



GDPR

ΓΕΝΙΚΟΣ ΚΑΝΟΝΙΣΜΟΣ ΠΡΟΣΤΑΣΙΑΣ
ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΤΙ ΕΙΝΑΙ Ο ΓΚΠΔ / GDPR

Αποτελεί τον Κανονισμό της (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27^{ης} Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

Ονομάζεται αλλιώς Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ) (GDPR- **General Data Protection Regulation**) και αναλύει τις υποχρεώσεις των Υπεύθυνων αλλά και των Χειριστών επεξεργασίας των προσωπικών δεδομένων.



Ο νέος Κανονισμός τέθηκε σε ισχύ στις 5 Μαΐου 2016 με μεταβατική περίοδο 2 ετών και θα εφαρμοσθεί άμεσα, ως Νομοθέτημα άμεσης εφαρμογής που ισχύει αυτόματα σε όλες τις χώρες μέλη της Ευρωπαϊκής Ένωσης στις 25 Μαΐου 2018.

Η μη συμμόρφωση με τις απαιτήσεις του κανονισμού επιφέρει τεράστια πρόστιμα που αγγίζουν ακόμα και το **4%** του ετήσιου Κύκλου Εργασιών.

ΤΙ ΕΙΝΑΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ

Ο Κανονισμός ορίζει ως «Προσωπικό Δεδομένο» ΚΑΘΕ ΠΛΗΡΟΦΟΡΙΑ που τελικά ταυτοποιεί ένα **Φυσικό Πρόσωπο** που είναι και το «Υποκείμενο» των προσωπικών δεδομένων.

Το «Υποκείμενο» ή αλλιώς το Φυσικό Πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί με άμεσα ή έμμεσο τρόπο.

Τι είναι τα προσωπικά δεδομένα;

- Όνομα
- Διεύθυνση
- Τόπος
- Ηλεκτρονικό αναγνωριστικό
- Πληροφορίες υγείας
- Εισόδημα
- Πολιτιστικά χαρακτηριστικά
- και άλλα

**ΣΥΛΛΟΓΗ
ΑΠΟΘΗΚΕΥΣΗ
ΧΡΗΣΗ
ΔΕΔΟΜΕΝΩΝ;**

Πρέπει να ακολουθείτε τους κανόνες.

**Επεξεργάζεστε δεδομένα
για άλλες εταιρείες;
Αυτό ισχύει και για σας.**

ΚΑΛΥΤΕΡΟΙ ΚΑΝΟΝΕΣ – ΓΙΑΤΙ ΑΛΛΑΖΟΥΝ ΟΙ ΚΑΝΟΝΕΣ;

Η εφαρμογή αυστηρότερων κανόνων σχετικά με την προστασία των δεδομένων, συνεπάγεται ότι οι Πολίτες, θα ασκούν μεγαλύτερο έλεγχο όσον αφορά τα δεδομένα τους, καθώς επίσης οι Επιχειρήσεις και οι Οργανισμοί θα δρέπουν επιχειρηματικά οφέλη με πιο ισότιμους όρους.

Η συγκεκριμένη Ευρωπαϊκή Οδηγία, αποτελεί ουσιαστικά μια «Δέσμη» Κανόνων που αφορούν σε όλες τις Επιχειρήσεις και τους Οργανισμούς που δραστηριοποιούνται στην (ΕΕ), όπου και αν βρίσκεται η έδρα τους.

Συγκεκριμένα, ο Κανονισμός ρυθμίζει τα δικαιώματα των Φυσικών Προσώπων σχετικά με (4) άξονες:

1. Τα προσωπικά τους δεδομένα.
2. Την επεξεργασία των προσωπικών τους δεδομένων.
3. Την ελεύθερη και ανεμπόδιστη κυκλοφορία και μεταβίβαση των προσωπικών τους δεδομένων εντός των ορίων της Ευρωπαϊκής Ένωσης.
4. Τις διαδικασίες μεταφοράς προσωπικών δεδομένων εκτός Ευρωπαϊκής Ένωσης.

Είναι θέμα εμπιστοσύνης...

Η έλλειψη εμπιστοσύνης στους παλιούς κανόνες για την προστασία των δεδομένων ανέκοψε την πορεία της ψηφιακής οικονομίας και πολύ πιθανώς τις επιχειρήσεις σας.

Μόνο το **15%**

των ανθρώπων αισθάνονται ότι έχουν πλήρη έλεγχο των πληροφοριών που παρέχουν ηλεκτρονικά.



