Π.Ο.Φ.Ε.Ε.

ΑΠΡΙΛΙΟΣ 2018

General Data Protection Regulation (GDPR)

Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ)

Μάθετε τι πρέπει να κάνει επιχείρηση σας για να συμμορφώνεται με τους κανόνες της ΕΕ για την προστασία των δεδομένων και πώς μπορείτε να βοηθήσετε τους πολίτες να ασκούν τα δικαιώματά τους σύμφωνα με τον κανονισμό.

Περιεχόμενα

Εφαρμογή του κανονισμού

Εισαγωγή

Ο Χάρτης των Θεμελιωδών Δικαιωμάτων της ΕΕ προβλέπει ότι οι πολίτες της ΕΕ έχουν το δικαίωμα προστασίας των προσωπικών τους δεδομένων.

Ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (Κανονισμός (ΕΕ) 2016/679) της Ευρωπαϊκής Ένωσης (ΕΕ), για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών, τέθηκε σε ισχύ στις 24 Μαΐου 2016 και **θα αρχίσει να εφαρμόζεται από τις 25 Μαΐου 2018.**

Ο κανονισμός αποκτά αυτομάτως δεσμευτικό χαρακτήρα σε όλη την ΕΕ από την ημερομηνία έναρξης ισχύος του και αντικαθιστά την παλαιότερη Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου.

Οι κανονισμοί της Ε.Ε. δεν απαιτούν εθνική νομοθεσία για την εφαρμογή τους, ωστόσο υπάρχει η δυνατότητα έκδοσης εφαρμοστικού νόμου, ο οποίος θα παρέχει ερμηνεία σε θέματα υλοποίησης του κανονισμού.

Σε τι εφαρμόζεται ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ);

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ), ρυθμίζει την επεξεργασία από **άτομο, εταιρεία ή οργανισμό** των **δεδομένων προσωπικού χαρακτήρα** που αφορούν **άτομα** στην ΕΕ.

Δεν υπάγεται σε αυτόν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποθανόντων προσώπων ή νομικών προσώπων.

Οι κανόνες δεν εφαρμόζονται σε δεδομένα που υποβάλλονται σε επεξεργασία από ένα άτομο για αυστηρά προσωπικούς λόγους ή για δραστηριότητες που διενεργούνται κατ' οίκον, υπό την προϋπόθεση ότι δεν συνδέονται με κάποια επαγγελματική ή εμπορική δραστηριότητα. Όταν ένα άτομο χρησιμοποιεί δεδομένα προσωπικού χαρακτήρα εκτός της ιδιωτικής σφαίρας, παραδείγματος χάρη για κοινωνικοπολιτιστικές ή χρηματοοικονομικές δραστηριότητες, τότε το δίκαιο περί προστασίας δεδομένων πρέπει να τηρείται.

Παραδείγματα

Πότε εφαρμόζεται ο κανονισμός: Μια εταιρεία με επαγγελματική εγκατάσταση στην ΕΕ παρέχει ταξιδιωτικές υπηρεσίες σε πελάτες που βρίσκονται στις χώρες της Βαλτικής και σε αυτό το πλαίσιο υποβάλλει σε επεξεργασία δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων.

Πότε δεν εφαρμόζεται ο κανονισμός: Ένα άτομο χρησιμοποιεί το ιδιωτικό του βιβλίο διευθύνσεων για να προσκαλέσει φίλους μέσω ηλεκτρονικού μηνύματος σε μια γιορτή που διοργανώνει (εξαίρεση οικιακών δραστηριοτήτων).

Σε ποιους εφαρμόζεται η νομοθεσία περί προστασίας των δεδομένων;

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) εφαρμόζεται:

α) σε κάθε εταιρεία ή οντότητα η οποία επεξεργάζεται δεδομένα προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων ενός από τα υποκαταστήματά της που έχουν έδρα στην ΕΕ, ανεξάρτητα από το πού γίνεται η επεξεργασία των δεδομένων ή

β) σε κάθε εταιρεία η οποία έχει έδρα εκτός της ΕΕ και προσφέρει αγαθά/υπηρεσίες (επί πληρωμή ή δωρεάν) ή παρακολουθεί τη συμπεριφορά φυσικών προσώπων στην ΕΕ.

Εάν η εταιρεία σας είναι μικρομεσαία επιχείρηση (ΜΜΕ) και επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, όπως περιγράφεται παραπάνω, πρέπει να συμμορφώνεστε με τον ΓΚΠΔ. Ωστόσο, εάν η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν αποτελεί βασικό μέρος της επιχειρηματικής σας δραστηριότητας και η δραστηριότητά σας δεν δημιουργεί κινδύνους για φυσικά πρόσωπα, τότε ορισμένες από τις υποχρεώσεις του ΓΚΠΔ δεν ισχύουν για εσάς [π.χ. ο διορισμός υπεύθυνου προστασίας δεδομένων (ΥΠΔ)]. Σημειώνεται ότι οι «βασικές δραστηριότητες» θα πρέπει να περιλαμβάνουν δραστηριότητες όπου η επεξεργασία δεδομένων αποτελεί αναπόσπαστο μέρος της δραστηριότητας του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Παραδείγματα:

Πότε εφαρμόζεται ο κανονισμός: Είστε μικρή εταιρεία τριτοβάθμιας εκπαίδευσης που δραστηριοποιείται στο διαδίκτυο με επαγγελματική εγκατάσταση που έχει έδρα εκτός της ΕΕ. Η εταιρεία σας απευθύνεται κυρίως σε ισπανόφωνα και πορτογαλόφωνα πανεπιστήμια στην ΕΕ. Προσφέρει δωρεάν συμβουλές σχετικά με διάφορα πανεπιστημιακά προγράμματα σπουδών, και οι φοιτητές χρειάζονται ένα όνομα χρήστη και έναν κωδικό πρόσβασης για να αποκτήσουν πρόσβαση στο υλικό σας στο διαδίκτυο. Η εταιρεία σας παρέχει το εν λόγω όνομα χρήστη και κωδικό πρόσβασης αφού οι φοιτητές συμπληρώσουν μια φόρμα εγγραφής.

Πότε δεν εφαρμόζεται ο κανονισμός: Η εταιρεία σας είναι πάροχος υπηρεσιών με έδρα εκτός της ΕΕ. Παρέχει υπηρεσίες σε πελάτες εκτός της ΕΕ. Οι πελάτες της μπορούν να χρησιμοποιούν τις υπηρεσίες της όταν ταξιδεύουν σε άλλες χώρες, συμπεριλαμβανομένης της ΕΕ. Εφόσον η εταιρεία σας δεν απευθύνει ειδικά τις υπηρεσίες της σε φυσικά πρόσωπα στην ΕΕ, δεν υπόκειται στους κανόνες του ΓΚΠΔ.

Οι κανόνες ισχύουν για τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) ;

Ναι, η **εφαρμογή του κανονισμού για την προστασία των δεδομένων δεν εξαρτάται από το μέγεθος της εταιρείας ή του οργανισμού σας αλλά από τη φύση των δραστηριοτήτων σας.** Οι δραστηριότητες που ενέχουν υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, είτε πραγματοποιούνται από μια ΜΜΕ είτε από μια μεγάλη επιχείρηση, συνεπάγονται την εφαρμογή πιο αυστηρών κανόνων. Ωστόσο, μερικές από τις υποχρεώσεις του ΓΚΠΔ μπορεί να μην εφαρμόζονται σε όλες τις ΜΜΕ.

Για παράδειγμα, εταιρείες που **απασχολούν λιγότερους από 250 εργαζομένους δεν χρειάζεται να τηρούν αρχεία** των δραστηριοτήτων επεξεργασίας εκτός εάν η επεξεργασία δεδομένων προσωπικού χαρακτήρα αποτελεί τακτική δραστηριότητα, ενέχει κινδύνους για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων ή αφορά ευαίσθητα δεδομένα ή ποινικά μητρώα.

Παρομοίως, οι ΜΜΕ θα πρέπει να διορίσουν έναν υπεύθυνο προστασίας δεδομένων μόνο εάν η επεξεργασία συνιστά την κύρια επιχειρηματική τους δραστηριότητα και ενέχει συγκεκριμένους κινδύνους για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων (όπως η παρακολούθηση φυσικών προσώπων ή η επεξεργασία ευαίσθητων δεδομένων ή ποινικών μητρώων), ιδίως επειδή πραγματοποιείται σε μεγάλη κλίμακα.

