντυπο «Προγραμματισμός Εκπαίδευσης»

ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ ΕΚΠΑΙΔΕΥΣΗΣ ΓΙΑ ΤΟ ΕΤΟΣ:_____

Α/Α	ΤΙΤΛΟΣ ΕΚΠΑΙΔΕΥΣΗΣ / ΕΝΗΜΕΡΩΣΗΣ	ΕΚΠΑΙΔΕΥΟΜΕΝΟΙ	ΕΚΠΑΙΔΕΥΤΗΣ	ΠΡΟΓΡΑΜΜΑΤΙΣΜΕΝΗ ΠΕΡΙΟΔΟΣ	ΠΕΡΙΟΔΟΣ ΥΛΟΠΟΙΗΣΗΣ	ΑΞΙΟΛΟΓΗΣΗ ΕΚΠΑΙΔΕΥΣΗΣ*	ΠΑΡΑΤΗΡΗΣΕΙΣ

** Η αξιολόγηση της εκπαίδευσης χαρακτηρίζεται ως Καλή, Μέτρια, Κακή, από τον Υπεύθυνο Διεργασίας.*

Ο Υπεύθυνος Εκπαίδευσης: Ημερομηνία:

3.13.3 Έντυπο «Καρτέλα Εργαζόμενου»

Κοι.Σ.Π.Ε..... ***LOGO***	**ΕΝΤΥΠΟ Ε.GEN.06.03. «ΚΑΡΤΕΛΑ ΕΚΠΑΙΔΕΥΣΗΣ ΠΡΟΣΩΠΙΚΟΥ»**

ΠΡΟΣΩΠΙΚΑ ΣΤΟΙΧΕΙΑ

Ονοματεπώνυμο:	
Τμήμα/Θέση:	

ΠΡΟΫΠΗΡΕΣΙΑ

ΕΤΑΙΡΙΑ	ΘΕΣΗ	ΑΠΟ	ΕΩΣ

ΣΤΟΙΧΕΙΑ ΕΚΠΑΙΔΕΥΣΗΣ

ΠΕΡΙΓΡΑΦΗ ΕΚΠΑΙΔΕΥΣΗΣ	ΗΜ/ΝΙΑ	ΔΙΑΡΚΕΙΑ	ΑΞΙΟΛΟΓΗΣΗ	ΦΟΡΕΑΣ ΥΛΟΠΟΙΗΣΗΣ

Επιχειρησιακό Πρόγραμμα
ΜΕΤΑΡΡΥΘΜΙΣΗ ΔΗΜΟΣΙΟΥ ΤΟΜΕΑ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
Ευρωπαϊκή Ένωση
ΕΣΠΑ 2014-2020

ΚΕΦΑΛΑΙΟ 4. Εγχειρίδιο Καλών Πρακτικών

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (GDPR)

ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ

Καλή Πρακτική 1

- Ακολουθείστε τις **πολιτικές** και τις **διαδικασίες** της εταιρίας.

- **Διαχειριστείτε** τα δεδομένα των **άλλων** όπως θα θέλατε κι εκείνοι να διαχειριστούν τα**δικά σας** προσωπικά δεδομένα.

Καλή Πρακτική 2

- Θυμηθείτε – οι **άμεσα ενδιαφερόμενοι** έχουν το **δικαίωμα** να ζητήσουν **πρόσβαση** στα δεδομένα που καταγράφετε για εκείνους. Οπότε σιγουρευτείτεότι:
  - Καταγράφετε **καθαρά** τα δεδομένα ώστε οι άλλοινα μπορούν να βασιστούν στις εγγραφές σας.
  - Να είστε **ακριβείς** και να ανανεώνετε ορθά καιτακτικά τις πληροφορίες.

- Να **ενημερώνεστε τακτικά** για τις προσθήκες στον **Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR).**

Καλή Πρακτική 3

Καταγραφή Αρχείου

Είναι κρίσιμης σημασίας τα **αρχεία** να:

- Είναι **ανανεωμένα** και **ακριβή**.
- Πρέπει να γνωρίζετε **τι** και **γιατί** πρέπει να καταγραφεί και ποιο είναι το **κατάλληλο αρχείο** στο οποίο πρέπει να γίνει η καταγραφή αυτή.
- Πρέπει να **ελέγχετε** τις πληροφορίες.
- Πρέπει να **αναφέρετε** τυχόν **λάθη** ή **παραλείψεις** στον υπεύθυνο.
- Τα δεδομένα πρέπει να **καταγράφονται** τη **στιγμή** που κάποιο **γεγονός** που απαιτεί καταγραφή **λαμβάνει χώρα**.

- Πρέπει να **αποφεύγεται** η δημιουργία **διπλοτύπων**.

Σενάριο: Ο Βασίλης ακολουθεί θεραπεία για την κατάθλιψη και δεν το έχει μοιραστεί με κανένα στη δουλειά του. Λόγω ενός λάθους στην καταγραφή των δεδομένων του, η κλινική τον καλεί στον αριθμό της δουλειάς αντί για τον προσωπικό του αριθμό. Ένας συνάδελφός του απαντά την κλήση και ο υπάλληλος της κλινικής αυθαίρετα θεωρεί πως αυτός είναι ο Βασίλης. Ο συνάδελφος μαθαίνει για την κατάσταση του Βασίλη και σπεύδει να ενημερώσει και τους υπόλοιπους συναδέλφους. Ντροπιασμένος ο Βασίλης παραιτείται και κάνει επίσημο παράπονο στην κλινική.

Το σενάριο αυτό δείχνει τη σημαντικότητα:

1. Του να **καταγράφουμε** τα δεδομένα με **ακρίβεια** και στα σωστά συστήματα.
2. Να **πιστοποιούμε** την **ταυτότητα** του ενδιαφερόμενου πριν **αποκαλύψουμε** εμπιστευτικές πληροφορίες.

4.1 Αποφυγή Απειλών της Ασφάλειας των Δεδομένων

Πιθανές **απειλές** της ασφάλειας των πληροφοριών στο **χώρο εργασίας**.

Ενημέρωση για:

- Την **κοινωνική μηχανική**
- Το **email phishing** καθώς και το **κακόβουλο** λογισμικό
- **Καλές πρακτικές** για την προστασία των πληροφοριών

4.1.1 Η Κοινωνική Μηχανική (Social Engineering)

Όσοι θέλουν να υποκλέψουν δεδομένα θα χρησιμοποιήσουν **τεχνάσματα** προκειμένου να **χειραγωγήσουν** τους ανθρώπους για να τους παρέχουν **πρόσβαση** σε πολύτιμες πληροφορίες. Το φαινόμενο αυτό καλείται **κοινωνική μηχανική (social engineering)**.

Παραδείγματα:

- ***Στο τηλέφωνο:*** Ο εγκληματίας μπορεί να καλέσει υποδυόμενος ένα συνάδελφο ή μία έμπιστη εξωτερική Αρχή.
- ***Στο γραφείο:*** Σίγουρα έχετε ακούσει τη φράση «Μπορείτε να κρατήσετε την πόρτα παρακαλώ; Έχω ξεχάσει τα κλειδιά/κάρτα μου σήμερα». Μπορεί το άτομο που θα σας το ζητήσει να μη φαίνεται ύποπτο, αλλά αυτή είναι μία συνήθης τακτική για φυσική είσοδο σε χώρο γραφείων.
- ***Στο διαδίκτυο:*** Τα κοινωνικά δίκτυα είναι ένας ακόμη χώρος στον οποίο δρουν οι εγκληματίες. Οι τελευταίοι, υποδύονται τους φίλους στο Facebook, μιας και ποτέ δε

μπορείς να είσαι σίγουρος ποιο άτομο βρίσκεται στην άλλη άκρη της οθόνης (κλοπές κωδικών, παραβίαση λογαριασμών, κτλ) με σκοπό το οικονομικό τους όφελος.

Καλή Πρακτική 4 – Αντιμετώπιση Κοινωνικής Μηχανικής

Πάντοτε να είστε **προσεκτικοί**:

- Όταν χρησιμοποιείτε το **κινητό** σας τηλέφωνο.
- Όταν λαμβάνετε **αυτόκλητα** ηλεκτρονικά **μηνύματα**.
- Όταν χρησιμοποιείτε τα **μέσα κοινωνικής δικτύωσης**.
- Ακόμη και όταν περπατάτε κοντά στο χώρο εργασίας σας.

Όπου κρίνετε ότι είναι ασφαλές:

- Ζητάτε **στοιχεία** που αποδεικνύουν την **ταυτότητα** του συνομιλητή σας.
- Μη φοβηθείτε να **αντιμετωπίσετε** και να καταστείλετε **ύποπτες** συμπεριφορές.

