Π.Ο.Φ.Ε.Ε.

ΜΑΪΟΣ 2018

General Data Protection Regulation (GDPR)

Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ)

ΛΙΣΤΑ ΕΛΕΓΧΟΥ ΕΤΟΙΜΟΤΗΤΑΣ

Προετοιμάζοντας την επιχείρηση σας για τον
Γενικό Κανονισμό για την Προστασία Δεδομένων

Τι σημαίνει ο ΓΚΠΔ για την επιχείρηση/οργανισμό σας;

Στις 25 Μαΐου 2018, ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) θα εφαρμοστεί σε όλα τα κράτη μέλη της ΕΕ. Ο ΓΚΠΔ παρέχει ένα πλαίσιο νόμου προστασίας δεδομένων για την Ευρώπη, το οποίο αντιπροσωπεύει μια σημαντική εναρμόνιση των απαιτήσεων και των προτύπων για την προστασία των δεδομένων σε ολόκληρη την ΕΕ. Έχοντας να κάνουμε με ένα μόνο οριζόντιο πλαίσιο δικαίου θα ωφελήσει τις επιχειρήσεις, θα προάγει την ευθύνη κατά την αντιμετώπιση των δεδομένων προσωπικού χαρακτήρα, και θα συμβάλει στη διασφάλιση ότι τα ίδια πρότυπα προστασίας των δεδομένων ισχύουν σε όλη την ΕΕ.

Ωστόσο, παρ' όλο που είναι ένας άμεσης-εφαρμογής κανονισμός της Ευρωπαϊκής Ένωσης, ο ΓΚΠΔ παρέχει περιορισμένες δυνατότητες στα κράτη μέλη της ΕΕ να εφαρμόσουν περαιτέρω νομοθεσία για να καθορίσουν εθνικά πρότυπα σε ορισμένους τομείς, όπως η επεξεργασία δεδομένων υγείας και οι ποινικές καταδίκες, την ηλικία της ψηφιακής συγκατάθεσης και τις περιστάσεις υπό τις οποίες μπορούν να περιοριστούν τα δικαιώματα προστασίας των δεδομένων ενός ατόμου. Κατά συνέπεια, είναι σημαντικό για όλες τις επιχειρήσεις και τους οργανισμούς να γνωρίζουν ότι θα υποχρεούνται να συμμορφωθούν με τα πρότυπα και τις υποχρεώσεις προστασίας δεδομένων που καθορίζονται τόσο στον ΓΚΠΔ όσο και από την εθνική νομοθεσία.

Αυτός ο οδηγός με την λίστα ελέγχου έχει σχεδιαστεί για να βοηθήσει ιδίως τον τομέα των μικρών και μεσαίων επιχειρήσεων, όπου ενδέχεται να μην έχουν πρόσβαση σε εκτενείς σχεδιασμούς και νομικούς πόρους. Ακόμα, θα βοηθήσει τις μικρομεσαίες επιχειρήσεις να προετοιμαστούν για ένα επιχειρηματικό μέλλον συμβατό με την προστασία των δεδομένων.

Εάν επεξεργάζεστε δεδομένα προσωπικού χαρακτήρα ως μέρος των λειτουργιών της επιχείρησής σας, ο ΓΚΠΔ ισχύει για εσάς. Είναι σημαντικό να θυμάστε ότι:

- τα δεδομένα των πελατών και των εργαζομένων είναι δεδομένα προσωπικού χαρακτήρα
- η απλή αποθήκευση προσωπικών δεδομένων ηλεκτρονικά ή σε έντυπη μορφή αποτελεί «επεξεργασία» προσωπικών δεδομένων

Βασικοί ορισμοί του ΓΚΠΔ

ΓΚΠΔ: ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (2016/679) είναι ο νέος κανονισμός της ΕΕ για την προστασία των δεδομένων, ο οποίος θα τίθεται σε ισχύ στις 25 Μαΐου 2018.

Δεδομένα προσωπικού χαρακτήρα: πληροφορίες που αφορούν ένα ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο, όπως και διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου. Αυτό μπορεί να είναι ένας πολύ ευρύς ορισμός - ανάλογα με τις περιστάσεις - και μπορεί να περιλάβει τα στοιχεία που αφορούν την ταυτότητα, τα χαρακτηριστικά ή τη συμπεριφορά ενός ατόμου ή να επηρεάζουν τον τρόπο με τον οποίο αυτό το άτομο αντιμετωπίζεται ή αξιολογείται.

Επεξεργασία: η εκτέλεση οποιασδήποτε εργασίας ή συνόλου εργασιών σε δεδομένα προσωπικού χαρακτήρα, μεταξύ των οποίων:

- συλλογή, καταχώριση ή διατήρηση δεδομένων
- οργάνωση ή τροποποίηση των δεδομένων
- ανάκτηση, αναζήτηση ή χρήση των δεδομένων
- αποκάλυψη των δεδομένων σε τρίτο μέρος (συμπεριλαμβανομένης της δημοσίευσης)
- διαγραφή ή καταστροφή των δεδομένων.

Υπεύθυνος επεξεργασίας: είναι το πρόσωπο ή εταιρία ή ο οργανισμός που αποφασίζει τους «σκοπούς για τους οποίους» και τα «μέσα με τα οποία» γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Ο «σκοπός» της επεξεργασίας των δεδομένων περιλαμβάνει «γιατί» τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και τα «μέσα» της επεξεργασίας περιλαμβάνουν «πώς» τα δεδομένα υποβάλλονται σε επεξεργασία.