Τήρηση αρχείων

Οι μικρομεσαίες επιχειρήσεις πρέπει να τηρούν αρχεία αν η επεξεργασία δεδομένων:

- Είναι τακτική
- Αποτελεί απειλή για τα δικαιώματα και τις ελευθερίες των ατόμων
- Αφορά ευαίσθητα δεδομένα ή ποινικό μητρώο

Τα αρχεία θα πρέπει να περιλαμβάνουν:

- Επωνυμία και στοιχεία επικοινωνίας της επιχείρησης
- Τους λόγους για την επεξεργασία των δεδομένων
- Περιγραφή των κατηγοριών των υποκειμένων των δεδομένων και των προσωπικών δεδομένων
- Κατηγορίες των οργανισμών που λαμβάνουν τα δεδομένα
- Διαβίβαση δεδομένων σε άλλη χώρα ή οργανισμό
- Προθεσμία για αφαίρεση δεδομένων, εάν είναι δυνατό
- Περιγραφή των μέτρων ασφαλείας που χρησιμοποιούνται κατά την επεξεργασία, εάν είναι δυνατό

Ελέγξτε αν χρειάζεστε έναν υπεύθυνο για την προστασία των δεδομένων

Αυτό δεν είναι πάντα υποχρεωτικό. Εξαρτάται από τον τύπο και τον αριθμό των δεδομένων που συλλέγετε, αν η επεξεργασία είναι η κύρια επιχειρηματική σας δραστηριότητα και αν το κάνετε σε μεγάλη κλίμακα.

Παραδείγματα:

Επεξεργάζεστε προσωπικά δεδομένα για να εξατομικεύσετε τις διαφημίσεις μέσω μηχανών αναζήτησης με βάση τη συμπεριφορά των ατόμων στο διαδίκτυο.	*ΝΑΙ*
Αποστέλλετε στους πελάτες σας μια διαφήμιση μια φορά τον χρόνο για να προωθήσετε την τοπική επιχείρηση τροφίμων που διαθέτετε.	*ΟΧΙ*
Είστε γιατρός και συλλέγετε δεδομένα για την υγεία των ασθενών σας.	*ΟΧΙ*
Επεξεργάζεστε προσωπικά δεδομένα σχετικά με τη γενετική και την υγεία για ένα νοσοκομείο.	*ΝΑΙ*

(αναλυτικά για το συγκεκριμένο θέμα μπορείτε να δείτε στην ενότητα Υπεύθυνοι προστασίας δεδομένων (ΥΠΔ)

Τι αποτελεί 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:

- 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 παρακαλούμε 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.*

Ισχύουν οι κανόνες προστασίας δεδομένων για τα δεδομένα εταιρείας;

Όχι, οι κανόνες ισχύουν μόνο για τα δεδομένα προσωπικού χαρακτήρα φυσικών προσώπων, δεν διέπουν τα δεδομένα που αφορούν εταιρείες ή άλλες νομικές οντότητες. Ωστόσο, πληροφορίες που σχετίζονται με μονοπρόσωπες εταιρείες μπορεί να αποτελούν δεδομένα προσωπικού χαρακτήρα όταν καθιστούν δυνατή την ταυτοποίηση ενός φυσικού προσώπου. Οι κανόνες ισχύουν επίσης για όλα τα δεδομένα προσωπικού χαρακτήρα που σχετίζονται με φυσικά πρόσωπα κατά τη διάρκεια επαγγελματικής δραστηριότητας, όπως είναι, π.χ., οι εργαζόμενοι μιας εταιρείας/ενός οργανισμού, οι διευθύνσεις ηλεκτρονικού ταχυδρομείου επιχείρησης του τύπου «όνομα.επώνυμο@εταιρεία.eu» ή οι επαγγελματικοί αριθμοί τηλεφώνου εργαζομένων.

Τι είναι τα δεδομένα προσωπικού χαρακτήρα;

Τα δεδομένα προσωπικού χαρακτήρα είναι πληροφορίες που αφορούν ένα **ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή άτομο**. Διαφορετικές πληροφορίες οι οποίες, εάν συγκεντρωθούν όλες μαζί, μπορούν να οδηγήσουν στην ταυτοποίηση ενός συγκεκριμένου ατόμου, αποτελούν επίσης δεδομένα προσωπικού χαρακτήρα.

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.

Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταστεί **ανώνυμα** με τέτοιον τρόπο ώστε το άτομο να μην είναι ή να μην είναι πια ταυτοποιήσιμο δεν θεωρούνται πλέον δεδομένα προσωπικού χαρακτήρα. Για να είναι πραγματικά ανώνυμα τα δεδομένα, η ανωνυμοποίηση πρέπει να είναι μη αντιστρέψιμη.

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:

- *όνομα και επώνυμο*
- *διεύθυνση κατοικίας*
- *ηλεκτρονική διεύθυνση ταχυδρομείου, π.χ. όνομα.επώνυμο@εταιρεία.com*
- *αριθμός εγγράφου ταυτοποίησης (π.χ. αριθμός ταυτότητας, διαβατηρίου, διπλώματος οδήγησης, κ.λπ.)*
- *δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο*)*
- *διεύθυνση διαδικτυακού πρωτοκόλλου (IP address)*
- *αναγνωριστικό διαδικτυακής περιήγησης (π.χ. cookie*)*
- *το αναγνωριστικό διαφήμισης του τηλεφώνου σας*
- *δεδομένα που φυλάσσονται από νοσοκομείο ή γιατρό, που θα μπορούσαν να είναι ένα σύμβολο που προσδιορίζει 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)].*

Παραδείγματα δεδομένων που δεν θεωρούνται δεδομένα προσωπικού χαρακτήρα:

- *αριθμός μητρώου εταιρίας*
- *ηλεκτρονική διεύθυνση του τύπου info@εταιρία.com*
- *ανώνυμα δεδομένα (όπως π.χ. σε μια ανώνυμη έρευνα αγοράς)*

Τι πρέπει να κάνει η εταιρία σας;

Επικοινωνία

Χρησιμοποιήστε απλή γλώσσα. Πείτε τους **ποιοι** είστε όταν ζητάτε τα δεδομένα. Πείτε **τον λόγο** που επεξεργάζεστε τα δεδομένα τους, **για πόσο** καιρό θα τα φυλάξετε και **ποιος** τα λαμβάνει.

Πρόσβαση και δυνατότητα μεταφοράς

Δώστε στα άτομα πρόσβαση στα δεδομένα τους και επιτρέψτε τους να τα δώσουν σε άλλη εταιρεία.

Διαγραφή δεδομένων

Δώστε τους το «δικαίωμα στη λήθη». Διαγράψτε τα προσωπικά τους δεδομένα αν το ζητήσουν, αλλά μόνο αν δεν θίγεται η ελευθερία έκφρασης ή η δυνατότητα διεξαγωγής έρευνας.

Μάρκετινγκ

Δώστε στα άτομα το δικαίωμα να εξαιρεθούν από πρακτικές άμεσου μάρκετινγκ που χρησιμοποιούν τα δεδομένα τους.

Διαβίβαση δεδομένων εκτός της ΕΕ

Συνάψτε νομικές συμφωνίες όταν διαβιβάζετε δεδομένα σε χώρες που δεν έχουν λάβει έγκριση από τις αρχές της ΕΕ.

Συγκατάθεση

Λάβετε τη ρητή συγκατάθεσή τους για την επεξεργασία των δεδομένων.[1]

(βλ. ενότητα: πως θα πρέπει να ζητείται η συγκατάθεση μου)

Προειδοποιήσεις

Ενημερώστε τα άτομα σχετικά με παραβιάσεις δεδομένων αν ενέχει σοβαρός κίνδυνος για αυτούς.

Δημιουργία προφίλ

Αν χρησιμοποιείτε προφίλ για την επεξεργασία αιτήσεων για νομικά δεσμευτικές συμφωνίες, για παράδειγμα για δάνεια, πρέπει:

- Να ενημερώνετε τους πελάτες σας
- Να ορίζετε ένα πρόσωπο και όχι μια μηχανή να ελέγχει τη διαδικασία αν η αίτηση τελικά απορρίπτεται
- Να χορηγείτε στον αιτούντα το δικαίωμα να προσβάλλει την απόφαση.

Προστασία ευαίσθητων δεδομένων

Χρησιμοποιήστε πρόσθετα μέτρα προστασίας για πληροφορίες που αφορούν την υγεία, τη φυλή, τον σεξουαλικό προσανατολισμό, τη θρησκεία και τις πολιτικές πεποιθήσεις.

Μεριμνήστε για την προστασία των δεδομένων από τον σχεδιασμό. Αναπτύξτε μέτρα προστασίας στα προϊόντα και τις υπηρεσίες σας από τα πρώιμα στάδια ανάπτυξης.

