9/9/2024

Πολιτική για την προστασία των Προσωπικών Δεδομένων

ΠΕΡΙΕΧΟΜΕΝΑ

1. Ορισμοί

Για τους σκοπούς της παρούσας Πολιτικής, ισχύουν οι ακόλουθοι ορισμοί:

Εταιρεία: νοείται η εταιρεία «IDEAL Holdings A.E.».

Όμιλος: νοείται ο όμιλος συμμετοχών της εταιρείας «IDEAL Holdings A.E.», ήτοι η Εταιρεία και οι εταιρείες στις οποίες άμεσα ή έμμεσα συμμετέχει (**«θυγατρικές εταιρείες»**).

ΓΚΠΔ: νοείται ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

Πολιτική: νοείται η Πολιτική Προστασίας Προσωπικών Δεδομένων.

Προσωπικά Δεδομένα: κάθε πληροφορία μέσω της οποίας ταυτοποιείται ή μπορεί να ταυτοποιηθεί ένα φυσικό πρόσωπο («**Υποκείμενο των δεδομένων**»).

Υπεύθυνος επεξεργασίας: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Εν προκειμένω, το Ίδρυμα επιτελεί ρόλο Υπευθύνου Επεξεργασίας ή/και από Κοινού Υπευθύνου Επεξεργασίας.

Υποκείμενο Προσωπικών Δεδομένων: το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

Νομοθετικό Πλαίσιο: Ο ΓΚΠΔ, ο Ν.4624/2019, κάθε νομοθέτημα της Ελληνικής και Ευρωπαϊκής νομοθεσίας και κάθε δευτερογενή νομοθεσία/γνωμοδότηση/αποφάσεις που εκδίδει η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) που ρυθμίζει την προστασία των Δεδομένων Προσωπικού Χαρακτήρα ή την ιδιωτική ζωή.

2. Σκοπός Πολιτικής

Ο σκοπός της παρούσας Πολιτικής Προστασίας Προσωπικών Δεδομένων είναι η διασφάλιση της νόμιμης, διαφανούς και υπεύθυνης επεξεργασίας των προσωπικών δεδομένων που συλλέγονται και διατηρούνται από την Εταιρεία, σε συμμόρφωση με το Νομοθετικό Πλαίσιο.

Ειδικότερα, η παρούσα Πολιτική επιδιώκει:

- Τη συμμόρφωση με την ισχύουσα νομοθεσία, καθώς και με τις κανονιστικές απαιτήσεις, διασφαλίζοντας ότι οι διαδικασίες της Εταιρείας είναι σύμφωνες με το Νομοθετικό Πλαίσιο.
- Την ενίσχυση της διαφάνειας στις διαδικασίες συλλογής και επεξεργασίας προσωπικών δεδομένων

- Τη θέσπιση των βασικών αρχών για την επεξεργασία και την προστασία των προσωπικών δεδομένων
- Την προστασία των δικαιωμάτων των Υποκειμένων των Δεδομένων και τη θέσπιση διαδικασίας για την ενάσκησή τους.
- Τη θέσπιση αρμοδιοτήτων και ευθυνών σχετικά με την επεξεργασία Προσωπικών Δεδομένων και την παρακολούθηση της συμμόρφωσης.
- Την προστασία από παραβιάσεις και περιστατικά διαρροής δεδομένων, διασφαλίζοντας ότι λαμβάνονται όλα τα κατάλληλα μέτρα και οι διαδικασίες για την αποτροπή αυτών των συμβάντων.

3. Πεδίο Εφαρμογής

Η παρούσα Πολιτική Προστασίας Προσωπικών Δεδομένων ισχύει για όλες τις δραστηριότητες συλλογής, επεξεργασίας, αποθήκευσης και διαχείρισης προσωπικών δεδομένων που πραγματοποιούνται από την Εταιρεία. Εφαρμόζεται για κάθε φυσικό πρόσωπο με το οποίο η Εταιρεία διατηρεί επαγγελματική σχέση, συμπεριλαμβανομένων, ενδεικτικά, μετόχων, συνεργατών, εργαζομένων, προμηθευτών και άλλων τρίτων.

Συγκεκριμένα, στο πεδίο εφαρμογής της παρούσας είναι:

- Προσωπικά δεδομένα που συλλέγονται με ηλεκτρονικά μέσα και τηρούνται ηλεκτρονικά (π.χ emails, βάσεις δεδομένων).
- Δεδομένα που συλλέγονται και διατηρούνται σε έντυπη μορφή (π.χ. συμβόλαια, φόρμες, αιτήσεις).
- Κάθε μορφή επεξεργασίας δεδομένων, συμπεριλαμβανομένης της συλλογής, καταγραφής, οργάνωσης, αποθήκευσης, τροποποίησης, ανάκτησης, διαβίβασης ή διαγραφής.

Η Πολιτική εφαρμόζεται σε όλα τα τμήματα της Εταιρείας, καθώς και σε όλους τους υπαλλήλους, συνεργάτες και τρίτα μέρη που έχουν πρόσβαση στα προσωπικά δεδομένα που επεξεργάζεται η Εταιρεία. Οποιαδήποτε μη συμμόρφωση με την Πολιτική αυτή θα αντιμετωπίζεται σύμφωνα με τις προβλεπόμενες διαδικασίες και τις σχετικές κυρώσεις, όπου απαιτείται.

Ο Υπεύθυνος Προστασίας Προσωπικών Δεδομένων είναι υπεύθυνος για την παρακολούθηση της εφαρμογής της παρούσας Πολιτικής και την τήρηση των προβλεπόμενων διαδικασιών. Επίσης, λογοδοτεί απευθείας στη Μονάδα Κανονιστικής Συμμόρφωσης της Εταιρείας, αναφέροντας τυχόν αποκλίσεις ή ζητήματα που προκύπτουν κατά την εφαρμογή της Πολιτικής, καθώς και προτείνοντας βελτιώσεις ή τροποποιήσεις όπου αυτό κρίνεται αναγκαίο.