Εκτελών την επεξεργασία: ένα πρόσωπο ή μια εταιρία ή ένας οργανισμός που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό ενός υπεύθυνου δεδομένων.

Υποκείμενο των δεδομένων: το άτομο στο οποίο σχετίζονται τα δεδομένα προσωπικού χαρακτήρα.

Εκτίμηση Αντίκτυπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ): περιγράφει μια διαδικασία που αποσκοπεί στον εντοπισμό των κινδύνων που προκύπτουν από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την ελαχιστοποίηση των κινδύνων αυτών όσο το δυνατόν νωρίτερα. Οι ΕΑΠΔ είναι σημαντικά εργαλεία για την αποτροπή κινδύνου, και για την επίδειξη της συμμόρφωσης, συμπεριλαμβανομένης της συνεχούς συμμόρφωσης, με τον ΓΚΠΔ.

Νόμιμη βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα: προκειμένου να επεξεργαστείτε τα δεδομένα προσωπικού χαρακτήρα, πρέπει να έχετε μια νόμιμη βάση για να το κάνετε. Οι νόμιμοι λόγοι για την επεξεργασία δεδομένων προσωπικού χαρακτήρα καθορίζονται στο άρθρο 6 του ΓΚΠΔ. Αυτά είναι: η συγκατάθεση του ατόμου, εκτέλεση σύμβασης, συμμόρφωση με νομική υποχρέωση, είναι αναγκαία για την προστασία των ζωτικών συμφερόντων ενός προσώπου, είναι αναγκαία για την εκτέλεση ενός έργου που διενεργείται προς το δημόσιο συμφέρον ή προς το έννομο συμφέρον της εταιρίας/οργανισμού (εκτός εάν τα συμφέροντα αυτά υπερισχύονται από τα συμφέροντα ή τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων).

Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα (ευαίσθητα δεδομένα): αυτό ορίζεται στο άρθρο 9 παρ. 1 του ΓΚΠΔ ως δεδομένα «δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, 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».

Συγκατάθεση: το άρθρο 7 του ΓΚΠΔ έχει τροποποιήσει τις προϋποθέσεις που απαιτούνται για τη συγκατάθεση ως νομική βάση για να είναι έγκυρη η επεξεργασία δεδομένων. Είναι πλέον αναγκαίο να εξεταστεί αν η συγκατάθεση δόθηκε ελεύθερα και το υποκείμενο των δεδομένων πρέπει να έχει την δυνατότητα να αποσύρει τη συγκατάθεσή του για την επεξεργασία ανά πάσα στιγμή. Η συγκατάθεση δεν πρέπει να υπονοείται και πρέπει να λαμβάνεται πριν από την έναρξη της επεξεργασίας δεδομένων (π.χ. μέσω ειδοποιήσεων απορρήτου). Κατά την επεξεργασία των δεδομένων των παιδιών στο πλαίσιο των διαδικτυακών υπηρεσιών, είναι απαραίτητο να εξασφαλίζεται ότι η ηλικία τους επαληθεύεται και η συγκατάθεση του νόμιμου κηδεμόνα πρέπει να λαμβάνεται.

