Ενημέρωση για τον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 ΓΚΠΔ (GDPR)

Υπεύθυνος επικοινωνίας
Μπρης Δημήτρης
Μαθηματικός . MSc στα Πληροφοριακά συστήματα
Τηλ.: 210.64.25.819 6944.810.572
www.e-dinet.gr info@e-dinet.gr

Περιεχόμενα

1. Τι είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων ΓΚΠΔ (GDPR)

Με τον νέο Ευρωπαϊκό Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) 2016/679, που τίθεται σε εφαρμογή στις 25 Μαΐου 2018, καθιερώνεται ενιαίο νομικό πλαίσιο για την προστασία των προσωπικών δεδομένων σε όλα τα κράτη μέλη της ΕΕ.

Ο κανονισμός θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα (ΔΠΧ) και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα, προστατεύει θεμελιώδη δικαιώματα και ελευθερίες των φυσικών προσώπων και ειδικότερα το δικαίωμά τους στην προστασία των δεδομένων προσωπικού χαρακτήρα.

2. Πεδίο Εφαρμογής - ποιους αφορά;

Εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων μιας εγκατάστασης ενός υπευθύνου επεξεργασίας[1] ή εκτελούντος την επεξεργασία[2] στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός της Ένωσης.

3. Βασικά δικαιώματα των πολιτών

- ✓ Δικαίωμα ενημέρωσης και πρόσβασης στα δεδομένα
- ✓ Δικαίωμα διόρθωσης
- ✓ Δικαίωμα περιορισμού της επεξεργασίας
- ✓ Δικαίωμα εναντίωσης στην
- ✓ επεξεργασία
- ✓ Δικαίωμα στη λήθη
- ✓ Δικαίωμα στη φορητότητα των δεδομένων
- ✓ Λήψη εγγυήσεων για την ασφάλεια, την νομιμότητα της επεξεργασίας και το χρόνο τήρησης
- ✓ Συγκατάθεση (όπου απαιτείται)

[1] το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους,

[2] το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

4. Υποχρεώσεις υπευθύνου επεξεργασίας

Ο Κανονισμός επιβάλλει μια σειρά νέων υποχρεώσεων στους υπευθύνους επεξεργασίας, οι οποίες απορρέουν από τις βασικές αρχές και ιδίως την ενισχυμένη **αρχή της διαφάνειας** στον τρόπο συλλογής, επεξεργασίας και τήρησης δεδομένων και τη νέα **αρχή της λογοδοσίας**, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωσή του με όλες τις αρχές που διέπουν την επεξεργασία προσωπικών δεδομένων:

- ✓ **Ευθύνη**: 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.
- ✓ Προστασία δεδομένων εξ ορισμού Ο Κανονισμός επιβάλλει την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων που να διασφαλίζουν ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα δεδομένα που είναι απαραίτητα για τον σκοπό της επεξεργασίας.
- ✓ **Γνωστοποίηση παραβιάσεων δεδομένων:** Ο υπεύθυνος επεξεργασίας έχει υποχρέωση, μόλις αντιληφθεί παραβίαση, να ενημερώσει τις αρμόδιες εποπτικές Αρχές και εσάς, εφ' όσον η παραβίαση σάς θέτει σε σοβαρό κίνδυνο.
- ✓ **Υπεύθυνος προστασίας δεδομένων (DPO):** Προβλέπεται, υπό προϋποθέσεις, ο ορισμός «υπευθύνου προστασίας δεδομένων» ο οποίος έχει εχέγγυα ανεξαρτησίας και παρακολουθεί τη συμμόρφωση με τον νόμο αποτελώντας, συγχρόνως, το σημείο επαφής με την εποπτική
- ✓ Προστασία δεδομένων κατά τον σχεδιασμό («Data protection by design»):
- ✓ **Ασφάλεια επεξεργασίας**: Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει να εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το ενδεδειγμένο επίπεδο ασφάλειας.
- ✓ **Εκτίμηση επιπτώσεων και προηγούμενη Διαβούλευση** Όταν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα των ατόμων, ιδίως επειδή είναι συστηματική, μεγάλης κλίμακας, αφορά ειδικές κατηγορίες δεδομένων και βασίζεται στη χρήση νέων τεχνολογιών, ο υπεύθυνος επεξεργασίας πρέπει να διενεργήσει εκτίμηση επιπτώσεων σχετικά με την προστασία των δεδομένων («Data protection impact assessment»).