4. Βασικές Αρχές Επεξεργασίας Δεδομένων και Νομιμότητα Επεξεργασίας

Η Εταιρεία οφείλει να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα συλλέγονται και επεξεργάζονται νομίμως. Σύμφωνα με το άρθρο 5 ΓΚΠΔ, για να είναι νόμιμη η επεξεργασία προσωπικών δεδομένων (απλών και ειδικών κατηγοριών), πρέπει η επεξεργασία να διέπεται από συγκεκριμένες αρχές:

- **Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας**. Σύμφωνα με τη συγκεκριμένη αυτή αρχή, τα δεδομένα πρέπει να υποβάλλονται σε σύννομη και θεμιτή επεξεργασία, με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Η διαφάνεια

απαιτεί η ενημέρωση του υποκειμένου να είναι συνοπτική, εύκολα προσβάσιμη, κατανοητή, με σαφή και απλή διατύπωση.

- **Η αρχή του περιορισμού του σκοπού,** σύμφωνα με την οποία, τα δεδομένα πρέπει να συλλέγονται για καθορισμένους, ρητούς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς**.**
- **Η αρχή της αναλογικότητας** («ελαχιστοποίηση των δεδομένων»), σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι πρόσφορα, συναφή και αναγκαία για τους επιδιωκόμενους σκοπούς επεξεργασίας.
- **Η αρχή της ακρίβειας των δεδομένων**, σύμφωνα με την οποία τα δεδομένα θα πρέπει να είναι ακριβή, να επικαιροποιούνται και να λαμβάνονται τα κατάλληλα μέτρα για την άμεση διόρθωση ή διαγραφή ανακριβών σε σχέση με τους επιδιωκόμενους σκοπούς επεξεργασίας δεδομένων.
- **Η αρχή του καθορισμού της χρονικής διάρκειας της επεξεργασίας («περιορισμός της περιόδου αποθήκευσης»)**, σύμφωνα με την οποία τα δεδομένα πρέπει να τηρούνται σε μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για την επίτευξη των σκοπών της επεξεργασίας
- **Η αρχή της «ακεραιότητας και εμπιστευτικότητας»**, σύμφωνα με την οποία τα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλεια και προστασία τους από παράνομη επεξεργασία, απώλεια, καταστροφή ή φθορά τους
- **Η αρχή της λογοδοσίας του υπευθύνου επεξεργασίας**, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωσή του με τον ΓΚΠΔ ενώπιον των εποπτικών αρχών και των δικαστηρίων

Νομιμότητα Επεξεργασίας: Η Εταιρεία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα μόνο στο βαθμό που ισχύει ένας από τους ακόλουθους λόγους:

- **Το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του** για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους συγκεκριμένους σκοπούς. Όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων, η συγκατάθεση λαμβάνεται με συγκεκριμένο, σαφή και ενημερωμένο τρόπο. Για διαφορετικές δραστηριότητες επεξεργασίας, πρέπει να λαμβάνεται νέα συγκατάθεση. Όταν η συγκατάθεση χρησιμοποιείται ως νόμιμη βάση για την επεξεργασία, μπορεί να ανακληθεί ανά πάσα στιγμή. Στην περίπτωση αυτή, τα δεδομένα προσωπικού χαρακτήρα διαγράφονται το συντομότερο δυνατό. Ο υπεύθυνος προστασίας δεδομένων είναι υπεύθυνος για την τήρηση αρχείου με όλες τις συγκαταθέσεις που λαμβάνονται από τα υποκείμενα των δεδομένων.
- **Η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης** στην οποία το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για τη λήψη μέτρων κατόπιν αιτήματος του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,
- **Η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με νομική υποχρέωση** στην οποία υπόκειται
- **Η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει**. Τα συμφέροντα αυτά δεν υπερισχύουν ποτέ των θεμελιωδών δικαιωμάτων και

των ελευθεριών του υποκειμένου των δεδομένων που απαιτούν την προστασία των δεδομένων προσωπικού χαρακτήρα.

Ειδοποιήσεις προς τα Υποκείμενα των Δεδομένων : Κατά τη στιγμή της συλλογής ή πριν από τη συλλογή δεδομένων προσωπικού χαρακτήρα για κάθε είδους δραστηριότητες επεξεργασίας, συμπεριλαμβανομένων ενδεικτικά της συλλογής δεδομένων από εργαζομένους της ή από μετόχους της, η Εταιρεία ενημερώνει κατάλληλα τα Υποκείμενα των Δεδομένων. Ειδικότερα, το Υποκείμενο των Δεδομένων πρέπει να ενημερώνεται σχετικά με:

- την ταυτότητα του υπεύθυνου επεξεργασίας δεδομένων,
- στοιχεία επικοινωνίας του ΥΠΔ,
- το είδος των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, π.χ. δεδομένα ταυτοποίησης, οικονομικά δεδομένα, δεδομένα υγείας,
- σκοπός της επεξεργασίας,
- το έννομο συμφέρον του πελάτη για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, κατά περίπτωση,
- κατηγορίες του αποδέκτη των δεδομένων, εάν προβλέπεται αποκάλυψη, π.χ. δημόσιες αρχές, εταίροι, δικαστήρια, αντιπρόσωποι,
- λεπτομέρειες μιας προγραμματισμένης διασυνοριακής μεταφοράς, δηλαδή όταν τα δεδομένα αποστέλλονται εκτός Ε.Ε.,
- την περίοδο διατήρησης των δεδομένων ή τα κριτήρια που χρησιμοποιούνται για τον καθορισμό της,
- εάν εφαρμόζεται αυτοματοποιημένη λήψη αποφάσεων και τη σημασία της επεξεργασίας για το υποκείμενο των δεδομένων,
- οδηγίες σχετικά με τα δικαιώματα του υποκειμένου των δεδομένων.

5. Δικαιώματα των Υποκειμένων των Δεδομένων

Τα Υποκείμενα των Δεδομένων έχουν τα ακόλουθα δικαιώματα σύμφωνα με το ΓΚΠΔ:

- Το δικαίωμα ενημέρωσης,
- Το δικαίωμα πρόσβασης,
- Το δικαίωμα διόρθωσης,
- Το δικαίωμα διαγραφής,
- Το δικαίωμα περιορισμού της επεξεργασίας,
- Το δικαίωμα στη φορητότητα δεδομένων,
- Το δικαίωμα αντίρρησης,
- Δικαιώματα σχετικά με την αυτοματοποιημένη λήψη αποφάσεων και τη δημιουργία προφίλ.

Διαδικασία Απόκρισης σε Αιτήματα των Υποκειμένων των Δεδομένων.