Τα βασικά βήματα για την εξασφάλιση συμμόρφωσης με τον ΓΚΠΔ

- Προσδιορίστε ποια δεδομένα προσωπικού χαρακτήρα έχετε (αυτό μπορεί να επιτευχθεί χρησιμοποιώντας τις πληροφορίες που περιέχοντα στο άρθρο 30 του ΓΚΠΔ ή για τις μικρότερες επιχειρήσεις μια προσαρμοσμένη διαδικασία, όπως το παρακάτω πρότυπο που προσδιορίζει τις λεπτομέρειες των προσωπικών δεδομένων που κατέχονται).
    - Διεξάγετε μια εκτίμηση κινδύνου για τα δεδομένα προσωπικού χαρακτήρα που κατέχετε και για τις δραστηριότητες επεξεργασίας των δεδομένων (άρθρο 24 και αιτιολογική σκέψη 75 του ΓΚΠΔ και το τμήμα με τίτλο "Μια προσέγγιση βάσει αξιολόγησης κινδύνου στην συμμόρφωση με τον ΓΚΠΔ" σε αυτόν τον οδηγό).
- Εφαρμόστε τα κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να εξασφαλίζεται η ασφαλής αποθήκευση των δεδομένων (σε ψηφιακά και έντυπα αρχεία). Τα μέτρα ασφαλείας που θα πρέπει να θέσει σε εφαρμογή η επιχείρησή σας θα πρέπει να εξαρτώνται από τον τύπο των προσωπικών δεδομένων που κρατάτε και τον κίνδυνο για τους πελάτες και τους υπαλλήλους σας σε περίπτωση που τα μέτρα ασφαλείας σας παραβιαστούν (άρθρο 32 του ΓΚΠΔ).
- Να γνωρίζετε τη νομική βάση στην οποία βασίζεστε (συγκατάθεση; συμβόλαιο; έννομο συμφέρον;) για να δικαιολογήσετε την επεξεργασία των δεδομένων προσωπικού χαρακτήρα (άρθρα 6 έως 8 του ΓΚΠΔ).
- Βεβαιωθείτε ότι συγκεντρώνετε μόνο τα ελάχιστα απαραίτητα δεδομένα προσωπικού χαρακτήρα για τη διεξαγωγή της εργασίας σας, ότι τα δεδομένα είναι ακριβή και δεν διατηρούνται για περισσότερο από ότι απαιτείται για τον σκοπό για τον οποίο έχουν συλλεχθεί (άρθρο 5 του ΓΚΠΔ).
- Να είστε διαφανείς με τους πελάτες σας σχετικά με τους λόγους για τη συλλογή των δεδομένων προσωπικού χαρακτήρα τους, τις συγκεκριμένες χρήσεις τους, και πόσο καιρό θα πρέπει να διατηρήσετε τα δεδομένα τους σε αρχείο (π.χ. ανακοινώσεις στον ιστότοπο σας ή πινακίδες στα σημεία πώλησης) (άρθρα 12, 13 και 14).
- Δείτε αν τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεστε εμπίπτουν στην κατηγορία των ειδικών κατηγοριών προσωπικών δεδομένων (όπως ευαίσθητα δεδομένα), και αν ναι, να γνωρίζετε τις πρόσθετες προφυλάξεις που πρέπει να λάβετε (άρθρο 9 του ΓΚΠΔ).
- Αποφασίστε εάν θα χρειαστεί να διορίσετε έναν υπεύθυνο προστασίας δεδομένων (DPO) (άρθρο 37 του ΓΚΠΔ).
- Να είστε σε θέση να διευκολύνετε τις αιτήσεις από χρήστες που επιθυμούν να ασκήσουν τα δικαιώματά τους στο πλαίσιο του ΓΚΠΔ, συμπεριλαμβανομένων των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής, ανάκλησης της συγκατάθεσης, της φορητότητας των δεδομένων και του δικαιώματος ένστασης στην αυτοματοποιημένη επεξεργασία (άρθρα 12 έως 22 του ΓΚΠΔ).
- Όπου ενδείκνυται, να έχετε ενημερωμένα έγγραφα πολιτικής/διαδικασίας που να περιγράφουν λεπτομερώς τον τρόπο με τον οποίο η οργάνωσή σας πληροί τις υποχρεώσεις προστασίας δεδομένων.

Μια προσέγγιση βάσει αξιολόγησης κινδύνου στην συμμόρφωση με τον ΓΚΠΔ

- Όταν η επιχείρηση σας συλλέγει, αποθηκεύει ή χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα, τα άτομα των οποίων τα δεδομένα επεξεργάζεστε ενδέχεται να εκτεθούν σε κινδύνους. Είναι σημαντικό οι εταιρίες/οργανισμοί που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα να λαμβάνουν μέτρα για να εξασφαλίσουν ότι τα δεδομένα αυτά αντιμετωπίζονται νόμιμα, με ασφάλεια, αποτελεσματικά και αποτελεσματικά, προκειμένου να παρέχουν την καλύτερη δυνατή φροντίδα.
- Το προφίλ κινδύνου των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται η επιχείρηση σας θα πρέπει να προσδιορίζεται σύμφωνα με τις διαδικασίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διενεργούνται, την πολυπλοκότητα και την κλίμακα της επεξεργασίας δεδομένων, την ευαισθησία των δεδομένων που υποβάλλονται σε επεξεργασία και την προστασία που απαιτείται για την επεξεργασία των δεδομένων αυτών. Για παράδειγμα, όταν μια δραστηριότητα επεξεργασίας δεδομένων είναι ιδιαίτερα περίπλοκη, ή όπου γίνεται σε μεγάλη κλίμακα ή αφορά ευαίσθητα δεδομένα (δηλ. μια διαδικτυακή, υγειονομική, οικονομική ή ασφαλιστική εταιρία), αυτό εμπεριέχει υψηλότερο κίνδυνο από τα συνήθη δεδομένα προσωπικού χαρακτήρα που αφορούν αποκλειστικά στα στοιχεία του λογαριασμού ενός υπαλλήλου ή ενός πελάτη.
- Όταν εξετάζετε το προφίλ κινδύνου των δεδομένων προσωπικού χαρακτήρα που επεξεργάζεται η επιχείρηση σας, είναι χρήσιμο να εξετάσετε τις απτές βλάβες που μπορεί να προκληθούν στα άτομα και για τις οποίες η επιχείρηση σας πρέπει να λάβει μέτρα προστασίας. Αυτά αναφέρονται λεπτομερώς στην αιτιολογική σκέψη 75 του ΓΚΠΔ και περιλαμβάνουν επεξεργασία που θα μπορούσε να οδηγήσει σε: διακρίσεις, κλοπή ταυτότητας ή απάτη, οικονομική ζημία, ζημία στη φήμη, απώλεια του εμπιστευτικού χαρακτήρα των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από το επαγγελματικό απόρρητο, μη εξουσιοδοτημένη αντιστροφή του ψευδωνύμου, ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα.
- Η διεξαγωγή μιας αξιολόγησης κινδύνου θα βελτιώσει την ευαισθητοποίηση στην επιχείρηση σας, στα ενδεχόμενα μελλοντικά ζητήματα που αφορούν την προστασία των δεδομένων που σχετίζονται με ένα έργο. Αυτό με τη σειρά του θα βοηθήσει στη βελτίωση του σχεδιασμού του έργου σας και θα ενισχύσει την επικοινωνία σας σχετικά με τους κινδύνους προστασίας δεδομένων προσωπικού χαρακτήρα με τους σχετικούς ενδιαφερομένους.
- Ο ΓΚΠΔ προβλέπει δύο κρίσιμες έννοιες για το μελλοντικό σχεδιασμό ενός έργου: προστασία δεδομένων «ήδη από τον σχεδιασμό» και «εξ ορισμού». Αν και για πολύ καιρό συνιστώνται ως ορθές πρακτικές, και οι δύο αυτές αρχές κατοχυρώνονται από το νόμο στο πλαίσιο του ΓΚΠΔ (άρθρο 25 του ΓΚΠΔ).