4.1.2 Email Phishing και κακόβουλο λογισμικό

Παρόλο που το ηλεκτρονικό ταχυδρομείο είναι ένα **αποτελεσματικό** μέσο επικοινωνίας, **ενέχει κινδύνους**.

- Χρησιμοποιούνται **επισυναπτόμενα** ή και **σύνδεσμοι** (links) προκειμένου να **εξαπατηθεί** ο χρήστης ώστε να παρέχει πληροφορίες.
- Τα επισυναπτόμενα μπορεί να αποτελούν **εκτελέσιμα** ("*όνομα*".exe) **αρχεία** που περιέχουν **κακόβουλο** λογισμικό, στο οποίο εν αγνοία του ο χρήστης να προκαλέσει **εγκατάσταση**.

Τα ηλεκτρονικά αυτά μηνύματα, σε **παροτρύνουν** να κάνεις κάποιο **λάθος**.

- Ποτέ **μη μοιράζεστε** τα στοιχεία σύνδεσής σας με άλλα πρόσωπα.
- Σε περίπτωση που λάβετε κάποιο ηλεκτρονικό **μήνυμα** από κάποιο **συνεργάτη**, ο οποίος ζητά **ευαίσθητα** δεδομένα, ***διασταυρώστε*** την εγκυρότητα καλώντας και **τηλεφωνικά** το συνεργάτη σας.
- **Μην ανοίγετε συνδέσμους** ή **επισυναπτόμενα** σε αυτόκλητα ηλεκτρονικά μηνύματα.
- ***Πάντοτε*** να ενημερώνετε για **ύποπτα** μηνύματα στο ηλεκτρονικό ταχυδρομείο σας τους **υπεύθυνους των πληροφοριακών Συστημάτων**.

Καλή Πρακτική 5 – Αντιμετώπιση Email Phishing και κακόβουλου λογισμικού

Να είστε προσεκτικοί:

- **Μην εγκαθιστάτε** νέα λογισμικά **εκτός** εάν αυτά είναι εξουσιοδοτημένα.
- **Συζητάτε** τα **προβλήματα** που δημιουργούνται με τον **προϊστάμενό** σας.

Στην περίπτωση που **εντοπίσετε** ένα phishing email, ακολουθείστε τα παρακάτω βήματα:

- **Μην** απαντήσετε.
- **Επιλέξτε** το ηλεκτρονικό μήνυμα, κάντε δεξί κλικ και σημαδέψτε το ως "**spam**".
- **Μπλοκάρετε** ύποπτες ηλεκτρονικές διευθύνσεις, αποτρέποντάς τες από το να σας **αποστέλλουν** ηλεκτρονικά μηνύματα.
- Ενημερώστε τους **υπεύθυνους**, καθώς είναι πιθανό ο Οργανισμός να απειλείται από ηλεκτρονική επίθεση και να πρέπει να **ληφθούν** τα απαραίτητα **μέτρα**.

Το **κακόβουλο** λογισμικό ενδέχεται να:

- **Βρίσκεται** στον υπολογιστή σας και **να μη γίνει αντιληπτό**.
- Κάνει τον υπολογιστή σας **πιο αργό** ή αυτός να **λειτουργεί με ασυνήθιστους τρόπους**.

Πρέπει να ενημερώνετε τον **Υπεύθυνο Πληροφοριακών Συστημάτων** σας.

Καλή Πρακτική 6 – Κωδικοί Χρήστη

- Χρησιμοποιείτε πάντα **δυνατούς κωδικούς** σε όλες τις συσκευές προκειμένου να αποφευχθεί μη εξουσιοδοτημένη πρόσβαση (χρησιμοποιείτε **διαφορετικούς** κωδικούς για κάθε **λογαριασμό**).

Ακολουθείτε **απλές πρακτικές** ώστε οι κωδικοί σας να είναι δυνατοί:

- Να περιέχουν αριθμούς, γράμματα, σύμβολα και να είναι μεταξύ 8-12 χαρακτήρων είναι το ιδανικό.

Καλή Πρακτική 7 – Κλείδωμα των Συσκευών

- **Κλειδώστε** τη συσκευή σας αμέσως μόλις **σταματήσετε** να τη **χρησιμοποιείτε**.
- Θέστε **κωδικούς** στα κινητά σας τηλέφωνα, τους ηλεκτρονικούς υπολογιστές, τα λάπτοπ και τα τάμπλετ σας.
- Εάν δείτε τη συσκευή κάποιου **συναδέλφου** σας ξεκλείδωτη και ανοιχτή, **κλειδώστε την εσείς για εκείνον** και υπενθυμίστε του ευγενικά να κάνει το ίδιο στο μέλλον.

- Στις εταιρικές συσκευές, πρέπει να είναι **ενεργοποιημένη η λειτουργία κλειδώματος**.

Σημείωση: επιλέξτε το κουμπί των Windows + L στο πληκτρολόγιό σας για να κλειδώσετε γρήγορα το λάπτοπ ή τον Η/Υ σας.

Καλή Πρακτική 8 – Αφαιρούμενες Συσκευές/Δίσκοι

- **Μη** χρησιμοποιείτε **μη εξουσιοδοτημένες** συσκευές αποθήκευσης.
- **Μη συνδέετε** συσκευές που **δεν** είναι εγκεκριμένες για φόρτιση **μέσω καλωδίου USB**.
- **Σκανάρετε** τις συσκευές USB πριν τη χρήση.
- Εάν έχετε αμφιβολίες/απορίες, ρωτήστε τον υπεύθυνο.

Καλή Πρακτική 9 – Μη έμπιστες Ιστοσελίδες (Untrusted Websites)

- Να είστε **επιφυλακτικοί** όταν **επισκέπτεστε** κάποια ιστοσελίδα που είναι δηλωμένη ως «**μη έμπιστη**».
- Εάν ένας περιηγητής (**web browser**) σας εμφανίσει ότι η σελίδα που προσπαθείτε να ανοίξετε είναι **μη έμπιστη**, πρέπει να **προσέξετε** – μπορεί να είναι μία ψεύτικη/phishing ιστοσελίδα, δομημένη με τρόπο ώστε να φαίνεται αξιόλογη.
- Ο περιηγητής μπορεί να εμφανίσει ένα κόκκινο λουκέτο, ή μία προειδοποίηση με μήνυμα *«**Your connection is not private**»*.

Καλή Πρακτική 10 – Κινητές Συσκευές

- Τι να κάνετε:
  - ✓ Διαβάστε, κατανοείτε και συμμορφώνεστε με τις **πολιτικές** και τις **διαδικασίες** της εταιρίας.
  - ✓ **Αποθηκεύετε** τα ψηφιακά σας υπάρχοντα με **ασφάλεια** όταν δεν τα χρησιμοποιείτε.
  - ✓ Εάν οι ψηφιακές συσκευές σας, **εμφανίσουν** μήνυμα για **ενημέρωση** του **antivirus** λογισμικού, **μην παραλείψετε** να το ενημερώσετε.
  - ✓ Να διατηρείτε **τακτικά Backups** των αποθηκευμένων δεδομένων τα οποία θα αποθηκεύετε κατάλληλα, **σύμφωνα** με τις **πολιτικές** της εταιρίας.
  - ✓ **Ενημερώστε τις αρχές** για τυχόν χαμένα ή κλεμμένα ψηφιακά υπάρχοντά σας.
  - ✓ Να ακολουθείτε τις πολιτικές της εταιρίας για τη διαχείριση των περιστατικών (**incident management**).

- ✓ Βεβαιωθείτε ότι σε περίπτωση που **φύγετε** από την εταιρία, έχετε **παραδώσει** τα **ψηφιακά υπάρχοντα** που ανήκουν σε αυτή καθώς και **όλους τους κωδικούς** που ανήκουν σε αυτά και στην εταιρία γενικότερα.

❖ Τι να ***ΜΗΝ*** κάνετε:

- X **Μη χρησιμοποιείτε** τις **προσωπικές** σας συσκευές για **επαγγελματικούς** σκοπούς, εκτός εάν είστε εξουσιοδοτημένοι.
- X Μη χρησιμοποιείτε ψηφιακά υπάρχοντα που σας παρέχονται από την εταιρία, σε **άγνωστα ή μη έμπιστα δίκτυα** – για παράδειγμα δημόσια Wi-Fi Hotspots.
- X Μην επιτρέπετε **σε μη εξουσιοδοτημένα** πρόσωπα, φίλους ή συγγενείς να χρησιμοποιούν ψηφιακά υπάρχοντα που σας **παρέχονται από την εταιρία**.
- X Μη χρησιμοποιείτε **μη εξουσιοδοτημένο εξοπλισμό** κανενός είδους στα ψηφιακά υπάρχοντα που σας παρέχει η εταιρία.
- X Μην **αφαιρείτε** ή **αντιγράφετε προσωπικά δεδομένα**, συμπεριλαμβανομένων ψηφιακών δεδομένων (με email ή κάποιο USB) σε σημείο που δεν είναι εμφανές, χωρίς εξουσιοδότηση.
- X Μην αφήνετε ψηφιακά υπάρχοντα σε σημείο από το οποίο είναι εύκολο να **κλαπούν**.
- X **Μην εγκαθιστάτε** μη εξουσιοδοτημένο λογισμικό ή κατεβάζετε λογισμικό ή δεδομένα από το διαδίκτυο.
- X **Μην απενεργοποιείτε** το antivirus λογισμικό στα ψηφιακά σας υπάρχοντα.

