|Τι είναι ο GDPR;

GDPR είναι ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (General Data Protection Regulation GDPR). Στοχεύει να προσφέρει στους πολίτες της ΕΕ μια ενιαία και εναρμονισμένη προσέγγιση όσον αφορά την προστασία της ιδιωτικής ζωής στην Ευρωπαϊκή Ένωση. Ο GDPR εγκρίθηκε από το κοινοβούλιο της ΕΕ στις 14 Απριλίου 2016 και η ημερομηνία υποχρεωτικής εφαρμογής του GDPR καθορίστηκε στις 25 Μαΐου 2018 και οι επιχειρήσεις πρέπει να συμμορφωθούν με αυτόν άμεσα μέσα στο αμέσως επόμενο διάστημα σύμφωνα με πρώτη οδηγία της ΑΑΔΕ(Αρχή Προστασίας Δεδομένων) .

|Σε ποιους απευθύνεται;

Ο νόμος ισχύει για:

- οποιαδήποτε επιχείρηση, εταιρεία ή οντότητα εγκατεστημένη στην ΕΕ που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα ως μέρος των δραστηριοτήτων της ή
- οποιαδήποτε επιχείρηση, εταιρεία ή οντότητα εγκατεστημένη εκτός της ΕΕ που προσφέρει αγαθά / υπηρεσίες (αμειβόμενες ή δωρεάν) ή παρακολούθηση της συμπεριφοράς των ατόμων στην ΕΕ.

Εάν η εταιρεία σας είναι μια μικρή και μεσαία επιχείρηση («ΜΜΕ») που επεξεργάζεται τα προσωπικά δεδομένα όπως περιγράφεται παραπάνω, πρέπει να συμμορφώνεστε με το GDPR. Ωστόσο, εάν η επεξεργασία προσωπικών δεδομένων δεν αποτελεί βασικό μέρος της επιχείρησής σας ή δεν γίνεται σε μεγάλη κλίμακα ή η δραστηριότητά σας δεν δημιουργεί κινδύνους για τα άτομα, τότε ορισμένες υποχρεώσεις του GDPR δεν θα ισχύουν για εσάς (πχ. ο διορισμός υπευθύνου προστασίας δεδομένων DPO για την συνεχή παρακολούθηση). Οι κατηγορίες επαγγελματιών πρυ πρέπει να συμμορφωθούν άμεσα (ως πιο « επικίνδυνες για ελέγχους» λόγω της διαχείρισης «ευαίσθητων» δεδομένων είναι γιατροί, λογιστές , δικηγόροι , ασφαλιστές , επιχειρήσεις συστημάτων ασφαλείας και εν συνεχεία όλοι οι υπόλοιποι κλάδοι.

|Ποια θεωρούνται προσωπικά δεδομένα;

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα. Τα δεδομένα προστατεύονται ανεξάρτητα από την μορφή στην οποία επεξεργάζονται ψηφιακή ή έντυπη μορφή.

Τα δεδομένα αυτά μπορεί να αφορούν όχι μόνο πελάτες ή εν δυνάμει πελάτες μια επιχείρησης αλλά και τους εργαζομένους ή συνεργάτες της.

Πχ. Το όνομα και επώνυμο, η διεύθυνση κατοικίας, τηλέφωνα, ο αριθμός ταυτότητας, η προσωπική ηλεκτρονική διεύθυνση (e-mail), ο αναγνωριστικός αριθμός τραπεζικής κάρτας, στοιχεία τραπεζικών λογαριασμών, τα δεδομένα τοποθεσίας (π.χ. GPS σε κινητό τηλέφωνο), η διεύθυνση διαδικτυακού πρωτοκόλλου (IP), τα δεδομένα υγείας που φυλάσσονται από νοσοκομείο ή γιατρό (βιομετρικά στοιχεία, γενετικά στοιχεία, εξετάσεις κ.α), οικονομικά στοιχεία ατόμων(ΑΦΜ, ΑΜΚΑ, ΑΜΙ, ΑΜ ΟΑΕΔ, λογιστικά στοιχεία κλπ.)

Παραδείγματα δεδομένων που δεν θεωρούνται προσωπικού χαρακτήρα, είναι ο αριθμός μητρώου εταιρείας, η εταιρική ηλεκτρονική διεύθυνση του τύπου «πληροφορίες@εταιρεία.com» και κάθε είδους ανώνυμα δεδομένα.

Κάποια δεδομένα θεωρούνται όχι μόνο προσωπικά αλλά και ευαίσθητα και ο κανονισμός είναι ιδιαίτερα αυστηρός σχετικά με την επεξεργασία τους .

Τα ακόλουθα προσωπικά δεδομένα θεωρούνται «ευαίσθητα» και υπόκεινται σε συγκεκριμένες συνθήκες επεξεργασίας:

-τα προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τις πολιτικές απόψεις, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις,
-συνδικαλιστική ιδιότητα μέλους ·
-γενετικά δεδομένα, βιομετρικά δεδομένα που έχουν υποστεί επεξεργασία αποκλειστικά για τον εντοπισμό ενός ανθρώπου ·
-δεδομένα σχετικά με την υγεία ·
-δεδομένα σχετικά με τη σεξουαλική ζωή ενός ατόμου ή τον γενετήσιο προσανατολισμό.