  Η προστασία δεδομένων «ήδη από τον σχεδιασμό» σημαίνει την ενσωμάτωση των χαρακτηριστικών του απορρήτου δεδομένων και των τεχνολογιών προστασίας της ιδιωτικής ζωής των δεδομένων απευθείας στο σχεδιασμό των έργων σε πρώιμο στάδιο. Αυτό θα συμβάλει στην εξασφάλιση καλύτερης και πιο βέλτιστου-κόστους προστασίας της ιδιωτικής ζωής των υποκειμένων.

  Η προστασία δεδομένων «εξ ορισμού» σημαίνει ότι οι ρυθμίσεις της υπηρεσίας χρήστη (π.χ. όχι αυτόματες συγκαταθέσεις στις σελίδες του λογαριασμού του πελάτη) πρέπει να είναι εξ αρχής ευνοϊκές για την προστασία των δεδομένων και ότι μόνο τα δεδομένα που είναι απαραίτητα για κάθε συγκεκριμένο σκοπό επεξεργασίας θα πρέπει να συγκεντρώνονται.
- Στο πλαίσιο του ΓΚΠΔ, μια εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) θα είναι υποχρεωτική προϋπόθεση προ-επεξεργασίας όταν τα προβλεπόμενα σχέδια/πρωτοβουλίες/υπηρεσίες περιλαμβάνουν επεξεργασία δεδομένων η οποία "είναι πιθανό να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων". Αυτό είναι ιδιαίτερα σημαντικό όταν εισάγεται στην επιχείρηση σας μια νέα τεχνολογία επεξεργασίας δεδομένων. Στις περιπτώσεις που δεν είναι σαφές κατά πόσον μια ΕΑΠΔ είναι αυστηρά υποχρεωτική, η εκτέλεση μιας ΕΑΠΔ εξακολουθεί να είναι η καλύτερη πρακτική και είναι ένα πολύ χρήσιμο εργαλείο για να βοηθήσει τους ελεγκτές δεδομένων να αποδείξουν τη συμμόρφωσή τους με τη νομοθεσία περί προστασίας δεδομένων. Η ΕΑΠΔ είναι επεκτάσιμη και μπορεί να λάβει διαφορετικές μορφές, αλλά ο ΓΚΠΔ καθορίζει τη βασική απαίτηση μιας αποτελεσματικής ΕΑΠΔ.
- Η διατήρηση ενός καταλόγου κινδύνων που αφορούν την προστασία δεδομένων μπορεί να σας επιτρέψει να προσδιορίσετε και να μετριάσετε τους που μπορεί να προκύψουν, καθώς και να σας βοηθήσει στο να αποδείξετε τη συμμόρφωση σας σε περίπτωση έρευνας ή ελέγχου από μια ρυθμιστική αρχή.

Η παρακάτω λίστα στοχεύει στο να βοηθήσει τις μικρομεσαίες επιχειρήσεις στην χαρτογράφηση των δεδομένων προσωπικού χαρακτήρα που κατέχουν και επεξεργάζονται αυτή τη στιγμή, τη νόμιμη βάση στην οποία συγκεντρώθηκαν τα δεδομένα, και την περίοδο διατήρησης για κάθε κατηγορία δεδομένων.

Η εκτέλεση αυτής της άσκησης θα βοηθήσει στον εντοπισμό των άμεσων διορθωτικών ενεργειών που απαιτούνται προκειμένου να είναι σύμφωνες με τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Αν σε οποιοδήποτε σημείο χρειαστείτε επιπλέον πληροφορίες για τον ΓΚΠΔ, μπορείτε να ανατρέξετε στις πηγές που βρίσκονται στην τελευταία σελίδα αυτού του εντύπου.

