Θανάσης Δαβαλάς • Άννα Αγγελάκη
Μαρία Ταβουλάρη • Βίκτωρ Γασπαράκης
Ευάγγελος Τζανίδης

Εξεταστέα ύλη για Data Protection Officer
Το μοναδικό που περιλαμβάνει υποδείγματα για τον επαγγελματία DPO

GDPR

FYLATOS PUBLISHING

GDPR

Εξεταστέα ύλη για Data Protection Officer
Το μοναδικό που περιλαμβάνει υποδείγματα για τον επαγγελματία DPO

Α. Αγγελάκη
Β. Γασπαράκης
Α. Δαβαλάς
Μ. Ταβουλάρη
Ε. Τζανίδης

Εκδόσεις Φυλάτος
Θεσσαλονίκη
MMXX

© Εκδόσεις Φυλάτος, © Fylatos Publishing
e-mail. contact@fylatos.com
web: www.fylatos.com
Σχεδιασμός Εξωφύλλου: © Εκδόσεις Φυλάτος
Σελιδοποίηση-Σχεδιασμός: © Εκδόσεις Φυλάτος
ISBN:978-960-658-024-6

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Εισαγωγή

Το βιβλίο αυτό γράφτηκε για να βοηθήσει και να διευκολύνει τις επιχειρήσεις στη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας προσωπικών Δεδομένων (Γ.Κ.Π.Δ.) ευρέως γνωστό ως GDPR από την αγγλική ονομασία General Data Protection Regulation. Κεντρικό πρόσωπο για την εφαρμογή του κανονισμού είναι ο Υπεύθυνος Προστασίας Δομένων (Υ.Π.Δ.). Στο βιβλίο περιλαμβάνονται αναλυτικά τα καθήκοντα του Υ.Π.Δ. καθώς και πολλά από τα έγγραφα που θα τον διευκολύνουν στην εργασία του. Επίσης περιλαμβάνονται λεπτομερείς οδηγίες για τη συμμόρφωση ιστοτόπων και ηλεκτρονικών καταστημάτων.

Το βιβλίο περιλαμβάνει την ύλη εξέτασης για την πιστοποίηση του Data Protection Officer βάσει των εξετάσεων του Εργαστηρίου ΤΠΕ – Ήρων καθώς και υποδείγματα DPIA (Εκτίμηση Αντικτύπου) – Gap Analysis (Έκθεση Ελλείψεων) – Data Mapping (Χαρτογράφηση Ροής Δεδομένων) για όσους παρέχουν υπηρεσίες συμμόρφωσης με τον GDPR .

- Στο πρώτο κεφάλαιο παρουσιάζουμε τον Γενικό Κανονισμό Προστασίας Δεδομένων.
- Το δεύτερο κεφάλαιο είναι αφιερωμένο στον τρόπο με τον οποίο ο Γ.Κ.Π.Δ. επηρεάζει τις επιχειρήσεις. Τι πρέπει να κάνει μια επιχείρηση ώστε να συμμορφωθεί με το Γ.Κ.Π.Δ.
- Στο τρίτο κεφάλαιο παρουσιάζουμε κάποια τεστ αυτοαξιολόγησης όσον αφορά τη συμμόρφωση με το Γ.Κ.Π.Δ. Δίνουμε αρκετές ερωτήσεις τις οποίες μπορείτε να υποβάλλετε στον εαυτό σας ώστε να κάνετε μια γρήγορη εκτίμηση σχετικά με το κατά πόσο η επιχείρησή σας συμμορφώνεται με το Γ.Κ.Π.Δ.
- Στο τέταρτο κεφάλαιο παρουσιάζουμε τις αρμοδιότητες του Υ.Π.Δ. Η νομοθεσία αναθέτει στον Υ.Π.Δ. μεγάλο μέρος της ευθύνης για την εφαρμογή του Γ.Κ.Π.Δ.
- Στο πέμπτο κεφάλαιο περιλαμβάνονται κάποια από τα έγγραφα που έχει υποχρέωση να συμπληρώνει ο Υ.Π.Δ. ή ο υπεύθυνος επεξεργασίας για να συμβάλλει στη συμμόρφωση της επιχείρησης.
- Το έκτο κεφάλαιο είναι αφιερωμένο στην Εκτίμηση Αντικτύπου σχετικά με την Προστασία
- Δεδομένων (DPIA).
- Το έβδομο κεφάλαιο είναι αφιερωμένο στην Ανάλυση Ελλείψεων (GAP Analysis).
- Στο όγδοο κεφάλαιο εξετάζουμε τους τρόπους προστασίας ιστοσελίδων και ηλεκτρονικών καταστημάτων. Πώς να αντιμετωπίσετε θέματα που αφορούν τα cookies και τις φόρμες επικοινωνίας. Τα σημαντικότερα βήματα για τη συμμόρφωση κάθε ιστοτόπου.