ΣΤΟΧΟΙ ΤΟΥ ΓΚΠΔ/GDPR

Βασικός σκοπός του νέου Κανονισμού είναι η διαφύλαξη των προσωπικών δεδομένων των πολιτών της ΕΕ.



Ενίσχυση των
Ατομικών
Δικαιωμάτων

- Δικαίωμα στη λήθη.
- Δικαίωμα στη διαγραφή.
- Δικαίωμα στη φορητότητα των δεδομένων.
- Υποχρέωση της λογοδοσίας για όσους επεξεργάζονται προσωπικά δεδομένα.
- Υποχρέωση της ρητής συγκατάθεσης για την χρήση των προσωπικών δεδομένων.



Διευρυμένο
Πεδίο
Εφαρμογής

- Σχεδόν όλες οι Επιχειρήσεις και οι Οργανισμοί επηρεάζονται -> Αυστηρότερες Αρχές
- Ισχύς του κανονισμού για Επιχειρήσεις και Οργανισμούς εκτός της ΕΕ οι οποίες επεξεργάζονται δεδομένα πολιτών της ΕΕ.
- Εισαγωγή της έννοιας του Υπεύθυνου Προστασίας προσωπικών Δεδομένων (DPO)
- Νέοι κανόνες για Ευαίσθητα Προσωπικά Δεδομένα

- Αυξημένο Ρίσκο Μη Συμμόρφωσης: Πρόστιμα έως το 4% του ετήσιου Κύκλου Εργασιών.
- Πολιτικές / Αστικές Αγωγές
- Έλεγχος και έγκριση από την Αρχή Προστασίας Δεδομένων.



Ισχυροποίηση της
επιβολής & της
Υποχρέωσης
Λογοδοσίας

- Εναρμονισμένοι Κανόνες - απλούστερο νομικό τοπίο.
- Εποπτεία από (1) Ευρωπαϊκή Επιτροπή + από τις Τοπικές Ρυθμιστικές Αρχές.
- Αξιολογήσεις και Αλλαγές συφισταμένων Σμβάσεων.



Εναρμόνιση σε
όλη την ΕΕ

ΤΙ ΥΠΟΧΡΕΟΥΤΑΙ ΝΑ ΚΑΝΕΙ Η ΕΠΙΧΕΙΡΗΣΗ ή Ο ΟΡΓΑΝΙΣΜΟΣ ΣΑΣ ΜΕ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR

Επικοινωνία

- Χρησιμοποιήστε απλή γλώσσα.
- Πείτε τους **ποιοι** είστε όταν ζητάτε τα δεδομένα.
- Πείτε **τον λόγο** που επεξεργάζεστε τα δεδομένα τους, **για πόσο** καιρό θα τα φυλάξετε και **ποιος** τα λαμβάνει.

Συγκατάθεση

Λάβετε τη ρητή συγκατάθεσή τους για την επεξεργασία των δεδομένων.

Συλλέγετε δεδομένα από παιδιά για τα μέσα κοινωνικής δικτύωσης; Ελέγξτε το όριο ηλικίας για τη συγκατάθεση των γονιών.

Πρόσβαση και δυνατότητα μεταφοράς

Δώστε στα άτομα πρόσβαση στα δεδομένα τους και επιτρέψτε τους να τα δώσουν σε άλλη εταιρεία.

Προειδοποιήσεις

Ενημερώστε τα άτομα σχετικά με παραβιάσεις δεδομένων αν ενέχει σοβαρό κίνδυνο για αυτούς.

Προστασία ευαίσθητων δεδομένων

Χρησιμοποιήστε πρόσθετα μέτρα προστασίας για πληροφορίες που αφορούν την υγεία, τη φυλή, τον σεξουαλικό προσανατολισμό, τη θρησκεία και τις πολιτικές πεποιθήσεις.

ΤΙ ΥΠΟΧΡΕΟΥΤΑΙ ΝΑ ΚΑΝΕΙ Η ΕΠΙΧΕΙΡΗΣΗ ή Ο ΟΡΓΑΝΙΣΜΟΣ ΣΑΣ ΜΕ ΤΗΝ ΕΦΑΡΜΟΓΗ ΤΟΥ GDPR

Διαγραφή Δεδομένων

Δώστε τους το «δικαίωμα στη λήθη».
Διαγράψτε τα προσωπικά τους δεδομένα αν το ζητήσουν, αλλά μόνο αν δεν θίγεται η ελευθερία έκφρασης ή η δυνατότητα διεξαγωγής έρευνας.