Κατηγορίες δεδομένων προσωπικού χαρακτήρα καθώς και κατηγορίες υποκειμένων των δεδομένων	Στοιχεία δεδομένων προσωπικού χαρακτήρα που εμπεριέχονται σε κάθε κατηγορία δεδομένων	Πηγή των δεδομένων προσωπικού χαρακτήρα	Σκοπούς για τους οποίους γίνεται επεξεργασία των δεδομένων προσωπικού χαρακτήρα	Νομική βάση για κάθε σκοπό επεξεργασίας (μη ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα)	Ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα	Νομική βάση για την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα	Περίοδος διατήρησης	Ενέργειες που απαιτούνται για την συμμόρφωση με τον ΓΚΠΔ
Καταγράψτε όλες τις κατηγορίες υποκειμένων στα οποία αναφέρονται τα δεδομένα και των δεδομένων προσωπικού χαρακτήρα που συλλέγονται και διατηρούνται *π.χ. δεδομένα των εργαζομένων, δεδομένα συνταξιούχων δεδομένα πελατών (πληροφορίες πωλήσεων). βάση δεδομένων μάρκετινγκ; βίντεο από κάμερες ασφαλείας (κλειστού κυκλώματος).*	*Καταγράψτε κάθε τύπο δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται σε κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα,* *π.χ. όνομα, διεύθυνση, στοιχεία τραπεζικού λογαριασμού, ιστορικό αγορών, ιστορικό διαδικτυακής περιήγησης, βίντεο και εικόνες.*	*Καταγράψτε την πηγή (ή πηγές) των δεδομένων προσωπικού χαρακτήρα.* *π.χ. συλλέχθηκαν απευθείας από τα ίδια τα άτομα ή από τρίτους (στην περίπτωση τρίτων θα πρέπει να αναφέρεται ο υπεύθυνος επεξεργασίας ως πηγή και να εκπληρώνονται οι υποχρεώσεις βάσει του άρθρου 14)*	*Μέσα σε κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα οι σκοποί των δεδομένων συλλέγονται και διατηρούνται* *π.χ.* • *μάρκετινγκ,* • *ενίσχυση υπηρεσιών,* • *έρευνα,* • *ανάπτυξη προϊόντων,* • *ακεραιότητα συστημάτων* • *θέματα ανθρώπινου δυναμικού,* • *διαφήμιση.*	*Για κάθε σκοπό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα καταγράφεται η νομική βάση στην οποία βασίζεται,* *π.χ. συγκατάθεση, σύμβαση, νομική υποχρέωση (άρθρο 6).*	*Εάν συλλέγονται και διατηρούνται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, καθορίζονται λεπτομέρειες σχετικά με τη φύση των δεδομένων,* *π.χ. την υγεία, τα γενετικά, βιομετρικά δεδομένα.*	*Καταγράψτε τη νομική βάση επί της οποίας συλλέγονται και διατηρούνται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα* *π.χ. ρητή συναίνεση, νομοθετική βάση (άρθρο 9).*	*Για κάθε κατηγορία δεδομένων προσωπικού χαρακτήρα, παρατίθεται η περίοδος για την οποία τα δεδομένα θα διατηρούνται* *(π.χ. ένα μήνα, ένα χρόνο)* *Κατά γενικό κανόνα, τα δεδομένα δεν πρέπει να διατηρούνται για χρονικό διάστημα πέρα του πλέον αναγκαίου για τον σκοπό για τον οποίο συλλέχθηκαν αρχικά.*	*Προσδιορίστε τις ενέργειες που απαιτούνται για να εξασφαλίσετε ότι όλες οι λειτουργίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα συμμορφώνονται με τον ΓΚΠΔ.* *π.χ. αυτό μπορεί να περιλαμβάνει τη διαγραφή στοιχείων όπου δεν υπάρχει κανένας λόγος για περεταίρω διατήρηση.*

Δεδομένα Προσωπικού Χαρακτήρα

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Επεξεργασία δεδομένων με βάση τη συναίνεση	Έχετε αξιολογήσει τους μηχανισμούς της επιχείρησής σας για τη συγκέντρωση συγκατάθεσης έτσι ώστε να εξασφαλιστεί ότι παρέχεται ελεύθερα, για συγκεκριμένο σκοπό, με επίγνωση και ότι είναι μια σαφή ένδειξη ότι ένα άτομο έχει επιλέξει να συμφωνήσει στην επεξεργασία των στοιχείων του μέσω της δήλωσης ή μιας σαφούς θετικής ενέργειας;			
	Εάν τα δεδομένα προσωπικού χαρακτήρα που διαθέτετε επί του παρόντος βάσει της συγκατάθεσης δεν πληρούν τα απαιτούμενα πρότυπα στο πλαίσιο του ΓΚΠΔ, αναζητάτε εκ νέου τη συγκατάθεση του ατόμου για να διασφαλίσετε τη συμμόρφωση με τον ΓΚΠΔ;			
	Υπάρχουν διαδικασίες που να αποδεικνύουν ότι ένα άτομο έχει συναινέσει στην επεξεργασία των δεδομένων του;			
	Υπάρχουν διαδικασίες που επιτρέπουν σε ένα άτομο να αποσύρει τη συναίνεσή του για την επεξεργασία των προσωπικών του δεδομένων;			
Δεδομένα προσωπικού χαρακτήρα παιδιών	Όταν παρέχονται διαδικτυακές υπηρεσίες σε ένα παιδί, υπάρχουν διαδικασίες για την επαλήθευση της ηλικίας και για την συγκατάθεση του γονέα/νόμιμου κηδεμόνα, όπου απαιτούνται;			
Επεξεργασία δεδομένων βάσει έννομου συμφέροντος	Εάν το έννομο συμφέρον αποτελεί νομική βάση για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα, διενεργήθηκε η κατάλληλη ανάλυση για να διασφαλιστεί ότι η χρήση αυτής της νομικής βάσης είναι ενδεδειγμένη; Η ανάλυση αυτή πρέπει να αποδεικνύει ότι: 1) υπάρχει βάσιμο έννομο συμφέρον, 2) η επεξεργασία των δεδομένων είναι απολύτως αναγκαία για την επίτευξη του θεμιτού συμφέροντος, και 3) η επεξεργασία δεν είναι επιζήμια ή παρακάμπτει τα δικαιώματα του ατόμου.			

