1. ΕΙΣΑΓΩΓΗ

Η προστασία των προσωπικών δεδομένων αποτελεί βασική προτεραιότητα της εταιρείας μας. Στο πλαίσιο εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (Κανονισμός ΕΕ 2016/679 - GDPR) και του προτύπου ISO/IEC 27701, η παρούσα ενημέρωση έχει σκοπό να σας εξοικειώσει με τους βασικούς κανόνες και τις υποχρεώσεις που σχετίζονται με τη διαχείριση προσωπικών δεδομένων στο πλαίσιο της εργασίας σας.

2. ΤΙ ΕΙΝΑΙ ΠΡΟΣΩΠΙΚΟ ΔΕΔΟΜΕΝΟ

Προσωπικό δεδομένο είναι κάθε πληροφορία που αφορά ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Αυτό σημαίνει ότι αν μια πληροφορία, μόνη της ή σε συνδυασμό με άλλες, μπορεί να οδηγήσει στην αναγνώριση ενός ατόμου, τότε θεωρείται προσωπικό δεδομένο.

Παραδείγματα προσωπικών δεδομένων:

- Ονοματεπώνυμο
- Αριθμός ταυτότητας ή διαβατηρίου
- ΑΦΜ, ΑΜΚΑ
- Διεύθυνση κατοικίας ή e-mail
- Αριθμός τηλεφώνου
- IP διεύθυνση (σε κάποιες περιπτώσεις)
- Φωτογραφία ή βίντεο με το πρόσωπο κάποιου
- Φωνητικό αποτύπωμα
- Στοιχεία μισθοδοσίας
- Στοιχεία υγείας (ευαίσθητα δεδομένα)
- Τοποθεσία σε πραγματικό χρόνο (μέσω GPS)

Ιδιαίτερες Κατηγορίες (Ευαίσθητα Προσωπικά Δεδομένα):
Ο GDPR καθορίζει κάποιες πληροφορίες ως «ιδιαίτερες κατηγορίες», που απαιτούν αυξημένη προστασία. Αυτές περιλαμβάνουν:

- Δεδομένα υγείας
- Γενετικά και βιομετρικά δεδομένα
- Πολιτικές απόψεις
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- Σεξουαλικός προσανατολισμός
- Συνδικαλιστική δράση.

3. ΤΙ ΕΙΝΑΙ ΕΠΕΞΕΡΓΑΣΙΑ

Επεξεργασία προσωπικών δεδομένων είναι οποιαδήποτε πράξη ή σειρά πράξεων που πραγματοποιείται πάνω σε προσωπικά δεδομένα, με ή χωρίς τη χρήση αυτοματοποιημένων μέσων.

Σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR - Κανονισμός ΕΕ 2016/679), η επεξεργασία καλύπτει όλο τον κύκλο ζωής των δεδομένων.

Παραδείγματα πράξεων επεξεργασίας:

- Συλλογή (π.χ. όταν ένας εργαζόμενος υποβάλλει το βιογραφικό του)
- Καταγραφή
- Οργάνωση ή ταξινόμηση
- Δομή και αποθήκευση (σε φυσικά ή ψηφιακά αρχεία)
- Προσαρμογή ή τροποποίηση
- Ανάκτηση ή αναζήτηση
- Χρήση (π.χ. επεξεργασία για μισθοδοσία)
- Αποστολή σε τρίτους / κοινοποίηση / διάδοση
- Περιορισμός πρόσβασης
- Διαγραφή ή καταστροφή.

4. ΡΟΛΟΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ

Ο ρόλος του προσωπικού στο πλαίσιο της προστασίας προσωπικών δεδομένων είναι κρίσιμος για τη συμμόρφωση της εταιρείας με τον Κανονισμό GDPR και το πρότυπο ISO 27701. Κάθε εργαζόμενος που έχει πρόσβαση σε προσωπικά δεδομένα οφείλει να κατανοεί τις υποχρεώσεις του, να εφαρμόζει τις εσωτερικές πολιτικές και διαδικασίες και να ενεργεί με υπευθυνότητα και εμπιστευτικότητα. Το προσωπικό πρέπει να διασφαλίζει ότι τα δεδομένα που επεξεργάζεται χρησιμοποιούνται αποκλειστικά για τους επιτρεπόμενους σκοπούς, δεν κοινοποιούνται σε μη εξουσιοδοτημένα άτομα, και προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, απώλεια ή αλλοίωση. Επιπλέον, πρέπει να ενημερώνει άμεσα τον Υπεύθυνο Προστασίας Δεδομένων ή το αρμόδιο τμήμα σε περίπτωση παραβίασης ή ύποπτης δραστηριότητας. Μέσα από την καθημερινή του δραστηριότητα, το προσωπικό συμβάλλει στην εμπέδωση κουλτούρας προστασίας της ιδιωτικότητας και αποτελεί βασικό κρίκο στην αλυσίδα ασφάλειας των δεδομένων.

5. ΑΡΧΕΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Οι αρχές επεξεργασίας προσωπικών δεδομένων αποτελούν τον πυρήνα του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) και καθορίζουν τον τρόπο με τον οποίο πρέπει να γίνεται η διαχείριση των δεδομένων από κάθε οργανισμό. Σύμφωνα με το άρθρο 5 του Κανονισμού, η επεξεργασία πρέπει να πραγματοποιείται με νομιμότητα, διαφάνεια και σεβασμό στα δικαιώματα των υποκειμένων. Πρώτον, η νομιμότητα, αντικειμενικότητα και διαφάνεια απαιτούν η επεξεργασία να γίνεται με τρόπο θεμιτό και ξεκάθαρο απέναντι στο φυσικό πρόσωπο. Δεύτερον, η αρχή του περιορισμού του σκοπού επιβάλλει τα δεδομένα να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και να μην υποβάλλονται σε περαιτέρω επεξεργασία για άλλους σκοπούς. Τρίτον, η ελαχιστοποίηση των δεδομένων υπαγορεύει τη συλλογή μόνο των απολύτως απαραίτητων στοιχείων για την επίτευξη του σκοπού της επεξεργασίας. Τέταρτον, η ακρίβεια των δεδομένων διασφαλίζει ότι τα προσωπικά στοιχεία είναι ενημερωμένα και διορθώνονται άμεσα όταν εντοπίζονται ανακρίβειες. Πέμπτον, η περιορισμένη χρονική διατήρηση προβλέπει ότι τα δεδομένα δεν διατηρούνται περισσότερο από όσο απαιτείται. Έκτον, η ακεραιότητα και εμπιστευτικότητα εγγυώνται την προστασία των δεδομένων από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά. Τέλος, η αρχή της λογοδοσίας ορίζει ότι ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει την τήρηση όλων των παραπάνω αρχών.

6. ΔΙΚΑΙΩΜΑΤΑ ΥΠΟΚΕΙΜΕΝΩΝ

Τα υποκείμενα των δεδομένων, δηλαδή τα φυσικά πρόσωπα των οποίων τα προσωπικά δεδομένα συλλέγονται και επεξεργάζονται, διαθέτουν συγκεκριμένα δικαιώματα βάσει του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR), τα οποία διασφαλίζουν τον έλεγχο επί των προσωπικών τους πληροφοριών. Το δικαίωμα ενημέρωσης επιτρέπει

στο άτομο να γνωρίζει ποιος συλλέγει τα δεδομένα του, για ποιο σκοπό, για πόσο χρόνο και σε ποιον ενδέχεται να διαβιβαστούν. Το δικαίωμα πρόσβασης παρέχει τη δυνατότητα να λάβει επιβεβαίωση για το αν τα δεδομένα του υπόκεινται σε επεξεργασία και να αποκτήσει αντίγραφο αυτών. Μέσω του δικαιώματος διόρθωσης, μπορεί να ζητήσει τη διόρθωση ανακριβών ή ελλιπών στοιχείων. Το δικαίωμα διαγραφής (ή «δικαίωμα στη λήθη») δίνει τη δυνατότητα διαγραφής των δεδομένων όταν αυτά δεν είναι πλέον απαραίτητα ή όταν η επεξεργασία είναι παράνομη. Με το δικαίωμα περιορισμού της επεξεργασίας, το άτομο μπορεί να ζητήσει τον προσωρινό περιορισμό χρήσης των δεδομένων του. Το δικαίωμα στη φορητότητα δίνει τη δυνατότητα λήψης των δεδομένων σε δομημένη, κοινώς χρησιμοποιούμενη μορφή και διαβίβασής τους σε άλλον υπεύθυνο επεξεργασίας. Το δικαίωμα εναντίωσης επιτρέπει στο υποκείμενο να αντιταχθεί στην επεξεργασία των δεδομένων του για λόγους που σχετίζονται με τη δική του ιδιαίτερη κατάσταση ή όταν η επεξεργασία αφορά απευθείας εμπορική προώθηση. Τέλος, το άτομο έχει το δικαίωμα να μην υπόκειται σε απόφαση που βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, εφόσον αυτή η απόφαση έχει έννομες συνέπειες. Οι οργανισμοί οφείλουν να διευκολύνουν την άσκηση των δικαιωμάτων αυτών, να ανταποκρίνονται εντός ενός μηνός και να διατηρούν διαφάνεια στις διαδικασίες τους.