Η Εταιρεία οφείλει να ανταποκρίνεται στα αιτήματα που λαμβάνει από Υποκείμενα των Δεδομένων για την ενάσκηση των ανωτέρω δικαιωμάτων τους **(«Αίτημα»)** το αργότερο εντός ενός (1) μήνα από τη λήψη του ή μέσα σε τρεις (3) μήνες σε περίπτωση πολύπλοκων ή πολυάριθμων Αιτημάτων. Σε αυτή την περίπτωση, η Εταιρεία θα πρέπει να ενημερώσει το Υποκείμενο για την παράταση της προθεσμίας και τους λόγους αυτής μέσα σε ένα (1) μήνα από την υποβολή του Αιτήματος.

Η διαχείριση και αντιμετώπιση των Αιτημάτων θα γίνεται πάντα με την καθοδήγηση του Υπεύθυνου Προστασίας Δεδομένων ως ακολούθως:

- **Λήψη Αιτήματος:** Τα δικαιώματα των Υποκειμένων θα πρέπει να ασκούνται εγγράφως είτε σε έγχαρτη είτε σε ηλεκτρονική μορφή. Η ημερομηνία και το περιεχόμενο του εκάστοτε αιτήματος πρέπει να καταγράφονται στο μητρώο αιτημάτων των υποκειμένων των δεδομένων από τον υπεύθυνο προστασίας δεδομένων.
- **Επαλήθευση Στοιχείων Αιτούντος:** Ο αποδέκτης του Αιτήματος, πριν την καταχώρηση του Αιτήματος, θα πρέπει να επαληθεύσει την ταυτότητα του Αιτούντος. Η Εταιρεία θα λάβει τα κατάλληλα μέτρα για την επαλήθευση της ταυτότητας του Υποκειμένου, ζητώντας μόνο ό,τι κρίνεται απαραίτητο για την ταυτοποίηση των στοιχείων του (π.χ. αντίγραφο ταυτότητας). Σε περίπτωση εύλογων αμφιβολιών, η Εταιρεία μπορεί να ζητήσει πρόσθετες πληροφορίες για να επιβεβαιώσει την ταυτότητα του Υποκειμένου των Δεδομένων, ωστόσο το αίτημα πρέπει να είναι ανάλογο προς το είδος των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Εάν η ταυτοποίηση δεν είναι δυνατή με βάση τις πληροφορίες που περιλαμβάνονται στο αίτημα πρόσβασης, η Εταιρεία οφείλει να ενημερώσει το Υποκείμενο των Δεδομένων και δικαιούται να απορρίψει το αίτημα, εκτός εάν το Υποκείμενο των Δεδομένων παράσχει τις πρόσθετες πληροφορίες που απαιτούνται για να καταστεί δυνατή η ταυτοποίηση. Τα στοιχεία/έγγραφα που συλλέχθηκαν για την επαλήθευση της ταυτότητας θα πρέπει να διατηρούνται για περιορισμένο χρονικό διάστημα και όχι περισσότερο απ' όσο χρειάζεται για την ικανοποίηση του Αιτήματος του Υποκειμένου. Μετά το πέρας του διαστήματος αυτού, τα ως άνω στοιχεία/έγγραφα θα πρέπει να καταστρέφονται.
- **Καταχώρηση και Έλεγχος Βασιμότητας Αιτήματος**: Εφαρμόζεται το κριτήριο του κατά πόσον το αίτημα είναι "προδήλως αβάσιμο ή υπερβολικό". Εάν ναι, λαμβάνεται απόφαση για την απόρριψη του Αιτήματος ή την επιβολή τέλους/ χρέωσης, λαμβάνεται. Επιπρόσθετα κατά την αξιολόγηση του Αιτήματος λαμβάνεται απόφαση σχετικά με το κατά πόσον το αίτημα είναι εύλογο και νόμιμο. Κατά τον έλεγχο βασιμότητας του αιτήματος θα πρέπει να αξιολογηθούν εντός των άλλων η ύπαρξη περιορισμών στην άσκηση των δικαιωμάτων όπως είναι ενδεικτικά οι περιπτώσεις κινδύνου αποτροπής της διαπίστωσης, διερεύνησης και δίωξης ποινικών αδικημάτων, η ανάγκη για την προστασία δικαιωμάτων και ελευθεριών τρίτων κλπ. Εάν το Αίτημα αξιολογηθεί αβάσιμο, τότε απορρίπτεται και το Υποκείμενο των Δεδομένων ενημερώνεται εγγράφως για την απόφαση αυτή, τους λόγους άρνησης ικανοποίησης καθώς και για το δικαίωμά του να υποβάλλει καταγγελία στην Εποπτική Αρχή. Η εν λόγω ενημέρωση για την άρνηση ικανοποίησης του Αιτήματος παρέχεται εντός (1) μηνός από την λήψη του.
- **Απάντηση στο Αίτημα του Υποκειμένου**. Το αρμόδιο Τμήμα της Εταιρείας που παρέλαβε το Αίτημα είναι αρμόδιο να απαντήσει στο Αίτημα του Υποκειμένου, αφού λάβει τις απαραίτητες πληροφορίες από τα εμπλεκόμενα Τμήματα της Εταιρείας (ή/και από τρίτους που επεξεργάζονται δεδομένα του Αιτούντος) και πάντοτε με βάση τις οδηγίες και τις γνωμοδοτήσεις του Υπεύθυνου Προστασίας Δεδομένων.