ΚΕΦΑΛΑΙΟ 1: Ο Γενικός Κανονισμός Προστασίας Δεδομένων

Ο κανονισμός γενικής προστασίας δεδομένων της ΕΕ (GDPR) τέθηκε σε εφαρμογή στις 25 Μαΐου 2018. Ο κανονισμός αντικαθιστά όλους τους ισχύοντες εθνικούς νόμους για την προστασία των δεδομένων των κρατών μελών της ΕΕ. Σημαντικός και με ευρύ πεδίο εφαρμογής, ο κανονισμός φέρνει μια προσέγγιση του 21ου αιώνα για την προστασία των δεδομένων. Διευρύνει τα δικαιώματα των ατόμων να ελέγχουν τον τρόπο συλλογής και επεξεργασίας των προσωπικών τους πληροφοριών και θέτει μια σειρά υποχρεώσεων στους οργανισμούς που είναι υπεύθυνοι για την προστασία των δεδομένων.

Η συμμόρφωση δεν είναι επιλογή και ο χρόνος τελειώνει

Η συμμόρφωση με το GDPR δεν είναι απλώς θέμα σχεδιασμού πεδίων σε φόρμες εγγραφής. Ο κανονισμός απαιτεί να αποδείξετε την τήρηση των αρχών προστασίας δεδομένων. Αυτό προϋποθέτει την υιοθέτηση μιας προσέγγισης που βασίζεται στην προστασία των δεδομένων, διασφαλίζοντας την ύπαρξη κατάλληλων πολιτικών και διαδικασιών για την αντιμετώπιση των αρχών της διαφάνειας και της λογοδοσίας, καθώς και των δικαιωμάτων των ατόμων και της δημιουργίας μιας κουλτούρας στον χώρο εργασίας του ιδιωτικού απορρήτου και της ασφάλειας των δεδομένων.

Τα επιχειρησιακά οφέλη του GDPR

Με το κατάλληλο πλαίσιο συμμόρφωσης, όχι μόνο θα είστε σε θέση να αποφύγετε σημαντικά πρόστιμα και ζημιές στη φήμη σας. Θα είστε επίσης σε θέση να δείξετε στους πελάτες σας ότι είστε αξιόπιστοι και υπεύθυνοι και να αποκομίσετε πρόσθετη αξία από τα δεδομένα που διατηρείτε. Επιγραμματικά αναφέρουμε ενδεικτικά κάποια από τα επιχειρησιακά οφέλη του GDPR:

- Δημιουργία εμπιστοσύνης πελατών,
- Βελτίωση της εικόνας και της φήμης της μάρκας,
- Βελτίωση του ελέγχου των δεδομένων,
- Βελτίωση της ασφάλειας των πληροφοριών,
- Βελτίωση του ανταγωνιστικού πλεονεκτήματος.

Νομοθεσία

Σε αυτή την ενότητα παρουσιάζουμε το νομικό πλαίσιο που σχετίζεται με την εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων.

Οδηγία Προστασίας Δεδομένων

Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ αποτελούσε το νομικό πλαίσιο για την επεξεργασία προσωπικών δεδομένων στην ΕΕ πριν από τις 25 Μαΐου 2018. Αντικαταστάθηκε από τον GDPR στις 25 Μαΐου 2018. Η Οδηγία εισήγαγε βασικές προϋποθέσεις που έπρεπε να εφαρμοστούν μέσω ξεχωριστής νομοθεσίας σε κάθε κράτος-μέλος της ΕΕ. Αυτό έδωσε στα μέλη τη δυνατότητα να επεκτείνουν το πεδίο εφαρμογής της Οδηγίας ή να διατηρήσουν προϋπάρχουσες αυστηρότερες προϋποθέσεις ή να αποφασίσουν να μην εκμεταλλευθούν πλήρως τις παρεκκλίσεις, το οποίο εξηγεί την εφαρμογή διαφορετικών πλαισίων προστασίας δεδομένων στην Ευρώπη. Μπορείτε να βρείτε online περισσότερες πληροφορίες για την Ευρωπαϊκή Οδηγία 95/46/ΕΚ στον ακόλουθο σύνδεσμο: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

EU GDPR

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) υιοθετήθηκε ως Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου στις 27 Απριλίου 2016.

Σε αντίθεση με την Οδηγία Προστασίας Δεδομένων, ο GDPR εφαρμόζεται απευθείας σε κάθε κράτος μέλος της ΕΕ χωρίς εφαρμοστική νομοθεσία και σχηματίζει ένα πλαίσιο μέσα στο οποίο μπορούν να δημιουργηθούν πιο λεπτομερείς κανόνες. Αυτό εναρμονίζει την νομοθεσία σε όλη την Ευρώπη.

Η απαίτηση ειδοποίησης της αρμόδιας αρχής (DPA) σε περίπτωση νέας επεξεργασίας, για παράδειγμα, καταργείται (εκτός από έναν μικρό αριθμό περιπτώσεων) και αντικαθίσταται από την υποχρέωση καταγραφής όλων των επεξεργασιών. Υπεύθυνοι επεξεργασίας και επεξεργαστές πρέπει να συμφωνήσουν ως προς τις αρμοδιότητες, αλλιώς θα είναι υπόλογοι από κοινού. Ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) μπορεί να βρεθεί online εδώ:

http://eur-lex.europa.eu/legal-content/EN/TXT/

Οδηγία e-Privacy

Η Οδηγία e-Privacy υιοθετήθηκε ως Οδηγία 2002/58/EC του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου. Αυτή τη στιγμή ελέγχει τα δικαιώματα ιδιωτικότητας που εφαρμόζονται στην τεχνολογία και το περιεχόμενο ηλεκτρονικής επικοινωνίας. Η Οδηγία μπορεί να βρεθεί online εδώ:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do

Κανονισμός e-Privacy

Ακολουθώντας την υιοθέτηση του GDPR, η Οδηγία e-Privacy θα αναθεωρηθεί ώστε να συμμορφωθεί με τον GDPR και να καλύψει τις τεχνολογικές καινοτομίες από την τελευταία τροποποίηση της Οδηγίας το 2009. Μία πρόταση με τίτλο “Κανονισμός Ιδιωτικότητας και Ηλεκτρονικής Επικοινωνίας” δημοσιοποιήθηκε στις 10 Ιανουαρίου 2017.