Αν η επεξεργασία των δεδομένων γίνεται για λογαριασμό άλλης εταιρίας, σιγουρευτείτε ότι έχετε συνάψει μια δεσμευτική σύμβαση η οποία θα απαριθμεί τις ευθύνες κάθε συμβαλλόμενου μέρους.

[1] Αν συλλέγετε δεδομένα από παιδιά για τα μέσα κοινωνικής δικτύωσης, ελέγξτε το όριο ηλικίας για τη συγκατάθεση των γονιών.

Αρχές του ΓΚΠΔ

Ποια δεδομένα μπορούν να υποβληθούν σε επεξεργασία και υπό ποιες προϋποθέσεις;

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: *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.*

Σκοπός της επεξεργασίας δεδομένων

Μπορούν να υποβληθούν δεδομένα σε επεξεργασία για οποιονδήποτε σκοπό;

Ο σκοπός της επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να είναι γνωστός και να ενημερώνονται γι' αυτόν τα άτομα στα οποία αναφέρονται τα δεδομένα. Δεν αρκεί να επισημαίνεται απλώς ότι θα συλλέγονται και θα υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα. Αυτή η αρχή είναι γνωστή ως «περιορισμός του σκοπού».

Μπορούν να χρησιμοποιηθούν δεδομένα για άλλον σκοπό;

Ναι, αλλά μόνο σε μερικές περιπτώσεις. Εάν η εταιρεία ή ο οργανισμός σας έχει συλλέξει δεδομένα με βάση **έννομο συμφέρον**, **σύμβαση** ή **ζωτικά συμφέροντα,** μπορεί να τα χρησιμοποιήσει για άλλον σκοπό αλλά μόνο αφού ελέγξει ότι **ο νέος σκοπός είναι συμβατός με τον αρχικό σκοπό**.

Στο πλαίσιο αυτό, πρέπει να λαμβάνονται υπόψη τα εξής:

- η σύνδεση μεταξύ του αρχικού και του νέου/μελλοντικού σκοπού
- το πλαίσιο στο οποίο συλλέχθηκαν τα δεδομένα (ποια είναι η σχέση μεταξύ της εταιρείας ή του οργανισμού σας και του φυσικού προσώπου;)
- το είδος και η φύση των δεδομένων (είναι ευαίσθητα;)
- οι ενδεχόμενες συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας (πώς θα επηρεάσει το άτομο;)
- η ύπαρξη κατάλληλων εγγυήσεων (όπως η κρυπτογράφηση ή η ψευδωνυμοποίηση).

Εάν η εταιρεία ή ο οργανισμός σας θέλει να χρησιμοποιήσει τα δεδομένα για στατιστικούς σκοπούς ή για επιστημονική έρευνα, δεν απαιτείται έλεγχος συμβατότητας.

Εάν η εταιρεία ή ο οργανισμός σας έχει συλλέξει τα δεδομένα βάσει **συγκατάθεσης ή σύμφωνα με νομική υποχρέωση**, δεν είναι δυνατή περαιτέρω επεξεργασία πέραν των σκοπών που καλύπτονται από την αρχική συγκατάθεση ή τις διατάξεις της νομοθεσίας. Τυχόν περαιτέρω επεξεργασία απαιτεί τη λήψη νέας συγκατάθεσης ή νέα νομική βάση.

Παραδείγματα

Η περαιτέρω επεξεργασία είναι δυνατή: *Μια τράπεζα έχει σύμβαση με έναν πελάτη για να του παρέχει τραπεζικό λογαριασμό και προσωπικό δάνειο. Στο τέλος του πρώτου έτους η τράπεζα χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα του πελάτη για να ελέγξει εάν είναι επιλέξιμος για καλύτερο είδος δανείου και πρόγραμμα αποταμίευσης. Ενημερώνει σχετικά τον πελάτη. Η τράπεζα μπορεί να επεξεργαστεί τα δεδομένα του πελάτη ξανά καθώς οι νέοι σκοποί είναι συμβατοί με τους αρχικούς.*

Η περαιτέρω επεξεργασία δεν είναι δυνατή: *Η ίδια τράπεζα επιθυμεί να κοινοποιήσει τα δεδομένα του πελάτη σε ασφαλιστικές εταιρείες, με βάση την ίδια σύμβαση για τραπεζικό λογαριασμό και προσωπικό δάνειο. Αυτή η επεξεργασία δεν επιτρέπεται χωρίς τη ρητή συγκατάθεση του πελάτη, καθώς ο σκοπός δεν είναι συμβατός με τον αρχικό σκοπό επεξεργασίας των δεδομένων.*

Πόσα δεδομένα μπορούν να συλλεχθούν;

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: Η εταιρεία ή ο οργανισμός σας προσφέρει υπηρεσίες κοινής χρήσης αυτοκινήτων σε φυσικά πρόσωπα. Για τις εν λόγω υπηρεσίες επιτρέπεται να ζητά το ονοματεπώνυμο, τη διεύθυνση και τον αριθμό πιστωτικής κάρτας των πελατών και, ενδεχομένως, ακόμα και πληροφορίες σχετικά με το εάν το άτομο πάσχει από κάποια αναπηρία (με άλλα λόγια, δεδομένα υγείας), αλλά όχι τη φυλετική καταγωγή.

Για ποιο χρονικό διάστημα μπορούν να φυλάσσονται δεδομένα και είναι υποχρεωτικό να ενημερώνονται;

Τα δεδομένα πρέπει να αποθηκεύονται για την **ελάχιστη δυνατή περίοδο**. Η εν λόγω περίοδος θα πρέπει να λαμβάνει υπόψη τους λόγους για τους οποίους η εταιρεία ή ο οργανισμός σας χρειάζεται να επεξεργαστεί τα δεδομένα, καθώς και τυχόν νομικές υποχρεώσεις για τη φύλαξη των δεδομένων για συγκεκριμένη χρονική περίοδο (π.χ. εθνικό εργατικό δίκαιο, φορολογικό δίκαιο, νομοθεσία για την καταπολέμηση της απάτης που απαιτεί να τηρείτε δεδομένα προσωπικού χαρακτήρα για τους εργαζομένους σας για μια συγκεκριμένη περίοδο, διάρκεια εγγύησης προϊόντος κ.λπ.).

Η εταιρεία ή ο οργανισμός σας πρέπει να θεσπίζει **προθεσμίες** για τη **διαγραφή ή την επανεξέταση** των δεδομένων που έχουν αποθηκευτεί.

Κατ' εξαίρεση, μπορείτε να φυλάσσετε δεδομένα προσωπικού χαρακτήρα για μεγαλύτερη περίοδο για σκοπούς αρχειοθέτησης για το δημόσιο συμφέρον ή με σκοπό επιστημονική ή ιστορική έρευνα, αρκεί να θεσπίζονται κατάλληλα τεχνικά και οργανωτικά μέτρα (π.χ. ανωνυμοποίηση, κρυπτογράφηση κ.λπ.).

Επίσης, η εταιρεία ή ο οργανισμός σας πρέπει να διασφαλίζει ότι τα δεδομένα που φυλάσσει είναι ακριβή και ενημερωμένα.

Παράδειγμα: Δεδομένα φυλάσσονται για υπερβολικά μεγάλο χρονικό διάστημα χωρίς να ενημερωθούν

Η εταιρεία ή ο οργανισμός σας εκμεταλλεύεται ένα γραφείο εύρεσης εργασίας και για αυτόν τον σκοπό συλλέγει βιογραφικά ατόμων που ζητούν απασχόληση και τα οποία, ως αντάλλαγμα για τις παρεχόμενες υπηρεσίες μεσάζοντα, σας καταβάλλουν αμοιβή. Προγραμματίζετε να φυλάξετε τα δεδομένα για 20 χρόνια και δεν λαμβάνετε μέτρα για την ενημέρωση των βιογραφικών. Η περίοδος αποθήκευσης δεν φαίνεται ανάλογη με τον σκοπό εύρεσης εργασίας για ένα άτομο σε βραχυπρόθεσμο με μεσοπρόθεσμο ορίζοντα. Επιπλέον, το γεγονός ότι δεν ζητάτε να ενημερώνονται τα βιογραφικά ανά τακτά διαστήματα καθιστά ορισμένες από τις αναζητήσεις άσκοπες για το άτομο που αναζητά απασχόληση έπειτα από μια συγκεκριμένη χρονική περίοδο (για παράδειγμα επειδή το άτομο έχει αποκτήσει νέα προσόντα).

