Συμμόρφωση με τον GDPR
από την Νόπη Τιντζογλίδου

Τι είναι ο GDPR;

Ο GDPR είναι ο Κανονισμός 2016/679, ο οποίος αφορά την προστασία των προσωπικών δεδομένων.

Ισχύει από 25.05.2018.

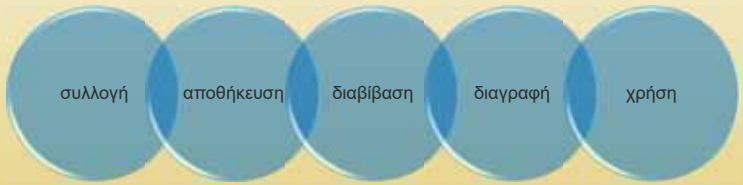
Βασικοί κανόνες εφαρμογής του GDPR →Η αυτορρύθμιση και η αρχή της λογοδοσίας. Ο υπεύθυνος επεξεργασίας φέρει την ευθύνη να αποδεικνύει ότι λαμβάνει όλα τα κατάλληλα οργανωτικά και τεχνικά μέτρα προστασίας των προσωπικών δεδομένων και ότι συμμορφώνεται με τον Κανονισμό.

Σκοπός του GDPR → ένα ενιαίο θεσμικό πλαίσιο που καθορίζει τη νόμιμη επεξεργασία και διακίνηση των προσωπικών δεδομένων σε όλα τα κράτη - μέλη της Ευρωπαϊκής Ένωσης με γνώμονα τη μεγαλύτερη δυνατή προστασία του ατόμου

Ποιους αφορά;

- Εταιρείες/ Επιχειρήσεις που λειτουργούν ως Υπεύθυνοι Επεξεργασίας ή Εκτελούντες την Επεξεργασία και βρίσκονται εγκατεστημένοι εντός Ε.Ε.
- Εταιρείες/ Επιχειρήσεις που λειτουργούν ως Υπεύθυνοι Επεξεργασίας ή Εκτελούντες την Επεξεργασία και που επεξεργάζονται προσωπικά δεδομένα Ευρωπαίων πολιτών ακόμα και αν δεν είναι εγκατεστημένοι εντός Ε.Ε.

Πράξεις που συνιστούν επεξεργασία προσωπικών δεδομένων



Ποιες κυρώσεις προβλέπονται;

Διοικητικές κυρώσεις

Επιβάλλονται από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

- έως **10.000.000€** ή **2%** του παγκόσμιου τζίρου μιας επιχείρησης
  - Για παραβιάσεις των υποχρεώσεων του Υπευθύνου Επεξεργασίας ή του Εκτελούντος την Επεξεργασίας σύμφωνα με τα άρθρα 8, 11, 25 έως 39, 42 και 43.
- έως **20.000.000€** ή **4%** του παγκόσμιου τζίρου μιας επιχείρησης
  - Για παραβιάσεις των βασικών αρχών για την επεξεργασία,
  - Για παραβιάσεις που αφορούν διαβιβάσεις δεδομένων σε αποδέκτη σε Τρίτη χώρα ή σε διεθνή οργανισμό,
  - Για παραβιάσεις οποιονδήποτε υποχρεώσεων σύμφωνα με το δίκαιο του κράτους μέλους σχετικά με ειδικές περιπτώσεις επεξεργασίας,
  - Για μη συμμόρφωση με εντολή της ΑΠΔΠΧ.