7. ΠΕΡΙΣΤΑΤΙΚΑ ΠΑΡΑΒΙΑΣΗΣ

Τα περιστατικά παραβίασης προσωπικών δεδομένων αφορούν περιπτώσεις όπου τα προσωπικά δεδομένα επηρεάζονται από ακούσιες ή παράνομες ενέργειες, όπως η καταστροφή, η απώλεια, η αλλοίωση ή η μη εξουσιοδοτημένη πρόσβαση. Αυτές οι παραβιάσεις μπορεί να προκύψουν από διάφορες αιτίες, όπως επιθέσεις από χάκερς, λάθη των υπαλλήλων, τεχνικές δυσλειτουργίες ή φυσικά καταστροφικά γεγονότα.

Τα περιστατικά παραβίασης μπορούν να κατηγοριοποιηθούν ως εξής:

Μη εξουσιοδοτημένη πρόσβαση: Όταν τρίτο άτομο αποκτά πρόσβαση σε προσωπικά δεδομένα χωρίς τη συναίνεση του υποκειμένου ή χωρίς τη σωστή εξουσιοδότηση.

Απώλεια δεδομένων: Όταν προσωπικά δεδομένα χάνονται λόγω καταστροφής ή ατυχήματος, χωρίς να υπάρχει δυνατότητα ανάκτησης τους.

Αλλοίωση ή καταστροφή δεδομένων: Όταν τα δεδομένα τροποποιούνται ή καταστρέφονται ακούσια ή από κακόβουλη ενέργεια, καθιστώντας τα άχρηστα ή μη αξιόπιστα.

Μη εξουσιοδοτημένη διαβίβαση δεδομένων: Όταν τα δεδομένα διαβιβάζονται ή κοινοποιούνται σε τρίτους χωρίς την απαραίτητη συναίνεση ή εξουσιοδότηση.

Κλοπή δεδομένων: Όταν τα δεδομένα κλαπούν από εξωτερικούς παράγοντες, όπως χάκερς ή εγκληματίες.

Διαδικασία Αντιμετώπισης Παραβίασης Δεδομένων:
Όταν συμβαίνει μια παραβίαση προσωπικών δεδομένων, η εταιρεία οφείλει να ακολουθήσει συγκεκριμένα βήματα:

Ενημέρωση του Υπεύθυνου Προστασίας Δεδομένων (DPO): Άμεση ενημέρωση και αξιολόγηση της σοβαρότητας της παραβίασης.

Αξιολόγηση του κινδύνου: Εκτίμηση της σοβαρότητας της παραβίασης και της πιθανής βλάβης για τα υποκείμενα των δεδομένων.

Ενημέρωση της Αρχής Προστασίας Δεδομένων: Εφόσον η παραβίαση ενδέχεται να προκαλέσει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων, η Αρχή Προστασίας Δεδομένων πρέπει να ενημερωθεί εντός 72 ωρών.

Ενημέρωση των υποκειμένων των δεδομένων: Αν υπάρχει υψηλός κίνδυνος για τα δικαιώματα των υποκειμένων, η εταιρεία πρέπει να ενημερώσει άμεσα τα άτομα των οποίων τα δεδομένα παραβιάστηκαν.