Ο Κανονισμός θα έχει εφαρμογή σε κάθε πάροχο υπηρεσιών ηλεκτρονικής επικοινωνίας ή σε κάθε οντότητα που επεξεργάζεται δεδομένα ηλεκτρονικής επικοινωνίας. Θα έχει επίδραση στον τρόπο με τον οποίο οργανισμοί αλληλεπιδρούν ηλεκτρονικά με πολίτες της ΕΕ, συμπεριλαμβανομένων της ιχνηλάτησης χρηστών, της συλλογής δεδομένων σε συσκευές χρηστών και της άμεσης εμπορικής προώθησης. Το σχέδιο του Κανονισμού και τα σχετικά έγγραφα μπορούν να βρεθούν online εδώ:

https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

Όργανα GDPR

Σε αυτή την ενότητα παρουσιάζουμε τα αρμόδια όργανα που έχουν σχέση με την εφαρμογή του Γενικού Κανονισμού προστασίας Δεδομένων:

EDPS

Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (EDPS) δημιουργήθηκε το 2004 με στόχο τη διασφάλιση του σεβασμού από οργανισμούς και όργανα της ΕΕ του δικαιώματος των ανθρώπων στην ιδιωτικότητα όταν επεξεργάζονται τα προσωπικά δεδομένα τους. Στις βασικές λειτουργίες του, ο EDPS:

(1) επιβλέπει την επεξεργασία από τη διοίκηση της ΕΕ προσωπικών δεδομένων ώστε να εξασφαλίζεται η συμμόρφωση με κανόνες ιδιωτικότητας, διαχειρίζεται καταγγελίες και διεξάγει έρευνες, και

(2) συμβουλεύει οργανισμούς και όργανα της ΕΕ σχετικά με όλες τις απόψεις της επεξεργασίας προσωπικών δεδομένων και τις σχετικές πολιτικές και νομοθεσία.

Η Ομάδα Εργασίας Άρθρου 29

Η Ομάδα Εργασίας Άρθρου 29 (“A29WP”) είναι ένα μη ρυθμιστικό όργανο προστασίας δεδομένων. Η κύρια λειτουργία του είναι η παροχή συμβουλών και συστάσεων στα κράτη-μέλη και το κοινό σχετικά με την προστασία δεδομένων και την επεξεργασία προσωπικών δεδομένων. Το όργανο αποτελείται από εκπροσώπους εθνικών αρχών προστασίας δεδομένων της ΕΕ, του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (“EDPS”) και της Ευρωπαϊκής Επιτροπής. Μετατράπηκε στο “Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων” (“EDPB”) με τον GDPR.

EDPB

Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων θα αντικαταστήσει την Ομάδα Εργασίας Άρθρου 29 και οι λειτουργίες του θα περιλαμβάνουν την εξασφάλιση της ομοιομορφίας της εφαρμογής του GDPR, συμβουλές προς την Ευρωπαϊκή Επιτροπή, την έκδοση οδηγιών, κανόνων συμπεριφοράς και συστάσεων, την αναγνώριση οργάνων πιστοποίησης και την έκδοση γνωμοδοτήσεων για σχέδια αποφάσεων εποπτικών αρχών.

Αρχές Προστασίας Δεδομένων (DPA / Supervisory Authority / Lead Authority)

Οι Αρχές Προστασίας Δεδομένων (ΑΠΔ, DPAs) είναι οι εθνικές αρχές προστασίας δεδομένων, επιφορτισμένες με την ιδιωτικότητα και την προστασία προσωπικών δεδομένων. Κάθε κράτος όρισε ένα όργανο DPA για να εφαρμόσει την τοπική νομοθεσία προστασίας δεδομένων και για να προσφέρει καθοδήγηση. Οι DPAs έχουν αξιοσημείωτες δυνατότητες επιβολής, συμπεριλαμβανομένης της δυνατότητας να επιβάλλουν υψηλά πρόστιμα.

Οι Αρχές Προστασίας Δεδομένων επιβλέπουν τον Γενικό Κανονισμό για την Προστασία των Δεδομένων και τις σχετικές εθνικές νομοθεσίες μέσω εξουσιών έρευνας και διορθωτικών εξουσιών. Είναι ανεξάρτητες δημόσιες αρχές, οι οποίες παρέχουν εξειδικευμένες συμβουλές σχετικά με ζητήματα προστασίας δεδομένων. Οι καταγγελίες που αφορούν πιθανές παραβιάσεις του δικαίου περί προστασίας δεδομένων πρέπει να υποβάλλονται στις Αρχές Προστασίας Δεδομένων. Κάθε χώρα μέλος της ΕΕ διαθέτει μια Αρχή Προστασίας Δεδομένων.