Καλή Πρακτική 11 – Διαγραφή εμπιστευτικής πληροφορίας

❖ Ιδιαίτερη σημασία πρέπει να δοθεί στην ασφαλή διαγραφή των:

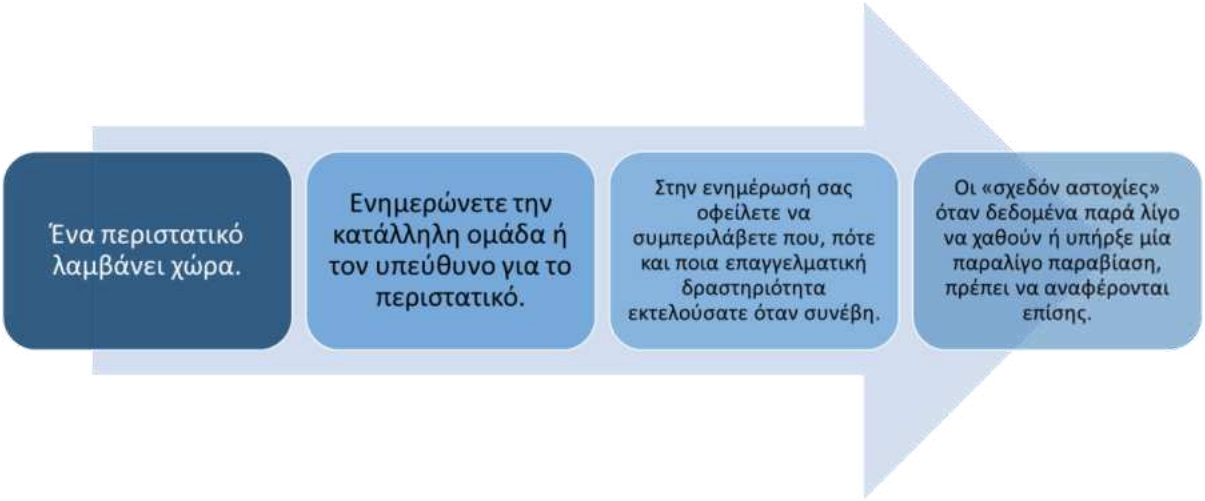
- ➢ Εγγράφων που περιέχουν εμπιστευτικές πληροφορίες
- ➢ Σταθερών ηλεκτρονικών υπολογιστών
- ➢ Laptop, tablets και ηλεκτρονικά notebooks
- ➢ Ψηφιακών καταγραφών
- ➢ Καμερών
- ➢ Φορητών Συσκευών USB, CD, DVD και γενικά αφαιρούμενων δίσκων.

❖ Ακολουθείτε σε κάθε περίπτωση τις διαδικασίες της επιχείρησης αναφορικά με τις ασφαλείς διαγραφές.

Καλή Πρακτική 12 – Clear Desks

- Ακολουθείτε τις πολιτικές για **clear desk** της εταιρίας.
- Μην αφήνετε πληροφορίες σε **ανασφαλείς τοποθεσίες** μετά το πέρας της εργασίας σας.
- Με το να διατηρείτε ένα **άδειο γραφείο**, οι πιθανότητες να παραμείνουν εμπιστευτικά δεδομένα χωρίς επιτήρηση **μειώνεται,** μειώνοντας έτσι και τον κίνδυνο παραβίασης.

4.2 Αναφορά Περιστατικών



Καλή Πρακτική 13 – Αποφυγή ταχυδρομικής παραβίασης

- Απευθύνετε προσωπικά δεδομένα **ονομαστικά** στο άτομο στο οποίο αυτά αφορούν.
- Χρησιμοποιείτε καταγεγραμμένη ή **ελεγχόμενη** αποστολή για τα προσωπικά δεδομένα.
- Σημειώσεις που αφορούν σε προσωπικά δεδομένα πρέπει να αποστέλλονται σε **εύρωστη** και **εγκεκριμέν**η συσκευασία.

4.3 Παραβίαση Email

Η κατάσταση:

- Ο κύριος Παπάς πρόσφατα διαγνώστηκε με κατάθλιψη και εντάχθηκε σε μία ομάδα υποστήριξης για να τον βοηθήσει ψυχολογικά.

- Ο οργανισμός χρησιμοποιεί το ηλεκτρονικό ταχυδρομείο για την αποστολή ενημερωτικών μηνυμάτων στα μέλη της ομάδας.
- Πρόσφατα, άρχισαν να δέχονται παράπονα από ιδιώτες για τη διαρροή των ονομάτων και των ηλεκτρονικών τους διευθύνσεων σε περισσότερα από 500 άτομα.

Η αντίδραση του οργανισμού:

- Ο υπεύθυνος του οργανισμού ερευνά το θέμα και βρίσκει πως ένα νέο μέλος του προσωπικού έχει στείλει το email. Ο υπάλληλος αυτός, κατά λάθος **έβαλε** τα μέλη της ομάδας στην ενότητα "**CC**" αντί του πεδίου "**BCC**" στα email που στάλθηκαν.

Συνέπειες:

- Όλοι όσοι είχαν λάβει το email γνώριζαν ποιος ήταν μέλος της ομάδας υποστήριξης για την κατάθλιψη.
- Η έρευνα επίσης έδειξε, ότι παρόλο που οι υπόλοιποι υπάλληλοι γνώριζαν πώς να κάνουν τη δουλειά τους σωστά, κανένας δεν ήλεγξε εάν το νέο μέλος του προσωπικού έκανε σωστά τη δουλειά του.

Καλή Πρακτική 14

- **ΠΡΙΝ** στείλετε κάποιο ηλεκτρονικό μήνυμα σε τρίτους:
  - **Ελέγχετε** εάν είναι **αποδεκτό** να στείλετε προσωπικά δεδομένα.
  - **Επιβεβαιώνετε** την **εγκυρότητα** της ηλεκτρονικής διεύθυνσης.
  - **Ελέγχετε** ότι όλοι όσοι βρίσκονται στη λίστα **παραληπτών** έχουν λόγο να «γνωρίζουν».
  - Χρησιμοποιείτε όσο το δυνατόν **λιγότερες** πληροφορίες που είναι αναγνωριστικές για τους παραλήπτες.
  - Ελέγχετε τις απαιτήσεις **κρυπτογράφησης**.
- Όταν πρέπει ένα email να σταλεί σε έναν μη **διαπιστωμένο** παραλήπτη:
  - Ελέγχετε ότι κατανοούν και αποδέχονται τους κινδύνους.
  - Ελέγχετε αν μπορείτε να κρυπτογραφήσετε το ηλεκτρονικό μήνυμα.

4.4 Τηλεφωνική Παραβίαση

Η κατάσταση:

- Ένας υπάλληλος μιας ασφαλιστικής εταιρίας, λαμβάνει ένα τηλεφώνημα, μέσω του οποίου μια άλλη ασφαλιστική αιτείται στοιχεία για την κυρία Κανελλοπούλου, μία πελάτισσά του.

- Ο ίδιος γνωρίζει την ασφαλιστική αυτή καθώς και το γεγονός ότι έχει γίνει σύσταση στην κυρία Κανελλοπούλου να απευθυνθεί εκεί για κάποια ειδική ασφάλεια, οπότε δίνει τις πληροφορίες στον υπάλληλο της άλλης ασφαλιστικής.

Συνέπειες:

- Το επόμενο πρωί, η κυρία Κανελλοπούλου τηλεφωνεί στον υπάλληλο της ασφαλιστικής εταιρίας και ενημερώνει πως ο κουμπάρος της έχει πληροφορίες για την ίδια, που μόνο η ασφαλιστική εταιρία της θα μπορούσε να γνωρίζει.
- Στο σημείο αυτό ο υπάλληλος συνειδητοποιεί ότι δεν έχει αποδείξεις για την κλήση της προηγούμενης ημέρας και το αν αυτή έγινε από την άλλη ασφαλιστική.

