

### GDPR Εγχειρίδιο βασικών αλλαγών

Το ακόλουθο έγγραφο δημιουργήθηκε από την ιστοσελίδα: <https://eugdpr.org/the-regulation/>. Όλο το κείμενο λήφθηκε από αυτή την ιστοσελίδα, δε δημιουργήθηκε από την εταιρική DIGIT.

---

Ο σκοπός του GDPR είναι να προστατέψει όλους τους Ευρωπαίους πολίτες από την ιδιωτικότητα και τις παραβιάσεις δεδομένων στον κατευθυνόμενο από δεδομένα σημερινό κόσμο. Αν και οι βασικές αρχές της ιδιωτικότητας δεδομένων παραμένουν σε ισχύ από την προηγούμενη οδηγία, αρκετές αλλαγές έχουν προταθεί σε ρυθμιστικές πολιτικές. Τα βασικά σημεία του GDPR καθώς και η πληροφορία για την επίπτωση που θα έχει στις επιχειρήσεις μπορεί να βρεθεί παρακάτω.



#### Αυξημένη εδαφική εμβέλεια (εφαρμογή και εκτός Ε.Ε. εδάφους)

- Αναμφισβήτητη η μεγαλύτερη αλλαγή στο ρυθμιστικό περιβάλλον της ιδιωτικότητας των δεδομένων έρχεται με την **εκτεταμένη αρμοδιότητα του GDPR**, καθώς ισχύει για όλες τις εταιρείες που επεξεργάζονται τα προσωπικά δεδομένα όσων διαμένουν στην Ένωση, ανεξαρτήτως της τοποθεσίας της εταιρείας.
- Πριν, η εδαφική εφαρμογή της οδηγίας ήταν ασαφής.
- Το GDPR ισχύει επίσης για την επεξεργασία προσωπικών δεδομένων στην ΕΕ από τον υπεύθυνο επεξεργασίας ή επεξεργαστή που δεν είναι εγκατεστημένος στην ΕΕ, όπου οι δραστηριότητες αφορούν: προσφορά αγαθών ή υπηρεσιών σε πολίτες της ΕΕ (ανεξάρτητα από το αν απαιτείται πληρωμή) και την παρακολούθηση της συμπεριφοράς που λαμβάνει χώρα εντός της ΕΕ.

#### Ποινικές ρήτρες

- Σε οργανισμούς που παραβιάζουν το GDPR μπορούν να επιβληθούν πρόστιμα **μέχρι 4% του ετήσιου συνολικού κύκλου εργασιών ή € 20 εκατ.** (Όποιο είναι μεγαλύτερο). Αυτό είναι το μέγιστο πρόστιμο που μπορεί να επιβληθεί για τις πιο σοβαρές παραβάσεις π.χ. χωρίς τη δέουσα συγκατάθεση του πελάτη να επεξεργάζεται δεδομένα ή να παραβιάζει τον πυρήνα των εννοιών «Απόρρητο από το σχεδιασμό».

#### Συναίνεση

- **Οι όροι για τη συναίνεση έχουν ενισχυθεί** και οι εταιρείες δεν είναι πλέον σε θέση να χρησιμοποιούν μακρούς δυσανάγνωστους όρους και συνθήκες γεμάτους νομικά.
- Η αίτηση συναίνεσης πρέπει να παρέχεται με κατανοητή και εύκολα προσπελάσιμη μορφή, με σκοπό την επεξεργασία δεδομένων που επισυνάπτεται στη συναίνεση αυτή.
- Η συναίνεση πρέπει να είναι σαφής και διακριτή από άλλα θέματα και να παρέχεται με ευανάγνωστη και εύκολα προσιτή μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα.
- Πρέπει να είναι τόσο εύκολο να αποσύρετε τη συγκατάθεση, όπως είναι να την δώσετε.

#### Κοινοποίηση Παραβίασης

- Σύμφωνα με το GDPR, οι κοινοποιήσεις παραβίασης είναι πλέον υποχρεωτικές σε όλα τα κράτη μέλη όπου μια παραβίαση δεδομένων είναι πιθανό να "οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων".