6. Αρμοδιότητες

Υπεύθυνος Προστασίας Δεδομένων (ΥΠΔ). Ο ΥΠΔ είναι υπεύθυνος για τον συντονισμό της προστασίας δεδομένων. Ο ΥΠΔ πρέπει να εμπλέκεται από τον οργανισμό έγκαιρα. Ο ΥΠΔ δεν πρέπει να λαμβάνει οδηγίες από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για την άσκηση των καθηκόντων του. Ο ΥΠΔ αναφέρεται απευθείας στο Διοικητικό Συμβούλιο. Ειδικότερα, ο ΥΠΔ:

- Επικουρεί την Εταιρεία σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα.
- Ενημερώνει και συμβουλεύει την Εταιρεία καθώς και το προσωπικό που απασχολεί, σχετικά με τις υποχρεώσεις τους σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων
- Παρακολουθεί τη συμμόρφωση του οργανισμού με το σύνολο της νομοθεσίας που αφορά την προστασία δεδομένων, επίσης κατά τη διάρκεια ελέγχων, δραστηριοτήτων ενημέρωσης και εκπαίδευσης του προσωπικού που συμμετέχει σε πράξεις επεξεργασίας.
- Λειτουργεί ως σημείο επαφής για αιτήματα φυσικών προσώπων που αφορούν την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους·
- Συνεργάζεται με την Εποπτική Αρχή Προστασίας Δεδομένων και να λειτουργεί ως σημείο επαφής για τις αρχές σχετικά με ζητήματα που αφορούν την επεξεργασία προσωπικών δεδομένων.
- Παρακολουθεί και να βοηθά στην εκτίμηση του αντικτύπου στα προσωπικά δεδομένα
- Παρακολουθεί τακτικά την τήρηση της πολιτικής αυτής και την επικαροποιεί εφόσον απαιτείται.
- Αναλαμβάνει την εκπαίδευση και την ευαισθητοποίηση του Προσωπικού.
- Τήρηση Αρχείου Δραστηριοτήτων της Εταιρείας σύμφωνα με το άρθρο 30 του ΓΚΠΔ.

Εργαζόμενοι. Οι Εργαζόμενοι είναι υπεύθυνοι για την ορθή εφαρμογή και επιβολή της παρούσας πολιτικής και πρέπει να αναφέρουν απευθείας στον Υπεύθυνο Προστασίας Δεδομένων, κάθε περίπτωση μη συμμόρφωσης με την πολιτική ή με την ισχύουσα νομοθεσία περί προστασίας δεδομένων, που υποπίπτει στην αντίληψή τους. Οι ιεραρχικώς αρμόδιοι υπεύθυνοι θα πρέπει να διασφαλίζουν ότι οι υφιστάμενοί τους λαμβάνουν την καθοδήγηση και την εκπαίδευση που χρειάζονται προκειμένου να εργάζονται σύμφωνα με την παρούσα Πολιτική και τους ισχύοντες νόμους.

Υπεύθυνος Ασφάλειας Πληροφοριών. Ο Υπεύθυνος Ασφάλειας Πληροφοριών είναι υπεύθυνος για την ασφάλεια των συστημάτων δικτύου και πληροφοριών του φορέα και συνεργάζεται με τον Υπεύθυνο Προστασίας Δεδομένων προκειμένου να διασφαλιστεί η προστασία των προσωπικών δεδομένων, η υλοποίηση των αναγκαίων τεχνικών και οργανωτικών μέτρων που προβλέπονται από το άρθρο 32 του ΓΚΠΔ. Ειδικότερα, ο Υπεύθυνος Ασφάλειας Πληροφορικών έχει τις κάτωθι αρμοδιότητες:

- Ανάπτυξη, διαμόρφωση πολιτικών και διαδικασιών ασφάλειας δεδομένων της Εταιρείας
- Διαρκής μέριμνα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών του φορέα.

- Προτείνει κατάλληλα μέτρα ασφαλείας και μηχανισμούς για την προστασία από μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικά αποθηκευμένα ή/και μεταδιδόμενα δεδομένα και προστατεύει από τις συνήθεις αναμενόμενες απειλές και κινδύνους.
- Εποπτεία της τήρησης της πολιτικής ασφάλειας συστημάτων πληροφορικής και επικοινωνιών
- Παρακολούθηση και αξιοποίηση νέων τεχνολογιών και εργαλείων ασφάλειας συστημάτων πληροφορικής και επικοινωνιών για την ενίσχυση του επιπέδου κυβερνοασφάλειας.
- Παρακολουθεί την υλοποίηση της συνεχούς επίβλεψης της ασφάλειας των συστημάτων πληροφοριών οργανισμού, συμπεριλαμβανομένων:
    - Περιοδικών αξιολογήσεων του κινδύνου ασφάλειας πληροφοριών και της διαδικασίας διαχείρισης αλλαγών (change management) της Εταιρείας.
    - Αναλύσεων των λειτουργιών για τον προσδιορισμό του βαθμού συμμόρφωσης των βασικών επιχειρηματικών τομέων και υποδομών με τις κανονιστικές απαιτήσεις.
    - Αξιολόγησης και σύστασης νέων τεχνολογιών ασφάλειας πληροφοριών και αντιμέτρων, για την αντιμετώπιση των απειλών κατά της πληροφορίας ή/και της ιδιωτικότητας

7. Προστασία Προσωπικών Δεδομένων από το Σχεδιασμό και Εξ ορισμού

Όταν εισάγονται νέα συστήματα επεξεργασίας δεδομένων, η Εταιρεία εξασφαλίζει υψηλό επίπεδο προστασίας δεδομένων. Ιδιαίτερα, κάθε νέο σύστημα και διαδικασία πρέπει να συμμορφώνεται με τις ακόλουθες αρχές:

- Πρέπει να λαμβάνονται τεχνικά και οργανωτικά μέτρα για τη διασφάλιση της συστηματικής και ασφαλούς διαχείρισης του κύκλου ζωής των προσωπικών δεδομένων από τη συλλογή έως την επεξεργασία έως τη διαγραφή.
- Τα συστήματα επεξεργασίας δεδομένων πρέπει να αποσκοπούν στη συλλογή όσο το δυνατόν λιγότερων προσωπικών δεδομένων για την εκπλήρωση του σκοπού για τον οποίο συλλέχθηκαν τα δεδομένα.
- Όταν η ανωνυμοποίηση των δεδομένων δεν παρεμποδίζει τον σκοπό της επεξεργασίας δεδομένων, τα προσωπικά δεδομένα πρέπει να καταστούν ανώνυμα κατά τρόπο που το πρόσωπο στο οποίο αναφέρονται τα δεδομένα να μη μπορεί πλέον να ταυτοποιείται.
- Εφόσον τα προσωπικά δεδομένα δεν μπορούν να είναι ανώνυμα, πρέπει να λαμβάνονται μέτρα ασφαλείας ανάλογα με τη φύση των δεδομένων, όπως η ψευδωνυμία, η κρυπτογράφηση ή ο περιορισμός πρόσβασης.
- Η πρόσβαση σε δεδομένα προσωπικού χαρακτήρα χορηγείται σύμφωνα με την αρχή «need to know», το οποίο σημαίνει ότι τα προσωπικά δεδομένα καθίστανται προσβάσιμα μόνο σε εκείνα τα πρόσωπα που την απαιτούν για να εκτελούν καθορισμένους ρόλους και ευθύνες.
- Ο συστηματικός έλεγχος ποιότητας των προσωπικών δεδομένων πρέπει να αποτελεί μέρος της διαχείρισης του κύκλου ζωής των δεδομένων, ώστε να εξασφαλίζεται υψηλή ποιότητα δεδομένων.
- Τα συστήματα επεξεργασίας δεδομένων πρέπει να προστατεύονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση μέσω τεχνικών και οργανωτικών μέτρων.
- Τα υποκείμενα των δεδομένων πρέπει να διαθέτουν διαφανή, φιλικά προς το χρήστη και αποτελεσματικά μέσα ελέγχου σχετικά με τα προσωπικά τους δεδομένα.