Τι αποτελεί επεξεργασία δεδομένων & πως πρέπει να γίνεται;

Ο όρος «επεξεργασία» καλύπτει ένα ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Παραδείγματα επεξεργασίας αποτελούν η διαχείριση προσωπικού και η μισθοδοσία, η προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα, η αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων, η δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο, η περιήγηση ενός επισκέπτη σε μια ιστοσελίδα, η αποθήκευση διευθύνσεων IP , η μαγνητοσκόπηση με τηλεόραση κλειστού κυκλώματος-κάμερες κλπ..

Ο τύπος και η ποσότητα των προσωπικών δεδομένων που μπορείτε να επεξεργαστείτε εξαρτάται από τον λόγο για τον οποίο το επεξεργάζεστε (νομικός λόγος που χρησιμοποιήθηκε) και τι θέλετε να κάνετε με αυτόν. Πρέπει να σέβεστε αρκετούς βασικούς κανόνες, μεταξύ των οποίων και

- τα προσωπικά δεδομένα **πρέπει να διεκπεραιώνονται με νόμιμο και διαφανή τρόπο,** διασφαλίζοντας τη δικαιοσύνη έναντι των ατόμων των οποίων τα προσωπικά δεδομένα επεξεργάζεστε («νομιμότητα, δικαιοσύνη και διαφάνεια»).
- πρέπει να έχετε συγκεκριμένους σκοπούς για την επεξεργασία των δεδομένων και **πρέπει να αναφέρετε τους σκοπούς αυτούς στα άτομα** όταν συλλέγουνται τα προσωπικά τους δεδομένα. Δεν μπορείτε απλά να συλλέγετε προσωπικά δεδομένα για απροσδιόριστους σκοπούς («περιορισμός του σκοπού»).
-πρέπει να συλλέξετε και **να επεξεργαστείτε μόνο τα προσωπικά δεδομένα που είναι απαραίτητα** για την εκπλήρωση αυτού του σκοπού («ελαχιστοποίηση δεδομένων»).
-πρέπει **να διασφαλίσετε ότι τα προσωπικά δεδομένα είναι ακριβή και ενημερωμένα**, λαμβάνοντας υπόψη τους σκοπούς για τους οποίους έχουν υποβληθεί σε επεξεργασία και να διορθώσετε αν όχι

(«ακρίβεια»).

-δεν μπορείτε να χρησιμοποιήσετε περαιτέρω τα προσωπικά δεδομένα για άλλους σκοπούς που δεν είναι συμβατοί με τον αρχικό σκοπό της συλλογής.

- πρέπει **να διασφαλίσετε ότι τα δεδομένα προσωπικού χαρακτήρα αποθηκεύονται για χρονικό διάστημα που δεν υπερβαίνει τα αναγκαία για τους σκοπούς** για τους οποίους συλλέχθηκαν («περιορισμός αποθήκευσης»).

-πρέπει **<u>να εγκαταστήσετε τις κατάλληλες τεχνικές και οργανωτικές διασφαλίσεις που διασφαλίζουν την ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και κατά τυχαίας απώλειας, καταστροφής ή ζημίας, χρησιμοποιώντας την κατάλληλη τεχνολογία («ακεραιότητα και εμπιστευτικότητα»).</u>**

Με δεδομένες τις παραπάνω συνθήκες και την σωστή τήρησή τους, μπορείτε να επεξεργάζεστε προσωπικά δεδομένα στις ακόλουθες περιπτώσεις:

-όταν έχετε την συγκατάθεση του ατόμου (πχ για να στείλετε ένα ενημερωτικό)

- όπου υπάρχει συμβατική υποχρέωση με τον πελάτη πχ. για να λειτουργήσει το ηλεκτρονικό σας κατάστημα (πχ. στάδια παραγγελίας)

- για να παρέχετε τις υπηρεσίες σας(πχ γιατρός, λογιστής κλπ.)

-για να τηρείτε τις υποχρεώσεις σας προς το κράτος(πχ . τήρηση στοιχείων για εργαζομένους, μισθοδοσίες κλπ.) ή για τη συμμόρφωση με νομοθεσίες

-για τα νόμιμα συμφέροντα της επιχείρησης και την ομαλή της λειτουργία(στο βαθμό που δεν επηρεάζονται σοβαρά τα θεμελιώδη δικαιώματα του ατόμου)

-για την προστασία της ζωής και της υγείας ενός ατόμου

|Τι πληροφορίες πρέπει να δίνονται;

Κατά τη στιγμή της συλλογής των δεδομένων τους, οι πολίτες πρέπει να ενημερώνονται τουλάχιστον για τα εξής:

-ποια είναι η εταιρεία / ο οργανισμός σας (τα στοιχεία επικοινωνίας σας και αυτά του ΥΠΔ σας, αν υπάρχουν);
-γιατί η εταιρεία / ο οργανισμός σας θα χρησιμοποιεί τα προσωπικά δεδομένα (τους σκοπούς)?
-τις κατηγορίες των σχετικών προσωπικών δεδομένων ·
-τη νομική αιτιολόγηση της επεξεργασίας των δεδομένων τους ·
-για πόσο χρόνο θα διατηρούνται τα δεδομένα και το χρονικό διάστημα στο οποίο θα διαγραφούν ή επικαιροποιηθούν.
-ποιος άλλος μπορεί να την λάβει;
-εάν τα προσωπικά τους δεδομένα θα μεταφερθούν σε παραλήπτη εκτός της ΕΕ ·
-ότι έχουν δικαίωμα σε αντίγραφο των δεδομένων (δικαίωμα πρόσβασης σε προσωπικά δεδομένα) δικαίωμα αλλαγής-τροποποίησης αυτών, δικαίωμα μεταφοράς, δικαίωμα διαγραφής