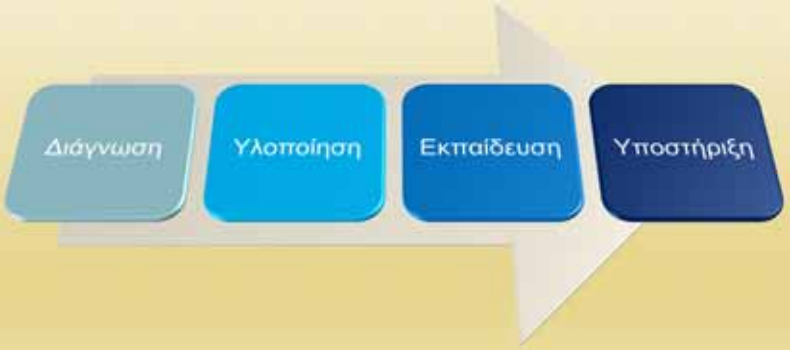
Αστικές κυρώσεις

Τα ΥΔ μπορούν να ζητήσουν αποζημίωση ασκώντας αγωγή στα αστικά δικαστήρια.

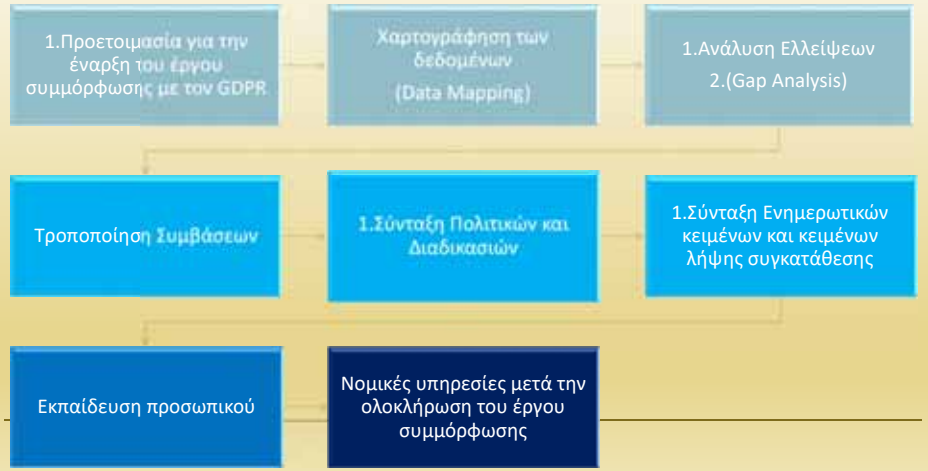
Ποινικές κυρώσεις

Ο Κανονισμός επιτρέπει στον εκάστοτε εθνικό νομοθέτη να ρυθμίσει την ποινική κύρωση. Στο σχέδιο νόμου, το βασικό έγκλημα της παράνομης επεξεργασίας έχει πλημμελητικό χαρακτήρα, διώκεται κατ' έγκληση και τιμωρείται αποκλειστικά με φυλάκιση. Στις διακεκριμένες μορφές του εγκλήματος επιβάλλεται και χρηματική ποινή έως 100.000,00 ευρώ. Σε περίπτωση πρόκλησης κινδύνου του δημοκρατικού πολιτεύματος ή εθνικής ασφάλειας επιβάλλεται ποινή κάθειρξης και χρηματική ποινή έως 300.000,00 ευρώ.

Στάδια υλοποίησης συμμόρφωσης



Διαδρομή της συμμόρφωσης



1. Προετοιμασία για την έναρξη του έργου συμμόρφωσης με τον GDPR

- Ενημέρωση των στελεχών της επιχείρησης σχετικά με το αντικείμενο του έργου και εν γένει με τον Κανονισμό GDPR.
- Κατανόηση του αντικειμένου της επιχείρησης.
- Συναπόφαση για το πλάνο ενεργειών συμμόρφωσης της επιχείρησης.