Τι πληροφορίες πρέπει να παρέχονται στα άτομα των οποίων δεδομένα συλλέγονται;

Τη στιγμή της συλλογής δεδομένων, πρέπει να παρέχονται με σαφήνεια στα άτομα πληροφορίες οπωσδήποτε για τα εξής:

- **ποια είναι** η εταιρεία ή ο οργανισμός σας (τα στοιχεία επικοινωνίας σας και τα στοιχεία του ΥΠΔ, εάν υπάρχει)
- **τον λόγο** για τον οποίο θα χρησιμοποιηθούν τα παρεχόμενα δεδομένα προσωπικού χαρακτήρα (σκοποί)
- τις κατηγορίες των σχετικών δεδομένων προσωπικού χαρακτήρα
- τη **νομική αιτιολόγηση** για την επεξεργασία των δεδομένων των ατόμων
- το **χρονικό διάστημα** για το οποίο θα φυλαχθούν τα δεδομένα
- **ποιοι άλλοι** μπορεί να τα λάβουν
- εάν τα δεδομένα τους προσωπικού χαρακτήρα θα **διαβιβαστούν** σε αποδέκτη εκτός της ΕΕ
- ότι τα άτομα έχουν δικαίωμα να λάβουν **αντίγραφο των δεδομένων** (δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα) και άλλα **βασικά δικαιώματα** στον τομέα της προστασίας δεδομένων (βλ. ενότητα δικαιώματα για τους πολίτες)
- το **δικαίωμα υποβολής καταγγελίας** ενώπιον αρχής προστασίας δεδομένων (ΑΠΔ)
- το **δικαίωμα ανάκλησης της συγκατάθεσής** τους οποιαδήποτε στιγμή
- ενδεχομένως, την ύπαρξη **αυτοματοποιημένης λήψης αποφάσεων** και τη λογική αυτής, συμπεριλαμβανομένων των σχετικών συνεπειών.

Δείτε τον πλήρη κατάλογο πληροφοριών που πρέπει να παρέχονται.

Αυτές οι πληροφορίες μπορούν να παρέχονται **γραπτά ή προφορικά** κατόπιν αιτήματος του φυσικού προσώπου όταν η ταυτότητά του αποδεικνύεται με άλλα μέσα ή με ηλεκτρονικά μέσα στις κατάλληλες περιπτώσεις. Αυτό πρέπει να γίνεται με **συνοπτικό, διαφανή, κατανοητό και εύκολα προσβάσιμο τρόπο**, σε **σαφή και απλή γλώσσα** και **δωρεάν**.

Όταν λαμβάνονται δεδομένα από άλλη εταιρεία/οργανισμό, η εταιρεία ή ο οργανισμός σας πρέπει να παρέχει τις ως άνω απαριθμούμενες πληροφορίες στο οικείο άτομο το αργότερο εντός ενός μηνός από τη στιγμή της λήψης των δεδομένων προσωπικού χαρακτήρα ή, εάν η εταιρεία ή ο οργανισμός σας επικοινωνήσει με το άτομο, όταν τα δεδομένα χρησιμοποιηθούν με σκοπό την επικοινωνία , ή, εάν προβλέπεται γνωστοποίηση σε άλλη εταιρεία, όταν τα δεδομένα προσωπικού χαρακτήρα γνωστοποιούνται για πρώτη φορά.

Η εταιρεία ή ο οργανισμός σας υποχρεούται επίσης να ενημερώνει το άτομο σχετικά με τις κατηγορίες δεδομένων και την πηγή από όπου τα απέκτησε, περιλαμβανομένου του κατά πόσον τα δεδομένα προέρχονται από δημόσια προσβάσιμες πηγές. Σε ορισμένες ειδικές περιπτώσεις που αναφέρονται στο άρθρο 13 παράγραφος 4 και στο άρθρο 14 παράγραφος 5 του ΓΚΠΔ, η εταιρεία ή ο οργανισμός σας μπορεί να εξαιρείται από την υποχρέωση ενημέρωσης του φυσικού προσώπου. Παρακαλούμε να ελέγξετε αν η εταιρεία ή ο οργανισμός σας εμπίπτει σε κάποιες από αυτές τις περιπτώσεις.

Νομικοί λόγοι επεξεργασίας δεδομένων

Λόγοι επεξεργασίας

Πότε μπορούν να υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα;

Η εταιρεία ή ο οργανισμός σας μπορεί να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα μόνο στις ακόλουθες περιπτώσεις:

- με τη **συγκατάθεση** των οικείων ατόμων
- εάν υπάρχει **συμβατική υποχρέωση** (σύμβαση ανάμεσα στην εταιρεία ή τον οργανισμό σας και έναν πελάτη)
- για την εκπλήρωση **νομικής υποχρέωσης** (σύμφωνα με τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία)
- όταν η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το **δημόσιο συμφέρον** (σύμφωνα με τη νομοθεσία της ΕΕ ή την εθνική νομοθεσία)
- για την προστασία των **ζωτικών συμφερόντων** ενός ατόμου
- προς χάριν των **έννομων συμφερόντων** του οργανισμού σας, αλλά μόνο αφού ελέγξετε ότι τα θεμελιώδη δικαιώματα και οι ελευθερίες του ατόμου του οποίου δεδομένα επεξεργάζεστε δεν επηρεάζονται σοβαρά. Εάν τα δικαιώματα του ατόμου υπερισχύουν των συμφερόντων σας, τότε δεν επιτρέπεται επεξεργασία με βάση έννομο συμφέρον. Η αξιολόγηση σχετικά με το εάν τα έννομα συμφέροντα της εταιρείας ή του οργανισμού σας για επεξεργασία υπερισχύουν των συμφερόντων των οικείων ατόμων εξαρτάται από τις ιδιαίτερες περιστάσεις κάθε περίπτωσης.

Παραδείγματα

Συγκατάθεση: *Η εταιρεία ή ο οργανισμός σας προσφέρει μια μουσική εφαρμογή και ζητάτε τη συγκατάθεση των πολιτών για να επεξεργαστείτε τις μουσικές τους προτιμήσεις έτσι ώστε να τους προτείνετε ειδικά επιλεγμένα τραγούδια και πιθανές συναυλίες.*

Συμβατική υποχρέωση: *Η εταιρεία ή ο οργανισμός σας πουλά αγαθά στο διαδίκτυο. Μπορεί να επεξεργάζεται δεδομένα που είναι απαραίτητα για ορισμένες ενέργειες κατόπιν αιτήματος του ατόμου πριν από τη σύναψη της σύμβασης και για την εκτέλεση της σύμβασης. Έτσι μπορείτε να επεξεργαστείτε το ονοματεπώνυμο, τη διεύθυνση παράδοσης, τον αριθμό πιστωτικής κάρτας (εάν η πληρωμή γίνεται με κάρτα) κ.λπ.*

Νομική υποχρέωση: *Είστε ο ιδιοκτήτης μιας εταιρείας που απασχολεί εργαζομένους. Για τη λήψη κάλυψης κοινωνικής ασφάλισης, η νομοθεσία σάς υποχρεώνει να παρέχετε δεδομένα προσωπικού χαρακτήρα (π.χ. εβδομαδιαίο εισόδημα των εργαζομένων σας) στη σχετική αρχή.*

Δημόσιο συμφέρον: *Παράδειγμα: μια επαγγελματική ένωση, π.χ. ένας δικηγορικός σύλλογος ή μια ένωση επαγγελματιών υγείας, μπορεί, σύμφωνα με δημόσια εξουσία που της έχει ανατεθεί, να κινήσει πειθαρχικές διαδικασίες εναντίον κάποιων εκ των μελών της.*

Ζωτικά συμφέροντα ενός ατόμου: *Ένα νοσοκομείο περιθάλπει έναν ασθενή μετά από ένα σοβαρό τροχαίο ατύχημα το νοσοκομείο δεν χρειάζεται τη συγκατάθεσή του για να ψάξει την ταυτότητά του έτσι ώστε να ελέγξει εάν το εν λόγω άτομο συμπεριλαμβάνεται στη βάση δεδομένων του νοσοκομείου για να βρει το ιατρικό ιστορικό του ή να επικοινωνήσει με τους συγγενείς του.*