-το δικαίωμα υποβολής καταγγελίας στην Αρχή Προστασίας Δεδομένων (DPA) ·
-το δικαιωμά τους να αποσύρουν τη συγκατάθεσή τους ανά πάσα στιγμή ·

Οι πληροφορίες μπορούν να παρέχονται γραπτώς, προφορικά κατόπιν αιτήματος του ατόμου όταν αποδεικνύεται η ταυτότητά του με άλλα μέσα ή με ηλεκτρονικά μέσα, εφόσον χρειάζεται. Η εταιρεία / ο οργανισμός σας πρέπει να το κάνει με συνοπτικό, διαφανή, κατανοητό και εύκολα προσβάσιμο τρόπο, με σαφή και απλή γλώσσα και δωρεάν.

|Υποχρεώσεις της επιχείρησης

Με τον GDPR ενισχύονται σημαντικά τα δικαιώματα των υποκειμένων σχετικά με τα προσωπικά τους δεδομένα. Αντίστοιχα αυξάνονται και οι υποχρεώσεις των υπευθύνων επεξεργασίας, οι οποίοι επιφορτίζονται με την λεγόμενη αρχή της λογοδοσίας. Η αρχή αυτή αναλύεται σε πολλές επιμέρους ενέργειες που πρέπει να πραγματοποιεί ο υπεύθυνος ο οποίος «φέρει την ευθύνη και (πρέπει να) είναι σε θέση να αποδείξει τη συμμόρφωση» του με τις λοιπές γενικές αρχές που προβλέπει ο Κανονισμός.

Η αρχή της λογοδοσίας αποτελεί ομπρέλα υπό την οποία τίθενται όλες οι πράξεις επεξεργασίας και τονίζει τόσο την υποχρέωση συμμόρφωσης όσο και απόδειξης της συμμόρφωσής του αυτής.

- Για παράδειγμα στο άρθρο 7 παρ. 1 ορίζεται ότι όταν η επεξεργασία βασίζεται στην **συγκατάθεση**, ο υπεύθυνος πρέπει να **μπορεί να αποδείξει** ότι η συγκατάθεση έλαβε χώρα.
- Στο άρθρο 12 παρ. 1 υπογραμμίζεται η υποχρέωση του υπευθύνου επεξεργασίας να παρέχει στα υποκείμενα γραπτώς ή με άλλα μέσα (ακόμα και ηλεκτρονικά) τις **πληροφορίες που αφορούν επεξεργασία των δεδομένων** τους, και δη εντός ενός μήνα (παρ 3).
- Το άρθρο 15 κάνει λόγο για υποχρέωση παροχής **αντιγράφου** των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, άπαξ το υποκείμενο ασκήσει το δικαίωμα πρόσβασης προς τον υπεύθυνο.
- Στο άρθρο 24 όπου γίνεται λόγος για την **ευθύνη** του υπεύθυνου επεξεργασίας αναφέρεται ρητά η υποχρέωση του υπεύθυνου να αποδεικνύει ότι η επεξεργασία γίνεται σύμφωνα με τον Κανονισμό, παρέχοντας τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Προβλέπεται επίσης η δυνατότητα επιλογής **πολιτικών προστασίας** ικανών να εφαρμοστούν, καθώς και η **τήρηση εγκεκριμένου κώδικα δεοντολογίας** ή **μηχανισμού πιστοποίησης** ως αποδεικτικά της συμμόρφωσης, οι οποίες προστίθενται στην λίστα των υποχρεώσεων του υπεύθυνου επεξεργασίας.

Privacy by Design/Privacy by Default: Ο υπεύθυνος επεξεργασίας(ο ιδιοκτήτης της επιχ/σης), προκειμένου να συμμορφώνεται με τις επιταγές του Κανονισμού και να αποδεικνύει την συμμόρφωση του, λαμβάνει **κατάλληλα τεχνικά και οργανωτικά μέτρα**, όπως:

- ψευδωνυμοποίηση,
- μέτρα σχεδιασμένα για την εφαρμογή των αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων και
- μέτρα σχεδιασμένα, ώστε να προάγουν την διαφάνεια, όσον αφορά τις λειτουργίες και τις επεξεργασίες δεδομένων, προκειμένου να μπορεί το υποκείμενο των δεδομένων να παρακολουθεί την επεξεργασία και να είναι σε θέση ο υπεύθυνος επεξεργασίας να δημιουργεί και να βελτιώνει τα χαρακτηριστικά ασφαλείας