Καλή Πρακτική 15

- Όταν είναι δυνατό:
  - **Ελέγχετε τα στοιχεία του συνομιλητή** σας (όνομα, τίτλος εργασίας, οργανισμό/εταιρία)
  - Ελέγχετε αν ο **λόγος** είναι **κατάλληλος** για παροχή δεδομένων.
  - Κρατάτε **αριθμό τηλεφώνου** του συνομιλητή σας.
  - Ελέγχετε αν τα δεδομένα μπορούν να δοθούν. **Εάν έχετε αμφιβολίες**, πείτε στο συνομιλητή σας ότι **θα καλέσετε εσείς** και ρωτήστε κάποιον υπεύθυνο.
  - Δίνετε τις πληροφορίες **μόνο** στον ενδιαφερόμενο.
- Καταγράψτε το όνομά σας και τις λεπτομέρειες σχετικά με τις πληροφορίες που παρέχετε, μαζί με τα στοιχεία του παραλήπτη.

ΠΑΡΑΡΤΗΜΑ

Παράρτημα 1. Φόρμα αυτοαξιολόγησης της συμμόρφωσης

5. GAP ANALYSIS

Στον πίνακα που ακολουθεί αποτυπώνονται οι συμμορφώσεις, αλλά κυρίως οι ελλείψεις και οι σημαντικές ή μη παρεμβάσεις που πρέπει να γίνουν, ώστε η επιχείρηση να συμμορφωθεί με τα όσα προβλέπονται στον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων όσο και με τις κυριότερες απαιτήσεις του προτύπου ISO 27001:2013.

Για την καλύτερη κατανόηση του πίνακα που ακολουθεί:

Control	Τα σημεία ελέγχου που αφορούν τη συμμόρφωση της επιχείρησης με τον GDPR και το ISO 27001.
Απαίτηση	Επιμέρους απαιτήσεις κάλυψης των απαιτήσεων του σημείου ελέγχου
Ναι – Μερικώς – Όχι – N/A	**ΝΑΙ** - Οι απαιτήσεις του Κανονισμού (GDPR) ή/και του προτύπου ISO 27001 **καλύπτονται** πλήρως και δεν απαιτείται κάποια περαιτέρω ενέργεια **ΜΕΡΙΚΩΣ** - Οι απαιτήσεις του Κανονισμού (GDPR) ή/και του προτύπου ISO 27001 **δεν καλύπτονται μερικώς ή πλήρως** και απαιτείται ο σχεδιασμός κάποιας πολιτικής ή διαδικασίας. **ΟΧΙ** - Οι απαιτήσεις του Κανονισμού (GDPR) ή/και του προτύπου ISO 27001 **δεν καλύπτονται μερικώς ή πλήρως** και απαιτείται η υλοποίηση διαφόρων ενεργειών από την πλευρά της εταιρείας (π.χ. προμήθεια νέου εξοπλισμού) ή ο σχεδιασμός κάποιας πολιτικής ή διαδικασίας. **N/A** – Δεν έχει εφαρμογή
Ευρήματα Τεκμηρίωση	Αποτύπωση της υφιστάμενης κατάστασης (σε οργανωτικό, λειτουργικό, τεχνολογικό επίπεδο)
Ενέργειες	Απαιτούμενες ενέργειες για την κάλυψη των απαιτήσεων του σημείου ελέγχου.

Ι. ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ ΠΟΥ ΑΠΑΙΤΟΥΝΤΑΙ ΑΠΟ ΤΟΝ ΚΑΝΟΝΙΣΜΟ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΕΕ 2016/679

1. Προσωπικά Δεδομένα

	Control	*Απαίτηση*	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Προσωπικά Δεδομένα (ΠΔ) (άρθ.4§1)	Επεξεργάζεστε ΠΔ;						
2.	Ευαίσθητα ΠΔ (άρθ 9)	Επεξεργάζεστε ευαίσθητα Π.Δ.;						
3.	ΠΔ ανηλίκων (παιδιά κάτω των 16 χρονών Ελλην. Νομοθεσία 18 έτη– άρθ. 8 και 12)	Επεξεργάζεστε Π.Δ. παιδιών;						

2. Υπεύθυνος Επεξεργασίας και Εκτελών την Επεξεργασία

	Control	*Απαίτηση*	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Υπεύθυνος επεξεργασίας (άρθρο 24)	Είστε υπεύθυνος επεξεργασίας;						
2.	Εκτελών επεξεργασία (άρθ. 28)	Είστε ο εκτελών της επεξεργασίας;						
3.	Υπεύθυνος/ Εκτελών Επεξεργασία εκτός ΕΕ	Μήπως μια ομάδα εταιρειών βρίσκεται εκτός της ΕΕ και στοχεύει / παρακολουθεί τα υποκείμενα της ΕΕ;						
		Αν ναι, ο εγκατεστημένος εκπρόσωπος για την ΕΕ σε ένα από τα κράτη μέλη της ΕΕ όπου βρίσκονται τα υποκείμενα των δεδομένων έχει οριστεί γραπτώς (όπου ενδείκνυται);						
		Υποχρεώνεται ο αντιπρόσωπος της ΕΕ από τις εποπτικές αρχές και τα υποκείμενα δεδομένων να απευθυνθεί (πέραν του Υπεύθυνου Επεξεργασίας / Εκτελούντος Επεξεργασία) σε θέματα επεξεργασίας;						
4.	Κοινοί Υπεύθυνοι Επεξεργασίας (άρθ. 26)	Παρατηρούνται κοινές σχέσεις επεξεργασίας ανάμεσα στους Υπεύθυνους Επεξεργασίας δεδομένων						

		διαφορετικών οντοτήτων;						

3. Εδαφικό πεδίο εφαρμογής

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Κύρια Εγκατάσταση (άρθ. 3)	Που βρίσκονται τα κεντρικά σας γραφεία;						

4. Νόμιμοι λόγοι επεξεργασίας (άρθρο 6)

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Νόμιμοι λόγοι επεξεργασίας (άρθ. 6)	Αντιστοιχεί η κάθε επεξεργασία σε μία νόμιμη βάση;						
		Υπάρχουν νόμιμοι λόγοι επεξεργασίας ευαίσθητων προσωπικών δεδομένων για κάθε διαδικασία επεξεργασίας;						
2.	Συγκατάθεση (άρθ. 7 και 8)	Λαμβάνεται συγκατάθεση, όπου δεν υπάρχει άλλη νόμιμη βάση επεξεργασίας;						

5. Απαιτήσεις Διαφάνειας

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Ενημέρωση του υποκείμενου δεδομένων (άρθρα 12, 13 και 14)	Έχει ενημερωθεί το υποκείμενο δεδομένων για την επεξεργασία;						
2.	Πηγή προσωπικών δεδομένων και πληροφορίες που παρέχονται στο υποκείμενο δεδομένων (άρθρα 12, 13 και 14)	Τα δεδομένα συλλέγονται απευθείας από τα υποκείμενα και τους παρέχονται οι απαιτούμενες πληροφορίες;						
		Τα δεδομένα δεν συλλέγονται απευθείας από τα υποκείμενα και τους παρέχονται οι απαιτούμενες πληροφορίες;						

6. Αρχές επεξεργασίας δεδομένων

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Νομιμότητα (άρθρο 5,1α)	Επεξεργάζονται τα προσωπικά δεδομένα με νόμιμο, θεμιτό και διαφανή τρόπο;						
2.	Περιορισμός σκοπού (άρθρο 5,1β)	Χρησιμοποιούνται προσωπικά δεδομένα μόνο για τους σκοπούς για τους οποίους συλλέχθηκαν αρχικά;						
3.	Ελαχιστοποίηση δεδομένων (άρθρο 5,1γ)	Τα προσωπικά δεδομένα περιορίζονται σε αυτά που είναι απαραίτητα για τους σκοπούς για τους οποίους γίνεται η επεξεργασία τους;						
4.	Ακρίβεια (άρθρο 5,1δ)	Έχουν θεσπιστεί πολιτικές και έχει γίνει κατάρτιση για τη διασφάλιση της επαλήθευσης των προσωπικών δεδομένων και την άμεση αποκατάσταση των ανακριβών στοιχείων;						
5.	Περιορισμός αποθήκευσης (διατήρηση) (άρθρο 5,1ε)	Οι πολιτικές απορρήτου ενσωματώνουν πληροφορίες σχετικά με τη διατήρηση; Υπάρχουν διαδικασίες για την αρχειοθέτηση και την καταστροφή δεδομένων;						
6.	Ακεραιότητα και Εμπιστευτικότητα (άρθρο 5,1στ)	Χρησιμοποιούνται κατάλληλα μέτρα ασφαλείας για την προστασία των δεδομένων;						
7.	Λογοδοσία (άρθρο 5,2)	Μπορείτε να επιδείξετε τη συμμόρφωση με τις αρχές προστασίας δεδομένων;						