Τα έννομα συμφέροντα του οργανισμού σας: *Η εταιρεία ή ο οργανισμός σας διασφαλίζει την ασφάλεια του δικτύου που χρησιμοποιεί μέσω της παρακολούθησης της χρήσης των συσκευών τεχνολογίας πληροφοριών των εργαζομένων. Μπορεί να επεξεργάζεται νομίμως δεδομένα προσωπικού χαρακτήρα για αυτόν τον σκοπό μόνο εάν επιλέξει τη λιγότερο επεμβατική μέθοδο όσον αφορά τα δικαιώματα προστασίας της ιδιωτικής ζωής και των δεδομένων των εργαζομένων σας, για παράδειγμα, περιορίζοντας την πρόσβαση σε ορισμένους ιστότοπους. (Σημειωτέον ότι αυτό δεν μπορεί να γίνει σε κράτη μέλη της ΕΕ όπου η εθνική νομοθεσία ορίζει αυστηρότερους κανόνες για την επεξεργασία στο πλαίσιο της απασχόλησης).*

Σε τι αναφέρεται ο όρος «λόγοι έννομου συμφέροντος»;

Ως εταιρεία/οργανισμός, συχνά χρειάζεται να επεξεργαστείτε δεδομένα προσωπικού χαρακτήρα για να εκτελέσετε εργασίες που σχετίζονται με τις επιχειρηματικές σας δραστηριότητες. Η επεξεργασία των δεδομένων προσωπικού χαρακτήρα σε αυτό το πλαίσιο μπορεί να μη δικαιολογείται απαραίτητα από νομική υποχρέωση ή να μην πραγματοποιείται για την εκτέλεση των όρων σύμβασης με φυσικό πρόσωπο. Σε τέτοιες περιπτώσεις, η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε να βασισθεί σε λόγους έννομου συμφέροντος.

Η εταιρεία ή ο οργανισμός σας οφείλει να ενημερώνει τα άτομα σχετικά με την επεξεργασία κατά τον χρόνο λήψης των προσωπικών τους δεδομένων.

Η εταιρεία ή ο οργανισμός σας πρέπει επίσης να ελέγξει ότι η επιδίωξη των έννομων συμφερόντων της/του δεν έχει σοβαρό αντίκτυπο στα δικαιώματα και τις ελευθερίες των σχετικών ατόμων σε διαφορετική περίπτωση, η εταιρεία ή ο οργανισμός σας δεν μπορεί να βασισθεί σε λόγους έννομου συμφέροντος για να δικαιολογήσει την επεξεργασία των δεδομένων και πρέπει να βρει άλλον νομικό λόγο.

Παράδειγμα: *Η εταιρεία ή ο οργανισμός σας έχει έννομο συμφέρον όταν η επεξεργασία πραγματοποιείται στο πλαίσιο πελατειακής σχέσης, όταν επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης, για την πρόληψη απάτης ή για τη διασφάλιση της ασφάλειας του δικτύου και των πληροφοριών των συστημάτων τεχνολογίας πληροφοριών που χρησιμοποιεί.*

Μπορεί συγκατάθεση δοθείσα πριν από τις 25 Μαΐου 2018 να παραμείνει έγκυρη αφού τεθεί σε ισχύ ο ΓΚΠΔ κατά την ίδια ημερομηνία;

Εάν συγκατάθεση που παραχωρήθηκε από ένα άτομο πριν από τη θέση σε εφαρμογή του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ) είναι σύμφωνη με τις προϋποθέσεις του ΓΚΠΔ, τότε δεν υπάρχει λόγος να ζητηθεί και πάλι η συγκατάθεση του ατόμου. Η εταιρεία ή ο οργανισμός σας πρέπει να βεβαιωθεί ότι η συγκατάθεση που παραχωρήθηκε πριν από τον ΓΚΠΔ πληροί τις προϋποθέσεις που καθορίζονται σε αυτόν.

Παραδείγματα

Δεν χρειάζεται νέα συγκατάθεση: *Ο ΓΚΠΔ θα τεθεί σε εφαρμογή στις 25 Μαΐου 2018. Αναθεωρήσατε πρόσφατα την πολιτική ιδιωτικού απορρήτου της εταιρείας ή του οργανισμού σας. Ελέγξατε ότι η συγκατάθεση στους κόλπους της εταιρείας ή του οργανισμού ελήφθη γραπτώς και συμμορφώνεται με όλες τις απαιτήσεις του ΓΚΠΔ. Σε αυτήν την περίπτωση, δεν χρειάζεται να ζητήσετε από τους πελάτες σας ξανά τη συγκατάθεσή τους τον Μάιο του 2018.*

Χρειάζεται να δοθεί ξανά συγκατάθεση: *Η εταιρεία ή ο οργανισμός σας έλαβε συγκατάθεση από πελάτες πριν από χρόνια χρησιμοποιώντας ένα σύστημα που περιελάβανε προεπιλεγμένα πλαίσια στο διαδίκτυο. Είναι τώρα σαφές ότι ο εν λόγω τρόπος λήψης συγκατάθεσης δεν θα είναι έγκυρος από τις 25 Μαΐου 2018. Η εταιρεία ή ο οργανισμός σας θα πρέπει να λάβει νέα συγκατάθεση εάν επιθυμεί να συνεχίσει να επεξεργάζεται τα δεδομένα.*

Τι γίνεται αν κάποιος αποσύρει τη συγκατάθεσή του;

Η ανάκληση θα πρέπει να γίνεται με την ίδια ευκολία όσο και η παροχή της συγκατάθεσης. Εάν αποσυρθεί η συγκατάθεση, η εταιρεία ή ο οργανισμός σας δεν μπορεί πλέον να επεξεργάζεται τα δεδομένα αλλά πρέπει να φροντίσει για τη διαγραφή τους, εκτός εάν η επεξεργασία μπορεί να στηριχθεί σε άλλο νομικό λόγο (π.χ. απαιτήσεις αποθήκευσης ή στον βαθμό που είναι απαραίτητο για την εκτέλεση σύμβασης).

Εάν τα δεδομένα υποβάλλονταν σε επεξεργασία για διάφορους σκοπούς, η εταιρεία ή ο οργανισμός σας δεν μπορεί να χρησιμοποιεί τα δεδομένα προσωπικού χαρακτήρα για το τμήμα της επεξεργασίας για το οποίο έχει γίνει ανάκληση της συγκατάθεσης ή για οποιονδήποτε από τους σκοπούς, ανάλογα με τη φύση της ανάκλησης της συγκατάθεσης.

Παράδειγμα: *Είστε πάροχος ηλεκτρονικού ενημερωτικού δελτίου. Ο πελάτης σας δίνει για να εγγραφεί σε αυτό συγκατάθεση η οποία σας επιτρέπει να επεξεργάζεστε όλα τα δεδομένα σχετικά με τα ενδιαφέροντά του για να δημιουργήσετε ένα προφίλ με τα άρθρα που επισκέπτεται. Μετά από έναν χρόνο, σας ενημερώνει ότι δεν*

επιθυμεί να λαμβάνει πλέον το ηλεκτρονικό ενημερωτικό δελτίο. Πρέπει να διαγράψετε από τη βάση δεδομένων σας όλα τα δεδομένα προσωπικού χαρακτήρα σχετικά με το εν λόγω άτομο που συλλέχθηκαν στο πλαίσιο της εγγραφής στο ενημερωτικό δελτίο συμπεριλαμβανομένων τυχόν προφίλ που σχετίζονται με το εν λόγω άτομο.

Ευαίσθητα δεδομένα

Ποια δεδομένα προσωπικού χαρακτήρα θεωρούνται ευαίσθητα;

Τα παρακάτω δεδομένα προσωπικού χαρακτήρα θεωρούνται «ευαίσθητα» και υπόκεινται σε συγκεκριμένες προϋποθέσεις επεξεργασίας:

- 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.