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

5. Τι σας παρέχουμε

5.1 Υπηρεσίες συμμόρφωσης με το κανονισμό

1. ΕΝΗΜΕΡΩΣΗ - ΕΤΟΙΜΟΤΗΤΑ:

- ✓ Ενημερώνουμε το ανθρώπινο δυναμικό του οργανισμού σας για τις επερχόμενες μεταβολές, υπογραμμίζοντας τις σημαντικές επιπτώσεις σε περίπτωση παραβιάσεων. Αξιολογούμε τους πιθανούς κινδύνους για τα προσωπικά δεδομένα που συλλέγετε και επεξεργάζεστε.
- ✓ Διαμορφώνουμε στρατηγική αντιμετώπισης των πιθανών κινδύνων με τεχνικά και οργανωτικά μέτρα.

2. ΚΑΤΑΓΡΑΦΗ:

- ✓ Οφείλετε να τηρείτε ειδικά αρχεία επεξεργασιών; Αν ναι, καταγράφουμε ενδελεχώς τα δεδομένα που τηρείτε και μεταβιβάζετε, τις επεξεργασίες στις οποίες προβαίνετε, τον σκοπό τους και τη νομική βάση.
- ✓ Πλήρης καταγραφή προσωπικού που επεξεργάζεται ΔΠΧ, συμβάσεις εμπιστευτικότητας κ.λ.π.

3. ΕΛΕΓΧΟΣ ΤΗΡΗΣΗΣ ΤΗΣ ΣΥΜΜΟΡΦΩΣΗΣ:

- ✓ Εξετάζουμε 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:

- ✓ Εξετάζουμε τις μεθόδους για εξασφάλιση συγκατάθεσης για κάθε επιδιωκόμενο σκοπό επεξεργασίας.

5. ΑΝΑΘΕΩΡΗΣΗ ΠΟΛΙΤΙΚΩΝ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΙΑΔΙΚΑΣΙΩΝ:

- ✓ Επικαιροποίηση διαδικασιών 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 - risk management:

- ✓ Αφού καταγράψουμε και χαρτογραφήσουμε τα πληροφοριακά συστήματα που διαθέτετε, θα εκτιμήσουμε τις πιθανότητες επέλευσης κινδύνων και τις συνέπειες στα προσωπικά δεδομένα.
- ✓ Εξετάζουμε αδυναμίες πληροφοριακών συστημάτων, πιθανές ευπάθειες και τρόποι αντιμετώπισης, απειλές – βαρύτητα & επιπτώσεις

7. ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO):

- ✓ Ανάλογα με τη δραστηριότητα που ασκείτε, εξετάζουμε αν χρειάζεται να ορίσετε «υπεύθυνο προστασίας δεδομένων» (DPO).

8. ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ:

- ✓ Διαθέτετε διαδικασία για τις γνωστοποιήσεις παραβιάσεων προς την Αρχή και τα υποκείμενα; Μαζί θα αναλύσουμε διαδικασίες για την ανίχνευση, την καταγραφή και τη διερεύνηση περιστατικών παραβιάσεων (σε φυσικό & ηλεκτρονικό αρχείο).

9. ΕΛΓΧΟΣ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ ΣΕ ΠΕΡΙΣΣΟΤΕΡΑ ΚΡΑΤΗ ΜΕΛΗ:

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).

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

Ο ανωτέρω πίνακας, αναφέρει συνοπτικά τα σημεία στα οποία θα πρέπει να γίνουν παρεμβάσεις και έλεγχοι συμμόρφωσης με το κανονισμό. Σε καμία περίπτωση δε αναφέρεται λεπτομερώς στις περεταίρω ενέργειες που πρέπει να γίνουν κατά περίπτωση. Για παράδειγμα αναφέρεται στον πίνακα (παρ.8) η ενότητα «ΠΑΡΑΒΙΑΣΕΙΣ ΔΕΔΟΜΕΝΩΝ». Στην πραγματικότητα όμως αυτή η ενότητα περιλαμβάνει δεκάδες ενέργειες οι οποίες διαφοροποιούνται ανάλογα με τι δραστηριότητα της επιχείρησης/οργανισμού και τα πληροφοριακά συστήματα (διαδικασίες) που χρησιμοποιεί.