Η αρχή της λογοδοσίας επεκτείνεται και στον **εκτελούντα την επεξεργασία(υπάλληλος ή συνεργάτης)** (Άρθρο 28). Ο εκτελών την επεξεργασία, ο οποίος επιλέγεται από τον υπεύθυνο, οφείλει να παρέχει **επαρκείς διαβεβαιώσεις** για την εφαρμογή κατάλληλων οργανωτικών και τεχνικών μέτρων. Η επεξεργασία διενεργείται μόνο κατόπιν σύμβασης γραπτής και δεσμευτικής για τον εκτελούντα, ο οποίος επεξεργάζεται τα δεδομένα μόνο **σύμφωνα με τις καταγεγραμμένες εντολές** του υπευθύνου. Επίσης,

οφείλει να παρέχει στον υπεύθυνο επεξεργασίας πληροφορίες ως απόδειξη της συμμόρφωσης προς τις υποχρεώσεις του. Ο υπεύθυνος, δηλαδή, επιφορτίζεται με την υποχρέωση προσεκτικής επιλογής του υπευθύνου και φέρει ευθύνη σε περίπτωση που αυτός δεν επιτελεί τα καθήκοντά του από τη μεταξύ τους σύμβαση σύμφωνα με τον Κανονισμό.

Τήρηση αρχείων δραστηριοτήτων επεξεργασίας για επιχειρήσεις (άρθρο 30)

Ο υπεύθυνος και εκτελών την επεξεργασία πρέπει να τηρούν εγγράφως ή ηλεκτρονικά αρχείο δραστηριοτήτων επεξεργασιών τους το οποίο και να μπορούν να θέτουν στην διάθεση της Εποπτικής Αρχής κατόπιν αιτήματος της.

Η τήρηση αρχείου καταγραφής των δραστηριοτήτων επεξεργασιών είναι υποχρεωτική στις ακόλουθες περιπτώσεις:

- Όταν η επιχείρηση ή ο οργανισμός απασχολεί άνω των 250 ατόμων.
- Όταν η επεξεργασία δημιουργεί κινδύνους για τα δεδομένα
- Όταν η επεξεργασία δεν είναι περιστασιακή
- Όταν η επεξεργασία περιλαμβάνει ειδικές κατηγορίες δεδομένων των άρθρων 9 και 10 ΓΚΠΔ («ευαίσθητα δεδομένα», ήτοι βιομετρικά, γενετικά δεδομένα, δεδομένα που αφορούν ποινικές καταδίκες, αδικήματα και μέτρα ασφαλείας)

Γνωστοποίηση Παραβίασης δεδομένων προσωπικού χαρακτήρα (άρθρο 33)

Εντός 72 ωρών από την στιγμή της απόκτησης γνώσης του γεγονότος της παραβίασης, ο υπεύθυνος οφείλει να την γνωστοποιήσει στην αρμόδια Εποπτική Αρχή. Αυτό δεν είναι υποχρεωτικό όταν δεν ενδέχεται να προκληθεί κίνδυνος από την παραβίαση. Την απουσία κινδύνου οφείλει να αποδείξει ο υπεύθυνος. Επίσης, οφείλει να δικαιολογήσει την παραβίαση βάσει πραγματικών περιστατικών και να αναφερθεί στις συνέπειες και τα ληφθέντα διορθωτικά μέτρα, δίνοντας την δυνατότητα στην Εποπτική Αρχή να επαληθεύσει την συμμόρφωση.

Privacy Impact Assessment (Εκτίμηση Αντικτύπου σχετικά με την προστασία των δεδομένων) (άρθρο 35)

Ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους. Η εκπόνηση της μελέτης αυτής απαιτείται ιδίως σε περιπτώσεις:

1. συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ η οποία οδηγεί σε λήψη αποφάσεων,
2. μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στα άρθρα 9 και 10 και
3. συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

Η εκπόνηση της μελέτης δεν είναι υποχρεωτική για τους υπευθύνους που δεν ανήκουν στις κατηγορίες που αναφέρονται στο άρθρο 35.

Ορισμός DPO (Υπεύθυνος Προστασίας Δεδομένων) (άρθρο 39)

Οι επιχειρήσεις και οι οργανισμοί ορισμένης κλίμακας και δραστηριότητας οφείλουν να ορίζουν έναν υπεύθυνο προστασίας δεδομένων (DPO/ ΥΠΔ) στα καθήκοντα του οποίου περιλαμβάνεται και η

παρακολούθηση η συμμόρφωσης με τον Κανονισμό και τις πολιτικές προστασίας προσωπικών δεδομένων του υπευθύνου ή εκτελούντος την επεξεργασία. Επίσης, αναλαμβάνει την ανάθεση αρμοδιοτήτων και την ευαισθητοποίηση και κατάρτιση των υπαλλήλων, που διαχειρίζονται και επεξεργάζονται προσωπικά δεδομένα ενώ, παράλληλα, προβαίνει και στους απαραίτητους ελέγχους.

Η εταιρεία / ο οργανισμός σας πρέπει να ορίσει έναν υπεύθυνο προστασίας δεδομένων, είτε πρόκειται για υπεύθυνο επεξεργασίας είτε για επεξεργαστή, **εάν οι κύριες δραστηριότητές του περιλαμβάνουν την επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή περιλαμβάνουν μεγάλης κλίμακας, τακτική και συστηματική παρακολούθηση ατόμων.** Από την άποψη αυτή, η παρακολούθηση της συμπεριφοράς των υποκειμένων των δεδομένων περιλαμβάνει όλες τις μορφές παρακολούθησης και δημιουργίας προφίλ στο Διαδίκτυο, μεταξύ άλλων για σκοπούς διαφήμισης συμπεριφοράς.