7. Δικαιώματα Υποκείμενων Δεδομένων

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Πρόσβαση σε προσωπικά δεδομένα (άρθρο 15)	Υπάρχει τεκμηριωμένη πολιτική / διαδικασία για το χειρισμό των αιτήσεων πρόσβασης σε δεδομένα από τα υποκείμενα (Subject Access Requests – SARs);						
		Παρέχεται στα άτομα μηχανισμός για να ζητήσουν πρόσβαση σε πληροφορίες σχετικά με αυτά;						
		Είναι ο Υπεύθυνος Επεξεργασίας ικανός να ανταποκριθεί στα SAR μέσα σε ένα μήνα;						
2.	Φορητότητα δεδομένων (άρθρο 20)	Μπορούν τα υποκείμενα των δεδομένων να αποκτήσουν τα προσωπικά τους δεδομένα σε δομημένη, ευρέως χρησιμοποιούμενη και μηχανικά αναγνώσιμη μορφή;						
3.	Διαγραφή και διόρθωση (άρθρο 16 και άρθρο 17)	Τα άτομα ενημερώνονται για το δικαίωμά τους να ζητήσουν τη διαγραφή ή τη διόρθωση των προσωπικών τους πληροφοριών (όπου ισχύει);						
		Υπάρχουν έλεγχοι και επίσημες διαδικασίες που επιτρέπουν τη διαγραφή των προσωπικών δεδομένων (Δικαίωμα στη λήθη);						
4.	Δικαίωμα αντικρούσεως (άρθρο 21- Δικαίωμα εναντίωσης)	Τα άτομα ενημερώνονται για το δικαίωμά τους να αντιταχθούν σε ορισμένους τύπους επεξεργασίας;						
5.	Προφίλ και αυτοματοποιημένη επεξεργασία (άρθρο 22- Αυτοματοποιημένη ατομική λήψη αποφάσεων, περιλαμβανομένης	Η δημιουργία προφίλ βασίζεται στη συγκατάθεση; (αν ναι, αυτό πρέπει να είναι σαφές)						
		Μήπως κάποιο προφίλ χρησιμοποιεί ευαίσθητα δεδομένα;						

	της κατάρτισης προφίλ)	Μήπως κάποιο προφίλ περιλαμβάνει δεδομένα παιδιών;						
6.	Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18)	Δίνεται η δυνατότητα στα υποκείμενα να περιορίσουν την επεξεργασία των δεδομένων που τα αφορούν;						

8. Μεταφορά δεδομένων εκτός ΕΟΧ

	Control	*Απαίτηση*	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΌΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Διεθνής χαρτογράφηση ροής δεδομένων (άρθρα 44 – 50)	Τα προσωπικά δεδομένα μεταφέρονται εκτός ΕΟΧ (Ευρωπαϊκός Οικονομικός Χώρος);						
		Μεταφέρονται και ευαίσθητα προσωπικά δεδομένα;						
		Ποιος είναι ο σκοπός (οι) της μεταφοράς;						
		Ποιος είναι ο παραλήπτης;						
		Είναι καταχωρημένες όλες οι μεταφορές - συμπεριλαμβανομένων των απαντήσεων στα προηγούμενα ερωτήματα (π.χ. η φύση των δεδομένων, ο σκοπός της επεξεργασίας, από ποια χώρα εξάγονται τα δεδομένα και ποια χώρα τα λαμβάνει, καθώς και ποιος είναι ο αποδέκτης της μεταφοράς;)						
		Είναι ο επαρκής μηχανισμός νόμιμης μεταφοράς για κάθε αναγνωρισμένη και καταχωρημένη μεταφορά εντοπισμένος και καταγεγραμμένος;						
2.	Νομιμότητα των διεθνών μεταφορών (άρθρα 44 – 50)	Οι συγκεκριμένες μεταφορές καλύπτονται κατάλληλα από έναν εφαρμοσμένο μηχανισμό επάρκειας ή καλύπτονται από μια εξαίρεση;						

3.	Διαφάνεια (άρθρα 44 – 50)	Αναφέρονται στα υποκείμενα τυχόν προβλεπόμενες μεταβιβάσεις των προσωπικών δεδομένων τους;						
4.	Μεταφορές που ζητούνται από υπερπόντιες αρχές ή δικαστήρια (άρθρα 44 – 50)	Υπάρχει πολιτική για τη διεκπεραίωση αιτήσεων για αποκάλυψη / μεταφορά προσωπικών δεδομένων σε υπερπόντιες αρχές ή δικαστήρια;						

9. Άλλες υποχρεώσεις Υπεύθυνων Επεξεργασίας

	Control	*Απαίτηση*	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΌΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Πολιτικές και διαδικασίες ενημέρωσης και συμμόρφωσης (*Δες και εκπαίδευση 27001*)	Παρέχει εκπαίδευση ο Υπεύθυνος Επεξεργασίας στους υπαλλήλους;						
		Υπάρχουν σαφείς τεκμηριωμένες πολιτικές και διαδικασίες για όλες τις πτυχές της συμμόρφωσης με τον ΓΚΠΔ;						
		Διεξάγετε μια τακτική διαδικασία ελέγχου;						
2.	Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (άρθρο 25)	Οι πολιτικές και οι διαδικασίες ενσωματώνουν τις αρχές Privacy by design σε κάθε επίπεδο ενός οργανισμού, συμπεριλαμβανομένων: 1. Της οργάνωσης, των πολιτικών και της διακυβέρνησης; 2. Των επιχειρηματικών διαδικασιών; 3. Των τυποποιημένων διαδικασιών λειτουργίας; 4. Της αρχιτεκτονικής συστημάτων και δικτύων; 5. Των πρακτικών σχεδιασμού και ανάπτυξης συστημάτων πληροφορικής;						
3.	Απόδειξη Συμμόρφωσης (τήρηση Αρχείων) – άρθρα 30, 83 και 84)	Πόσους εργαζόμενους διαθέτει η εταιρεία;						
		Αντιμετωπίζονται ευαίσθητα προσωπικά δεδομένα;						
		Οι νόμιμοι λόγοι για την επεξεργασία προσωπικών δεδομένων καταγράφονται;						

4.	Data Protection Impact Assessments DPIAs – άρθρα 35 και 36).	Έχετε μια διαδικασία για τον προσδιορισμό της ανάγκης και τη διεξαγωγή (και τεκμηρίωση) DPIAs;						
5.	Συμβάσεις με Εκτελούντα Επεξεργασία (άρθρα 24 και 28)	Εφαρμόζονται οι όροι που περιλαμβάνονται στις συμβάσεις με υπεύθυνο επεξεργασίας;						
		Υπάρχουν συμβάσεις των Υπευθύνων/Εκτελούντων Επεξεργασία που περιέχουν όλους τους προβλεπόμενους όρους;						

ΙΙ. ΓΕΝΙΚΑ ΣΤΟΙΧΕΙΑ ΠΟΥ ΑΠΑΙΤΟΥΝΤΑΙ ΑΠΟ ΤΟ ΣΥΣΤΗΜΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

10. Πολιτικές Ασφάλειας Πληροφοριών

	Control	**Απαίτηση**	***ΝΑΙ***	***ΜΕΡΙΚΩΣ***	***ΟΧΙ***	***Ν/Α***	***ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ***	***ΕΝΕΡΓΕΙΕΣ***
Κατευθύνσεις της Διοίκησης για την Ασφάλεια Πληροφοριών								
1.	Πολιτικές Ασφάλειας Πληροφοριών	Πρέπει να υπάρχουν καταγεγραμμένες πολιτικές ασφάλειας						
		Οι πολιτικές πρέπει να έχουν εγκριθεί από τη Διοίκηση						
		Οι πολιτικές πρέπει να έχουν δημοσιοποιηθεί και επικοινωνηθεί στο προσωπικό και σε εξωτερικούς συνεργάτες						
2.	Ανασκόπηση Πολιτικών Ασφάλειας Πληροφοριών	Πρέπει να γίνεται ανασκόπηση ανά τακτά χρονικά διαστήματα						
		Κάθε πολιτική πρέπει να έχει έναν owner που έχει την ευθύνη για ανάπτυξη, ανασκόπηση και αξιολόγηση της πολιτικής						
		Πρέπει να περιλαμβάνεται στις πολιτικές δήλωση σχετικά με τα μέτρα ασφάλειας που λαμβάνονται για την προστασία των PII (Personally Identifiable Information) και να λαμβάνεται υπόψη στην ανασκόπηση						