Σε κάθε περίπτωση όμως, μετά από ενδελεχή έλεγχο που πραγματοποιούμε, σας παρέχουμε έγγραφες βεβαιώσεις που περιλαμβάνουν τη πλήρη χαρτογράφηση του πληροφοριακού σας συστήματος, πλήρη καταγραφή διαδικασιών, πλήρη καταγραφή «εκτελούντων την επεξεργασία». Εξάλλου, σύμφωνα με το **Άρθρο 24** (**παρ.1**) του **κανονισμού**, «*…ο υπεύθυνος επεξεργασίας (οργανισμός, εταιρεία, επιχείρηση) εφαρμόζει κατάλληλα **τεχνικά** και **οργανωτικά** μέτρα προκειμένου να διασφαλίζει και να μπορεί να **αποδεικνύει** ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό…*»

5.2 Υπηρεσίες «Υπευθύνου προστασίας δεδομένων» ΥΠΔ - DPO

5.2.1 Εισαγωγή

Σύμφωνα με τα **Άρθρα 37,38 & 39** του κανονισμού, η εταιρεία ή ο οργανισμός σας, είτε είναι υπεύθυνος επεξεργασίας είτε εκτελών την επεξεργασία, οφείλει να διορίσει ΥΠΔ εφόσον οι βασικές δραστηριότητες που ασκεί περιλαμβάνουν την επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα ή την τακτική και συστηματική παρακολούθηση σε μεγάλη κλίμακα φυσικών προσώπων. Εν προκειμένω, η παρακολούθηση της συμπεριφοράς φυσικών προσώπων περιλαμβάνει όλες τις μορφές ανίχνευσης και κατάρτισης προφίλ στο διαδίκτυο, συμπεριλαμβανομένων των σκοπών της συμπεριφοριστικής διαφήμισης.

Οι δημόσιες διοικήσεις (*συμπεριλαμβανόμενων και των ΝΠΔΔ*) έχουν **πάντα** την **υποχρέωση** να διορίζουν ΥΠΔ (με εξαίρεση τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους ιδιότητα).

Ο ΥΠΔ μπορεί να είναι **μέλος** του **προσωπικού** του **οργανισμού** σας ή μπορεί να είναι εξωτερικός συνεργάτης με βάση σύμβαση παροχής υπηρεσιών. Ο ΥΠΔ μπορεί να είναι φυσικό πρόσωπο ή οργανισμός.

Να σημειωθεί, ότι παρόλο που δεν είναι υποχρεωτικός ο διορισμός DPO, α**ποτελεί καλή πρακτική απόδειξης συμμόρφωσης** (*ο διορισμός DPO*) σύμφωνα με τις απαιτήσεις του κανονισμού.

Δείτε τον πίνακα που ακολουθεί με τις παρεχόμενες υπηρεσίες DPO (παρ. 5.2.3).

5.2.2 Εμπειρογνωμοσύνη και δεξιότητες του υπευθύνου προστασίας δεδομένων – σωστή επιλογή

Σύμφωνα με το **άρθρο 37 παράγραφος 5**, ο υπεύθυνος προστασίας δεδομένων «διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και **βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39**». Στην αιτιολογική σκέψη 97 αναφέρεται ότι το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία.

Ο υπεύθυνος προστασίας δεδομένων θα πρέπει επομένως να επιλέγεται προσεκτικά, λαμβάνοντας δεόντως υπόψη τα ζητήματα προστασίας δεδομένων που ανακύπτουν στο εσωτερικό του οργανισμού.

Μολονότι το άρθρο 37 παράγραφος 5 δεν προσδιορίζει τα επαγγελματικά προσόντα που θα πρέπει να λαμβάνονται υπόψη κατά τον ορισμό του υπευθύνου προστασίας δεδομένων, ο τελευταίος πρέπει να διαθέτει **εμπειρογνωσία** στον τομέα του δικαίου και των πρακτικών **περί προστασίας δεδομένων**, τόσο σε εθνικό όσο και ευρωπαϊκό επίπεδο, και επιπλέον να έχει άριστη γνώση του ΓΚΠΔ.