Δικαιώματα προσώπων στα οποία αναφέρονται τα δεδομένα

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Πρόσβαση στα δεδομένα προσωπικού χαρακτήρα (άρθρο 15)	Υπάρχει τεκμηριωμένη πολιτική/διαδικασία για τον χειρισμό αιτημάτων πρόσβασης των υποκειμένων των δεδομένων;			
	Είναι η επιχείρηση σας σας σε θέση να ανταποκριθεί στο σε ένα τέτοιο αίτημα πρόσβασης μέσα σε ένα μήνα;			
Φορητότητα δεδομένων (άρθρο 20)	Υπάρχουν διαδικασίες που να παρέχουν στα άτομα τα δεδομένα προσωπικού χαρακτήρα τους σε μια δομημένη, ευρέως χρησιμοποιούμενη μηχαναγνώσιμη μορφή;			
Διαγραφή και διόρθωση (άρθρα 16 και 17)	Υπάρχουν έλεγχοι και διαδικασίες για να επιτραπεί η διαγραφή ή η διόρθωση των δεδομένων προσωπικού χαρακτήρα (κατά περίπτωση);			
Δικαίωμα περιορισμού της επεξεργασίας (άρθρο 18)	Υπάρχουν έλεγχοι και διαδικασίες για την ανάσχεση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όταν ένα άτομο έχει βάσιμους λόγους να επιδιώκει τον περιορισμό της επεξεργασίας;			

Δικαίωμα εναντίωσης στην επεξεργασία (άρθρο 21)	Ενημερώνονται τα άτομα σχετικά με το δικαίωμά τους να αντιτίθενται σε ορισμένα είδη επεξεργασίας, όπως το άμεσο μάρκετινγκ ή όταν η νομική βάση της επεξεργασίας είναι νόμιμα συμφέροντα ή είναι αναγκαία για ένα έργο που διεξάγεται προς το δημόσιο συμφέρον;			
	Υπάρχουν έλεγχοι και διαδικασίες για την ανάσχεση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα όταν ένα άτομο έχει αντιταχθεί στην επεξεργασία;			
Σκιαγράφηση και αυτοματοποιημένη επεξεργασία (άρθρο 22)	Εάν μια αυτοματοποιημένη λήψη αποφάσεων, η οποία έχει νομικό ή σημαντικό παρόμοιο αντίκτυπο για ένα άτομο, βασίζεται σε συγκατάθεση, κατά πόσο έχει συλλεχθεί ρητά αυτή η συγκατάθεση;			
	Όταν γίνεται αυτοματοποιημένη απόφαση η οποία είναι αναγκαία για τη σύναψη ή την εκτέλεση μιας σύμβασης, ή με βάση τη ρητή συγκατάθεση ενός ατόμου, υπάρχουν εγκατεστημένες διαδικασίες για τη διευκόλυνση του δικαιώματος του ατόμου να λάβει ανθρώπινη παρέμβαση και να αμφισβητήσει την απόφαση;			
Περιορισμοί στα δικαιώματα των υποθεμάτων δεδομένων (άρθρο 23)	Έχουν τεκμηριωθεί οι περιστάσεις στις οποίες τα δικαιώματα προστασίας δεδομένων ενός ατόμου μπορούν να περιοριστούν νομίμως;			

Ακρίβεια και διατήρηση

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Περιορισμός του σκοπού	Τα δεδομένα προσωπικού χαρακτήρα χρησιμοποιούνται μόνο για τους σκοπούς για τους οποίους είχαν αρχικά συλλεχθεί;			
Ελαχιστοποίηση δεδομένων	Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται περιορίζεται σε ό, τι είναι αναγκαίο για τους σκοπούς για τους οποίους γίνεται η επεξεργασία;			
Ακρίβεια	Οι διαδικασίες που εφαρμόζονται για την εξασφάλιση των δεδομένων προσωπικού χαρακτήρα είναι ενημερωμένες και ακριβείς και όπου απαιτείται διόρθωση, οι αναγκαίες αλλαγές γίνονται χωρίς καθυστέρηση;			
Διατήρηση	Υπάρχουν πολιτικές και διαδικασίες διατήρησης για να εξασφαλίζεται ότι τα δεδομένα δεν είναι πλέον αναγκαία για τους σκοπούς για τους οποίους συλλέχθηκαν;			
Άλλες νομικές υποχρεώσεις που διέπουν τη διατήρηση	Η επιχείρησή σας υπόκειται σε άλλους κανόνες που απαιτούν ελάχιστη περίοδο διατήρησης (π.χ. ιατρικά αρχεία/φορολογικά αρχεία);			
	Έχετε διαδικασίες για να διασφαλίσετε ότι τα δεδομένα καταστρέφονται με ασφάλεια, σύμφωνα με τις πολιτικές διατήρησης;			
Αλληλοεπικάλυψη εγγραφών	Υπάρχουν διαδικασίες που να διασφαλίζουν ότι δεν υπάρχει άσκοπη ή ανεξέλεγκτη αλληλοεπικάλυψη των εγγραφών;			

