G.D.P.R

General Data Protection Regulation

ALEXCIS
Advisors & Consultants of Information Systems

"Γενικός Κανονισμός για την Προστασία Δεδομένων"

Τι είναι το GDPR;

- Ο GDPR (General Data Protection Regulation General Data Protection Regulation)- «Γενικός Κανονισμός για την Προστασία Δεδομένων» , αφορά στην διαμόρφωση ενός ενιαίου νομοθετικού πλαισίου για την επεξεργασία προσωπικών δεδομένων στα κράτη μέλη της Ευρωπαϊκής Ένωσης.
- Ο «κανονισμός» είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος (δηλαδή δεν απαιτείται ειδική προσαρμογή της Εθνικής Νομοθεσίας). (άρθρο 83 του «Κανονισμού»).
- **Έναρξη εφαρμογής του «Κανονισμού».**
  Ο «Κανονισμός», τίθεται σε εφαρμογή από τις 25 Μαΐου 2018 (άρθρο 99 του «Κανονισμού») .Το χρονικό διάστημα των δύο ετών (από την ψήφιση του «Κανονισμού», μέχρι την έναρξη εφαρμογής) αποτελούσε περίοδο προσαρμογής για τις επιχειρήσεις.

Ποιές επιχειρήσεις αφορά;

- Αφορά όλες τις επιχειρήσεις (εντός και εκτός Ε.Ε.), (ιδιωτικού και δημόσιου τομέα) που με οποιοδήποτε τρόπο διαχειρίζονται προσωπικά δεδομένα εργαζομένων, συνεργατών, πελατών, ή άλλων φυσικών προσώπων εντός Ε.Ε. Δηλαδή αφορά σχεδόν το σύνολο των επιχειρήσεων.
- Για να ληφθεί υπόψη η ειδική κατάσταση των πολύ μικρών, των μικρών και των μεσαίων επιχειρήσεων, ο παρών κανονισμός περιλαμβάνει παρέκκλιση για οργανισμούς που απασχολούν λιγότερα από 250 άτομα (Άρθρο 30 παρ. 5) όσον αφορά την τήρηση αρχείων.

Πρόστιμα

- Για μικρές παραβάσεις τα πρόστιμα ορίζονται έως και **€ 10 εκατ**. ή **2% του ετήσιου τζίρου**
- Για μεγάλες παραβάσεις τα πρόστιμα ορίζονται έως και **€ 20 εκατ**. ή **4% του ετήσιου τζίρου**

Τι υποχρεούνται να κάνουν οι επιχειρήσεις;

- Να κάνουν έλεγχο όλων των δεδομένων της επιχείρησης τους και να προσδιορίσουν που βρίσκονται και που υπάρχουν προσωπικά δεδομένα
- Να δημιουργήσουν πολιτικές και διαδικασίες ασφαλείας και διαχείρισης κινδύνου για την προστασία των προσωπικών δεδομένων
- Να γίνονται τακτικοί έλεγχοι δικτύων και υποδομών
- Ο Κανονισμός επιβάλει μια σειρά νέων υποχρεώσεων στους υπεύθυνους επεξεργασίας σχετικά με τον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων καθώς επίσης και νέα αρχή λογοδοσίας
- Να ορίσουν Υπεύθυνο Προστασίας Δεδομένων όπου απαιτείται
- Πρέπει να ενημερώνουν τον κόσμο σχετικά με το δικαίωμα να αρνηθούν την επεξεργασία των δεδομένων τους με τρόπο που να είναι σαφές και ξεχωριστό από άλλα στοιχεία τα οποία πρέπει επίσης να παρέχουν σε αυτούς. Η συγκατάθεση θα πρέπει να προέρχεται από μια θετική ένδειξη συμφωνίας για τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και δεν μπορεί να συναχθεί από τη σιωπή του υποκειμένου, την αδράνειά του ή από προσημειωμένα πλαίσια ελέγχου.
- Να τεκμηριώνουν τι προσωπικά δεδομένα κατέχουν, από πού προήλθαν και με ποιους τα μοιράζονται
- Να ενημερώνουν την αντίστοιχη αρχή προστασίας δεδομένων σε περίπτωση παραβίασης δεδομένων εντός 72 ωρών από τν εντοπισμού της.

Ευθύνες

- Ένα υποκείμενο δεδομένων που έχει υποστεί ζημία λόγω παράνομης επεξεργασίας των δικών του προσωπικών δεδομένων δικαιούται να λάβει αποζημίωση από τον υπεύθυνο επεξεργασίας ή τον επεξεργαστή για τη ζημία αυτή
- Ένας επεξεργαστής έχει ευθύνη για την προκληθείσα ζημία από κάποια από τις ενέργειες επεξεργασίας (του ιδίου ή υπο-επεξεργαστή) που δεν είναι σύμφωνες με τις υποχρεώσεις που θέτει ο νέος Κανονισμός ή που παραβιάζει τις οδηγίες του υπεύθυνου επεξεργασίας
- Για τη διασφάλιση αποτελεσματικής αποζημίωσης, κάθε υπεύθυνος επεξεργασίας ή επεξεργαστής θα φέρουν ευθύνη για το σύνολο της προκληθείσας ζημίας, εάν εμπλέκονται στην ίδια επεξεργασία και ευθύνονται για τη ζημία αυτή.
- Τα υποκείμενα δικαιωμάτων έχουν δικαίωμα να στραφούν κατά οιουδήποτε συνδεδεμένου υπεύθυνου επεξεργασίας. Κάθε συνδεδεμένος υπεύθυνος επεξεργασίας φέρει ευθύνη για το σύνολο της ζημίας, παρ΄όλο που το εθνικό δίκαιο μπορεί να διαμοιράζει την ευθύνη ανάμεσα τους. Εάν ο ένας συνδεδεμένος υπεύθυνος επεξεργασίας έχει πληρώσει όλη την αποζημίωση, μπορεί μετά να στραφεί κατά των λοιπών συνδεδεμένων υπεύθυνων επεξεργασίας για να καλύψουν το μερίδιο της ζημίας.