Οι δημόσιες διοικήσεις έχουν πάντοτε την υποχρέωση να διορίσουν έναν ΥΠΔ (εκτός από τα δικαστήρια που ενεργούν υπό την ιδιότητα του δικαστή).

Ο ΥΠΔ μπορεί να είναι υπάλληλος του οργανισμού σας ή μπορεί να συνάπτεται εξωτερικά βάσει επικοινωνίας με την υπηρεσία. Ένας ΥΠΔ μπορεί να είναι ένα άτομο ή ένας οργανισμός.

Παραδείγματα
Υποχρεωτικός ΥΠΔ
Ένας ΥΠΔ είναι υποχρεωτικός για παράδειγμα όταν η εταιρεία / ο οργανισμός σας είναι:

-ένα νοσοκομείο που επεξεργάζεται μεγάλα σύνολα ευαίσθητων δεδομένων
-μια εταιρεία ασφαλείας υπεύθυνη για την παρακολούθηση εμπορικών κέντρων και δημόσιων χώρων
-μια μικρή εταιρεία ευρεσης εργασίας που διαχειρίζεται συνεχώς προφιλ και βιογραφικά άτομων

Ο ΥΠΔ δεν είναι υποχρεωτικός
Ένας ΥΠΔ δεν είναι υποχρεωτικός εάν:

-είστε ιατρός τοπικής κοινότητας και επεξεργάζεστε προσωπικά δεδομένα των ασθενών σας
-έχετε μια μικρή δικηγορική εταιρεία και επεξεργάζεστε προσωπικά δεδομένα των πελατών σας

Διασφάλιση δεδομένων

Λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, **ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση:**

α) της ψευδωνυμοποίησης και της κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα,

β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,

γ) της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος,

δ) διαδικασίας για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας.

2. Κατά την εκτίμηση του ενδεδειγμένου επιπέδου ασφάλειας λαμβάνονται ιδίως υπόψη οι κίνδυνοι που απορρέουν από την επεξεργασία, ιδίως από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

3. Η τήρηση εγκεκριμένου κώδικα δεοντολογίας όπως αναφέρεται στο άρθρο 40 ή εγκεκριμένου μηχανισμού πιστοποίησης όπως αναφέρεται στο άρθρο 42 δύναται να χρησιμοποιηθεί ως στοιχείο για την απόδειξη της συμμόρφωσης με τις απαιτήσεις της παραγράφου 1 του παρόντος άρθρου.

4. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία λαμβάνουν μέτρα ώστε να διασφαλίζεται ότι κάθε φυσικό πρόσωπο που ενεργεί υπό την εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία το οποίο έχει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα τα επεξεργάζεται μόνο κατ' εντολή του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο από το δίκαιο της Ένωσης ή του κράτους μέλους.

Κυρώσεις - πρόστιμα

Σε περίπτωση ελέγχου μετά από καταγγελία ή μετά από απόφαση της ΑΑΔΕ(Αρχή προστασίας δεδομένων) θα ελεγχθούν όλες οι διαδικασίες που έχουν υλοποιηθεί , θα αξιολογηθεί ο κίνδυνος που δημιουργήθηκε για τα άτομα μετά από μια διαρροή δεδομένων κ.α . Τα πρόστιμα που επιβάλλονται μπορεί να φτάσουν μέχρι και το 4% του ετήσιου τζίρου της επιχείρησης . Το κατώτατο πρόστιμο δεν έχει διαμορφωθεί ακόμη για την Ελλάδα , από εμπειρία όμως άλλων ευρωπαϊκών κρατών ξεκινάει για μικρές παραβιάσεις από 5000€ μαζί με την αποζημίωση του ατόμου /ατόμων που έπληξε η όποια παραβίαση του κανονισμού ή διαρροή .

Δικαιώματα των ατόμων

Η ουσιαστική ενίσχυση των δικαιωμάτων των υποκειμένων των δεδομένων αποτέλεσε έναν από τους βασικούς άξονες του GDPR.

Ως εκ τούτου, δεν προκαλεί έκπληξη το γεγονός ότι στον πυρήνα του νέου Κανονισμού ανήκει μεταξύ άλλων και η απλοποίηση των διαδικασιών ενημέρωσης και άσκησης των δικαιωμάτων των υποκειμένων. Για τον λόγο αυτό επαναλαμβάνεται σε πολλά σημεία η υποχρέωση του υπεύθυνου επεξεργασίας να ενημερώνει κατά τρόπο εύληπτο, δηλαδή σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή (άρθρο 12) το υποκείμενο για την επεξεργασία που υφίστανται τα προσωπικά του δεδομένα.

Αντίστοιχα ενισχύεται και η θέση του παιδιού στην κοινωνία της Πληροφορίας, καθώς ο Κανονισμός ρητά απαιτεί ήδη από τις αιτιολογικές σκέψεις την προσαρμογή της επεξεργασίας και της ενημέρωσης σχετικά με αυτήν στις ανάγκες των πιο ευάλωτων ομάδων, όπως τα παιδιά. Ιδίως δε στο άρθρο 8 αναλύονται οι προϋποθέσεις για την λήψη συγκατάθεσης από ανήλικο κάτω των 16 ετών.