2. Χαρτογράφηση των δεδομένων σύμφωνα με το άρθρο 30 του GDPR

- Το πρώτο βήμα και ίσως και το κρισιμότερο κατά την εκτέλεση του έργου συμμόρφωσης μιας επιχείρησης με τον GDPR.
- Σκοπός της χαρτογράφησης είναι να μάθουμε τί είδους δεδομένα (πελάτων, προμηθευτών, εργαζομένων) συλλέγει και επεξεργάζεται η επιχείρηση, για ποιο σκοπό, πού υπάρχουν, ποιος έχει πρόσβαση σε αυτά και για πόσο χρόνο τα διατηρεί.
- Στην πράξη, στο στάδιο αυτό, δημιουργείται το Αρχείο Δραστηριοτήτων Επεξεργασίας, το οποίο απαιτείται από τον GDPR και το οποίο συνήθως τηρείται σε ηλεκτρονική μορφή (αρχείο excel). Στο στάδιο αυτό αποτυπώνεται η υφιστάμενη κατάσταση της επιχείρησης.

3. Gap Analysis (Ανάλυση Ελλείψεων) Ο προσδιορισμός της υφιστάμενης κατάστασης της επιχείρησης και η απόσταση της από τη συμμόρφωση

- Νομοτεχνική και αιτιολογημένη αναλυτική έκθεση ελλείψεων, ορθών πρακτικών και προτάσεων βελτίωσης συμμόρφωσης με τον GDPR.
- Στο Gap Analysis καταγράφεται:
  I. Η υφιστάμενη κατάσταση, δηλαδή ο τρόπος που επεξεργάζεται η επιχείρηση τα δεδομένα σήμερα
  II. Η έλλειψη απόκλισης από τις απαιτήσεις του Κανονισμού και
  III. Οι αναγκαίες ενέργειες συμμόρφωσης με τον Κανονισμό.
- Ο «οδικός χάρτης» για το τι πρέπει να αλλάξουμε στην επιχείρηση.

4. Τροποποίηση Συμβάσεων της επιχείρησης με πελάτες/προμηθευτές/ εργαζόμενους. Τι πρέπει να περιλαμβάνει;

- Νέες απαιτήσεις Κανονισμού → Ανάγκη τροποποίησης συμβάσεων.
- Συμβάσεις με εργαζόμενους/ πελάτες/ προμηθευτές.
- Τροποποίηση των σχετικών με τα προσωπικά δεδομένα άρθρων των συμβάσεων.
- Συνήθως υπό μορφή παραρτήματος.

5. Σύνταξη Πολιτικών και Διαδικασιών

- Πολιτική Προστασίας Προσωπικών Δεδομένων → «νόμος» για την επιχείρηση

Παρέχει πληροφορίες σχετικά με:

I. τη συλλογή, αποθήκευση, επεξεργασία και χρήση των προσωπικών δεδομένων των πελατών μιας επιχείρησης

II. τη νομιμοποιητική βάση επεξεργασίας για κάθε σκοπό επεξεργασίας

III. τα δικαιώματα των υποκειμένων

IV. τον τρόπο που μπορούν να ασκήσουν τα δικαιώματά τους τα υποκείμενα

6. Ενημέρωση των υποκειμένων των δεδομένων και λήψη συγκατάθεσης όπου απαιτείται

- Ενημέρωση Εργαζομένων/ Πελατών/ Συνεργατών κ.λπ. σχετικά με την επεξεργασία των προσωπικών τους δεδομένων.
- Στις περιπτώσεις που απαιτείται συγκατάθεση του υποκειμένου των δεδομένων ο Υπεύθυνος Επεξεργασίας πρέπει να μπορεί να αποδείξει ότι το υποκείμενο των δεδομένων συγκατατέθηκε για την επεξεργασία των προσωπικών του δεδομένων.

7. Εκπαίδευση προσωπικού

- Απλός και κατανοητός τρόπος παρουσίασης των θεμάτων.
- Παραδείγματα από τον συνήθη κύκλο εργασιών της επιχείρησης.
- Επίλυση όλων των βασικών αποριών των συμμετεχόντων που σχετίζονται, βεβαίως, με το αντικείμενο της επιχείρησης.