Τέλος, σύμφωνα με τις **Κατευθυντήριες γραμμές της «***Ομάδας προστασίας των πρόσωπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29***»**, ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει καλή γνώση των πράξεων επεξεργασίας που διενεργούνται, καθώς και των **συστημάτων πληροφορικής**, και των αναγκών του υπευθύνου επεξεργασίας σε **επίπεδο ασφάλειας και προστασίας των δεδομένων.**

5.2.3 Παρεχόμενες Υπηρεσίες «Υπευθύνου προστασίας δεδομένων» DPO

Παρεχόμενες Υπηρεσίες «Υπευθύνου προστασίας δεδομένων» DPO

✓ Παροχή ενημέρωσης και συμβουλών στον υπεύθυνο επεξεργασίας (*εταιρεία, οργανισμό, ατομική επιχείρηση ή φυσικό πρόσωπο*) ή τον εκτελούντα την επεξεργασία, καθώς και το προσωπικό που απασχολούν, σχετικά με τις υποχρεώσεις τους σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων·	✓ Παρακολούθηση τη συμμόρφωσης του οργανισμού με το σύνολο της νομοθεσίας που αφορά την προστασία δεδομένων, επίσης κατά τη διάρκεια ελέγχων, δραστηριοτήτων ενημέρωσης και εκπαίδευσης του προσωπικού που συμμετέχει σε πράξεις επεξεργασίας·
✓ Παροχή συμβουλών όταν έχει πραγματοποιηθεί ΕΑΠΔ (Εκτίμηση Αντίκτυπου στα Προσωπικά Δεδομένα) και παρακολούθηση του αποτελέσματος	✓ Εκπροσώπηση ως σημείο επαφής για αιτήματα φυσικών προσώπων που αφορούν την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους. ✓ Υποχρεωτική δημοσιοποίηση των στοιχείων επικοινωνίας του DPO
✓ Συνεργασία με ΑΠΔ (Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα) και εκπροσώπηση ως σημείο επαφής για ΑΠΔ σχετικά με ζητήματα που αφορούν την επεξεργασία.	
Σημείωσεις: Ο ΥΠΔ δεν πρέπει να λαμβάνει οδηγίες από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για την άσκηση των καθηκόντων του. Ο ΥΠΔ αναφέρεται απευθείας στο υψηλότερο επίπεδο διοίκησης του οργανισμού.	

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

6. Συνήθεις ερωτήσεις απαντήσεις

1. Τι είναι τα «δεδομένα προσωπικού χαρακτήρα»

«δεδομένα προσωπικού χαρακτήρα» (Αρ 4 ΓΚΠΔ) είναι κάθε πληροφορία που αφορά ταχτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου

2. Τι είναι η «επεξεργασία δεδομένων»

«επεξεργασία» (Αρ 4 ΓΚΠΔ) είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή,

3. Τι είναι ο «εκτελών την επεξεργασία»

«εκτελών την επεξεργασία» (Αρ 4 ΓΚΠΔ) : το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου της επεξεργασίας,

4. Τι είναι η «παραβίαση δεδομένων προσωπικού χαρακτήρα»

«παραβίαση δεδομένων προσωπικού χαρακτήρα» (Αρ 4 ΓΚΠΔ): η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Η εταιρεία ή ο οργανισμός σας πρέπει να ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και το **αργότερο εντός 72 ωρών** αφού αντιληφθεί την παραβίαση. Εάν η εταιρεία ή ο οργανισμός σας είναι ο εκτελών την επεξεργασία, πρέπει να ενημερώνει τον **υπεύθυνο επεξεργασίας δεδομένων** για κάθε παραβίαση δεδομένων.

Εάν η παραβίαση δεδομένων θέτει σε υψηλό κίνδυνο τα φυσικά πρόσωπα που επηρεάζονται, τότε πρέπει επίσης να ενημερωθεί το καθένα εξ αυτών, εκτός εάν έχουν τεθεί σε εφαρμογή αποτελεσματικά τεχνικά και οργανωτικά μέτρα προστασίας ή άλλα μέτρα που διασφαλίζουν ότι ο κίνδυνος δεν είναι πλέον πιθανό να προκύψει.

5. Ποια δεδομένα προσωπικού χαρακτήρα θεωρούνται ευαίσθητα;

Τα παρακάτω δεδομένα προσωπικού χαρακτήρα θεωρούνται «ευαίσθητα» και υπόκεινται σε συγκεκριμένες προϋποθέσεις επεξεργασίας (ΓΚΠΔ - Άρθρο 4 σημεία 13, 14 και 15, άρθρο 9) :

- ✓ δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις·

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

- ✓ συμμετοχή σε συνδικαλιστική οργάνωση·
- ✓ γενετικά δεδομένα, βιομετρικά δεδομένα που υποβάλλονται σε επεξεργασία αποκλειστικά για την ταυτοποίηση ενός ατόμου·
- ✓ δεδομένα σχετικά με την υγεία·
- ✓ δεδομένα σχετικά με τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός ατόμου.