Στο Κεφάλαιο ΙΙΙ του Κανονισμού γίνεται αναλυτική παρουσίαση των δικαιωμάτων των υποκειμένων. Μέσω αυτών καθίσταται δυνατή η αποτελεσματική προστασία των προσωπικών δεδομένων, καθώς η πρόβλεψη αυτών με τον ΓΚΠΔ (GDPR) τα καθιστά αγώγιμα και υποχρεώνει τον υπεύθυνο επεξεργασίας σε ικανοποίηση τους. Τα βασικά δικαιώματα των πολιτών σχετικά με τα προσωπικά τους δεδομένα είναι:

Δικαίωμα ενημέρωσης (Άρθρα 12επ): όπως υποδεικνύει και ο τίτλος του άρθρου, ο Κανονισμός επιτάσσει διαφανή ενημέρωση. Ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα μέτρα, ώστε να παρέχει στο υποκείμενο κάθε πληροφορία και κάθε ανακοίνωση σχετικά με την επεξεργασία σε συνοπτική, διαφανή καθώς και κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας απλή και σαφή διατύπωση, ιδίως όταν η πληροφορία απευθύνεται σε παιδιά. Οφείλει να διευκολύνει την άσκηση των δικαιωμάτων για τα υποκείμενα και να παρέχει στο υποκείμενο πληροφορίες για την ενέργεια που πραγματοποιείται κατόπιν αιτήματός στηριζόμενο στα άρθρα 15 έως 22, χωρίς καθυστέρηση και μάλιστα εντός ενός μήνα από την παραλαβή του αιτήματος. Σημειωτέον ότι ο Κανονισμός διακρίνει το δικαίωμα ενημέρωσης αναφορικά με το αν η συλλογή των δεδομένων πραγματοποιείται από το ίδιο το υποκείμενο (άρθρο 13) ή από τρίτο πρόσωπο (άρθρο 14).

Δικαίωμα πρόσβασης (άρθρο 15): το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα που το αφορούν υφίστανται επεξεργασία και έχει πρόσβαση σε πλήθος πληροφοριών όπως αυτές σκιαγραφούνται από το άρθρο 15.

Δικαίωμα Διόρθωσης (άρθρο 16): Το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση τη διόρθωση ανακριβών δεδομένων προσωπικού χαρακτήρα που το αφορούν. Έχοντας υπόψη τους σκοπούς της επεξεργασίας, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει τη συμπλήρωση ελλιπών δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων μέσω συμπληρωματικής δήλωσης.

Δικαίωμα Διαγραφής – Δικαίωμα στην Λήθη (άρθρο 17 – Right to be forgotten): Το υποκείμενο των δεδομένων έχει το δικαίωμα να ζητήσει από τον υπεύθυνο επεξεργασίας τη διαγραφή δεδομένων προσωπικού χαρακτήρα, που το αφορούν, αν τα δεδομένα προσωπικού χαρακτήρα δεν είναι πλέον απαραίτητα ή αν το υποκείμενο ανακαλέσει τη συγκατάθεσή του ή αν δεν υπάρχει άλλη νομική βάση για την επεξεργασία ή αντιτίθεται στην επεξεργασία και δεν υπάρχουν επιτακτικοί και νόμιμοι λόγοι ή αν τα δεδομένα υποβλήθηκαν σε επεξεργασία παράνομα ή για να τηρηθεί νομική υποχρέωση βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους, στην οποία υπόκειται ο υπεύθυνος επεξεργασίας ή αν έχουν συλλεχθεί όντα το υποκείμενο ήταν παιδί.

Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18): το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο τον περιορισμό της επεξεργασίας όταν α) η ακρίβεια των δεδομένων αμφισβητείται ή β) είναι παράνομη ή γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για την θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων ή δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία, εν αναμονή της επαλήθευσης του κατά πόσον οι νόμιμοι λόγοι του υπεύθυνου επεξεργασίας υπερισχύουν έναντι όλων των λόγων του υποκειμένου των δεδομένων.

Δικαίωμα στην Φορητότητα των Δεδομένων (άρθρο 20): Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο, καθώς και το δικαίωμα να διαβιβάζει τα εν λόγω δεδομένα σε άλλον υπεύθυνο επεξεργασίας, χωρίς αντίρρηση από τον υπεύθυνο επεξεργασίας, στον οποίο παρασχέθηκαν τα δεδομένα προσωπικού χαρακτήρα.

Δικαίωμα Εναντίωσης (άρθρο 21): Το υποκείμενο των δεδομένων δικαιούται να αντιτάσσεται, ανά πάσα στιγμή και για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή του, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα που το αφορούν (επεξεργασία από δημόσιες αρχές ή από ιδιώτες), περιλαμβανομένης της κατάρτισης προφίλ βάσει των εν λόγω διατάξεων. Εάν δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για σκοπούς απευθείας εμπορικής προώθησης, το υποκείμενο των δεδομένων δικαιούται να αντιταχθεί ανά πάσα στιγμή στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν για την εν λόγω εμπορική προώθηση, περιλαμβανομένης της κατάρτισης προφίλ, εάν σχετίζεται με αυτήν την απευθείας εμπορική προώθηση.