8. Παροχή υποστηρικτικών υπηρεσιών μετά την ολοκλήρωση του έργου συμμόρφωσης

- Παρακολούθηση των αλλαγών του νομικού πλαισίου → Ενημέρωση της επιχείρησης.
- Συνδρομή στον DPO.
- Επικαιροποίηση Πολιτικών και Διαδικασιών.
- Συμβουλευτική υποστήριξη για τη διαχείριση τυχόν αιτημάτων υποκειμένων των δεδομένων/ περιστατικών παραβίασης του GDPR

Ενδεικτικά απαιτούμενα νομικά κείμενα

- Χαρτογράφηση δεδομένων (Data Flow Mapping) της επιχείρησης - Αρχείο Δραστηριοτήτων
- Έκθεση ελλείψεων (Gap Analysis)
- Πολιτική Προστασίας Προσωπικών Δεδομένων
- Πολιτική Χρήσης Cookies ιστοσελίδας
- Πολιτική ορθής χρήσης επικοινωνιακών μέσων και συσκευών
- Αιτήσεις άσκησης των δικαιωμάτων των υποκειμένων των δεδομένων (πρόσβασης, διόρθωσης, διαγραφής, περιορισμού, εναντίωσης ή ανάκλησης συγκατάθεσης και φορητότητας)
- Τροποποίηση των «Όρων Χρήσης» ιστοσελίδας αναφορικά με τα προσωπικά δεδομένα
- Κείμενα ενημέρωσης ή/και λήψης συγκατάθεσης σχετικά με την επεξεργασία προσωπικών δεδομένων
- Κείμενο ενημέρωσης και λήψης συγκατάθεσης για λήψη και χρήση φωτογραφιών/βίντεο
- Newsletter
- Disclaimer προσωπικών δεδομένων για emails

- Συμβάσεις/παραρτήματα συμβάσεων/τροποποίηση συμβάσεων μεταξύ α) Υπευθύνων Επεξεργασίας και Εκτελούντων την Επεξεργασία, β) Από Κοινού Υπευθύνων Επεξεργασίας
- Συμβάσεις ανάληψης καθηκόντων Υπευθύνου Προστασίας Προσωπικών Δεδομένων (DPO)
- Συμβάσεις/παραρτήματα συμβάσεων/τροποποίηση συμβάσεων εργαζομένων, ώστε να περιλαμβάνεται όλη η αναγκαία σύμφωνα με τον GDPR ενημέρωση για την επεξεργασία των προσωπικών τους δεδομένων και να δεσμεύονται με τήρηση εμπιστευτικότητας και πολιτικής «καθαρού γραφείου»
- Σχολιασμός συμβάσεων που αποστέλλονται στην επιχείρηση προς υπογραφή από προμηθευτές
- Αρχείο Καταγραφής Παραβιάσεων
- Πρωτόκολλο Καταστροφής
- Πινακίδα για βιντεοεπιτήρηση χώρου και βασικές αρχές για τη νόμιμη χρήση συστήματος βιντεοεπιτήρησης
- Privacy by design σε νέα προϊόντα και υπηρεσίες
- Προωθητικές ενέργειες και διαγωνισμοί
- Γνωμοδοτήσεις επί ζητημάτων που άπτονται της νομοθεσίας περί προσωπικών δεδομένων

! Ο GDPR δεν είναι μόνο αρχεία, πολιτικές και διαδικασίες, αλλά δημιουργεί μία νέα εταιρική κουλτούρα.

! Η επιλογή της συμμόρφωσης ως επιχειρηματική στρατηγική προσφέρει στην επιχείρηση όχι μόνο προστασία αλλά και ανταγωνιστικό πλεονέκτημα.

Νόπη Τιντζογλίδου,
δικηγόρος με εξειδίκευση σε θέματα προσωπικών δεδομένων
& στη συμμόρφωση επιχειρήσεων με τον GDPR
● Ακαδημίας 25, Αθήνα ● 2100080600