6. Πώς πρέπει να διεκπεραιώνονται τα αιτήματα ατόμων που ασκούν τα δικαιώματά τους σχετικά με την προστασία των δεδομένων;

(*Άρθρα 12 και 15 έως 22*)
Φυσικά πρόσωπα μπορούν να επικοινωνήσουν με την εταιρεία ή τον οργανισμό σας με σκοπό την άσκηση των δικαιωμάτων τους σύμφωνα με τον ΓΚΠΔ (δικαιώματα πρόσβασης, διόρθωσης, διαγραφής, φορητότητας κ.λπ.). Όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία **με ηλεκτρονικά μέσα**, η εταιρεία ή ο οργανισμός σας θα πρέπει να παρέχει μέσα για την υποβολή ηλεκτρονικών αιτημάτων. Επιπλέον, πρέπει να απαντά στα αιτήματα που λαμβάνει χωρίς αδικαιολόγητη καθυστέρηση και κατ' αρχή εντός ενός μηνός από τη λήψη του αιτήματος.

Η εταιρεία ή ο οργανισμός σας μπορεί να ζητά περαιτέρω πληροφορίες από τα πρόσωπα που έχουν υποβάλει αίτημα, για να επιβεβαιώσει την ταυτότητά τους.

Εάν η εταιρεία ή ο οργανισμός σας απορρίψει το αίτημα, πρέπει να ενημερώσει το άτομο σχετικά με τους λόγους για τους οποίους το έκανε και σχετικά με το δικαίωμα του ατόμου να υποβάλει καταγγελία ενώπιον της αρχής προστασίας δεδομένων και να επιδιώξει έννομη προστασία.

Η επεξεργασία αιτημάτων φυσικών προσώπων θα πρέπει να γίνεται δωρεάν. Όταν τα αιτήματα είναι προδήλως αβάσιμα ή υπερβολικά, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους, μπορείτε να χρεώσετε εύλογο τέλος ή να αρνηθείτε να δώσετε συνέχεια.

7. Τι επαγγελματικά προσόντα θα πρέπει να έχει ο υπεύθυνος προστασίας δεδομένων (άρθρο 37 παράγραφος 5);

Σύμφωνα με τον ΓΚΠΔ, ο υπεύθυνος προστασίας δεδομένων «διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39».

Το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία. Για παράδειγμα, όταν μια δραστηριότητα επεξεργασίας δεδομένων είναι ιδιαίτερα πολύπλοκη ή όταν εμπλέκεται μεγάλος όγκος ευαίσθητων δεδομένων, ο υπεύθυνος προστασίας δεδομένων είναι πιθανό να χρειάζεται υψηλότερο επίπεδο εμπειρογνωμοσύνης και υποστήριξης.

Ο υπεύθυνος προστασίας δεδομένων πρέπει να διαθέτει, μεταξύ άλλων, τις ακόλουθες δεξιότητες και εμπειρογνωμοσύνη:

- ✓ εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του ΓΚΠΔ,
- ✓ γνώση των πράξεων επεξεργασίας που διενεργούνται,

Μπρης Δημήτρης (*Μαθηματικός , Msc στα Πληροφοριακά Συστήματα*) Τηλ: 210.64.25.819 – 6944.810.572

- ✓ γνώση του τομέα των **τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων**,
- ✓ γνώση του τομέα δραστηριότητας και του οργανισμού,
- ✓ ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού.

8. **Ποιος είναι ο ρόλος του υπευθύνου προστασίας δεδομένων όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (άρθρο 37 παράγραφος 1 στοιχείο γ)) και το αρχείο των δραστηριοτήτων επεξεργασίας (άρθρο 30);**

Όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων για ζητήματα όπως, ενδεικτικά, τα ακόλουθα:

- ✓ εάν πρέπει ή όχι να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων·
- ✓ ποια μεθοδολογία πρέπει να ακολουθήσει κατά τη διενέργεια της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων·
- ✓ εάν πρέπει να διενεργήσει την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων εσωτερικά ή να την αναθέσει σε εξωτερικό συνεργάτη·
- ✓ τι εγγυήσεις (περιλαμβανομένων των τεχνικών και οργανωτικών μέτρων) πρέπει να εφαρμόσει προκειμένου να μετριαστούν οι κίνδυνοι για τα δικαιώματα και τα συμφέροντα των υποκειμένων των δεδομένων·
- ✓ εάν διενεργήθηκε σωστά ή όχι η εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και εάν τα συμπεράσματά της (σχετικά με το εάν θα δοθεί ή όχι συνέχεια στην επεξεργασία και τι εγγυήσεις θα εφαρμοστούν) είναι σύμφωνα με τον ΓΚΠΔ.