Δικαίωμα να μην υπόκειται σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, συμπεριλαμβανομένης της κατάρτισης προφίλ (άρθρο 22): Το δικαίωμα αυτό βασίζεται στο γεγονός ότι η ανθρώπινη παρέμβαση καταπολεμά το έλλειμμα εμπιστοσύνης της εκάστοτε αυτοματοποιημένης επεξεργασίας.

Διαδικασία συμμόρφωσης με τον κανονισμό

Οι επιχειρήσεις θα πρέπει να ακολουθήσουν τα εξής βήματα:

Α. Εσωτερική λειτουργία της επιχείρησης: μετά από προσεκτική μελέτη

-της δομής της επιχείρησης, του αντικειμένου και των προσώπων που διαχειρίζονται δεδομένα

-του τρόπου που διαχειρίζεται ως τώρα τα δεδομένα υπαλλήλων και πελατών ,

-των κενών ασφαλείας που υπάρχουν ως τώρα σε όλες τις διαδικασίες

-της υπάρχουσας δομής του δικτύου

η επιχείρηση θα πρέπει να προχωρήσει σε:

1. Διαμόρφωση του εσωτερικού δικτύου Η/Υ της ώστε να διασφαλιστεί η ασφάλεια των δεδομένων με προσαρμογές όπως:
   -σχεδιασμό διαδικασιών περιορισμένης πρόσβασης σε αυτά μόνο από τα εντεταλμένα άτομα
   -αποκλεισμό πιθανότητας πρόσβασης στα αρχεία του δικτύου από εξωτερικούς χρήστες του διαδικτύου και ηλεκτρονικές επιθέσεις (πχ firewalls , απομόνωση wifi κλπ.)
   - κρυπτογράφηση των αρχείων προσωπικών δεδομένων κ.α
2. Φύλαξη των δεδομένων σε έντυπη μορφή (αρχείο) σε ασφαλές μέρος και πρόσβαση σε αυτό μόνο εντεταλμένων ατόμων. Τήρηση αντιγράφων ασφαλείας των ηλεκτρονικών δεδομένων με ασφαλή τρόπο. Αν χρησιμοποιείται κάποιο πρόγραμμα όπου υπάρχει βάση δεδομένων διασφάλιση ότι αυτό τηρεί τις προδιαγραφές ασφαλείας.
3. Διαμόρφωση και υπογραφή κατάλληλων συμβάσεων όπου θα αναφέρονται τα εντεταλμένα για την επεξεργασία των δεδομένων άτομα και η διασφάλιση της εχεμύθειας αυτών

4. Διαμόρφωση διαδικασιών για την εξασφάλιση της έγκρισης των πελατών /συνεργατών αν απαιτείται και της γνωστοποίησης σε αυτούς του είδους των δεδομένων που επεξεργάζεται η επιχείρηση, του σκοπού επεξεργασίας, του τρόπου τήρησης της ασφάλειας των δεδομένων τους, του χρόνου επεξεργασίας και του τρόπου να ασκήσουν τα δικαιώματά τους
5. Καταγραφή όλων των διαδικασιών συμμόρφωσης με τον κανονισμό που υλοποιήθηκαν, ορισμός υπευθύνων και εντεταλμένων προσώπων και των τρόπων απόκρισης σε αιτήματα πελατών και συνεργατών σχετικά με τα δικαιώματά τους πάνω στα δεδομένα τους, σε ένα εγχειρίδιο που θα παρουσιάζεται και σε περίπτωση ελέγχου.

Β. Διαδικτυακή παρουσία επιχείρησης

- site παρουσίασης:

Στην ιστοσελίδα της επιχείρησης και στην ηλεκτρονική αλληλογραφία θα πρέπει απαραίτητα να υπάρχουν τα εξής:

1. SSL πιστοποιητικό ασφαλείας
2. Αυστηρές πολιτικές ασφαλείας στους σερβερς που φιλοξενείται
3. Κατάλληλα διατυπωμένοι όροι χρήσης και πολιτικές απορρήτου όπου θα περιγράφονται οι σκοποί , οι τρόποι και οι μηχανισμοί τήρησης των δεδομένων , καθώς και οι τρόποι που οι πελάτες θα μπορούν να ασκήσουν τα δικαιώματά τους
4. Μηχανισμοί αποδοχής της παροχής των προσωπικών δεδομένων από τους πελάτες, διαγραφής από λίστες ενημερωτικών, διαχείρισης του λογαριασμού τους

- **eshop**

Εαν διαθέτετε e-shop θα πρότειναμε σε πρώτη φάση τις ακόλουθες ενέργειες που είναι απαραίτητες για όλα τα e-shop ανεξάρτητα του τύπου ηλεκτρονικού καταστήματος και των ειδών/υπηρεσιών που εμπορεύονται:

