ΕΥΡΩΠΑΪΚΟΣ ΚΑΝΟΝΙΣΜΟΣ 2016/679 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

25.5.2018

Εισαγωγή

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της ΕΕ (General Data Protection Regulation - GDPR) έχει ως στόχο να διευρύνει την προστασία των δεδομένων στην εποχή των big data και του cloud computing, εξασφαλίζοντας ότι η προστασία των δεδομένων αποτελεί θεμελιώδες βασικό δικαίωμα, το οποίο θα ρυθμίζεται με συνέπεια σε όλη την Ευρώπη.

Κάθε οργανισμός που χειρίζεται προσωπικά δεδομένα τα οποία αφορούν σε <u>άτομα εντός της Ευρωπαϊκής Ένωσης</u>, είναι υποχρεωμένος να συμμορφωθεί πλήρως με τον κανονισμό, επανεξετάζοντας ή και αναθεωρώντας όλες τις διαδικασίες διαχείρισης των πληροφοριών του.

2016/679 Γενικός Κανονισμός (GDPR)

Διαμόρφωση ενός ενιαίου νομικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης, με τη θέσπιση μίας σειράς περιορισμών και νέων υποχρεώσεων στις επιχειρήσεις σχετικά με:

- **την επεξεργασία των προσωπικών δεδομένων σε όλο τον κύκλο ζωής τους, από τη συλλογή έως και την καταστροφή τους,**
- **τη δυνατότητα μεταφοράς τους σε άλλες χώρες,**
- **την προστασία των δικαιωμάτων των φυσικών προσώπων,**
- **την ασφάλεια (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) των προσωπικών δεδομένων και**
- **τις ενέργειες γνωστοποίησης που οφείλει να κάνει η επιχείρηση, σε περίπτωση παραβίασης.**

Ποιες επιχειρήσεις αφορά;

- ✓ **Ο κανονισμός GDPR, αφορά όλες τις επιχειρήσεις του ιδιωτικού και δημοσίου τομέα της Ευρωπαϊκή Ένωσης (και εκτός της ΕΕ που προσφέρουν αγαθά και υπηρεσίες σε άτομα που ζουν στην ΕΕ) που με οποιοδήποτε τρόπο συλλέγουν, επεξεργάζονται και αποθηκεύουν δεδομένα προσωπικού χαρακτήρα πελατών, προμηθευτών, συνεργατών και εργαζόμενων ή άλλων φυσικών προσώπων.**
- ✓ **Στην πραγματικότητα, ο GDPR καθίσταται το παγκόσμιο πρότυπο για την προστασία των προσωπικών δεδομένων. Ανάλογα με τα δεδομένα που συλλέγει η κάθε επιχείρηση, αλλά και το μέγεθος της, θα πρέπει να προχωρήσει σε βελτιώσεις, οι οποίες θα την καθιστούν συμβατή με όλα όσα ορίζει ο GDPR.**

Χρήσιμοι Ορισμοί (άρθρο 4 ΓΚΠΔ)

Δεδομένα προσωπικού χαρακτήρα	**Οποιαδήποτε πληροφορία προσδιορίζει ή ΜΠΟΡΕΙ να προσδιορίσει την ταυτότητα ενός φυσικού προσώπου εν ζωή**
Ευαίσθητα προσωπικά δεδομένα	**Οτιδήποτε μπορεί να δημιουργήσει διακρίσεις (φυλή, θρησκεία, υγεία, πολιτικές πεποιθήσεις, συμμετοχή σε ένωση, σωματείο ή συνδικαλιστική οργάνωση, σεξουαλικός προσανατολισμός, διώξεις & καταδίκες)**
Υποκείμενο των δεδομένων	**Το φυσικό πρόσωπο, η ταυτότητα του οποίου, μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως σε όνομα, σε αριθμό ταυτότητας, ή σε παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, κλπ ταυτότητα του εν λόγω φυσικού προσώπου**
Υπεύθυνος επεξεργασίας	**Το φυσικό ή νομικό πρόσωπο που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα**
Εκτελών την επεξεργασία	**Το φυσικό ή νομικό πρόσωπο που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας**
Εποπτική αρχή	**Ανεξάρτητη δημόσια αρχή που συγκροτείται από κάθε κράτος - μέλος**

Αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων (άρθρο 5 ΓΚΠΔ)

Προϋποθέσεις για νόμιμη επεξεργασία (άρθρο 6 ΓΚΠΔ)

- ✓ **<u>Με συγκατάθεση (άρθρο 7 ΓΚΠΔ)</u>: το υποκείμενο έχει δώσει τη συγκατάθεσή του** για την επεξεργασία των προσωπικών του δεδομένων για έναν ή περισσότερους σκοπούς

i. Η συγκατάθεση πρέπει να λαμβάνεται **πριν** από κάθε επεξεργασία.