Υπό ποιες προϋποθέσεις μπορεί η εταιρεία μου/ο οργανισμός μου να επεξεργάζεται ευαίσθητα δεδομένα;

Απάντηση

Η εταιρεία ή ο οργανισμός σας μπορεί να επεξεργάζεται ευαίσθητα δεδομένα μόνον εφόσον πληρούται μια από τις ακόλουθες προϋποθέσεις:

- έχει ληφθεί η **ρητή συγκατάθεση** του ατόμου (νόμος μπορεί να αποκλείει αυτήν την επιλογή σε ορισμένες περιπτώσεις)
- η εταιρεία ή ο οργανισμός σας έχει την **υποχρέωση, σύμφωνα με τη νομοθεσία της ΕΕ ή εθνική νομοθεσία ή συλλογική σύμβαση**, να επεξεργάζεται δεδομένα για να συμμορφώνεται με τις υποχρεώσεις και τα δικαιώματά της/του, και με τις υποχρεώσεις και τα δικαιώματα των φυσικών προσώπων, στους τομείς του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας
- διακυβεύονται τα **ζωτικά συμφέροντα** του φυσικού προσώπου ή ενός φυσικού προσώπου που δεν έχει τη φυσική ή νομική ικανότητα να παράσχει τη συγκατάθεσή του
- είστε **ίδρυμα, ένωση ή άλλος μη κερδοσκοπικός φορέας** με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό σκοπό, και επεξεργάζεστε δεδομένα σχετικά με **μέλη** σας ή με άτομα που επικοινωνούν τακτικά με τον οργανισμό σας
- τα δεδομένα προσωπικού χαρακτήρα είχαν **δημοσιοποιηθεί προδήλως** από το φυσικό πρόσωπο
- τα δεδομένα είναι απαραίτητα για τη θεμελίωση, την άσκηση ή την υποστήριξη **νομικών αξιώσεων**
- τα δεδομένα υποβάλλονται σε επεξεργασία για λόγους **ουσιαστικού δημόσιου συμφέροντος** με βάση τη νομοθεσία της ΕΕ ή εθνική νομοθεσία
- τα δεδομένα υποβάλλονται σε επεξεργασία για σκοπούς **προληπτικής ή επαγγελματικής ιατρικής**, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει της νομοθεσίας της ΕΕ ή εθνικής νομοθεσίας ή δυνάμει σύμβασης ως επαγγελματίας του τομέα της υγείας
- τα δεδομένα υποβάλλονται σε επεξεργασία για λόγους **δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας** με βάση τη νομοθεσία της ΕΕ ή εθνική νομοθεσία
- τα δεδομένα υποβάλλονται σε επεξεργασία για **σκοπούς αρχειοθέτησης, επιστημονικής ή ιστορικής έρευνας** ή στατιστικούς σκοπούς με βάση τη νομοθεσία της ΕΕ ή εθνική νομοθεσία.

Μπορεί να επιβάλλονται περαιτέρω προϋποθέσεις από την εθνική νομοθεσία για την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων σχετικά με την υγεία. Υποβάλετε σχετικό ερώτημα στην εθνική αρχή προστασίας δεδομένων.

Παράδειγμα

Μπορείτε να επεξεργάζεστε ευαίσθητα δεδομένα: Ένας γιατρός παρακολουθεί κάποιους ασθενείς στην κλινική του. Καταχωρίζει κάθε επίσκεψη σε βάση δεδομένων που περιλαμβάνει πεδία όπως το ονοματεπώνυμο του ασθενή, περιγραφή των συμπτωμάτων και η φαρμακευτική αγωγή που συνταγογραφήθηκε. Τα δεδομένα αυτά θεωρούνται ευαίσθητα. Η επεξεργασία δεδομένων υγείας από την κλινική επιτρέπεται σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων, διότι απαιτείται για τη θεραπεία του ατόμου και διεξάγεται υπό την ευθύνη γιατρού που υπόκειται στην υποχρέωση του επαγγελματικού απορρήτου.

Δεν μπορείτε να επεξεργάζεστε ευαίσθητα δεδομένα: Η εταιρεία σας πουλά φορέματα στο διαδίκτυο. Για να εξατομικεύσετε τις υπηρεσίες που προσφέρετε σύμφωνα με τα συγκεκριμένα ενδιαφέροντα των πελατών σας, τους ζητάτε να σας παρέχουν πληροφορίες σχετικά με μεγέθη, προτιμώμενο χρώμα, μέθοδο πληρωμής, ονοματεπώνυμο και διεύθυνση παράδοσης του προϊόντος. Επιπλέον, ζητάτε από τους πελάτες σας πληροφορίες για τα πολιτικά τους φρονήματα. Χρειάζεστε την πλειονότητα των πληροφοριών για να εκπληρώσετε το δικό σας μέρος της σύμβασης. Ωστόσο, τα πολιτικά φρονήματα των πελατών σας δεν είναι απαραίτητα για την παραγωγή και παράδοση των φορεμάτων τους. Κατά συνέπεια, η εταιρεία σας δεν μπορεί να ζητά τις συγκεκριμένες πληροφορίες στο πλαίσιο της εν λόγω σύμβασης.

Μπορούν να χρησιμοποιηθούν για εμπορική προώθηση δεδομένα που έχουν παρασχεθεί από τρίτο;

Πριν να αποκτήσετε έναν κατάλογο επαφών ή μια βάση δεδομένων με στοιχεία επικοινωνίας φυσικών προσώπων από άλλον οργανισμό, ο εν λόγω οργανισμός πρέπει να μπορεί να **αποδείξει ότι τα δεδομένα αποκτήθηκαν σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων** και ότι **μπορούν να χρησιμοποιηθούν για διαφημιστικούς σκοπούς**. Για παράδειγμα, εάν ο οργανισμός απέκτησε τα δεδομένα βάσει συγκατάθεσης, η συγκατάθεση θα πρέπει να περιελάβανε τη δυνατότητα διαβίβασης των δεδομένων σε άλλους αποδέκτες για τους δικούς τους σκοπούς άμεσης εμπορικής προώθησης.

Η εταιρεία ή ο οργανισμός σας πρέπει επίσης να διασφαλίζει ότι ο κατάλογος ή η βάση δεδομένων είναι ενημερωμένα και ότι δεν αποστέλλετε διαφημιστικό υλικό σε φυσικά πρόσωπα που αρνήθηκαν την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης. Η εταιρεία ή ο οργανισμός σας πρέπει επίσης να διασφαλίζει ότι, εάν χρησιμοποιεί μέσα επικοινωνίας όπως ηλεκτρονικά μηνύματα για σκοπούς άμεσης εμπορικής προώθησης, συμμορφώνεται με τους κανόνες που θεσπίζονται στην οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (οδηγία 2002/58/ΕΚ).

Τέτοιου είδους κατάλογοι υποβάλλονται σε επεξεργασία με βάση τα έννομα συμφέροντά σας, και τα φυσικά πρόσωπα θα έχουν δικαίωμα να αρνηθούν τέτοιου είδους επεξεργασία. Η εταιρεία ή ο οργανισμός σας πρέπει επίσης να ενημερώνει τα φυσικά πρόσωπα, το αργότερο την πρώτη φορά που επικοινωνείτε μαζί τους, ότι έχει συλλέξει τα δεδομένα τους προσωπικού χαρακτήρα και ότι σκοπεύει να τα επεξεργάζεται για την αποστολή διαφημίσεων.

Παράδειγμα: *Δύο φίλοι, η κ. Α και ο κ. Β, είναι ιδιοκτήτες, αντίστοιχα, ενός γυμναστηρίου και ενός βιβλιοπωλείου. Ο καθένας τους συλλέγει δεδομένα από τους πελάτες του. Το βιβλιοπωλείο του κ. Β δεν πηγαίνει καλά. Η βάση δεδομένων με τους πελάτες του έχει λίγες καταχωρίσεις και δεν επισκέπτονται πολλά άτομα το βιβλιοπωλείο του. Λέει στην κ. Α ότι παρέλαβε μια νέα βιογραφία ενός διάσημου αθλητή και ρωτά την κ. Α εάν οι πελάτες της θα ενδιαφέρονταν να λάβουν διαφημιστικό υλικό για το βιβλίο. Οι όροι της δήλωσης εχεμύθειας της κ. Α ενημέρωναν τους πελάτες της ότι θα μπορούσε να κοινολογήσει τα δεδομένα σε συνεργάτες που προσφέρουν προϊόντα στον τομέα της υγείας και της ευεξίας. Με την προϋπόθεση ότι έχει παρασχεθεί συγκεκριμένη συγκατάθεση με σκοπό τη διαβίβαση των δεδομένων σε άλλους αποδέκτες για τους δικούς τους σκοπούς άμεσης εμπορικής προώθησης, η κ. Α μπορεί να αποστείλει τον κατάλογο πελατών της στον κ. Β. Αντιθέτως, δεν μπορούν να αποσταλούν δεδομένα σχετικά με ένα άτομο το οποίο αρνήθηκε την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα.*

Υποχρεώσεις

Υπεύθυνος επεξεργασίας/εκτελών την επεξεργασία

Τι είναι ένας υπεύθυνος επεξεργασίας ή ένας εκτελών την επεξεργασία;

Ο **υπεύθυνος επεξεργασίας** ορίζει τους **σκοπούς** της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και τα μέσα με τα οποία αυτή πραγματοποιείται. Επομένως, εάν η εταιρεία ή ο οργανισμός σας αποφασίζει «γιατί» και «πώς» τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία, θεωρείται ο υπεύθυνος επεξεργασίας. Οι εργαζόμενοι που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα εντός του οργανισμού σας το κάνουν για να εκπληρώσουν τα δικά σας καθήκοντα ως υπεύθυνου επεξεργασίας.