Η ΑΠΔ μιας χώρας μέλους της ΕΕ αποτελεί το κύριο σημείο επαφής για ερωτήσεις σχετικά με την προστασία δεδομένων όσον αφορά εταιρείες και οργανισμούς που έχουν την έδρα τους στη συγκεκριμένη χώρα. Υπάρχουν όμως περιπτώσεις στις οποίες το κύριο σημείο επαφής ενδέχεται να είναι η ΑΠΔ άλλης χώρας μέλους της ΕΕ. Αυτό συμβαίνει για παράδειγμα εάν μια εταιρεία ή ένας οργανισμός επεξεργάζεται δεδομένα σε διαφορετικά κράτη μέλη της ΕΕ ή ανήκει σε όμιλο εταιρειών που έχουν έδρα σε διαφορετικά κράτη μέλη της ΕΕ.

Στον ακόλουθο σύνδεσμο βρίσκεται η λίστα με τις Εθνικές Αρχές Προστασίας Δεδομένων των χωρών της Ευρωπαϊκής Ένωσης:

http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm

Τα βασικά στοιχεία του GDPR

Τι είναι τα δεδομένα προσωπικού χαρακτήρα;

Κάθε πληροφορία σχετική με ένα ταυτοποιημένο/ταυτοποιήσιμο άτομο, είτε πληροφορία που σχετίζεται με την προσωπική, επαγγελματική ή δημόσια ζωή του/της. Μπορεί να είναι οτιδήποτε από ένα όνομα, φωτογραφία, διεύθυνση email, στοιχεία τραπεζικού λογαριασμού, δημοσιεύσεις σε ιστοσελίδες κοινωνικής δικτύωσης, ιατρικά δεδομένα, διεύθυνση IP ή έναν συνδυασμό δεδομένων που ταυτοποιεί άμεσα ή έμμεσα το πρόσωπο.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί ανώνυμα, έχουν κρυπτογραφηθεί ή για τα οποία έχουν χρησιμοποιηθεί ψευδώνυμα αλλά τα οποία μπορούν να χρησιμοποιηθούν για την επαναταυτοποίηση ενός ατόμου παραμένουν δεδομένα προσωπικού χαρακτήρα και εμπίπτουν στο πεδίο εφαρμογής του ΓΚΠΔ.

Εάν όμως η ανωνυμοποίηση είναι μη αντιστρέψιμη τότε τα δεδομένα θεωρούνται πραγματικά ανώνυμα. Αυτό συμβαίνει στις περιπτώσεις όπου η διαδικασία μετατροπής δεδομένων προσωπικού χαρακτήρα σε ανώνυμα γίνεται με τέτοιον τρόπο, ώστε το φυσικό πρόσωπο να μην είναι πλέον ταυτοποιήσιμο.

Ο ΓΚΠΔ προστατεύει τα δεδομένα προσωπικού χαρακτήρα ανεξάρτητα από την τεχνολογία που χρησιμοποιείται για την επεξεργασία τους. Είναι τεχνολογικά ουδέτερος και εφαρμόζεται τόσο στην αυτοματοποιημένη όσο και στη χειροκίνητη επεξεργασία, υπό την προϋπόθεση ότι τα δεδομένα οργανώνονται βάσει προκαθορισμένων κριτηρίων (π.χ. αλφαβητική σειρά). Επίσης, δεν έχει σημασία ο τρόπος που αποθηκεύονται τα δεδομένα – σε σύστημα τεχνολογίας πληροφοριών, μέσω βιντεοεπιτήρησης ή σε έντυπη μορφή. Σε όλες τις περιπτώσεις τα δεδομένα προσωπικού χαρακτήρα υπόκεινται στις απαιτήσεις προστασίας που προβλέπει ο ΓΚΠΔ.

Παραδείγματα δεδομένων προσωπικού χαρακτήρα:

- Ονοματεπώνυμο,
- Διεύθυνση,
- Διεύθυνση ηλεκτρονικού ταχυδρομείου,
- Φωτογραφία,
- Διεύθυνση IP,
- Δεδομένα τοποθεσίας,
- Ηλεκτρονική συμπεριφορά (cookies),
- Δεδομένα σχετικά με τα χαρακτηριστικά και την ανάλυση,
- Αναγνωριστικός αριθμός κάρτας ,
- Δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να προσδιορίζουν αποκλειστικά ένα άτομο.

Σημειώστε ότι σε ορισμένες περιπτώσεις, υπάρχει ειδική νομοθεσία σχετικά με συγκεκριμένους τομείς που ρυθμίζει, για παράδειγμα, τη χρήση δεδομένων τοποθεσίας ή τη χρήση cookie – οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες [οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002 (ΕΕ L 201 της 31.7.2002, σ. 37) και κανονισμός (ΕΚ) αριθ. 2006/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Οκτωβρίου 2004 (ΕΕ L 364 της 9.12.2004, σ. 1)].

Ειδικές κατηγορίες προσωπικών δεδομένων:

- Γένος,
- Θρησκεία,
- Πολιτικές απόψεις,
- Σύνταξη συνδικαλιστικών οργανώσεων,
- Σεξουαλικός προσανατολισμός,
- Πληροφορίες για την υγεία,
- Βιομετρικά δεδομένα,
- Γενετικά δεδομένα.

Παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα:

- αριθμός μητρώου εργαζομένου σε εταιρεία,
- ηλεκτρονική διεύθυνση της μορφής πληροφορίες@εταιρεία.com
- ανώνυμα δεδομένα.

Ευρύτερο πεδίο

Το GDPR ισχύει για όλες τις οργανώσεις της ΕΕ – εμπορικές, φιλανθρωπικές ή δημόσιες αρχές – που συλλέγουν, αποθηκεύουν ή επεξεργάζονται τα προσωπικά δεδομένα των κατοίκων της ΕΕ, ακόμη και αν δεν είναι πολίτες της ΕΕ.
Οργανισμοί που εδρεύουν εκτός της ΕΕ και προσφέρουν αγαθά ή υπηρεσίες σε κατοίκους της ΕΕ, παρακολουθούν τη συμπεριφορά τους ή επεξεργάζονται τα προσωπικά τους δεδομένα θα υπόκεινται στο GDPR.
Οι πάροχοι υπηρεσιών (επεξεργαστές δεδομένων) που επεξεργάζονται δεδομένα για λογαριασμό ενός οργανισμού εμπίπτουν στην αρμοδιότητα του GDPR και θα έχουν συγκεκριμένες υποχρεώσεις συμμόρφωσης. Ένα παράδειγμα μπορεί να είναι μια εταιρεία που επεξεργάζεται τη μισθοδοσία σας ή έναν παροχέα Cloud που προσφέρει αποθήκευση δεδομένων.

Αρχές προστασίας δεδομένων

Τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία σύμφωνα με τις έξι αρχές προστασίας δεδομένων:

- Επεξεργασμένα νόμιμα, δίκαια και με διαφάνεια,
- Να συλλέγονται μόνο για συγκεκριμένους νόμιμους σκοπούς,
- Επαρκή, σχετικά και περιορισμένα σε ό,τι είναι απαραίτητο,
- Πρέπει να είναι ακριβή και ενημερωμένα,
- Να αποθηκεύονται μόνο για όσο διάστημα είναι απαραίτητο,
- Να διασφαλίζουν την κατάλληλη ασφάλεια, ακεραιότητα και εμπιστευτικότητα.

Λογοδοσία και διακυβέρνηση

Πρέπει να είστε σε θέση να αποδείξετε τη συμμόρφωση με το GDPR:

- Η δημιουργία δομής επεξεργασίας και ελέγχου με ρόλους και ευθύνες,
- Διατηρήστε λεπτομερή καταγραφή όλων των λειτουργιών επεξεργασίας δεδομένων,
- Η τεκμηρίωση των πολιτικών και διαδικασιών προστασίας δεδομένων,
- Εκτιμήσεις επιπτώσεων προστασίας δεδομένων (DPIA) για εργασίες επεξεργασίας υψηλού κινδύνου.
- Εφαρμογή κατάλληλων μέτρων για την εξασφάλιση προσωπικών δεδομένων,
- Εκπαίδευση και ευαισθητοποίηση του προσωπικού,

- Όπου είναι απαραίτητο, διορίστε υπεύθυνο προστασίας δεδομένων (data protection officer).

Προστασία δεδομένων από τον σχεδιασμό και από προεπιλογή

Υπάρχει η απαίτηση να δημιουργηθούν αποτελεσματικές πρακτικές προστασίας δεδομένων και διασφαλίσεις από την αρχή κάθε επεξεργασίας:

- Η προστασία δεδομένων πρέπει να λαμβάνεται υπόψη κατά τον σχεδιασμό κάθε νέας διαδικασίας, συστήματος ή τεχνολογίας,
- Μια DPIA αποτελεί αναπόσπαστο μέρος της προστασίας της ιδιωτικής ζωής από τον σχεδιασμό,
- Ο προεπιλεγμένος τρόπος συλλογής πρέπει να είναι η συγκέντρωση μόνο των προσωπικών δεδομένων που είναι απαραίτητα για συγκεκριμένο σκοπό.

Νομιμότητα της επεξεργασίας

Πρέπει να προσδιορίσετε και να τεκμηριώσετε τη νόμιμη βάση για οποιαδήποτε επεξεργασία προσωπικών δεδομένων. Οι νόμιμες βάσεις είναι:

- Άμεση συγκατάθεση από το άτομο,
- Η αναγκαιότητα εκτέλεσης σύμβασης,
- Προστασία των ζωτικών συμφερόντων του ατόμου,
- Οι νομικές υποχρεώσεις του οργανισμού,
- Ανάγκη για το δημόσιο συμφέρον και τα έννομα συμφέροντα της οργάνωσης,
- Όπου κρίνεται απαραίτητο ο διορισμός ενός Υπευθύνου Προστασίας Προσωπικών Δεδομένων / Data Protection Officer.