Προετοιμασία των επιχειρήσεων

1. **ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ**: Ενημερώστε το ανθρώπινο δυναμικό του οργανισμού σας για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογήστε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε και επεξεργάζεστε. Διαμορφώστε στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.

2. **ΚΑΤΑΓΡΑΦΗ**: Οφείλετε να τηρείτε ειδικά αρχεία επεξεργασιών; Αν ναι, καταγράψτε ενδελεχώς τα δεδομένα που τηρείτε και μεταβιβάζετε, τις επεξεργασίες στις οποίες προβαίνετε, τον σκοπό τους και τη νομική βάση.

3. **ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ**: Εξετάζετε συνεχώς αν κατά την επεξεργασία των δεδομένων τηρούνται οι αρχές που διέπουν τη νόμιμη επεξεργασία των δεδομένων και αν γίνονται σεβαστά τα δικαιώματα των υποκειμένων.

4. **ΕΛΕΓΧΟΣ ΣΥΓΚΑΤΑΘΕΣΗΣ**: Εξετάστε τις μεθόδους για εξασφάλιση συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας.

5. **ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ**: Επικαιροποιήστε τις διαδικασίες για τον χειρισμό των αιτημάτων και την ικανοποίηση των δικαιωμάτων των πολιτών, ιδίως ως προς τη διαγραφή δεδομένων (δικαίωμα στη λήθη) ή την παροχή τους σε αναγνώσιμο ηλεκτρονικό μορφότυπο (φορητότητα δεδομένων).

6. **ΕΚΤΙΜΗΣΗ ΕΠΙΠΤΩΣΕΩΝ**: Θα πρέπει να είστε σε θέση να εκτιμήσετε τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.

7. **ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ**: Ανάλογα με τη δραστηριότητα που ασκείτε, εξετάστε αν χρειάζεται να ορίσετε «υπεύθυνο προστασίας δεδομένων».

8. **ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ**: Υιοθετήστε μεθόδους για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων. Διαθέτετε διαδικασία για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα;

9. **ΔΡΑΣΤΗΡΙΟΤΗΤΑ ΣΕ ΠΕΡΙΣΣΟΤΕΡΑ ΚΡΑΤΗ ΜΕΛΗ**: Στην περίπτωση αυτή πρέπει να προτείνετε το κράτος της κύριας εγκατάστασής σας.

10. **ΔΙΑΒΙΒΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ ΕΚΤΟΣ ΕΕ**: Αν διαβιβάζετε δεδομένα και σε τρίτες χώρες, επιλέξτε κάποιο μηχανισμό διαβίβασης, όπως δεσμευτικούς εταιρικούς κανόνες (BCRs), τυποποιημένες συμβατικές ρήτρες (SCCs), πιστοποιήσεις στο Privacy Shield (για τις ΗΠΑ).

Δικαιώματα Υποκειμένου Δεδομένων

- **Ενημέρωσης** :Ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να παρέχει στο χρήστη κάθε πληροφορία που αφορά τη συλλογή και επεξεργασία
- **Πρόσβασης:** 'Εχει το δικαίωμα να βεβαιώνεται για το εάν τα δεδομένα το έχουν υποστεί επεξεργασία και να έχει πρόσβαση στην πληροφόρηση για τους σκοπούς της επεξεργασίας, τους παραλήπτες, την περίοδο αποθήκευσης κλπ.
- **Διόρθωση:** Έχει το δικαίωμα να αιτεί τη διόρθωση ανακριβών δεδομένων ή συμπλήρωση ανολοκλήρωτων δεδομένων που τον αφορούν.
- **Διαγραφής – Δικαίωμα στη Λήθη:** Διαγραφή των δεδομένων του, καθώς αυτά δε θα μπορούσαν να συμβάλουν στη διατήρηση της ιστορικής μνήμης ή στην ελευθερία της ενημέρωσης.
- **Περιορισμού Επεξεργασίας** εάν τα δεδομένα υπό επεξεργασία ήταν ανακριβή, άχρηστα ή παραβιάζονταν από μια παράνομα εφαρμοσμένη επεξεργασία
- **Φορητότητα Δεδομένων:** Έχει το δικαίωμα να παραλάβει αντίγραφο από τον υπεύθυνο επεξεργασίας, ο οποίος επιτρέπει περαιτέρω χρήση και μεταφορά δεδομένων σε άλλο πρόσωπο.
- **Εναντίωσης:** Έχει το δικαίωμα να εναντιωθεί στην επεξεργασία προσωπικών δεδομένων