Επιπρόσθετα, η Εταιρεία εφαρμόζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των δεδομένων προσωπικού χαρακτήρα που συλλέγονται, τον βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Ειδικότερα, τα εν λόγω μέτρα διασφαλίζουν ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων. Εκτενέστερη επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο εάν το υποκείμενο των δεδομένων επιλέξει ή συμφωνεί με ένα χαμηλότερο επίπεδο προστασίας, π.χ. με τη χειροκίνητη αλλαγή των ρυθμίσεων απορρήτου σε έναν ιστότοπο, ένα εργαλείο πληροφορικής ή σε κάτι παρόμοιο με μια λιγότερο περιοριστική επιλογή και συνεπώς δίνει τη ρητή συγκατάθεσή του στην εκτεταμένη επεξεργασία ("opt-in").

8. Αρχείο Δραστηριοτήτων

Εταιρεία πρέπει να τηρεί αρχείο των δραστηριοτήτων επεξεργασίας. Το αρχείο αυτό αποτελεί εσωτερικό αρχείο που περιέχει πληροφορίες για όλες τις δραστηριότητες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που πραγματοποιεί η Εταιρεία Σύμφωνα με το άρθρο 30 του ΓΚΠΔ. Τα ανωτέρω πεδία επανεξετάζονται τακτικά από τον Υπεύθυνο Προστασίας Δεδομένων και το αρχείο δραστηριοτήτων επεξεργασίας επικαιροποιείται όταν απαιτείται. Οι επικεφαλής όλων των μονάδων/διευθύνσεων της Εταιρείας πρέπει να αναφέρουν τακτικά στον Υπεύθυνο Προστασίας Δεδομένων κάθε αλλαγή/τροποποίηση στο πλαίσιο των υφιστάμενων δραστηριοτήτων επεξεργασίας (π.χ. νέοι εκτελούντες την επεξεργασία δεδομένων, νέες κατηγορίες υποκειμένων των δεδομένων, νέες δραστηριότητες επεξεργασίας, κατάργηση δραστηριότητας επεξεργασίας κ.λπ.).

9. Χρόνος Διατήρησης Προσωπικών Δεδομένων

Τα δεδομένα και τα αρχεία διατηρούνται μόνο για την περίοδο που απαιτείται για την εκπλήρωση του αρχικού σκοπού για τον οποίο έχουν συλλεχθεί ή/και δημιουργηθεί και σύμφωνα με τους ισχύοντες κανονισμούς σχετικά με τη φύση των δεδομένων.

Τα χρονικά διαστήματα διατήρηση των δεδομένων προσδιορίζονται στο Παράρτημα Ι της παρούσας Πολιτικής. Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκευτούν για μεγαλύτερα χρονικά διαστήματα, κατόπιν της γνωμοδότησης του Υπευθύνου Προστασίας Δεδομένων, λαμβάνοντας υπόψη τις ακόλουθες παραμέτρους και υπό την προϋπόθεση ότι εφαρμόζονται κατάλληλα τεχνικά και οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και των ελευθεριών του υποκειμένου των δεδομένων:

- Ύπαρξη νομικής ή κανονιστικής υποχρέωσης που υποχρεώνει την εταιρεία να διατηρεί τα δεδομένα αυτά για πρόσθετο χρονικό διάστημα.
- Διακράτηση δεδομένων προσωπικού χαρακτήρα κρίνεται απαραίτητη για τη θεμελίωση, άσκηση ή υπεράσπιση νομικής αξίωσης.

Μετά τη λήξη των εν λόγω περιόδων, τα δεδομένα προσωπικού χαρακτήρα διαγράφονται με ασφαλή τρόπο ώστε να μην είναι δυνατή η περαιτέρω ταυτοποίηση των υποκειμένων των δεδομένων. Κατά τη φάση της καταστροφής των δεδομένων, η Εταιρεία διασφαλίζει ότι όλα τα απαιτούμενα δεδομένα προσωπικού χαρακτήρα έχουν διαγραφεί από όλα τα πληροφοριακά συστήματα, καθώς και από τυχόν έντυπα αντίγραφα, τα οποία κατέχει είτε η Εταιρεία είτε τρίτα

μέρη που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό της Εταιρείας. Η καταστροφή δεδομένων πραγματοποιείται σύμφωνα με το ισχύον νομοθετικό πλαίσιο και τις κατευθυντήριες γραμμές της αρμόδιας Αρχής Προστασίας Δεδομένων και συγκεκριμένα σύμφωνα με την Οδηγία υπ' αριθ. 1/2005 σχετικά με την «ασφαλή καταστροφή δεδομένων προσωπικού χαρακτήρα μετά τη λήξη του χρονικού διαστήματος που απαιτείται για τον σκοπό της επεξεργασίας» ή οποιαδήποτε νομοθετική πράξη που κατόπιν εφαρμογής της την τροποποιεί ή την αντικαθιστά

10. Παραβίαση Προσωπικών Δεδομένων

Κάθε παράβαση αυτής της Πολιτικής και του Νομοθετικού Πλαισίου συνιστά παραβίαση προσωπικών δεδομένων. Το άρθρο 4 (12) του ΓΚΠΔ ορίζει ως "παραβίαση δεδομένων προσωπικού χαρακτήρα": "*παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη αποκάλυψη ή πρόσβαση σε δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε άλλη επεξεργασία*". Η εν λόγω παραβίαση μπορεί να αφορά ηλεκτρονικά ή έντυπα αρχεία.