Ισχύουσα συναίνεση

Υπάρχουν αυστηρότεροι κανόνες για τη συναίνεση:

- Η συγκατάθεση πρέπει να παρέχεται ελεύθερα, συγκεκριμένη, ενημερωμένη και αδιαμφισβήτητη.,
- Η αίτηση συναίνεσης πρέπει να είναι κατανοητή και σε σαφή και απλή γλώσσα,
- Η σιωπή (σιωπηρή συναίνεση), τα τετραγωνίδια (check boxs) και η αδράνεια δεν θα αρκούν πλέον ως συγκατάθεση,
- Η συγκατάθεση μπορεί να αποσυρθεί ανά πάσα στιγμή,
- Η συγκατάθεση για ηλεκτρονικές υπηρεσίες από ένα παιδί κάτω των 13 ισχύει μόνο με τη γονική άδεια,
- Οι οργανισμοί πρέπει να είναι σε θέση να αποδεικνύουν τη συγκατάθεση.

Δικαιώματα ιδιωτών

Τα δικαιώματα των πελατών και επισκεπτών σας αναβαθμίζονται εντυπωσιακά όπως και οι ευθύνες σας.

Τα δικαιώματα των ατόμων βελτιώνονται και επεκτείνονται σε διάφορους σημαντικούς τομείς:

- Το δικαίωμα πρόσβασης σε προσωπικά δεδομένα μέσω αιτήσεων πρόσβασης σε θέματα,
- Το δικαίωμα διόρθωσης ανακριβών προσωπικών δεδομένων,
- Το δικαίωμα σε ορισμένες περιπτώσεις να διαγραφούν τα προσωπικά δεδομένα,

- Το δικαίωμα ένστασης,
- Το δικαίωμα μεταφοράς προσωπικών δεδομένων από έναν πάροχο υπηρεσιών σε άλλον (φορητότητα δεδομένων).

Διαφάνεια και ειδοποιήσεις απορρήτου

Οι οργανισμοί πρέπει να είναι σαφείς και διαφανείς όσον αφορά τον τρόπο με τον οποίο θα επεξεργάζονται τα προσωπικά δεδομένα, από ποιον και γιατί.

Οι ειδοποιήσεις προστασίας προσωπικών δεδομένων πρέπει να παρέχονται με συνοπτική, διαφανή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα.

Μεταφορές δεδομένων εκτός της ΕΕ

Η μεταφορά προσωπικών δεδομένων εκτός της ΕΕ επιτρέπεται μόνο:

- Όταν η ΕΕ έχει αναγνωρίσει στη χώρα ότι παρέχει επαρκές επίπεδο προστασίας των δεδομένων,
- Μέσω πρότυπων συμβάσεων ή δεσμευτικών εταιρικών κανόνων, ή
- Με τη συμμόρφωση με έναν εγκεκριμένο μηχανισμό πιστοποίησης, π.χ. Ασφάλεια απορρήτου ΕΕ-ΗΠΑ.

Ασφάλεια δεδομένων και αναφορά παραβίασης

Τα προσωπικά δεδομένα πρέπει να προστατεύονται από μη εξουσιοδοτημένη επεξεργασία και από τυχαία απώλεια, καταστροφή ή βλάβη.

- Οι παραβιάσεις δεδομένων πρέπει να αναφέρονται στην αρχή προστασίας δεδομένων εντός 72 ωρών από την ανακάλυψη,
- Τα άτομα που επηρεάζονται πρέπει να ενημερώνονται, όταν υπάρχει υψηλός κίνδυνος, για τα δικαιώματα και τις ελευθερίες τους, π.χ. κλοπή ταυτότητας, προσωπικήασφάλεια.

Data protection officer (DPO)

Ο διορισμός ενός ΥΠΔ είναι υποχρεωτικός για:

- Δημόσιες αρχές,
- Οργανισμούς που εμπλέκονται σε επεξεργασία υψηλού κινδύνου, και
- Οργανισμούς που επεξεργάζονται ειδικές κατηγορίες δεδομένων.

Ο Υπεύθυνος προστασίας δεδομένων (Data Protection Officer) :

- Ενημερώνει και συμβουλεύει την οργάνωση των υποχρεώσεών της αρχής / του οργανισμού πάνω στην προστασία των δεδομένων των πελατών, αλλά και των εργαζομένων τους,
- Παρακολούθηση της συμμόρφωσης, συμπεριλαμβανομένης της ευαισθητοποίησης, της κατάρτισης του προσωπικού και των ελέγχων,
- Συνεργάζεται με τις αρχές προστασίας δεδομένων και ενεργεί ως σημείο επαφής.

Συλλογή προσωπικών δεδομένων

Δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία μόνο στις περιπτώσεις που δεν είναι ευλόγως εφικτό να πραγματοποιηθεί η επεξεργασία με άλλον τρόπο. Όπου

είναι δυνατόν, πρέπει να προτιμάται η χρήση ανώνυμων δεδομένων. Στις περιπτώσεις όπου απαιτούνται δεδομένα προσωπικού χαρακτήρα, αυτά πρέπει να είναι επαρκή, συναφή και να περιορίζονται σε αυτά που είναι απαραίτητα για τον σκοπό («ελαχιστοποίηση δεδομένων»). Η εταιρεία ή ο οργανισμός σας, ως υπεύθυνος επεξεργασίας, έχει την υποχρέωση να αξιολογεί πόσα δεδομένα είναι απαραίτητα και να διασφαλίζει ότι δεν συλλέγονται δεδομένα που δεν είναι συναφή.