Απαιτήσεις διαφάνειας

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Διαφάνεια για τους πελάτες και τους εργαζόμενους (άρθρα 12, 13 και 14)	Είναι οι χρήστες/υπάλληλοι υπηρεσιών πλήρως ενημερωμένοι για το πώς χρησιμοποιείτε τα δεδομένα τους σε μια συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα;			
	Όταν τα δεδομένα προσωπικού χαρακτήρα συλλέγονται απευθείας από τα άτομα, υπάρχουν διαδικασίες για την παροχή των πληροφοριών που απαριθμούνται στο άρθρο 13 του ΓΚΠΔ;			
	Εάν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο αλλά από τρίτο (π.χ. αποκτηθείσα ως μέρος συγχώνευσης) υφίστανται διαδικασίες για την παροχή των πληροφοριών που απαριθμούνται στο άρθρο 14 του ΓΚΠΔ;			
	Κατά την επαφή με άτομα, όπως κατά την παροχή μιας υπηρεσίας, την πώληση ενός αγαθού ή παρακολούθησης κλειστού κυκλώματος, υφίστανται διαδικασίες για που να ενημερώνουν προληπτικά τα άτομα για τα δικαιώματα τους βάσει του ΓΚΠΔ;			
	Είναι πληροφορίες για το πώς η επιχείρηση σας διευκολύνει τα άτομα που ασκούν τα δικαιώματά τους βάσει του ΓΚΠΔ δημοσιευμένα σε μια εύκολα προσιτή και αναγνώσιμη μορφή;			

Λοιπές υποχρεώσεις των υπεύθυνων επεξεργασίας

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Συμφωνίες με προμηθευτές (άρθρα 27 έως 29)	Έχουν αναθεωρηθεί οι συμφωνίες με προμηθευτές και άλλους τρίτους που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό σας, ώστε να εξασφαλίζεται η συμπερίληψη όλων των κατάλληλων απαιτήσεων προστασίας δεδομένων;			
Υπεύθυνος Προστασίας Δεδομένων (DPO) (άρθρα 37 έως 39)	Χρειάζεται να διοριστεί ένας Υπεύθυνος Προστασίας Δεδομένων (DPO) σύμφωνα με το άρθρο 37 του ΓΚΠΔ;			
Διαβάστε τις κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων της ομάδας εργασίας του άρθρου 29: PDF (ελληνικά) Πηγή: EC/Article29 Newsroom	Εάν αποφασιστεί ότι δεν απαιτείται DPO, έχουν τεκμηριωθεί οι λόγοι για την απόφαση αυτή;			
	Όταν διορίζεται ένας DPO, και οι γραμμές ιεραρχίας και υποβολής αναφορών υφίστανται; Είναι τεκμηριωμένες αυτές οι διαδικασίες; Υπάρχουν εγκατεστημένες δομές ιεραρχίας και υποβολής αναφορών;			
	Έχετε δημοσιεύσει τα στοιχεία επικοινωνίας του DPO σας για να διευκολύνετε τους πελάτες ή/και υπαλλήλους σας να έρθουν σε επαφή του; *(Σημείωση: μετά τις 25 Μαΐου 2018 θα πρέπει επίσης να ανακοινώσετε στην αρχή προστασίας δεδομένων τα στοιχεία επικοινωνίας του DPO σας)*			
Εκτίμηση Αντίκτυπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ) (άρθρο 35)	Εάν η επεξεργασία των δεδομένων σας θεωρείται υψηλού κινδύνου, υφίσταται διαδικασία για τον προσδιορισμό της ανάγκης για - και τη διεξαγωγή της – Εκτίμησης Αντίκτυπου σχετικά με την Προστασία Δεδομένων (ΕΑΠΔ); Είναι τεκμηριωμένες αυτές οι διαδικασίες;			

Ασφάλεια δεδομένων

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Κατάλληλα τεχνικά και οργανωτικά μέτρα ασφαλείας (άρθρο 32)	Έχετε αξιολογήσει τους κινδύνους που εμπλέκονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα και έχετε εφαρμόσει μέτρα για τον περιορισμό τους;			
	Υπάρχει τεκμηριωμένο πρόγραμμα ασφαλείας που να προσδιορίζει τις τεχνικές, διοικητικές και φυσικές εγγυήσεις για τα δεδομένα προσωπικού χαρακτήρα;			
	Υπάρχει τεκμηριωμένη διαδικασία για την επίλυση των καταγγελιών και των ζητημάτων που σχετίζονται με την ασφάλεια;			
	Υπάρχει συγκεκριμένο άτομο που είναι υπεύθυνο για την πρόληψη και τη διερεύνηση παραβιάσεων ασφάλειας;			
	Χρησιμοποιούνται οι τυποποιημένες τεχνολογίες κρυπτογράφησης του κλάδου για τη μεταφορά, αποθήκευση και λήψη ευαίσθητων προσωπικών πληροφοριών των ατόμων;			
	Οι προσωπικές πληροφορίες καταστρέφονται συστηματικά, διαγράφονται ή καθίστανται ανώνυμες όταν δεν είναι πλέον νομικά απαιτούμενο να διατηρούνται;			
	Μπορεί η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα να αποκατασταθεί εγκαίρως σε περίπτωση φυσικού ή τεχνικού συμβάντος;			