1. Αγορά και εγκατάσταση πιστοποιητικού SSL για το e-shop σας

2. Αναθεώρηση της πολιτικής διατήρησης προσωπικών δεδομένων στο e-shop σας
3. Ενημερωτικό PopUp στην αρχική σελίδα που θα προτρέπει το χρήστη να αποδεχτεί την διατήρηση cookies και να αναγνώσει και αποδεχτεί την πολιτική διαχείρισης και προστασίας των προσωπικών δεδομένων που διατηρεί το eShop
4. Προσθήκη στο προφίλ του, δυνατότητας διαγραφής του λογαριασμού του και του ιστορικού παραγγελιών του από τη βάση δεδομένων του e-shop
5. Δυνατότητα πρόσβασης και αλλαγής των προσωπικών του δεδομένων μέσα από το προφίλ του
6. Προσθήκη συνδέσμου με check αποδοχής της πολιτικής διατήρησης προσωπικών δεδομένων στη φόρμα εγγραφής και τροποποίησης του προφίλ του. Η φόρμα να μην αποθηκεύεται αν ο χρήστης δεν τσεκάρει την επιλογή, κατοχυρώνοντας με την ψηφιακή υπογραφή του ότι συναινεί να παρέχει τα προσωπικά του δεδομένα στην επιχείρηση.
7. [Προαιρετικά] μηχανισμό αυτόματης απενεργοποίησης ή διαγραφής στοιχείων μελών που δεν είχαν πρόσβαση και δεν έκαναν καμία αγορά για τα τελευταία Χ έτη.
8. Μαζική αποστολή e-mail στους πελάτες του eShop για να διαβάσουν και να αποδεχτούν την νέα τροποποιημένη πολιτική διατήρησης και προστασίας των προσωπικών τους δεδομένων
9. Εαν το eShop διατηρεί δεδομένα όπως: φύλο, ημερομηνία γέννησης κτλ, και δεν είναι απαραίτητα στην εταιρεία, θα πρότειναμε να διαγραφούν από τη βάση δεδομένων και να αφαιρεθούν σαν πεδία από φόρμες εγγραφής/τροποποίησης προφίλ των μελών.

10. Σχετικά με το newsletter: θα πρέπει ο χρήστης να έχει τη δυνατότητα **OptOut** και **unsubscribe** από τη mailing list τόσο στο προφίλ του όσο και σαν σύνδεσμο διαγραφής στο κάτω μέρος των e-mail που στέλνει μαζικά η επιχείρηση
11. Διαγραφή ΟΛΩΝ των επαφών από τη βάση δεδομένων σας που καταχωρήθηκαν ΧΩΡΙΣ τη συγκατάθεση τους (μαζική εισαγωγή επαφών με import από άλλες βάσεις δεδομένων)
12. Σε περίπτωση που το e-shop σας είναι συνδεδεμένο με ERP ή λογιστικό πρόγραμμα, θα πρέπει οπωσδήποτε να συμβουλευτείτε το σύμβουλο GDPR και να σας ενημερώσει για την περίπτωση σας τι άλλες αλλαγές απαιτούνται τόσο στο e-shop όσο και στο ERP σας
13. Αυστηρές πολιτικές ασφαλείας στους σερβερς που φιλοξενείται
14. Αυστηρές πολιτικές ασφαλείας στους σερβερς που φιλοξενείται
15. τήρηση αντιγράφων ασφαλείας
16. Με προσοχή και μετά από κατάλληλες συμβουλές πρέπει να γίνεται επίσης η δραστηριότητα της επιχείρησης στα social media , στο mail marketing – newletters, προωθήσεις στο google κλπ.

ΠΡΟΣΟΧΗ:

Σε μια μικρομεσαία επιχείρηση που διαχειρίζεται προσωπικά δεδομένα στα πλαίσια της λειτουργίας της σε ένα φυσιολογικό βαθμό (όχι σε εκτεταμένη κλίμακα) απαιτούνται να γίνουν οι διαδικασίες συμμόρφωσης με τον κανονισμό που αναφέρθηκαν πιο πάνω, σε συνεργασία με έναν έμπειρο συνεργάτη στον τομέα της πληροφορικής που θα υλοποιήσει τις παρεμβάσεις στο εσωτερικό δίκτυο και την ιστοσελίδα και έναν δικηγόρο για τις νομικές παρεμβάσεις σε συμβάσεις κλπ. Καλό είναι να γίνεται μελλοντικά ένας έλεγχος του δικτύου και των διαδικασιών ότι όλα τηρούνται καλώς.

ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ δεν απαιτείται να έχουν υπεύθυνο προστασίας δεδομένων (DPO) που θα παρέχει υπηρεσίες συνεχούς παρακολούθησης με το μήνα ή σε άλλη συστηματική βάση έναντι υπέρογκων ποσών .

Μετά από ένα σωστό σχεδιασμό και υλοποίηση των διαδικασιών συμμόρφωσης και της κατάλληλης εκπαίδευσης του υπευθύνου της επιχείρησης και του προσωπικού της, αυτοί είναι σε θέση να τηρούν σωστά τις διαδικασίες ασφάλειας για το καλό της επιχείρησης και την αποφυγή προστίμων. Χρειάζονται απλά να μπορούν να απευθύνονται στον συνεργάτη πληροφορικής ή στο δικηγόρο τους ανάλογα το θέμα που προκύπτει για συμβουλή στη διαχείριση της όποιας κατάστασης.

Περισσότερες λεπτομέρειες για τον κανονισμό μπορείτε δείτε στον οδηγό της ευρωπαϊκής ένωσης

https://ec.europa.eu/info/law/law-topic/data-protection/reform_el