8. ΚΥΡΩΣΕΙΣ

Η μη συμμόρφωση με τις απαιτήσεις προστασίας προσωπικών δεδομένων ενδέχεται να επιφέρει:
- Εσωτερικές πειθαρχικές κυρώσεις
- Νομικές ευθύνες
- Διοικητικά πρόστιμα από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

9. ΡΟΛΟΣ DPO

Ο **Ρόλος του Υπεύθυνου Προστασίας Δεδομένων (DPO)** είναι κρίσιμος για την εφαρμογή και παρακολούθηση της συμμόρφωσης με τον κανονισμό GDPR και τις εσωτερικές πολιτικές προστασίας δεδομένων. Ο DPO διασφαλίζει ότι η επεξεργασία των προσωπικών δεδομένων εντός του οργανισμού γίνεται σύμφωνα με τις αρχές του GDPR, με σεβασμό στα δικαιώματα των υποκειμένων και με την κατάλληλη προστασία των δεδομένων. Ανάμεσα στις βασικές του αρμοδιότητες είναι η παρακολούθηση της συμμόρφωσης της εταιρείας με τους κανονισμούς προστασίας δεδομένων, η εκπαίδευση του προσωπικού σχετικά με τη διαχείριση και προστασία των προσωπικών δεδομένων, καθώς και η παροχή συμβουλών για τη σωστή εφαρμογή των πολιτικών προστασίας δεδομένων.
Ο DPO είναι υπεύθυνος για την αναγνώριση και την αξιολόγηση των κινδύνων που σχετίζονται με την επεξεργασία προσωπικών δεδομένων, και η συμβουλευτική του υποστήριξη είναι καθοριστική κατά την ανασκόπηση νέων έργων ή αλλαγών που αφορούν την επεξεργασία προσωπικών δεδομένων. Επίσης, έχει τον ρόλο του συντονιστή σε περιπτώσεις παραβίασης δεδομένων και υποβάλλει τις αναγκαίες αναφορές στην Αρχή Προστασίας Δεδομένων και, εφόσον απαιτείται, στα υποκείμενα των δεδομένων. Ο DPO παρακολουθεί συνεχώς την εκτέλεση των εσωτερικών διαδικασιών και πολιτικών και διασφαλίζει ότι η εταιρεία τηρεί τις διαδικασίες ασφάλειας για την αποφυγή τυχόν παραβιάσεων δεδομένων.
Αποτελεί επίσης τον σύνδεσμο μεταξύ της εταιρείας και των αρμόδιων εποπτικών αρχών, διασφαλίζοντας ότι η εταιρεία ανταποκρίνεται στις απαιτήσεις των αρχών και παραμένει ενημερωμένη για τυχόν τροποποιήσεις της νομοθεσίας ή νέες οδηγίες.

10. ΔΗΛΩΣΗ ΣΥΜΜΟΡΦΩΣΗΣ

Με την υπογραφή του παρόντος εγγράφου, ο εργαζόμενος δηλώνει ότι:
- Έχει λάβει γνώση του περιεχομένου
- Κατανοεί τις υποχρεώσεις του
- Δεσμεύεται να τηρεί τις αρχές και τις διαδικασίες που περιγράφονται

11. ΔΙΚΑΙΩΜΑΤΑ ΕΡΓΑΖΟΜΕΝΩΝ ΩΣ ΥΠΟΚΕΙΜΕΝΑ ΔΕΔΟΜΕΝΩΝ

Οι εργαζόμενοι διατηρούν, σύμφωνα με τον Κανονισμό (ΕΕ) 2016/679 (GDPR) και την ισχύουσα εθνική νομοθεσία, τα ακόλουθα δικαιώματα ως υποκείμενα των προσωπικών δεδομένων:

α) Δικαίωμα πρόσβασης: Ο εργαζόμενος έχει το δικαίωμα να λαμβάνει επιβεβαίωση σχετικά με το αν τα προσωπικά του δεδομένα υφίστανται επεξεργασία και, σε καταφατική περίπτωση, να ζητά πρόσβαση στα δεδομένα αυτά και πληροφορίες σχετικά με την επεξεργασία.

β) Δικαίωμα διόρθωσης: Ο εργαζόμενος μπορεί να ζητήσει τη διόρθωση ανακριβών ή ελλιπών προσωπικών δεδομένων που τον αφορούν, προκειμένου να διασφαλιστεί η ακρίβεια των στοιχείων.

γ) Δικαίωμα διαγραφής ("δικαίωμα στη λήθη"): Ο εργαζόμενος έχει το δικαίωμα να ζητήσει τη διαγραφή των προσωπικών του δεδομένων, εφόσον δεν υφίσταται πλέον νόμιμη βάση για την επεξεργασία ή εφόσον τα δεδομένα δεν είναι πλέον απαραίτητα για τον σκοπό συλλογής τους.