Σενάρια/Παραδείγματα Παραβίασης

Απώλεια δεδομένων

- Ένας κρυπτογραφημένος φορητός υπολογιστής που περιέχει προσωπικά δεδομένα έχει χαθεί ή κλαπεί, αλλά το κλειδί κρυπτογράφησης δεν έχει παραβιαστεί. Αυτό δεν θα αποτελούσε παραβίαση προσωπικών δεδομένων, δεδομένου ότι τα προσωπικά δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση μέσω της κρυπτογράφησης.
- Μια βάση δεδομένων με προσωπικά δεδομένα καταστράφηκε κατά λάθος λόγω ανθρώπινου λάθους ενός διαχειριστή συστήματος. Υπάρχει ένα πλήρες αντίγραφο ασφαλείας της βάσης δεδομένων, βάσει του οποίου η βάση δεδομένων μπορεί να αποκατασταθεί άμεσα. Σε αυτή την περίπτωση, δεν έχει σημειωθεί παραβίαση προσωπικών δεδομένων, καθώς τα δεδομένα μπορούν να ανακτηθούν.
- Έχουν κλαπεί έντυπα έγγραφα που περιέχουν προσωπικά δεδομένα. Αυτό θα αποτελούσε παραβίαση προσωπικών δεδομένων λόγω της απώλειας και της μη εξουσιοδοτημένης αποκάλυψης των προσωπικών δεδομένων.

Παράνομη επεξεργασία

- Ένα αρχείο που περιέχει προσωπικά δεδομένα έχει μεταφορτωθεί (σκόπιμα ή τυχαία) σε διακομιστή με δημόσια πρόσβαση. Αυτό θα αποτελούσε παραβίαση προσωπικών δεδομένων λόγω μη εξουσιοδοτημένου χειρισμού των προσωπικών δεδομένων.
- Ένας εργαζόμενος έχει παράσχει σε τρίτο πρόσωπο το όνομα χρήστη και τον κωδικό πρόσβασής του, γεγονός που δίνει στο μη εξουσιοδοτημένο πρόσωπο πρόσβαση σε όλα τα δεδομένα πελατών του εργοδότη. Αυτό θα αποτελούσε παραβίαση προσωπικών δεδομένων λόγω της μη εξουσιοδοτημένης πρόσβασης και χρήσης των προσωπικών δεδομένων.
- Φοροτεχνικός με πρόσβαση σε προσωπικά δεδομένα για την προετοιμασία των φορολογικών δηλώσεων πελατών είχε αθέμιτη πρόσβαση στα προσωπικά δεδομένα ενός πελάτη και τα δημοσιοποίησε. Αυτό θα αποτελούσε παραβίαση δεδομένων προσωπικού χαρακτήρα, δεδομένου ότι ο υπάλληλος χρησιμοποίησε τα δεδομένα του πελάτη για μη εξουσιοδοτημένη επεξεργασία εκτός του πεδίου εφαρμογής των υπηρεσιών.

Μη εξουσιοδοτημένη αποκάλυψη

- Ένας υπάλληλος έστειλε κατά λάθος μη κρυπτογραφημένα προσωπικά δεδομένα σε λάθος παραλήπτη. Αυτό θα αποτελούσε παραβίαση προσωπικών δεδομένων λόγω της ακούσιας αποκάλυψης των προσωπικών δεδομένων σε τρίτους.
- Τα έντυπα αρχεία δύο μερών έχουν συμπεριληφθεί κατά λάθος σε ένα πακέτο, με αποτέλεσμα να γνωστοποιούνται τα προσωπικά δεδομένα του ενός μέρους σε μη εξουσιοδοτημένο πρόσωπο. Αυτό θα αποτελούσε παραβίαση προσωπικών δεδομένων λόγω της ακούσιας αποκάλυψης των προσωπικών δεδομένων σε τρίτο μέρος.

Διαδικασία Αντιμετώπισης και Γνωστοποίησης Περιστατικού Παραβίασης.

Η ροή εργασιών για τη διαχείριση της παραβίασης προσωπικών δεδομένων αποτυπώνεται κάτωθι καθώς και στο **Παράρτημα ΙΙ** της Πολιτικής:

- Οποισδήποτε εργαζόμενος υποψιαστεί/αντιληφθεί ότι μπορεί να έχει λάβει ή λαμβάνει χώρα ένα περιστατικό ασφάλειας, οφείλει να αναφέρει αμέσως και χωρίς καθυστέρηση το περιστατικό στον υπεύθυνο προστασίας δεδομένων καθώς και στο τμήμα πληροφορικής της Εταιρείας. **Η παραβίαση αυτής της υποχρέωσης ή η αδικαιολόγητη καθυστέρηση για την γνωστοποίηση του συμβάντος παραβίασης μπορεί να οδηγήσει σε νομικές ενέργειες κατά του ατόμου.**
- **Διερεύνηση Περιστατικού.** Η διερεύνηση και η αξιολόγηση του αναφερόμενου περιστατικού παραβίασης δεδομένων πρέπει να πραγματοποιείται από τον ΥΠΔ σε συνεργασία με το Τμήμα Πληροφορικής και Ασφάλειας Πληροφοριών του Οργανισμού και σε κάθε περίπτωση να ολοκληρωθεί εντός εύλογου χρόνου ώστε να τηρούνται οι προθεσμίες που ορίζονται από την κείμενη νομοθεσία και συγκεκριμένα από το άρθρο 33 παράγραφος 1 του ΓΚΠΠΔ. Το περιστατικό αξιολογείται λαμβάνοντας υπόψη τις Κατευθυντήριες Γραμμές του Ευρωπαϊκού Συμβουλίου Προστασίας Προσωπικών Δεδομένων υπ' αριθμόν 9/2022 καθώς και το σύστημα υποβοήθησης της ΑΠΔΧ https://eservices.dpa.gr/wizard/?id=1331560
- **Ενημέρωση Αρχής Προστασίας Δεδομένων.** Εάν αξιολογηθεί ότι το περιστατικό πρέπει να γνωστοποιηθεί στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), καθώς η παραβίαση είναι πιθανό να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των των θιγόμενων υποκειμένων των δεδομένων, τότε η Εταιρεία σε συνεργασία με τον ΥΠΔ θα υποβάλει την εν λόγω γνωστοποίηση αμελλητί και σε κάθε περίπτωση εντός 72 ωρών από τη στιγμή η Εταιρεία έλαβε γνώση του περιστατικού. Η γνωστοποίηση πρέπει να περιέχει συγκεκριμένες πληροφορίες (π.χ. φύση/έκταση του περιστατικού, κατηγορίες προσώπων που επλήγησαν, αιτία και συνέπειες αυτού, ενέργειες που έγιναν προς αντιμετώπισή του, κ.ά.). Ακόμα και αν οι πληροφορίες αυτές δεν είναι όλες διαθέσιμες κατά την υποβολή της γνωστοποίησης, αυτή θα πρέπει να υποβληθεί ως αρχική και να ακολουθήσει στη συνέχεια, χωρίς αδικαιολόγητη καθυστέρηση, επικαιροποίησή της (με υποβολή συμπληρωματικής γνωστοποίησης) σύμφωνα με το υπόδειγμα της ΑΔΠΧ το οποίο είναι διαθέσιμο στον ακόλουθο σύνδεσμο:
  https://www.dpa.gr/index.php/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis
- **Ενημέρωση Υποκειμένων.** Περαιτέρω, όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τα οποία αφορά το