Παράδειγμα συλλογής προσωπικών δεδομένων

Ας πάρουμε για παράδειγμα μια εταιρεία η οποία προσφέρει υπηρεσίες ενοικίασης αυτοκινήτων σε φυσικά πρόσωπα. Για να ενοικιάσει κάποιο φυσικό πρόσωπο ένα αυτοκίνητο είναι απαραίτητο να δώσει το ονοματεπώνυμο, τη διεύθυνση και τον αριθμό πιστωτικής του κάρτας. Ενδεχομένως αν απαιτούνται και δεδομένα υγείας όπως για παράδειγμα ο βαθμός μυωπίας και πρεσβυωπίας ή ο βαθμός αναπηρίας. Αυτά τα δεδομένα δικαιούται να τα συλλέγει η εταιρεία ενοικίασης αυτοκινήτων.

Δεν δικαιούται όμως να συλλέγει δεδομένα που αφορούν τις πολιτικές απόψεις ή άλλα δεδομένα υγείας πέραν αυτών που σχετίζονται με την ικανότητα οδήγησης (όραση – κίνηση).

Τι θεωρείται ως επεξεργασία δεδομένων;

Ο όρος «επεξεργασία» καλύπτει ευρύ φάσμα πράξεων που πραγματοποιούνται σε δεδομένα προσωπικού χαρακτήρα, είτε με χειροκίνητα είτε με αυτοματοποιημένα μέσα. Περιλαμβάνει τη συλλογή, καταχώριση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών, χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, συσχέτιση ή συνδυασμό, περιορισμό, διαγραφή ή καταστροφή δεδομένων προσωπικού χαρακτήρα.

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) εφαρμόζεται στην εξ ολοκλήρου ή μερική επεξεργασία δεδομένων προσωπικού χαρακτήρα με αυτοματοποιημένα μέσα καθώς και στη μη αυτοματοποιημένη επεξεργασία, εάν αποτελεί μέρος διαρθρωμένου συστήματος αρχειοθέτησης.

Παραδείγματα επεξεργασίας δεδομένων:

- διαχείριση προσωπικού και μισθοδοσία,
- προσπέλαση/αναζήτηση πληροφοριών σε βάση δεδομένων επαφών που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα,
- αποστολή διαφημιστικών ηλεκτρονικών μηνυμάτων*,
- καταστροφή διά τεμαχισμού εγγράφων που περιέχουν δεδομένα προσωπικού χαρακτήρα,
- δημοσίευση/ανάρτηση φωτογραφίας ενός ατόμου σε ιστότοπο,
- αποθήκευση διευθύνσεων IP ή διευθύνσεων MAC,
- μαγνητοσκόπηση (τηλεόραση κλειστού κυκλώματος).

*Σας ενημερώνουμε να έχετε υπόψη ότι για την αποστολή ηλεκτρονικών μηνυμάτων απευθείας εμπορικής προώθησης πρέπει επίσης να συμμορφώνεστε με τους κανόνες για το μάρκετινγκ που ορίζονται στην οδηγία για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

Προϋποθέσεις επεξεργασίας δεδομένων

Το είδος και ο όγκος των δεδομένων προσωπικού χαρακτήρα που μπορεί να επεξεργάζεται η εταιρεία ή ο οργανισμός σας εξαρτώνται από τον λόγο της επεξεργασίας (νομικός λόγος που χρησιμοποιείται) και από τη σκοπούμενη χρήση. Η εταιρεία ή ο οργανισμός πρέπει να τηρεί διάφορους βασικούς κανόνες, όπως τους εξής:

- τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία με νόμιμο και διαφανή τρόπο, διασφαλίζοντας την αντικειμενικότητα προς τα άτομα των οποίων τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία («νομιμότητα, αντικειμενικότητα και διαφάνεια»),
- πρέπει να υπάρχουν συγκεκριμένοι σκοποί για την επεξεργασία των δεδομένων και η εταιρεία ή ο οργανισμός πρέπει να υποδεικνύει τους εν λόγω σκοπούς στα άτομα όταν συλλέγει τα δεδομένα τους προσωπικού χαρακτήρα. Δεν μπορεί απλώς να συλλέγει δεδομένα προσωπικού χαρακτήρα για απροσδιόριστους σκοπούς («περιορισμός του σκοπού»),
- η εταιρεία ή ο οργανισμός πρέπει να συλλέγει και να επεξεργάζεται μόνο τα δεδομένα προσωπικού χαρακτήρα που είναι απαραίτητα για την επίτευξη του εν λόγω σκοπού («ελαχιστοποίηση των δεδομένων»),
- η εταιρεία ή ο οργανισμός πρέπει να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και ενημερωμένα, λαμβάνοντας υπόψη τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία, και να τα διορθώνει στην αντίθετη περίπτωση («ακρίβεια»),
- η εταιρεία ή ο οργανισμός δεν μπορεί να κάνει περαιτέρω χρήση των δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς που δεν είναι συμβατοί με τον αρχικό σκοπό,
- η εταιρεία ή ο οργανισμός πρέπει να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα δεν αποθηκεύονται για διάστημα μεγαλύτερο από αυτό που είναι απαραίτητο για τους σκοπούς για τα οποία συλλέχθηκαν («περιορισμός της περιόδου αποθήκευσης»),
- η εταιρεία ή ο οργανισμός πρέπει να υλοποιήσει κατάλληλες τεχνικές και οργανωτικές εγγυήσεις που εξασφαλίζουν την ασφάλεια των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης της προστασίας από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά, χρησιμοποιώντας κατάλληλη τεχνολογία («ακεραιότητα και εμπιστευτικότητα»).