δ) Δικαίωμα περιορισμού της επεξεργασίας: Ο εργαζόμενος μπορεί να ζητήσει τον περιορισμό της επεξεργασίας σε περιπτώσεις όπου αμφισβητείται η ακρίβεια των δεδομένων ή η νομιμότητα της επεξεργασίας.

ε) Δικαίωμα εναντίωσης: Ο εργαζόμενος έχει το δικαίωμα να αντιταχθεί στην επεξεργασία των προσωπικών του δεδομένων, όταν αυτή βασίζεται σε έννομο συμφέρον του εργοδότη, υπό τις προϋποθέσεις του Κανονισμού.

στ) Δικαίωμα φορητότητας: Ο εργαζόμενος δύναται να λάβει τα δεδομένα που τον αφορούν σε δομημένη, κοινώς χρησιμοποιούμενη και αναγνώσιμη από μηχανή μορφή και να ζητήσει τη μεταφορά τους σε άλλον υπεύθυνο επεξεργασίας, εφόσον η επεξεργασία βασίζεται σε συγκατάθεση ή σύμβαση.

Η Εταιρεία υποχρεούται να απαντά στα ανωτέρω αιτήματα εντός της προβλεπόμενης προθεσμίας, λαμβάνοντας όλα τα απαραίτητα μέτρα για τη διευκόλυνση της άσκησης των δικαιωμάτων του εργαζομένου.

12. ΕΙΔΙΚΕΣ ΠΕΡΙΠΤΩΣΕΙΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΣΤΟΝ ΧΩΡΟ ΕΡΓΑΣΙΑΣ

Η Εταιρεία ενδέχεται να προβαίνει σε επεξεργασία προσωπικών δεδομένων στο πλαίσιο ειδικών περιστάσεων που σχετίζονται με την εργασιακή σχέση, οι οποίες ρυθμίζονται ως εξής:

5.1 Χρήση συστημάτων παρακολούθησης (π.χ. CCTV): Η καταγραφή μέσω συστημάτων παρακολούθησης επιτρέπεται μόνο σε χώρους όπου αυτό είναι απολύτως απαραίτητο για λόγους ασφάλειας προσώπων και περιουσίας. Η χρήση τέτοιων συστημάτων διενεργείται με σεβασμό στην αρχή της αναλογικότητας και πάντοτε κατόπιν ενημέρωσης των εργαζομένων μέσω σχετικής σήμανσης ή πολιτικής.

5.2 Παρακολούθηση χρήσης ηλεκτρονικών μέσων: Η Εταιρεία μπορεί να παρακολουθεί τη χρήση εταιρικών συστημάτων (ηλεκτρονικού ταχυδρομείου, διαδικτύου, εταιρικών συσκευών), με αποκλειστικό σκοπό τη διασφάλιση της ορθής και ασφαλούς λειτουργίας των υποδομών. Η παρακολούθηση αυτή διενεργείται περιορισμένα, σύμφωνα με την αρχή της ελαχιστοποίησης, και κατόπιν προηγούμενης ενημέρωσης των εργαζομένων μέσω σχετικής πολιτικής αποδεκτής χρήσης.

5.3 Επεξεργασία ειδικών κατηγοριών δεδομένων (π.χ. υγείας): Η Εταιρεία ενδέχεται να επεξεργάζεται δεδομένα που αφορούν την υγεία των εργαζομένων, μόνο στον βαθμό που αυτό απαιτείται για σκοπούς συμμόρφωσης με την εργατική νομοθεσία ή για λόγους προστασίας της υγείας και ασφάλειας στην εργασία. Η επεξεργασία των δεδομένων αυτών διενεργείται με αυξημένα μέτρα ασφαλείας και εχεμύθειας και, όπου απαιτείται, βάσει ρητής συγκατάθεσης του εργαζομένου.

Η Εταιρεία δεσμεύεται να τηρεί την αρχή της αναγκαιότητας, της διαφάνειας και της ελαχιστοποίησης της επεξεργασίας για όλες τις ανωτέρω περιπτώσεις, διασφαλίζοντας την ιδιωτικότητα των εργαζομένων και συμμορφούμενη με τις απαιτήσεις του GDPR και της εθνικής νομοθεσίας.