Η εταιρεία ή ο οργανισμός σας θεωρείται **από κοινού υπεύθυνος επεξεργασίας** όταν σε συνεργασία με έναν ή περισσότερους οργανισμούς αποφασίζει από κοινού «γιατί» και «πώς» θα πρέπει να υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα. Οι από κοινού υπεύθυνοι επεξεργασίας πρέπει να συνάπτουν μεταξύ τους συμφωνία που καθορίζει τις αντίστοιχες αρμοδιότητές τους για τη συμμόρφωση με τους κανόνες του ΓΚΠΔ. Τα κύρια σημεία της συμφωνίας πρέπει να κοινοποιούνται στα φυσικά πρόσωπα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία.

Ο **εκτελών την επεξεργασία** επεξεργάζεται δεδομένα προσωπικού χαρακτήρα μόνο **εκ μέρους του υπεύθυνου επεξεργασίας**. Ο εκτελών την επεξεργασία είναι συνήθως τρίτος εκτός εταιρείας. Ωστόσο, στην περίπτωση ομίλων επιχειρήσεων, μια επιχείρηση μπορεί να ενεργεί ως εκτελούσα την επεξεργασία για λογαριασμό άλλης επιχείρησης.

Τα καθήκοντα του εκτελούντος την επεξεργασία προς τον υπεύθυνο επεξεργασίας πρέπει να καθορίζονται σε σύμβαση ή άλλη νομική πράξη. Για παράδειγμα, η σύμβαση πρέπει να αναφέρει τι γίνεται με τα δεδομένα προσωπικού χαρακτήρα μετά τη λήξη της σύμβασης. Μια τυπική δραστηριότητα των εκτελούντων την επεξεργασία είναι η παροχή λύσεων τεχνολογίας πληροφοριών, συμπεριλαμβανομένης της αποθήκευσης σε νέφος (cloud). Ο εκτελών την επεξεργασία των δεδομένων μπορεί να αναθέτει μέρος των εργασιών του σε άλλον εκτελούντα την επεξεργασία υπεργολάβο ή να διορίζει από κοινού εκτελούντα την επεξεργασία μόνον εφόσον έχει λάβει προηγούμενη γραπτή άδεια από τον υπεύθυνο επεξεργασίας των δεδομένων.

Υπάρχουν περιπτώσεις όπου μια οντότητα μπορεί να είναι υπεύθυνος επεξεργασίας δεδομένων ή εκτελών την επεξεργασία ή και τα δύο.

Παραδείγματα

Υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία: *Μια ζυθοποιία έχει πολλούς εργαζομένους. Υπογράφει σύμβαση με εταιρεία πληρωμών για την καταβολή των μισθών. Η ζυθοποιία ενημερώνει την εταιρεία πληρωμών για το πότε πρέπει να γίνεται η πληρωμή των μισθών, πότε ένας εργαζόμενος αποχωρεί ή παίρνει αύξηση και παρέχει όλα τα υπόλοιπα στοιχεία που είναι απαραίτητα για το εκκαθαριστικό σημείωμα αποδοχών και την πληρωμή. Η εταιρεία πληρωμών παρέχει σύστημα τεχνολογίας πληροφοριών και αποθηκεύει τα δεδομένα των εργαζομένων. Η ζυθοποιία είναι ο υπεύθυνος επεξεργασίας δεδομένων και η εταιρεία πληρωμών είναι ο εκτελών την επεξεργασία των δεδομένων.*

Από κοινού υπεύθυνοι επεξεργασίας: *Η εταιρεία ή ο οργανισμός σας προσφέρει υπηρεσίες φύλαξης παιδιών μέσω ηλεκτρονικής πλατφόρμας. Ταυτόχρονα, έχει σύμβαση με άλλη εταιρεία που σας επιτρέπει να προσφέρετε υπηρεσίες προστιθέμενης αξίας. Οι εν λόγω υπηρεσίες περιλαμβάνουν τη δυνατότητα των γονιών όχι μόνο να επιλέγουν τον/την φροντιστή των παιδιών αλλά και να νοικιάζουν παιχνίδια και DVD που αυτός ή αυτή μπορεί να φέρνει. Και οι δύο εταιρείες συμμετέχουν στην τεχνική ρύθμιση του ιστότοπου. Σε αυτήν την περίπτωση, οι δύο εταιρείες έχουν αποφασίσει να χρησιμοποιούν την πλατφόρμα και για τους δύο σκοπούς (υπηρεσίες φύλαξης παιδιών και ενοικίαση DVD/παιχνιδιών) και θα ανταλλάσσουν πολύ συχνά τα ονόματα των πελατών. Επομένως, οι δύο εταιρείες είναι από κοινού υπεύθυνοι επεξεργασίας όχι μόνο επειδή συμφωνούν να προσφέρουν τη δυνατότητα «συνδυασμένων υπηρεσιών» αλλά και γιατί σχεδιάζουν και χρησιμοποιούν κοινή πλατφόρμα.*

Μπορεί κάποιος άλλος να επεξεργαστεί τα δεδομένα εκ μέρους του οργανισμού μου;

Κάποιος άλλος (φυσικό ή νομικό πρόσωπο ή άλλος φορέας) **μπορεί να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα** εκ μέρους σας με την προϋπόθεση ότι **υπάρχει σύμβαση ή άλλη νομική πράξη**. Είναι σημαντικό ο εκτελών την επεξεργασία που διορίζετε να παρέχει επαρκείς εγγυήσεις για την υλοποίηση κατάλληλων τεχνικών και οργανωτικών μέτρων έτσι ώστε να διασφαλίζεται ότι η επεξεργασία θα γίνεται σύμφωνα με τα πρότυπα του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ) και να παρέχονται εγγυήσεις για την προστασία των δικαιωμάτων των φυσικών προσώπων.

Ο διορισμένος εκτελών την επεξεργασία δεν μπορεί στη συνέχεια να διορίσει άλλον εκτελούντα την επεξεργασία χωρίς προηγουμένως να ζητήσει ειδική ή γενική γραπτή άδεια από την εταιρεία ή τον οργανισμό σας. Η σύμβαση ή η νομική πράξη ανάμεσα στην εταιρεία ή τον οργανισμό σας και τον εκτελούντα την επεξεργασία πρέπει να συμπεριλαμβάνει τις εξής πρόνοιες:

- η επεξεργασία μπορεί να πραγματοποιείται μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας
- ο εκτελών την επεξεργασία διασφαλίζει ότι τα άτομα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας
- ο εκτελών την επεξεργασία πρέπει να προσφέρει ένα ελάχιστο επίπεδο ασφάλειας το οποίο καθορίζεται από τον υπεύθυνο επεξεργασίας
- ο εκτελών την επεξεργασία πρέπει να συμβάλλει στη διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ.

Παραδείγματα

Μια κατασκευαστική εταιρεία χρησιμοποιεί υπεργολάβο για συγκεκριμένες κατασκευαστικές εργασίες και του παρέχει τα στοιχεία επικοινωνίας των πελατών στους οποίους χρειάζεται να πραγματοποιηθούν οι κατασκευαστικές εργασίες. Ο υπεργολάβος χρησιμοποιεί περαιτέρω τα δεδομένα για να αποστείλει στους πελάτες υλικό εμπορικής προώθησης. Ο υπεργολάβος σε αυτήν την περίπτωση δεν θεωρείται μόνο ως «εκτελών την επεξεργασία» σύμφωνα με τον ΓΚΠΔ, καθώς δεν επεξεργάζεται μόνο δεδομένα προσωπικού χαρακτήρα εκ μέρους της κατασκευαστικής εταιρείας, αλλά τα επεξεργάζεται περαιτέρω για δικούς του σκοπούς. Επομένως, ο υπεργολάβος ενεργεί ως «υπεύθυνος επεξεργασίας δεδομένων».

Είστε εταιρεία λιανικής πώλησης που αποφασίζει να αποθηκεύσει αντίγραφο ασφαλείας της βάσης δεδομένων των πελατών σε διακομιστή νέφους. Για αυτόν τον σκοπό, συνάπτετε σύμβαση με έναν πάροχο υπηρεσιών νέφους που είναι γνωστός για τα υψηλά πρότυπα προστασίας δεδομένων που εφαρμόζει και ο οποίος διαθέτει επίσης πιστοποιημένο σύστημα κρυπτογράφησης δεδομένων. Ο πάροχος υπηρεσιών νέφους είναι ο εκτελών την επεξεργασία καθώς, αποθηκεύοντας τα δεδομένα προσωπικού χαρακτήρα των πελατών σας στους διακομιστές του, θα επεξεργάζεται δεδομένα προσωπικού χαρακτήρα εκ μέρους σας.