περιστατικό, τότε η Εταιρεία οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά. Αυτή η ανακοίνωση είναι ανεξάρτητη της προαναφερθείσας γνωστοποίησης στην Αρχή (η οποία γνωστοποίηση στην Αρχή υποβάλλεται ακόμα και αν ο σχετικός κίνδυνος δεν κρίνεται ως υψηλός). Η ανακοίνωση στα φυσικά πρόσωπα θα πρέπει να γίνει με τον πλέον πρόσφορο και αποτελεσματικό τρόπο, με τη μορφή προσωποποιημένης πληροφόρησης και όχι μέσω κάποιας γενικού χαρακτήρα ανακοίνωσης, στο βαθμό που αυτό είναι εφικτό.

- **Ενέργειες Μετά το Συμβάν.** Ο Υπεύθυνος Προστασίας Δεδομένων με τη συνδρομή του Υπευθύνου Ασφάλειας Πληροφοριών και το τμήμα Πληροφορικής της Εταιρείας, διεξάγει ανάλυση της αιτίας του συμβάντος, αξιολογώντας το επίπεδο των τηρούμενων μέτρων ασφάλειας του Οργανισμού προκειμένου να διαπιστώσει αν το συμβάν είναι αποτέλεσμα κοινών, συχνά επαναλαμβανόμενων ενεργειών. Εάν ναι, ο υπεύθυνος προστασίας δεδομένων συμπεριλαμβάνει την ενημέρωση για τις προληπτικές και διορθωτικές ενέργειες στις μελλοντικές επικοινωνίες και ενσωματώνει τα διδάγματα που προκύπτουν στη διαδικασία για συνεχή βελτίωση. Ο Υπεύθυνος Προστασίας Δεδομένων εξετάζει επίσης εάν υπάρχει ανάγκη αλλαγής, τροποποίησης ή προσθήκης πολιτικής, κατευθυντήριων γραμμών ή κάποιας διαδικασίας για να συμβάλει στον περιορισμό του κινδύνου παρόμοιων περιστατικών στο μέλλον. Μετά την ολοκλήρωση της προαναφερθείσας διαδικασίας, ο Υπεύθυνος Προστασίας Δεδομένων καταγράφει κάθε περιστατικό σε εσωτερικό μητρώο περιστατικών. Αυτό θα πρέπει να περιλαμβάνει τα γεγονότα που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τα αποτελέσματά της και τα διορθωτικά μέτρα που ελήφθησαν.

11. Εκτίμηση Αντικτύπου

Η Εταιρεία διεξάγει εκτίμηση αντικτύπου στα προσωπικά δεδομένα, κάθε φορά που η προγραμματισμένη δραστηριότητα επεξεργασίας μπορεί να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων. Ο σκοπός της εκτίμησης του αντικτύπου είναι να αξιολογηθούν και να μετριαστούν οι κίνδυνοι για το απόρρητο των δεδομένων. Η αξιολόγηση διενεργείται πριν ξεκινήσουν οι εργασίες επεξεργασίας υψηλού κινδύνου. Οι δραστηριότητες επεξεργασίας υψηλού κινδύνου περιλαμβάνουν:

- συστηματική και εκτενή αξιολόγηση των προσωπικών στοιχείων του υποκειμένου των δεδομένων. Ειδικότερα, εάν τα προσωπικά δεδομένα υποβάλλονται αυτόματα σε επεξεργασία, εάν η επεξεργασία περιλαμβάνει τη διαμόρφωση της προσωπικότητας και εάν οι αποφάσεις που επηρεάζουν τα δικαιώματα και τις υποχρεώσεις του υποκειμένου των δεδομένων βασίζονται στην αξιολόγηση αυτή,
- επεξεργασία ευαίσθητων προσωπικών δεδομένων σε μεγάλη κλίμακα,
- συστηματική και ευρείας κλίμακας παρακολούθηση μίας προσβάσιμης στο κοινό περιοχής, π.χ. παρακολούθηση με βίντεο ενός δημόσιου χώρου.

Η εκτίμηση του αντικτύπου στα προσωπικά δεδομένα τεκμηριώνεται δεόντως και πραγματοποιείται από τον Υπεύθυνο Προστασίας Δεδομένων, με τη συνδρομή του Υπευθύνου Ασφάλειας Πληροφοριών (όπου απαιτείται). Όταν η εκτίμηση του αντικτύπου στα προσωπικά δεδομένα οδηγεί

στο συμπέρασμα ότι υπάρχει υψηλός κίνδυνος για τα υποκείμενα των δεδομένων, η Εταιρεία ενημερώνει την εποπτική αρχή ώστε να γνωμοδοτεί σχετικά με τα κατάλληλα μέτρα για τη μείωση των κινδύνων.

12. Έγκριση και Αναθεώρηση της Πολιτικής

Η Πολιτική Προστασίας Προσωπικών Δεδομένων εγκρίνεται από το ΔΣ της Εταιρείας, κοινοποιείται στους εργαζόμενους και αναρτάται επικαιροποιημένη τόσο στον ενδοεταιρικό ιστοχώρο (SharePoint).