Δημιουργία προφίλ

Αν χρησιμοποιείτε προφίλ για την επεξεργασία αιτήσεων για νομικά δεσμευτικές συμφωνίες, για παράδειγμα για δάνεια, πρέπει:

- Να ενημερώνετε τους πελάτες σας.
- Να ορίζετε ένα πρόσωπο και όχι μια μηχανή να ελέγχει τη διαδικασία αν η αίτηση τελικά απορρίπτεται.
- Να χορηγείτε στον αιτούντα το δικαίωμα να προσβάλλει την απόφαση.

Διαβίβαση δεδομένων εκτός της ΕΕ

Συνάψτε νομικές συμφωνίες όταν διαβιβάζετε δεδομένα σε χώρες που δεν έχουν λάβει έγκριση από τις αρχές της ΕΕ.

Μάρκετινγκ

Δώστε στα άτομα το δικαίωμα να εξαιρεθούν από πρακτικές άμεσου μάρκετινγκ που χρησιμοποιούν τα δεδομένα τους.

ΕΠΙΠΤΩΣΕΙΣ ΑΠΟ ΤΗ ΜΗ ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ ΚΑΝΟΝΙΣΜΟ

Οι επιπτώσεις ποικίλουν και αφορούν ένα ευρύ φάσμα Επιχειρήσεων και Οργανισμών ορισμένων εκ των οποίων ανήκουν στην ομάδα ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ γιατί η δραστηριότητά τους αφορά σε:



ΤΟ ΚΟΣΤΟΣ ΤΗΣ ΜΗ ΣΥΜΜΟΡΦΩΣΗΣ

Το κόστος της παραβίασης των Κανόνων ή αλλιώς της μη συμμόρφωσης μπορεί να αποβεί πολύ υψηλό και η πορεία που ακολουθείται περιγράφεται ως εξής:





ΤΙ ΠΡΟΣΦΕΡΟΥΜΕ

ΟΙ (4) ΑΞΟΝΕΣ – ΤΑ (4) ΠΕΔΙΑ ΔΡΑΣΤΗΡΙΟΠΟΙΗΣΗΣ ΜΑΣ

Αναλαμβάνουμε την έγκαιρη προετοιμασία των Επιχειρήσεων και των Οργανισμών για την προσαρμογή τους στις υποχρεώσεις που επιφέρει ο ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR).

Στο πλαίσιο αυτό, παρέχουμε στους φορείς τις παρακάτω απαραίτητες υπηρεσίες προστασίας προσωπικών δεδομένων, οι οποίες επιμερίζονται σε (4) μεγάλες κατηγορίες:



ΔΙΑΓΝΩΣΗ (ΓΙΑΓΝΩΣΤΙΚΗ ΑΝΑΛΥΣΗ ΑΝΑΓΚΩΝ / GAP ANALYSIS)

Ο Γενικός Κανονισμός για τα Προσωπικά Δεδομένα συμπαρασύρει μια σημαντική εξέλιξη για τη διοίκηση της εκάστοτε Επιχείρησης ή Οργανισμού, η οποία θα την βοηθήσει να κατανοήσει τις διαδικασίες μέσα στις οποίες λαμβάνονται οι αποφάσεις και να εξασφαλίσει ότι όλα τα μέρη μπορούν να τις αντιληφθούν.

Συμφώνα με το νέο Κανονισμό είναι απαραίτητη η αναδιαμόρφωση παλαιών και η εισαγωγή νέων εσωτερικών Πολιτικών και Διαδικασιών, προκειμένου η Επιχείρηση ή ο Οργανισμός να καταλήξει να προστατεύει σύμφωνα με την Οδηγία τα προσωπικά δεδομένα τα οποία διαχειρίζεται.

Στο πλαίσιο αυτό, οι παρεχόμενες υπηρεσίες μας περιλαμβάνουν ενδεικτικά:

- Την αξιολόγηση των αναγκών για ασφάλεια που έχει ο κάθε πελάτης Επιχείρηση ή Οργανισμός.
- Την αποτίμηση των επιπτώσεων των παραβιάσεων προσωπικών δεδομένων – Data Protection Impact Assessment (DPIA).
- Διαγνωστικούς Ελέγχους επί των ελλείψεων σε επίπεδο ασφάλειας εντός των δομών της κάθε Επιχείρησης ή του κάθε Οργανισμού
- Κατάρτιση του πλάνου για προτεινόμενες λύσεις – παρεμβάσεις για θεραπεία του προβλήματος
- Εξειδικευμένες αναλύσεις καταγραφής της ροής των δεδομένων, αναλύσεων των επιπτώσεων ανά στάδια, αναλύσεις ρίσκου κλπ.
- Αναγνώριση των προσαρμογών των υφιστάμενων μέτρων προστασίας (GDPR stress testing).
- Προετοιμασία με υπηρεσίες νομικής συνδρομής στον οργανισμό για την προσαρμογή συμβάσεων, συμβολαίων, φορμών συναίνεσης και ρόλων.