9. **Δεν είμαι υποχρεωμένος να διορίσω Υπεύθυνο Προστασίας (DPO), ωστόσο πρέπει να συμμορφωθώ με τον κανονισμό;**

Εφόσον επεξεργάζεστε δεδομένα προσωπικού χαρακτήρα, οφείλετε να συμμορφωθείτε με τις απαιτήσεις του κανονισμού ακόμα και εάν δεν είστε υποχρεωμένοι να διορίσετε DPO

Παραδείγματα επαγγελματιών προς συμμόρφωση

Σας παραθέτουμε μερικά **παραδείγματα** επαγγελματιών που οφείλουν να συμμορφωθούν

- ✓ **Ιατρός – Επαγγέλματα Υγείας,** οι οποίοι μάλιστα επεξεργάζονται ευαίσθητα προσωπικά δεδομένα
- ✓ **ΝΠΔΔ** – σύλλογος (Υποχρεωτικά και διορισμός DPO)
- ✓ **Παιδικός σταθμός** που συλλέγει μάλιστα δεδομένα προσωπικού χαρακτήρα ανηλίκου (π.χ. ηλικίες 2-5 ετών). Η εταιρεία (παιδικός σταθμός) μπορεί να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα ενός παιδιού βάσει συγκατάθεσης (*Άρθρα 8 και 12 ΓΚΠΔ*) εφόσον έχει λάβει τη ρητή συγκατάθεση του γονιού ή κηδεμόνα τους μέχρι μια συγκεκριμένη ηλικία. Το όριο ηλικίας για τη λήψη γονικής συγκατάθεσης ποικίλλει από τα 13 έως τα 16 έτη, ανάλογα με την ηλικία που καθορίζεται εν προκειμένω σε κάθε κράτος μέλος της ΕΕ. Στη συγκεκριμένη περίπτωση πρέπει να διασφαλίζεται ότι οποιαδήποτε πληροφορία και επικοινωνία

που απευθύνεται σε ένα παιδί είναι εύκολα προσβάσιμη και σε σαφή και απλή γλώσσα η οποία είναι ευνόητη για ένα παιδί.

- ✓ **Web Site** – eshop το οποίο συλλέγει δεδομένα προσωπικού χαρακτήρα και πιθανώς να καταρτίζει προφίλ των μελών. Ακόμη και εάν η συλλογή είναι απαραίτητη προς την εκπλήρωση των συμβατικών υποχρεώσεων προς τον αγοραστή (*σχέση πωλητή αγοραστή*), ο ιστότοπος οφείλει να ενημερώσει το μέλος – επισκέπτη (ή αγοραστή) για τη δικαιώματα του και να του παράσχει τις εγγυήσεις για την ασφάλεια και το απόρρητο των δεδομένων που τον αφορούν
- ✓ **Κατάστημα λιανικής πώλησης** το οποίο μάλιστα συλλέγει πληροφορίες από το πελατολόγιο με σκοπό μελλοντικές προωθητικές ενέργειες
- ✓ **Γυμναστήριο,** το οποίο συλλέγει δεδομένα προσωπικού χαρακτήρα των μελών του και πιθανότατα επεξεργάζεται και «ευαίσθητα» δεδομένα με σκοπό δημιουργίας «σωματικού» προφίλ για δημιουργία προγράμματος εκγύμνασης
- ✓ **Παιδότοπος,** ο οποίος εκτός των απαραίτητων πληροφοριών που συλλέγει για τα ανήλικα (όνομα επίθετο κ.λ.π.) πιθανότατα να προβαίνει σε τακτική και συστηματική παρακολούθηση των «υποκείμενων» (π.χ. με σταθερή παρακολούθηση μέσω κάμερας ή/και WebCam)
- ✓ **Φροντιστήριο μέσης εκπαίδευσης – ξένων γλωσσών ,** το οποίο συλλέγει δεδομένα προσωπικού χαρακτήρα ανήλικων μαθητών, πιθανότατα δε και για ηλικίες<15-16.

Για οποιαδήποτε απορία – διευκρίνιση, επικοινωνήστε μαζί μας:

Μπρης Δημήτρης
Μαθηματικός . MSc στα Πληροφοριακά συστήματα
Τηλ.: 210.64.25.819 6944.810.572
www.e-dinet.gr info@e-dinet.gr