Η Πολιτική Προστασίας Προσωπικών Δεδομένων επισκοπείται σε ετήσια βάση και αναθεωρείται από την Εταιρεία ανάλογα με τις τυχόν τροποποιήσεις στο ισχύον δίκαιο ή στις πρακτικές που ακολουθεί η Εταιρεία ή γενικά όποτε παραστεί ανάγκη. Σε τέτοιες περιπτώσεις, αναρτημένη θα είναι κάθε φορά η πιο πρόσφατη Πολιτική.

ΠΑΡΑΡΤΗΜΑ Ι – Χρόνοι Διατήρησης Προσωπικών δεδομένων

ΔΕΔΟΜΕΝΑ ΕΡΓΑΖΟΜΕΝΩΝ		
Γενικές Αρχές: Οι περίοδοι διατήρησης δεδομένων των εργαζομένων μπορεί να παραταθούν έως και τα 20 έτη από τη συλλογή τους, λαμβάνοντας υπόψη τις διατάξεις του α. 95 του Ν. 4387/20216 (Παραγραφή αξιώσεων Ηλεκτρονικού Εθνικού Φορέα Κοινωνικής Ασφάλισης) για τις ανάγκες πιθανών ελέγχων.		
ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ	**ΠΕΡΙΟΔΟΣ ΔΙΑΤΗΡΗΣΗΣ**	**ΝΟΜΙΚΗ ΒΑΣΗ**
Δεδομένα Υποψήφιων Εργαζομένων	6 μήνες από λήξη διαδικασίας αποστολής βιογραφικού	Γνωμοδότηση 4/2013 της ΑΠΔΠΧ Απόφαση 101/2016 της ΑΠΔΠΧ
Λίστες Εργαζόμενων	10 έτη	Ν. 2556/1997 (Άρθρο 2, παρ. 2)
Άδειες	5 έτη από τη λήξη της εργασιακής σχέσης	Ν. 4254/14 (υπ. ΙΑ.5.2)
Συμβάσεις εργασίας εργαζομένων και σχετικά έγγραφα εργαζομένων και αρχεία μισθοδοσίας	5 έτη από τη λήξη της εργασιακής σχέσης	Ν. 3762/2009 (Άρθρο 7) Άρθρα 250-251 ΑΚ (γενική παραγραφή αξιώσεων)
Αναφορές Παραβιάσεων Κανόνων Δικαίου (Whistleblowing)	Κατ΄ελάχιστον 5 έτη από την ημερομηνία υποβολής της Αναφοράς.	Ν. 4990/2022 Συμμόρφωση της Εταιρείας με έννομες υποχρεώσεις

ΝΟΜΙΚΑ, ΕΤΑΙΡΙΚΑ ΚΑΙ ΦΟΡΟΛΟΓΙΚΑ ΔΕΔΟΜΕΝΑ		
Γενικές Αρχές: Οι τροποποιήσεις της φορολογικής νομοθεσίας που θεσπίζουν συνεχείς παρατάσεις των προθεσμιών παραγραφής, ενδέχεται να επιφέρουν την παράταση διακράτισης των προσωπικών δεδομένων και τα 20 έτη από τη συλλογή τους, για τη συμμόρφωση της Εταιρείας με ενδεχόμενους φορολογικούς ελέγχους.		
ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ	**ΠΕΡΙΟΔΟΣ ΔΙΑΤΗΡΗΣΗΣ**	**ΝΟΜΙΚΗ ΒΑΣΗ**
Λογιστικά βιβλία, τιμολόγια και αρχείο τεκμηρίωσης της νομιμότητας των συναλλαγών της Εταιρείας	Κατ' ελάχιστον 5 έτη από τη λήξη της χρήσης στην οποία αφορούν	Άρθρο 13 Ν. 4174/2013 και Ν. 4308/2014 Άρθρο 36 παρ. 2 του Ν. 4174/2013
Εταιρικά Αρχεία, Μετοχολόγιο, Πρακτικά Διοικητικού Συμβουλίου και Γενικών Συνελεύσεων Νομικά Έντυπα και Συμφωνητικά	Καθόλη τη διάρκεια λειτουργίας της Εταιρείας	Έννομο Συμφέρον Εταιρείας για τη διασφάλιση της επιχειρησιακής συνέχειας και της διαφύλαξης νομίμων συμφερόντων αυτής.

ΔΕΔΟΜΕΝΑ ΜΕΤΟΧΩΝ ΚΑΙ ΚΑΤΟΧΩΝ ΠΡΟΝΟΜΙΑΚΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ	ΠΕΡΙΟΔΟΣ ΔΙΑΤΗΡΗΣΗΣ	ΝΟΜΙΚΗ ΒΑΣΗ
Δεδομένα Κατόχων Προνομιακής Πληροφορίας	5 έτη από την ημερομηνία κατάρτισης του καταλόγου προσώπων που κατέχουν προνομιακές πληροφορίες	άρθρο 18 παρ. 5 του Κανονισμού (ΕΕ) αριθμ. 596/2014.
Ψηφοδέλτια, Επιστολικές Ψήφοι Γενικών Συνελεύσεων	1 έτος από τη λήψη απόφασης της Γενικής Συνέλευσης. Σε περίπτωση που η απόφαση της Γενικής Συνέλευσης υπόκειται σε δημοσιότητα 1 έτος από την ημερομηνία καταχώρησης της απόφασης στο Γ.Ε.ΜΗ	Άρθρο 138 παρ. 4 του Ν. 4548/2018

ΔΕΔΟΜΕΝΑ IT		
ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ	**ΠΕΡΙΟΔΟΣ ΔΙΑΤΗΡΗΣΗΣ**	**ΝΟΜΙΚΗ ΒΑΣΗ**
Βίντεο από το σύστημα CCTV της Εταιρείας	14 ημέρες	Κατευθυντήριες Αρχές 1/2011 της ΑΠΔΧ
Logs, Διευθύνσεις IP	6 μήνες	Οδηγίες 1/2008 Wp29
IT back ups	1 έτος	Έννομο συμφέρον της Εταιρείας για τη διασφάλιση της επιχειρησιακής συνέχειας

ΠΑΡΑΡΤΗΜΑ ΙΙ - Χαρτογράφηση της ροής εργασιών της διαδικασίας διαχείρισης της παραβίασης δεδομένων