Παράδειγμα προϋποθέσεων επεξεργασίας δεδομένων

Η εταιρεία ή ο οργανισμός σας εκμεταλλεύεται ένα ταξιδιωτικό πρακτορείο. Όταν λαμβάνετε τα δεδομένα προσωπικού χαρακτήρα των πελατών σας, θα πρέπει να τους εξηγείτε σε σαφή και απλή γλώσσα γιατί χρειάζεστε τα δεδομένα, πώς θα τα χρησιμοποιήσετε και για πόσο διάστημα σκοπεύετε να τα κρατήσετε. Η επεξεργασία θα πρέπει να είναι οργανωμένη με τρόπο που να τηρούνται οι βασικές αρχές προστασίας των δεδομένων.

Εφαρμογή του GDPR

Σε αυτή την ενότητα εξετάζουμε με περισσότερες λεπτομέρειες σε ποιες περιπτώσεις φυσικών και νομικών προσώπων καθώς και σε ποιες περιπτώσεις δεδομένων εφαρμόζεται ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ)

Σε ποια δεδομένα εφαρμόζεται η νομοθεσία περί προστασίας των δεδομένων

Ο κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου1, δηλαδή ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) της Ευρωπαϊκής Ένωσης (ΕΕ), ρυθμίζει

Το βιβλίο αυτό γράφτηκε για να βοηθήσει και να διευκολύνει τις επιχειρήσεις στη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας προσωπικών Δεδομένων (Γ.Κ.Π.Δ.) ευρέως γνωστό ως GDPR από την αγγλική ονομασία General Data Protection Regulation. Κεντρικό πρόσωπο για την εφαρμογή του κανονισμού είναι ο Υπεύθυνος Προστασίας Δομένων (Υ.Π.Δ.). Στο βιβλίο περιλαμβάνονται αναλυτικά τα καθήκοντα του Υ.Π.Δ. καθώς και πολλά από τα έγγραφα που θα τον διευκολύνουν στην εργασία του. Επίσης περιλαμβάνονται λεπτομερείς οδηγίες για τη συμμόρφωση ιστοτόπων και ηλεκτρονικών καταστημάτων.

Το βιβλίο περιλαμβάνει την ύλη εξέτασης για την πιστοποίηση του Data Protection Officer βάσει των εξετάσεων του Εργαστηρίου ΤΠΕ – Ήρων καθώς και υποδείγματα DPIA (Εκτίμηση Αντικτύπου) – Gap Analysis (Έκθεση Ελλείψεων) – Data Mapping (Χαρτογράφηση Ροής Δεδομένων) για όσους παρέχουν υπηρεσίες συμμόρφωσης με τον GDPR .

- Στο πρώτο κεφάλαιο παρουσιάζουμε τον Γενικό Κανονισμό Προστασίας Δεδομένων.
- Το δεύτερο κεφάλαιο είναι αφιερωμένο στον τρόπο με τον οποίο ο Γ.Κ.Π.Δ. επηρεάζει τις επιχειρήσεις. Τι πρέπει να κάνει μια επιχείρηση ώστε να συμμορφωθεί με το Γ.Κ.Π.Δ.
- Στο τρίτο κεφάλαιο παρουσιάζουμε κάποια τεστ αυτοαξιολόγησης όσον αφορά τη συμμόρφωση με το Γ.Κ.Π.Δ. Δίνουμε αρκετές ερωτήσεις τις οποίες μπορείτε να υποβάλλετε στον εαυτό σας ώστε να κάνετε μια γρήγορη εκτίμηση σχετικά με το κατά πόσο η επιχείρησή σας συμμορφώνεται με το Γ.Κ.Π.Δ.
- Στο τέταρτο κεφάλαιο παρουσιάζουμε τις αρμοδιότητες του Υ.Π.Δ. Η νομοθεσία αναθέτει στον Υ.Π.Δ. μεγάλο μέρος της ευθύνης για την εφαρμογή του Γ.Κ.Π.Δ.
- Στο πέμπτο κεφάλαιο περιλαμβάνονται κάποια από τα έγγραφα που έχει υποχρέωση να συμπληρώνει ο Υ.Π.Δ. ή ο υπεύθυνος επεξεργασίας για να συμβάλλει στη συμμόρφωση της επιχείρησης.
- Το έκτο κεφάλαιο είναι αφιερωμένο στην Εκτίμηση Αντικτύπου σχετικά με την Προστασία Δεδομένων (DPIA).
- Το έβδομο κεφάλαιο είναι αφιερωμένο στην Ανάλυση Ελλείψεων (GAP Analysis).
- Στο όγδοο κεφάλαιο εξετάζουμε τους τρόπους προστασίας ιστοσελίδων και ηλεκτρονικών καταστημάτων. Πώς να αντιμετωπίσετε θέματα που αφορούν τα cookies και τις φόρμες επικοινωνίας. Τα σημαντικότερα βήματα για τη συμμόρφωση κάθε ιστοτόπου.

FYLATOS PUBLISHING

ISBN 978-960-658-024-6

9 789606 580246 >