- Αυτό πρέπει να γίνει εντός 72 ωρών από την πρώτη στιγμή της συνειδητοποίησης της παραβίασης. Οι επεξεργαστές δεδομένων υποχρεούνται επίσης να ειδοποιούν τους πελάτες τους, τους ελεγκτές, "χωρίς αδικαιολόγητη καθυστέρηση", από την πρώτη στιγμή που θα καταλάβουν την παραβίαση δεδομένων.

### Δικαίωμα πρόσβασης

- Ένα μέρος των διευρυμένων δικαιωμάτων των προσώπων στα οποία αναφέρονται τα στοιχεία του GDPR είναι το δικαίωμα των υποκειμένων των δεδομένων να λαμβάνουν επιβεβαίωση από τον υπεύθυνο επεξεργασίας για το κατά πόσον τα προσωπικά δεδομένα που τους αφορούν υποβάλλονται σε επεξεργασία, πού και για ποιο σκοπό.
- Επιπλέον, ο υπεύθυνος επεξεργασίας παρέχει δωρεάν αντίγραφο των προσωπικών δεδομένων σε ηλεκτρονική μορφή. Αυτή η αλλαγή είναι μια δραματική τροποποίηση στη **διαφάνεια των δεδομένων** και την ενδυνάμωση των υποκειμένων των δεδομένων.

### Δικαίωμα να ξεχαστεί

- Επίσης γνωστό ως "Διαγραφή δεδομένων", το δικαίωμα να ξεχαστεί, παρέχει στο υποκείμενο των δεδομένων τη δυνατότητα να διαγράψει τα προσωπικά του δεδομένα από τον ελεγκτή δεδομένων, να παύσει την περαιτέρω διάδοση των δεδομένων και ενδεχομένως να σταματήσει την επεξεργασία των δεδομένων από τρίτους.

### Φορητότητα δεδομένων

- Το GDPR εισάγει τη φορητότητα δεδομένων - το δικαίωμα για ένα υποκείμενο των δεδομένων να λαμβάνει τα προσωπικά δεδομένα που το αφορούν.

### Υπεύθυνοι Προστασίας Δεδομένων

- Σύμφωνα με το GDPR, δεν είναι απαραίτητο να υποβάλλονται κοινοποιήσεις / καταχωρήσεις σε κάθε τοπική DPA των δραστηριοτήτων επεξεργασίας δεδομένων, ούτε αποτελεί υποχρέωση κοινοποίησης / απόκτησης έγκρισης για μεταφορές βάσει των πρότυπων ρητρών σύμβασης (MCC).
- Αντίθετα, υπάρχουν εσωτερικές απαιτήσεις τήρησης αρχείων, όπως εξηγείται παρακάτω, και ο διορισμός των DPO (Data Protection Officer) είναι υποχρεωτικός μόνο για εκείνους των οποίων οι κύριες δραστηριότητες συνίστανται σε εργασίες επεξεργασίας που απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων ή δεδομένων σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις.
- Σημαντικό είναι ότι ο υπεύθυνος προστασίας δεδομένων:
  - Πρέπει να διορίζεται με βάση τα επαγγελματικά προσόντα και, ειδικότερα, τις ειδικές γνώσεις σχετικά με το δίκαιο και τις πρακτικές προστασίας των δεδομένων
  - Μπορεί να είναι μέλος του προσωπικού ή εξωτερικός πάροχος υπηρεσιών
  - Τα στοιχεία επικοινωνίας πρέπει να παρέχονται στην αρμόδια αρχή προστασίας δεδομένων
  - Πρέπει να διαθέτει τους κατάλληλους πόρους για την εκτέλεση των καθηκόντων τους και τη διατήρηση των ειδικών γνώσεων τους
  - Πρέπει να αναφέρεται απευθείας στο ανώτατο επίπεδο διαχείρισης

- Δεν πρέπει να εκτελεί άλλα καθήκοντα που θα μπορούσαν να οδηγήσουν σε σύγκρουση συμφερόντων.

Παρακαλώ εξετάστε τις ακόλουθες ερωτήσεις:

- 1. Τι πιστεύετε για αυτές τις οδηγίες; Τι ξεχωρίζει για εσάς;**
- 2. Έχετε επηρεαστεί από αυτές στην προσωπική ή επαγγελματική σας ζωή; Εάν ναι, πώς;**
- 3. Υπάρχει κάτι άλλο που θα προσθέσετε ή θα αλλάξετε σχετικά με τους κανονισμούς GDPR;**