Η Διαγνωστική Μελέτη υλοποιείται από εξειδικευμένη ομάδα συνεργατών που περιλαμβάνει Νομικούς – Συμβούλους Επιχειρήσεων και Τεχνικούς Πληροφοριακών Συστημάτων.

Αξιολόγηση Αναγκών Ασφάλειας
Διαγνωστικός Έλεγχος
Ελλείψεων
Πλάνο Προτεινόμενων
Ενεργειών
Έλεγχος Ροής Δεδομένων
Ανάλυση Επιπτώσεων
Ανάλυση Ρίσκου
Διαχείριση Ρίσκου

ΔΙΑΓΝΩΣΗ

ΕΦΑΡΜΟΓΗ (IMPLEMENTATION):

Στο πλαίσιο αυτό, οι παρεχόμενες υπηρεσίες μας περιλαμβάνουν ενδεικτικά:

- Την αξιολόγηση των αναγκών για ασφάλεια που έχει ο κάθε πελάτης για δημιουργία νέων επιχειρησιακών μοντέλων και εσωτερικών δομών που θα προάγουν την εναρμόνιση της Επιχείρησης ή του Οργανισμού με τον Ευρωπαϊκό Κανονισμό περί προστασίας δεδομένων.
- Δημιουργία αρχείου δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων
- Ανάπτυξη διαδικασιών αντιμετώπισης βάση Νομικών – Διαδικαστικών και Τεχνικών ενεργειών για θέματα αντιμετώπισης διαρροής πληροφοριών προσωπικών δεδομένων.
- Ανάπτυξη σχεδίου ασφάλειας προστασίας προσωπικών δεδομένων για τον οργανισμό.
- Εγκατάσταση υπηρεσίας ηλεκτρονικής διαχείρισης των υποχρεώσεων βάσει GDPR.
- Εγκατάσταση συστήματος έγκαιρου προσδιορισμού παραβιάσεων ασφάλειας.
- Εγκατάσταση των απαραίτητων μηχανισμών ασφάλειας που εξασφαλίζουν την προστασία και τη συνέχεια ύπαρξης των προσωπικών δεδομένων.
- Εκπαίδευση των στελεχών στην εφαρμογή του GDPR.

Η Εφαρμογή του Πλάνου Δράσεων υλοποιείται από εξειδικευμένη ομάδα συνεργατών που περιλαμβάνει Νομικούς – Συμβούλους Επιχειρήσεων και Τεχνικούς Πληροφοριακών Συστημάτων.

ΕΦΑΡΜΟΓΗ

- Προσωπικά Δεδομένα και Γενική Διακυβέρνηση
- Δημιουργία Νέων Επιχειρησιακών Μοντέλων
- Διαχείριση Δομών Ενδοεπιχειρησιακά

ΔΙΑΧΕΙΡΙΣΗ:

Εξασφαλίζουμε σε κάθε Επιχείρηση ή Οργανισμό που αναλαμβάνουμε ότι:

- Τηρεί τις αρχές της νομιμότητας, της δικαιοσύνης και της διαφάνειας κατά τη συλλογή και επεξεργασία προσωπικών δεδομένων.
- Καθορίζει και περιορίζει τον σκοπό της συλλογής / επεξεργασίας προσωπικών δεδομένων.
- Διατηρεί τα ελάχιστα αναγκαία προσωπικά δεδομένα.
- Μεριμνά για την ακρίβεια και την ορθότητα των δεδομένων.
- Τηρεί τις καθορισμένες περιόδους παραγραφής των δεδομένων.
- Εξασφαλίζει την εμπιστευτικότητα των δεδομένων.
- Διαθέτει τους μηχανισμούς εκείνους για εντοπισμό προβλημάτων προσωπικών δεδομένων και έγκαιρης γνωστοποίησης παραβιάσεων.
- Είναι σε θέση να ανταποκριθεί σε απαιτήσεις διατήρησης λεπτομερών αρχείων επεξεργασίας και σε έγκαιρη γνωστοποίηση παραβιάσεων.
- Έχει καθορίσει και προσαρμόσει τις διαδικασίες για τη συναίνεση χρήσης των προσωπικών δεδομένων, συμβολαίων και συμβάσεων.
- Ακολουθώντας εφαρμόζει την συνεχή εναρμόνιση με την Ευρωπαϊκή Οδηγία και τις νέες διατάξεις που προκύπτουν.