11. Οργάνωση της Ασφάλειας Πληροφοριών

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
Εσωτερική Οργάνωση								
3.	Ρόλοι/Θέσεις ασφάλειας προσωπικού	Data Protection Officer (DPOs- άρθρα 37 - 39) Χρειάζεται να διορίσετε έναν DPO; Εάν δεν απαιτείται κάποιος DPO, εξετάστε εάν πρέπει να διοριστεί κάποιος.						
		Security Officer						
		Administrator						
		Απαιτείται η ύπαρξη καταγεγραμμένων ρόλων και αρμοδιοτήτων/ υπευθυνοτήτων που αφορούν την ασφάλεια των πληροφοριών						
		Κατανομή αρμοδιοτήτων στο προσωπικό						
		Διαχωρισμός καθηκόντων (πρόσβαση / έγκριση / έλεγχος)						
		Επικοινωνία με τις Αρχές και τα υποκείμενα σε περίπτωση απώλειας προσωπικών δεδομένων (Δες και ενότητα παραβίασης δεδομένων)						
		Συνεργασίες με ειδικούς σε θέματα ασφάλειας πληροφοριών						
4.	Συνεργασίες – Έργα	Συνεργασίες με ειδικούς σε θέματα ασφάλειας πληροφοριών						
		Μέτρα για την ασφάλεια πληροφοριών στα έργα υλοποίησης						
Κινητές συσκευές και Τηλε-εργασία								
5.	Πολιτικές ασφάλειας	Πολιτική χρήσης φορητών συσκευών						
		Πολιτική τηλε-εργασίας						

12.Ασφάλεια Ανθρώπινων Πόρων

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
Πριν την πρόσληψη								
1.		Έλεγχοι που πραγματοποιούνται για την αξιοπιστία του						

	Αξιοπιστία του υποψήφιου εργαζόμενου	υποψήφιου εργαζόμενου						
2.	Εργαζόμενοι σε συγκεκριμένες θέσεις	Έγγραφα που ζητάει η επιχείρηση (για εργαζόμενους σε συγκεκριμένες θέσεις)						
3.	Συμφωνητικά με τους εργαζόμενους	Έγγραφα/ συμφωνητικά που υπογράφει η επιχείρηση με το προσωπικό						
Κατά τη Διάρκεια της Συνεργασίας								
4.	Διασφάλιση κανόνων ασφαλείας	Διασφάλιση ότι το προσωπικό ακολουθεί τους κανόνες που έχουν θεσπιστεί για την ασφάλεια των πληροφοριών						
5.	Εκπαίδευση προσωπικού	Παρακολούθηση των εκπαιδεύσεων του προσωπικού που έχουν πραγματοποιηθεί ή/και έχουν προγραμματιστεί						
		Παρέχει εκπαίδευση ο Υπεύθυνος Επεξεργασίας στους υπαλλήλους;						
		Υπάρχουν σαφείς τεκμηριωμένες πολιτικές και διαδικασίες για όλες τις πτυχές της συμμόρφωσης με τον ΓΚΠΔ;						
		Διεξάγετε μια τακτική διαδικασία ελέγχου;						
6.	Πειθαρχική Διαδικασία	Υπάρχει πειθαρχική διαδικασία για το προσωπικό που ήταν υπεύθυνο για διαρροή θεμάτων ασφάλειας?						
Διακοπή της Συνεργασίας								
7.	Ενέργειες μετά την αποχώρηση εργαζομένου	Α. Στοιχεία Εργαζομένων Β. Επιστροφή χορηγημένων περιουσιακών στοιχείων (δες και 3.2.4 σημείο 4 παρακάτω) Γ. Διαγραφή Δικαιωμάτων Access						

13. Διαχείριση Περιουσιακών Στοιχείων

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
Αρμοδιότητες για του Πληροφοριακούς Πόρους								
1.	Κατάλογος με τους πληροφοριακούς πόρους της							

	επιχείρησης (Assets Inventory)							
2.	Ιδιοκτησία (χρέωση στο προσωπικό) πόρων							
3.	Αποδεκτή χρήση των πόρων							
4.	Επιστροφή των πόρων							
Ταξινόμηση Πληροφορίας								
5.	Διαβάθμιση πληροφορίας	Η πληροφορία πρέπει να διαβαθμίζεται ανάλογα με την αξία της, τις νομικές υποχρεώσεις, την ευαισθησία της και την κρισιμότητα για τον Οργανισμό						
6.	Σήμανση πληροφορίας	Υπάρχει διαδικασία σήμανσης (labeling) και χειρισμού για τις διαβαθμισμένες πληροφορίες?						
7.	Διαχείριση των Πληροφοριακών Πόρων	Η πρόσβαση στους πληροφοριακούς πόρους πρέπει να γίνεται σε συνάρτηση με την κατηγοριοποίηση των πληροφοριών						
Χειρισμός των Μέσων Αποθήκευσης								
8.	Διαχείριση των αφαιρούμενων μέσων	Πρέπει να υπάρχει πολιτική διαχείρισης αφαιρούμενων μέσων						
		Προτείνεται η κρυπτογράφηση δεδομένων που βρίσκονται σε αφαιρούμενα μέσα						
9.	Απόσυρσης Μέσων Αποθήκευσης	Πρέπει να υπάρχει πολιτική απόσυρσης των μέσων αποθήκευσης						
10.	Μεταφορά πληροφοριών	Πρέπει να υπάρχει πολιτική για τη μεταφορά πληροφοριών σε μαγνητικά μέσα						
		Μεταφορά σε έντυπη μορφή						

14. Διαχείριση Πρόσβασης (Access Control)

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΌΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
Επιχειρησιακές Απαιτήσεις Διαχείρισης Πρόσβασης								
1.		Γενικά (καταγεγραμμένες						

	Πολιτική πρόσβασης στα assets	πολιτικές ελέγχου πρόσβασης)						
		Χρήση credentials						
		Χρήση access cards						
		Απόδοση δικαιωμάτων πρόσβασης. Συσχέτιση πρόσβασης με τη διαβάθμιση των πληροφοριών						
		Περιοδική ανασκόπηση / αναθεώρηση των δικαιωμάτων πρόσβασης						
		Διαχείριση δικαιωμάτων πρόσβασης κατά την αποχώρηση του εργαζομένου						
		Πρέπει να υπάρχουν Ρόλοι χρηστών						
		Ρόλοι με αυξημένες δυνατότητες πρόσβασης σε πληροφορίες						
2.	Πολιτική πρόσβασης στο δίκτυο							
Διαχείριση Πρόσβασης Χρηστών								
3.	Διαδικασία απόδοσης δικαιωμάτων πρόσβασης	Πρόσβαση στις εφαρμογές (User Identification and Authentication)						
		Πρόσβαση στις πληροφορίες						
		Διαχείριση των ρόλων με αυξημένες δυνατότητες πρόσβασης σε πληροφορίες						
4.	Κεντρική Διαχείριση	Απαιτείται η λειτουργία λογισμικού κεντρικής διαχείρισης των credentials των χρηστών (Password Management System)						
5.	Δημιουργία Χρήστη							
6.	Διαγραφή χρήστη							
7.	Προσωρινοί λογαριασμοί χρηστών	Δυνατότητα για προσωρινά credentials						
8.	Ανασκόπηση δικαιωμάτων πρόσβασης							
9.	Διαχείριση αλλαγών στην εργασιακή σχέση του προσωπικού	Πρόσβαση στις πληροφορίες μετά από αλλαγή στην						

		εργασιακή σχέση του προσωπικού						
10.	Παραμετροποίηση εξοπλισμού	Αλλαγές στις ρυθμίσεις του εξοπλισμού μετά την εγκατάστασή του						
		Αλλαγές στους κωδικούς πρόσβασης του εξοπλισμού						
Υποχρεώσεις Χρηστών								
11.	Πολιτικές ασφαλούς χρήσης πρόσβασης	Ασφαλής χρήση credentials από τους χρήστες						
		Χρήση ασφαλούς κωδικού πρόσβασης						
12.	Ευθύνη Χρηστών	Υπάρχει υπογεγραμμένη δήλωση χρηστών ότι θα κρατούν το password εμπιστευτικό						
		Υπάρχει οδηγός καλής πρακτικής για τη χρήση και διατήρηση passwords						
Έλεγχος Πρόσβασης σε συστήματα και εφαρμογές								
13.	Need-to-know basis λογική στην πρόσβαση του προσωπικού	Η επιχείρηση πρέπει να ακολουθεί τη λογική «need to know basis»						
		Πρέπει να υπάρχουν διαφορές όσον αφορά την πρόσβαση των χρηστών στις πληροφορίες (read, write, delete, execute)						
		Πρέπει να υπάρχει ειδική πρόβλεψη για ευαίσθητες πληροφορίες (όσον αφορά την αποθήκευση και την πρόσβαση των χρηστών) (Δες και ενότητα προσωπικά δεδομένα άρθρο 9)						
14.	Είσοδος στις εφαρμογές	Πρέπει να υπάρχει ασφαλής διαδικασία σύνδεσης του προσωπικού στα πληροφοριακά συστήματα. (π.χ. Credentials, βιομετρικά, smart cards, tokens)						
		Πρέπει να τηρούνται log files για τα log on στα πληροφοριακά συστήματα (π.χ.						