Παραβιάσεις δεδομένων

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Υποχρεώσεις απόκρισης σε περίπτωση παραβίασης δεδομένων (άρθρο 33 και 34)	Η επιχείρηση σας διαθέτει τεκμηριωμένο σχέδιο απόκρισης σε περίπτωση παραβίασης απορρήτου και ασφάλειας;			
	Τα σχέδια και οι διαδικασίες εξετάζονται τακτικά;			
	Υπάρχουν διαδικασίες που να κοινοποιούν στο γραφείο του Επιτρόπου προστασίας δεδομένων μια παραβίαση δεδομένων;			
	Υπάρχουν διαδικασίες για την κοινοποίηση των υποκειμένων των δεδομένων σχετικά με την παραβίαση δεδομένων (κατά περίπτωση);			
	Όλες οι παραβιάσεις δεδομένων είναι πλήρως τεκμηριωμένες;			
	Υπάρχουν διαδικασίες συνεργασίας μεταξύ των ελεγκτών δεδομένων, των προμηθευτών και άλλων εταίρων για την αντιμετώπιση των παραβιάσεων δεδομένων;			

Διεθνείς μεταφορές δεδομένων (εκτός ΕΟΧ) – *αν ισχύει*

	Ερώτηση	Ναι	Όχι	Σχόλια / Διορθωτικά Μέτρα
Διεθνείς διαβιβάσεις δεδομένων (άρθρα 44 έως 50)	Διαβιβάζονται δεδομένα προσωπικού χαρακτήρα εκτός ΕΟΧ, π.χ. στις ΗΠΑ ή σε άλλες χώρες;			
	Αυτό περιλαμβάνει ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα;			
	Ποιος είναι ο σκοπός ή οι σκοποί της διαβίβασης;			
	Προς ποιον γίνεται η διαβίβαση;			
	Είναι όλες οι διαβιβάσεις καταγεγραμμένες - συμπεριλαμβανομένων των απαντήσεων στις προηγούμενες ερωτήσεις *(π.χ. η φύση των στοιχείων, ο σκοπός της επεξεργασίας, από ποια χώρα τα στοιχεία εξάγονται και ποια χώρα λαμβάνει τα στοιχεία και ποιος είναι ο αποδέκτης της μεταφοράς;)*			
Νομιμότητα διεθνών διαβιβάσεων	Υπάρχει νομική βάση για τη διαβίβαση, *(π.χ. απόφαση επάρκειας της Επιτροπής της ΕΕ, τυποποιημένες συμβατικές ρήτρες)*. Είναι τεκμηριωμένες αυτές οι βάσεις;			
Διαφάνεια	Έχουν ενημερωθεί πλήρως τα υποκείμενα των δεδομένων σχετικά με τις προβλεπόμενες διεθνείς διαβιβάσεις των προσωπικών τους δεδομένων;			

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Το περιεχόμενο που εμπεριέχεται σε αυτό τον οδηγό έχει προέλθει από τον ιστότοπο του γραφείου του Επιτρόπου Προστασίας Δεδομένων της Ιρλανδίας

Μάθετε περισσότερα στην ιστοσελίδα του Επιτρόπου Προστασίας Δεδομένων της Ιρλανδίας: www.dataprotection.ie (Αγγλικά)
Ακολουθήστε τον διαδραστικό οδηγό ενημέρωσης στον παρακάτω σύνδεσμο: http://gdprandyou.ie (Αγγλικά)

Μάθετε περισσότερα στην σελίδα της Ευρωπαϊκής Επιτροπής σχετικά με την μεταρρύθμιση των κανόνων προστασίας δεδομένων της ΕΕ στον σύνδεσμο: https://ec.europa.eu/info/law/law-topic/data-protection/reform_el
Ακολουθήστε τον διαδραστικό οδηγό ενημέρωσης της Ευρωπαϊκής Επιτροπής στον σύνδεσμο: http://ec.europa.eu/justice/smedataprotect/index_el.htm

Σας ενθαρρύνουμε να μελετήσετε τις παραπάνω πηγές για την καλύτερη ενημέρωση σας καθώς και τον ίδιο τον ΓΚΠΔ στον ιστότοπο της Ευρωπαϊκής Ένωσης.

Μπορείτε επίσης να δείτε τον οδηγό επιχειρήσεων για τον νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) της Π.Ο.Φ.Ε.Ε. κάνοντας κλικ εδώ

Αυτός ο οδηγός παρέχεται «ως έχει» για χρήση από το κοινό
Η Π.Ο.Φ.Ε.Ε. δεν φέρει καμία ευθύνη για τυχόν λάθη που μπορεί να εμπεριέχονται και για τις συνέπειες αυτών

Μπορείτε να αναδημοσιεύσετε ολόκληρο τον οδηγό ή μέρος αυτού (εξαιρούμενης της εμπορικής χρήσης) αναφέροντας τις πηγές: Πανελλήνια Ομοσπονδία Φοροτεχνικών Ελευθέρων Επαγγελματιών (Π.Ο.Φ.Ε.Ε.) και Office of the Data Protection Commissioner - Ireland

Για την πολιτική χρήσης πληροφοριών του ιστότοπου του Επιτρόπου Προστασίας Δεδομένων της Ιρλανδίας δείτε εδώ: http://gdprandyou.ie/terms-of-use/

επιμέλεια περιεχομένου για την Π.Ο.Φ.Ε.Ε.:
Θεόδωρος Κεντιστός - Ράννος

Πανελλήνια Ομοσπονδία Φοροτεχνικών Ελευθέρων Επαγγελματιών (Π.Ο.Φ.Ε.Ε.)
Διεύθυνση: Ιουλιανού 42-46, Αθήνα, ΤΚ 104 34 | τηλ.: 210.82.53.445 | φαξ: 210.82.53.446
site: www.pofee.gr | email(1): info @ pofee . gr | email(2): pofee @ otenet . gr