Επίσης οι υπηρεσίες μας περιλαμβάνουν:

- Την περιοδική παρακολούθηση περί εναρμόνισης της κάθε Επιχείρησης ή του κάθε Οργανισμού, σύμφωνα με τα ευρήματα που εξήχθησαν από την Διαγνωστική Μελέτη του προηγούμενου σταδίου
- Εξειδικευμένες υπηρεσίες DPO (Υπευθύνου Προστασίας Προσωπικών Δεδομένων) εντός και εκτός της Επιχείρησης ή του Οργανισμού
- Την περιοδική αξιολόγηση επιπτώσεων μη συμμόρφωσης με τον κανονισμό περί προστασία προσωπικών δεδομένων και τακτικός εντοπισμός των σημαντικότερων κινδύνων (Data Privacy Impact Assessment).

Ο DPO σύμβουλος μας που υλοποιεί τακτικούς ελέγχους σε Επιχειρήσεις ή Οργανισμούς είναι είτε **Νομικός** είτε **Οικονομολόγος - Σύμβουλος Επιχειρήσεων**, είτε **Τεχνικός Πληροφοριακών Συστημάτων**, ανάλογα με τις ιδιαίτερες ανάγκες του πελάτη μας.

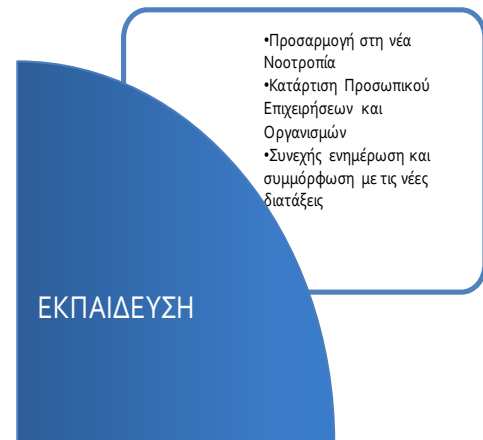
ΔΙΑΧΕΙΡΙΣΗ

- Συνχής εναρμόνιση με την Ευρωπαϊκή Οδηγία και τις νέες Διατάξεις που προκύπτουν
- Έλεγχος (Monitoring)
- Υπηρεσίες DPO (Υπευθύνου Προστασίας Προσωπικών Δεδομένων) εντός και εκτός της Επιχείρησης ή του Οργανισμού

ΕΚΠΑΙΔΕΥΣΗ

Στο πλαίσιο αυτό, οι παρεχόμενες υπηρεσίες μας περιλαμβάνουν ενδεικτικά:

- Ενημέρωση και συμμετοχή των Διευθυντών και του εμπλεκόμενου προσωπικού στη διαδικασία εναρμόνισης της εταιρείας ή του Οργανισμού, με τον Κανονισμό GDPR (ποιες είναι οι απαιτήσεις του και πως επηρεάζει τη λειτουργία των Διευθύνσεων – Τμημάτων και όλης της εταιρείας)
- Κατάρτιση εξειδικευμένων προγραμμάτων εκπαίδευσης για προσωπικό σε Επιχειρήσεις και Οργανισμούς
- Κατάρτιση εξειδικευμένων προγραμμάτων εκπαίδευσης για Υπευθύνους Προστασίας Προσωπικών Δεδομένων
- Συνεχής ενημέρωση των υπευθύνων στελεχών των Επιχειρήσεων – πελατών μας σχετικά με τις νέες διατάξεις.
- Εξειδικευμένες αναλύσεις καταγραφής της ροής των δεδομένων, αναλύσεων των επιπτώσεων ανά στάδια, αναλύσεις ρίσκου κλπ.
- Εκπαίδευση των Υπευθύνων εντός των Επιχειρήσεων και των Οργανισμών στην μεθοδολογία των «Καλών Πρακτικών» (Best Practices) που ακολουθούνται διεθνώς.



ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ:

“Ε.ΚΕ.Π.Ε.Ε.” Ι.Κ.Ε.

Κ.Δ.Β.Μ. 2 ,

ΕΚΠΑΙΔΕΥΤΙΚΗ - ΣΥΜΒΟΥΛΕΥΤΙΚΗ

Παπαφλέσσα 35,

Ασπρόπυργος ,19300

Τ. +30 210 5582372-373-374

Υπεύθυνος Έργου : Μακρής Κώστας

Αθανασίου Πολίτη, 11

Κέρκυρα, 49100

Τ. 26611 81206, 2661181232

Υπεύθυνος Έργου: Κρητικού Τατιάνα

E. ekepee@otenet.gr

W. www.ekepee.gr