ii. Το υποκείμενο των δεδομένων θα πρέπει **να γνωρίζει** τουλάχιστον την **ταυτότητα** του υπευθύνου επεξεργασίας και τους **σκοπούς** της επεξεργασίας και η συγκατάθεση να έχει δοθεί **ελεύθερα.**

iii. Εάν συντελείται **επεξεργασία πολλαπλών σκοπών/πράξεων** επεξεργασίας, θα πρέπει να παρέχεται συγκατάθεση για κάθε σκοπό/πράξη επεξεργασίας.

iv. Το υποκείμενο των δεδομένων πρέπει να έχει δυνατότητα ανάκλησης της συγκατάθεσης ανά πάσα στιγμή. Η ανάκληση πρέπει να είναι εξίσου εύκολη με την παροχή της. Η **ενημέρωση** για τη δυνατότητα ανάκλησης πρέπει να γίνεται **πριν από τη λήψη συγκατάθεσης**.

v. Η συγκατάθεση θα πρέπει να παρέχεται με σαφή θετική ενέργεια, όπως γραπτή δήλωση με ηλεκτρονικά μέσα. Η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια **δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση**.

Προϋποθέσεις για νόμιμη επεξεργασία (άρθρο 6 ΓΚΠΔ)

- ✓ **Χωρίς συγκατάθεση όταν (ύπαρξη νόμιμης βάσης)**:

i. η επεξεργασία είναι αναγκαία για την **εκτέλεση σύμβασης** της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για τη λήψη μέτρων πριν τη σύναψη της σύμβασης κατόπιν αιτήσεως του υποκειμένου των δεδομένων,

ii. η επεξεργασία είναι αναγκαία για την **εκπλήρωση εκ του νόμου υποχρέωσης** του υπευθύνου επεξεργασίας,

iii. η επεξεργασία είναι αναγκαία για τη **διαφύλαξη ζωτικού συμφέροντος** του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

iv. η επεξεργασία είναι αναγκαία για την **εκτέλεση έργου δημοσίου συμφέροντος** ή **άσκησης δημόσιας εξουσίας** που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, και

v. η επεξεργασία είναι απολύτως αναγκαία για την **ικανοποίηση εννόμου συμφέροντος** του υπεύθυνου της επεξεργασίας ή τρίτου, στον οποίο ανακοινώνονται τα δεδομένα, το οποίο (συμφέρον) υπερέχει προφανώς των δικαιωμάτων και συμφερόντων του υποκειμένου, <u>ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί</u>.

Επεξεργασία ευαίσθητων δεδομένων (άρθρο 9 ΓΚΠΔ)

- ✓ **Απαγορεύεται** η επεξεργασία προσωπικών δεδομένων που αποκαλύπτουν φυλετική-εθνοτική προέλευση, πολιτικά φρονήματα, θρησκευτικές-φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα, βιομετρικά δεδομένα, δεδομένα υγείας, σεξουαλικής ζωής, γενετήσιου προσανατολισμού.
- ✓ **Κατ' εξαίρεση επιτρέπεται:**
  - **Ρητή συγκατάθεση**
  - **Εκτέλεση των υποχρεώσεων και άσκηση των δικαιωμάτων σύμφωνα με το Εργατικό Δίκαιο**
  - **Διαφύλαξη ζωτικού συμφέροντος**
  - **Στο πλαίσιο δραστηριοτήτων Σωματείου/Ιδρύματος**
  - **Θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων**
  - **Προληπτική ιατρική, ιατρική διάγνωση, παροχή υγειονομικής ή κοινωνικής περίθαλψης**
  - **Λόγοι δημοσίου συμφέροντος στον τομέα της δημόσιας υγείας**
  - **Σκοποί αρχειοθέτησης προς το δημόσιο συμφέρον, σκοποί επιστημονικής, ιατρικής έρευνας ή στατιστικής**
  - **Δημοσιοποίηση δεδομένων από το ίδιο το υποκείμενο των δεδομένων**

Δικαιώματα του υποκειμένου των δεδομένων (άρθρα 12-21 ΓΚΠΔ)

Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

Δικαίωμα περιορισμού της επεξεργασίας

Δικαίωμα διόρθωσης

Δικαίωμα στη λήθη

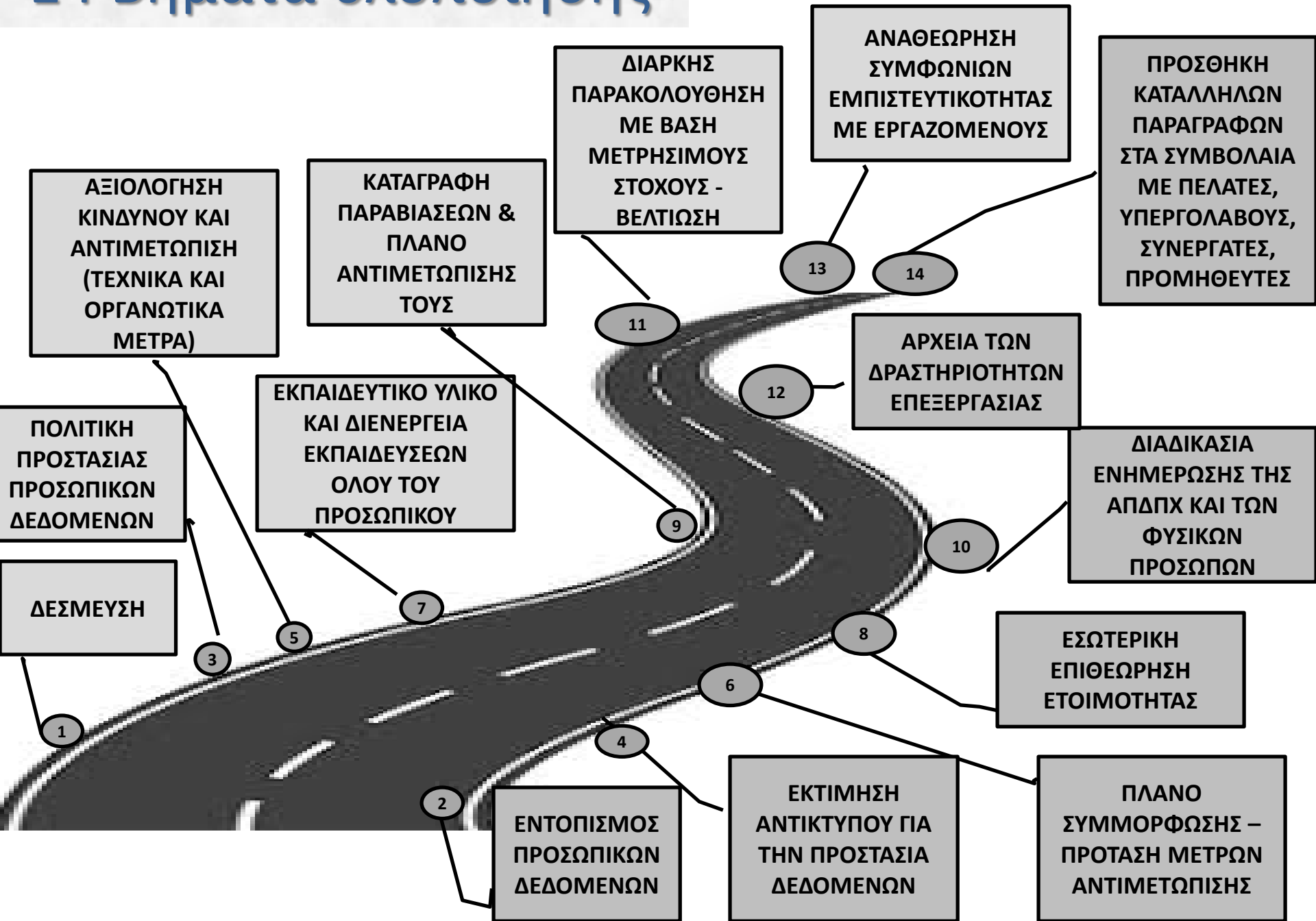
Υποχρέωση γνωστοποίησης της διόρθωσης, διαγραφής ή περιορισμού της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

Δικαίωμα στη φορητότητα των δεδομένων

Δικαίωμα εναντίωσης

Μη αυτοματοποιημένη λήψη αποφάσεων

14 Βήματα υλοποίησης



Διεθνή πρότυπα και οδηγίες

Τα απαιτούμενα από τον GDPR μέτρα, πολιτικές και διαδικασίες ασφάλειας δεδομένων και επιχειρησιακής συνέχειας καθορίζονται από τα εξής διεθνή πρότυπα και οδηγίες:

- **ISO 27001**, το βασικό διεθνές πρότυπο για την ασφάλεια πληροφοριών
- **ISO 22301**, το διεθνές πρότυπο για την επιχειρησιακή συνέχεια
- **ISO 27018**, οδηγία για την προστασία των προσωπικών δεδομένων στο cloud
- **ISO 27017**, οδηγία για την ασφάλεια των δεδομένων στην παροχή υπηρεσιών μέσω cloud
- **ISO 27015**, οδηγία για την ασφάλεια δεδομένων στις οικονομικές υπηρεσίες.

Συμμόρφωση ή όχι;

ΠΡΟΣΤΙΜΟ: **4%**

επί του παγκόσμιου κύκλου εργασιών της επιχείρησης [ή του ομίλου]

ή

20.000.000 €

ανάλογα με το ποιο είναι υψηλότερο

Στον εν λόγω Κανονισμό προβλέπονται τα πιο υψηλά πρόστιμα αμέσως μετά τα πρόστιμα για παραβάσεις του Ελεύθερου Ανταγωνισμού όπου εκεί το πρόστιμο μπορεί να ανέλθει έως και ***10% επί του παγκόσμιου κύκλου εργασιών της επιχείρησης*** [ή του ομίλου]

Σας ευχαριστώ πολύ για την προσοχή σας!