		ώρα εισόδου, ώρα εξόδου, αποτυχημένες προσπάθειες, εργασίες) Πρέπει να γίνεται ανασκόπηση των log files						
		Πρέπει να καταγράφονται οι επιτυχημένες και αποτυχημένες προσπάθειες						
		Πρέπει να γίνεται διακοπή inactive sessions						
15.	Διαχείριση κωδικών πρόσβασης	Πρέπει να υποχρεώνονται οι χρήστες να επιλέγουν ασφαλή passwords (δες και 3.2.5 ευθύνες χρηστών)						
		Πρέπει να υποχρεώνονται οι χρήστες να αλλάζουν password ανά τακτά χρονικά διαστήματα; (δες και 3.2.5 ευθύνες χρηστών)						
		Δεν πρέπει να φαίνονται οι χαρακτήρες του password όταν καταχωρείται						
16.	Χρήση Βοηθητικών Προγραμμάτων	Η χρήση Utilities πρέπει να είναι περιορισμένη στη χρήση των απαραίτητων για την εργασία του προσωπικού προγραμμάτων						
		Πρέπει να υπάρχει διαχωρισμός ανάμεσα στα utilities και στις εφαρμογές / πληροφοριακά συστήματα						

15. Κρυπτογραφία

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΌΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Χρήση κρυπτογράφησης							
2.	Πολιτικές κρυπτογράφησης	Πρέπει να υπάρχει πολιτική για τη χρήση κρυπτογράφησης η οποία να λαμβάνει υπόψη τις						

		αποτιμήσεις κινδύνου, τα επίπεδα ασφαλείας, τα ευαίσθητα δεδομένα κ.λπ.						

16. Φυσική & Περιβαλλοντική Ασφάλεια

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
Ασφαλείς Περιοχές								
3.	Μέτρα για τη φυσική ασφάλεια	Σύστημα συναγερμού						
		Σύστημα access control						
		Πυροπροστασία						
4.	Έλεγχος πρόσβασης	Έλεγχος πρόσβασης προσωπικού						
		Έλεγχος πρόσβασης επισκεπτών						
		Έλεγχος πρόσβασης συνεργατών/ προμηθευτών						
Computer Room & Υποδομές								
5.	Computer room	Έλεγχος εισόδου στο Computer Room						
		Έλεγχος θερμοκρασίας						
		Έλεγχος υγρασίας						
		Υποδομές computer room						
6.	Υποδομές	Ύπαρξη δομημένης καλωδίωσης						
		Rack εξοπλισμού σε κοινόχρηστους χώρους						
		Συντήρηση εξοπλισμού επιχείρησης						
		Χώροι, δωμάτια στα οποία εκτελείται επεξεργασία πρέπει να κλειδώνουν ή να διαθέτουν ερμάρια που κλειδώνουν						
		Πρέπει να είναι σχεδιασμένο σύστημα προστασίας έναντι ζημιών από φωτιά, σεισμό, πλημμύρας, ή άλλες φυσικές ή προκληθείσες από άνθρωπο καταστροφές.						
7.	Πολιτικές υποδομών	Χρήση εξοπλισμού εκτός των εγκαταστάσεων της επιχείρησης						
		Πολιτική clear desk						
		Πολιτική clear screen						

17. Λειτουργική Ασφάλεια

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
Λειτουργικές Διαδικασίες & Ευθύνες								
1.	Πολιτικές ή/και διαδικασίες ασφάλειας των πληροφοριών							
2.	Capacity Management του εξοπλισμού της επιχείρησης							
3.	Διαφορετικό περιβάλλον για development, testing και operation							
Προστασία από Ιούς/Κακόβουλο Λογισμικό								
4.	Λογισμικό antivirus/ antimalware	Λειτουργία του λογισμικού						
		Ενημέρωση του λογισμικού						
Αντίγραφα Ασφαλείας (Backup)								
5.	Πολιτικές/Διαδικασίες	Πολιτική αντιγράφων ασφαλείας						
		Διαδικασία αντιγράφων ασφαλείας						
		Φυλάσσονται αντίγραφα ασφαλείας σε ασφαλή απομακρυσμένο χώρο και σε ικανή απόσταση από την κύρια εγκατάσταση ώστε να διασωθούν σε περίπτωση ευρείας καταστροφής;						
		Τα αντίγραφα ασφαλείας που περιέχουν προσωπικά ή εμπιστευτικά δεδομένα είναι κρυπτογραφημένα;						
		Έλεγχος διαδικασίας ανάκτησης πληροφοριών						
Καταγραφή και Παρακολούθηση Συμβάντων								
6.	**Καταγραφή συμβάντων παραβίασης της ασφάλειας των πληροφοριών** Υποχρεώσεις αντιμετώπισης παραβίασης (άρθρα 33 και 34) (Από Ενότητα 8)	Διαθέτει ο οργανισμός ένα τεκμηριωμένο Σχέδιο Αντιμετώπισης (Incident Response Plan) για Συμβάντα ιδιωτικότητας και ασφάλειας, καθώς και Συστήματα Ταυτοποίησης Συμβάντων (Incident						

		Identification Systems);						
		Το σχέδιο και οι διαδικασίες επανεξετάζονται τακτικά και πραγματοποιούνται ασκήσεις;						
		Υπάρχει σαφής εσωτερική καθοδήγηση που να εξηγεί πότε απαιτείται ειδοποίηση και ποιες πληροφορίες χρειάζεται να αναφέρονται;						
		Υπάρχουν σαφείς διαδικασίες για την ενημέρωση του Υπεύθυνου Επεξεργασίας για οποιασδήποτε παραβίαση των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση,;						
		Τεκμηριώνονται οι παραβιάσεις δεδομένων;						
		Υπάρχουν διαδικασίες συνεργασίας μεταξύ του Υπεύθυνου Επεξεργασίας, των Προμηθευτών και άλλων Εταίρων για την αντιμετώπιση παραβιάσεων δεδομένων;						
		Έχετε σκεφτεί την ασφαλιστική κάλυψη, για παραβίαση δεδομένων; (δεν είναι υποχρεωτική σύμφωνα με το GDPR)						
7.	Φύλαξη log files							
8.	Συγχρονισμός ρολογιών των διαφόρων συστημάτων							
9.	Δικαιώματα διαχειριστή στους υπολογιστές της επιχείρησης							
Έλεγχος Λογισμικού Λειτουργίας								
10.	Πολιτική εγκατάστασης λογισμικού							

18. Ασφάλεια Επικοινωνιών

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Διαχείριση ασφάλειας δικτύων	Πολιτική διαχείρισης δικτύου						
		Μέτρα που λαμβάνονται για την ασφάλεια του δικτύου						
		Ομάδες δικαιωμάτων χρηστών						
		Πρέπει να υπάρχει μηχανισμός Αυθεντικοποίησης για ελεγχόμενη πρόσβαση των απομακρυσμένων χρηστών						
		Οι πόρτες για απομακρυσμένη διάγνωση πρέπει να προστατεύονται από μηχανισμό ασφάλειας						
		Πρέπει να υπάρχει διαχωρισμός δικτύων για τα πληροφοριακά συστήματα που είναι κρίσιμα.						

19. Προμηθευτές

	Control	Απαίτηση	ΝΑΙ	ΜΕΡΙΚΩΣ	ΌΧΙ	Ν/Α	ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ	ΕΝΕΡΓΕΙΕΣ
1.	Ασφάλεια πληροφοριών στη συνεργασία με τους προμηθευτές Συμβάσεις με Εκτελούντα Επεξεργασία (άρθρα 24 και 28) ΓΚΠΔ? (Δες και Ενότητα 3.1.8.)	Πολιτική σχέσεων που αφορά την ασφάλεια των πληροφοριών						
		Non-disclosure agreements Εφαρμόζονται όλοι οι όροι που περιλαμβάνονται στις συμβάσεις με υπεύθυνο επεξεργασίας;						
		Ειδικά άρθρα στις συμβάσεις για την ασφάλεια των πληροφοριών Υφίστανται συμβάσεις των Υπευθύνων/Εκτελούντων Επεξεργασία που περιέχουν όλους τους προβλεπόμενους όρους;						
2.	Χρήση υπεργολάβων επεξεργασίας (άρθρα 24 και 28) (Από Ενότητα 11)	Η επεξεργασία από υπεργολάβους υπόκειται σε σύμβαση που περιλαμβάνει καθορισμένους όρους;						
		Ισχύουν οι ίδιες υποχρεώσεις που καθορίζονται στη σύμβαση με τον Υπεύθυνο Επεξεργασίας και για τους υπεργολάβους -						

		Εκτελούντες Επεξεργασία;						
3.	Υποστήριξη στον Υπεύθυνο Επεξεργασίας (άρθρο 28) (Από Ενότητα 11)	Λαμβάνει ο Υπεύθυνος Επεξεργασίας υποστήριξη στην εξασφάλιση συμμόρφωσης σύμφωνα με το GDPR;						

20. Διαχείριση Συμβάντων Ασφάλειας Πληροφοριών

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙ-ΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Συμβάντα ασφαλείας πληροφοριών (Δες και control 6 στο 3.2.8)	Διαδικασία για την αντιμετώπιση περιστατικών ασφαλείας						
		Υπεύθυνος για την αντιμετώπιση των περιστατικών						
		Εσωτερική διαδικασία αναφοράς περιστατικών ασφάλειας						
		Ύπαρξη μηχανισμού συλλογής δεδομένων και νομική αντιμετώπιση για τυχόν απόδοση ευθυνών						

21. Επιχειρησιακή Συνέχεια

	Control	Απαίτηση	*ΝΑΙ*	*ΜΕΡΙΚΩΣ*	*ΟΧΙ*	*Ν/Α*	*ΕΥΡΗΜΑΤΑ - ΤΕΚΜΗΡΙΩΣΗ*	*ΕΝΕΡΓΕΙΕΣ*
1.	Σχεδιασμός για λειτουργία μετά από καταστροφή	Καταγεγραμμένη πολιτική Επιχειρησιακής συνέχειας συμπεριλαμβανόμενης της ασφάλειας πληροφοριών						
2.	Δοκιμαστική εφαρμογή πλάνου επιχειρησιακής συνέχειας	Επιβεβαίωση, ανασκόπηση και αξιολόγηση του πλάνου επιχειρησιακής συνέχειας						

Παράρτημα 2. Audit check list

Ημερομηνία: | **Επιθεωρητής:**

Εταιρεία:

Α. Νομικές Απαιτήσεις του Συστήματος Συμμόρφωσης		
Α/Α	**ΕΡΩΤΗΣΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
1.	Έχει οριστεί DPO (εάν απαιτείται);	
2.	Έχει εξεταστεί και τεκμηριωθεί για τους διάφορους σκοπούς η νόμιμη βάση επεξεργασίας των ΠΔ;	
3.	Έχει θεσπιστεί κατάλληλη και ενημερωμένη Πολιτική Ιδιωτικότητας; Είναι αναρτημένη στο διαδικτυακό ιστότοπο της εταιρείας;	
4.	Όταν η συγκατάθεση αποτελεί τη νόμιμη βάση επεξεργασίας, λαμβάνεται συγκατάθεση για την επεξεργασία των ΠΔ (π.χ. Ειδικών κατηγοριών προσωπικά δεδομένα υγείας) ;	
5.	Στη συγκατάθεση υπάρχει πρόβλεψη για διαχείριση προσωπικών δεδομένων ανηλίκων;	
6.	Έχει προβλεφθεί όταν ζητάτε προσωπικά δεδομένα, αυτά να είναι τα ελάχιστα δυνατά ώστε να πραγματοποιείται η εργασία;	
7.	Δίνεται η δυνατότητα στα υποκείμενα να ανακαλέσουν την συγκατάθεσή τους, εφόσον το επιθυμούν;	
8.	Υπογράφονται κατάλληλες συμβάσεις με αναφορά στον χειρισμό των ΠΔ και σύμφωνα με τις απαιτήσεις του άρθρου 28, του Κανονισμού;	
9.	Υπογράφονται κατάλληλες συμβάσεις με το προσωπικό για την εμπιστευτικότητα και τη διαχείριση των Προσωπικών Δεδομένων;	

Α. Νομικές Απαιτήσεις του Συστήματος Συμμόρφωσης		
Α/Α	**ΕΡΩΤΗΣΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
10.	Έχει προσδιοριστεί ο χρόνος διατήρησης των ΠΔ των υποκειμένων από την εταιρεία;	
11.	Διαθέτει η εταιρεία πολιτική ή μηχανισμό πρόσβασης των υποκειμένων στα δεδομένα τους;	
12.	Έχει θεσπιστεί πολιτική που ακολουθείται σε περίπτωση απώλειας ΠΔ ή παραβίασης; Υπάρχει διαδικασία αναφοράς τέτοιων περιστατικών στην ΑΠΔΠΧ;	
13.	Πραγματοποιείται Εκτίμηση Αντικτύπου σε αλλαγές που δύναται να επηρεάσουν την ασφάλεια των ΠΔ που διατηρεί η εταιρεία;	
14.	Έχει γίνει καταγραφή της ροής των ΠΔ εντός της εταιρείας; Υπάρχουν διαθέσιμα αρχεία Δραστηριοτήτων επεξεργασίας;	
15.	Στην περίπτωση μεταφοράς δεδομένων εκτός Ε.Ε. έχει προβλεφθεί η λήψη συγκαταθέσεων;	

Β. Τεχνικά & Οργανωτικά Μέτρα του Συστήματος Συμμόρφωσης		
Α/Α	**ΕΡΩΤΗΣΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
1.	Έχει γίνει Ανασκόπηση του συστήματος για το Προηγούμενο έτος; Έχουν συμπληρωθεί & υπογραφεί τα πρακτικά;	
2.	Υπάρχει και τηρείται διαδικασία εσωτερικών επιθεωρήσεων;	
3.	Έχουν προκύψει Διορθωτικές ενέργειες & Προτάσεις βελτίωσης; Αν ναι, έχουν υλοποιηθεί;	
4.	Είναι ενημερωμένος ο Φάκελος του Συστήματος Συμμόρφωσης με τις τελευταίες εκδόσεις της Τεκμηρίωσης;	

Β. Τεχνικά & Οργανωτικά Μέτρα του Συστήματος Συμμόρφωσης		
Α/Α	**ΕΡΩΤΗΣΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
5.	Έχει γίνει εκπαίδευση του προσωπικού σε θέματα Προστασίας ΠΔ; Είναι αυτή τεκμηριωμένη;	
6.	Έχει θεσπίσει η εταιρεία κατάλληλη πολιτική για την ασφάλεια των πληροφοριών & ΠΔ;	
7.	Έχει θεσπίσει η εταιρεία κατάλληλη πολιτική για την εσωτερική οργάνωση ασφάλειας & προστασίας ΠΔ;	
8.	Έχει θεσπίσει η εταιρεία κατάλληλη πολιτική για την ασφάλεια των ανθρωπίνων πόρων;	
9.	Έχει θεσπίσει η εταιρεία κατάλληλη πολιτική για την ασφάλεια των πληροφοριακών της πόρων; Είναι καταγεγραμμένοι οι πόροι της;	
10.	Γίνεται έλεγχος πρόσβασης στους πληροφοριακούς πόρους της εταιρείας;	
11.	Γίνεται έλεγχος πρόσβασης στις εγκαταστάσεις της εταιρείας;	
12.	Υπάρχει τεκμηριωμένη διαδικασία λειτουργίας των πληροφοριακών συστημάτων της εταιρείας;	
13.	Υπάρχουν κατάλληλα μέτρα ασφάλειας του εσωτερικού δικτύου της εταιρείας;	
14.	Έχουν οριστεί κατάλληλες απαιτήσεις ασφάλειας για την προμήθεια πληροφοριακών συστημάτων;	
15.	Υπάρχει διαδικασία ή πολιτική διαχείρισης της Επιχειρησιακής συνέχειας της εταιρείας;	
16.	Υπάρχει τεκμηριωμένη διαδικασία Backup;	
17.	Υπάρχει κατάλληλη διαδικασία χορήγησης πρόσβασης στους πληροφοριακούς πόρους της εταιρείας;	
18.	Υπάρχει κατάλληλη διαδικασία λήψης αντιγράφων & επαναφοράς δεδομένων;	

Β. Τεχνικά & Οργανωτικά Μέτρα του Συστήματος Συμμόρφωσης		
Α/Α	**ΕΡΩΤΗΣΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
19.	Τα credentials εισόδου στα πληροφοριακά συστήματα αλλάζουν τακτικά? Είναι σύνθετα;	
20.	Η προστασία οθόνης ενεργοποιείται αυτόματα;	
21.	Ακολουθείται η πολιτική clean desk;	
22.	Διαχειρίζεστε με κατάλληλο τρόπο τα βιογραφικά υποψήφιων εργαζομένων που λαμβάνει η εταιρεία;	
23.	Έχει εξεταστεί η περίπτωση ασφαλιστικής κάλυψης για το GDPR;	

ΠΑΡΑΤΗΡΗΣΕΙΣ - ΣΗΜΕΙΩΣΕΙΣ