Οι υποχρεώσεις παραμένουν οι ίδιες ανεξάρτητα από τον όγκο των δεδομένων που χειρίζεται η εταιρεία ή ο οργανισμός μου;

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) βασίζεται στην προσέγγιση με βάση τον κίνδυνο. Με άλλα λόγια, οι εταιρείες/οι οργανισμοί που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα ενθαρρύνονται να εφαρμόζουν μέτρα προστασίας **που να αντιστοιχούν στο επίπεδο κινδύνου των δραστηριοτήτων επεξεργασίας δεδομένων που εκτελούν**. Επομένως, οι υποχρεώσεις μιας εταιρείας που επεξεργάζεται πολλά δεδομένα είναι πιο επαχθείς συγκριτικά με μια εταιρεία που επεξεργάζεται μικρό όγκο δεδομένων.

Για παράδειγμα, η πιθανότητα πρόσληψης ενός υπεύθυνου προστασίας δεδομένων για μια εταιρεία/έναν οργανισμό που επεξεργάζεται πολλά δεδομένα είναι υψηλότερη συγκριτικά με μια εταιρεία/οργανισμό που επεξεργάζεται μικρό όγκο δεδομένων (σε αυτήν την περίπτωση αυτό σχετίζεται με την έννοια της επεξεργασίας

δεδομένων προσωπικού χαρακτήρα σε «μεγάλη κλίμακα»). Ταυτόχρονα, η φύση των δεδομένων προσωπικού χαρακτήρα και η επίδραση της σχεδιαζόμενης επεξεργασίας διαδραματίζουν επίσης έναν ρόλο. Η επεξεργασία μικρού όγκου δεδομένων, τα οποία όμως είναι ευαίσθητα (π.χ. δεδομένα υγείας), απαιτεί την εφαρμογή πιο αυστηρών μέτρων για συμμόρφωση με τον ΓΚΠΔ.

Σε κάθε περίπτωση, πρέπει να τηρούνται οι αρχές προστασίας δεδομένων και να δίνεται η δυνατότητα στα φυσικά πρόσωπα να ασκούν τα δικαιώματά τους.

Τι σημαίνει η προστασία δεδομένων «ήδη από τον σχεδιασμό» και «εξ ορισμού»;

Οι εταιρείες/οργανισμοί ενθαρρύνονται να εφαρμόζουν τεχνικά και οργανωτικά μέτρα, στα αρχικά στάδια του σχεδιασμού των πράξεων επεξεργασίας, με τέτοιον τρόπο ώστε να διασφαλίζονται οι αρχές ιδιωτικού απορρήτου και προστασίας δεδομένων ήδη από την αρχή («προστασία δεδομένων ήδη από τον σχεδιασμό»). Εξ ορισμού, οι εταιρείες/οργανισμοί θα πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με το υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής (π.χ. μόνο τα απαραίτητα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία, σύντομη περίοδος αποθήκευσης, περιορισμένη προσβασιμότητα) έτσι ώστε εξ ορισμού τα δεδομένα προσωπικού χαρακτήρα να μην είναι προσβάσιμα από αόριστο αριθμό φυσικών προσώπων («προστασία δεδομένων εξ ορισμού»).

Παραδείγματα

Προστασία δεδομένων ήδη από τον σχεδιασμό: *Χρήση ψευδωνυμοποίησης (αντικατάσταση προσωπικά ταυτοποιήσιμου υλικού με τεχνητά αναγνωριστικά στοιχεία) και κρυπτογράφησης (κωδικοποίηση μηνυμάτων έτσι ώστε μόνο όσοι είναι εξουσιοδοτημένοι να μπορούν να τα διαβάζουν).*

Προστασία δεδομένων εξ ορισμού: *Μια πλατφόρμα κοινωνικής δικτύωσης θα πρέπει να ενθαρρύνεται να ορίζει τις ρυθμίσεις των προφίλ των χρηστών έτσι ώστε να προστατεύουν όσο το δυνατόν περισσότερο το ιδιωτικό απόρρητο, για παράδειγμα, περιορίζοντας από την αρχή την προσβασιμότητα στα προφίλ των χρηστών έτσι ώστε να μην είναι προσβάσιμα εξ ορισμού από αόριστο αριθμό ατόμων.*

Τι είναι η παραβίαση δεδομένων και τι πρέπει να κάνουμε σε περίπτωση παραβίασης δεδομένων;

Παραβίαση δεδομένων επέρχεται όταν σημειώνεται συμβάν ασφαλείας σε σχέση με τα δεδομένα για τα οποία ευθύνεται η εταιρεία ή ο οργανισμός σας, το οποίο έχει ως αποτέλεσμα την παραβίαση του απορρήτου, της διαθεσιμότητας ή της ακεραιότητας. Εάν αυτό συμβεί, και είναι πιθανό η παραβίαση να θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικού προσώπου, 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.

Ως οργανισμός, είναι ζωτικής σημασίας να εφαρμόζετε τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποφυγή ενδεχόμενων παραβιάσεων δεδομένων.

Παραδείγματα

Ο οργανισμός πρέπει να ειδοποιήσει την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα: *Τα δεδομένα των εργαζομένων μιας κλωστοϋφαντουργίας γνωστοποιήθηκαν. Τα δεδομένα συμπεριλάμβαναν τις προσωπικές*

διευθύνσεις, τη σύνθεση της οικογένειας, τον μηνιαίο μισθό και τις ιατρικές αξιώσεις κάθε εργαζομένου. Σε αυτήν την περίπτωση, η κλωστοϋφαντουργία πρέπει να ενημερώσει την εποπτική αρχή σχετικά με την παραβίαση. Καθώς δε τα δεδομένα προσωπικού χαρακτήρα περιλαμβάνουν ευαίσθητα δεδομένα, όπως δεδομένα υγείας, η εταιρεία πρέπει επίσης να ειδοποιήσει τους εργαζομένους.

Ένας υπάλληλος νοσοκομείου αποφασίζει να αντιγράψει στοιχεία ασθενών σε CD και τα δημοσιεύει στο διαδίκτυο. Το νοσοκομείο το ανακαλύπτει μερικές μέρες αργότερα. Από τη στιγμή που λαμβάνει γνώση το νοσοκομείο, πρέπει σε 72 ώρες να ενημερώσει την εποπτική αρχή και επιπλέον, καθώς τα προσωπικά στοιχεία περιέχουν ευαίσθητες πληροφορίες, για παράδειγμα εάν ο/η ασθενής πάσχει από καρκίνο, είναι έγκυος κ.λπ., πρέπει να ενημερώσει και τους ασθενείς. Στην περίπτωση αυτή, είναι αμφίβολο εάν το νοσοκομείο είχε εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας . Εάν είχε πράγματι εφαρμόσει κατάλληλα μέτρα προστασίας (π.χ. κρυπτογράφηση των δεδομένων), δεν θα ήταν πιθανό να προκύψει ουσιώδης κίνδυνος και το νοσοκομείο θα μπορούσε να είχε απαλλαγεί από την υποχρέωση να ειδοποιήσει τους ασθενείς.

Η εταιρεία πρέπει να ειδοποιήσει τους πελάτες και αυτοί έπειτα μπορεί να πρέπει να ειδοποιήσουν την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα: *Σε μια υπηρεσία νέφους σημειώνεται απώλεια αρκετών σκληρών δίσκων που περιέχουν δεδομένα προσωπικού χαρακτήρα τα οποία ανήκουν σε αρκετούς πελάτες της. Η εταιρεία πρέπει να ειδοποιήσει τους εν λόγω πελάτες αμέσως μόλις αντιληφθεί την παραβίαση. Οι πελάτες της πρέπει να ειδοποιήσουν την Αρχή Προστασίας Δεδομένων και τα φυσικά πρόσωπα ανάλογα με τα δεδομένα που είχαν υποβληθεί σε επεξεργασία από τον εκτελούντα την επεξεργασία.*

Πότε πρέπει να γίνεται εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ);

ΕΑΠΔ απαιτείται όταν η επεξεργασία είναι πιθανό να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων. ΕΑΠΔ απαιτείται οπωσδήποτε στις ακόλουθες περιπτώσεις:

- σε μια συστηματική και εκτενή εκτίμηση των προσωπικών πτυχών φυσικού προσώπου, συμπεριλαμβανομένης της κατάρτισης προφίλ
- στην επεξεργασία ευαίσθητων δεδομένων σε μεγάλη κλίμακα
- στη συστηματική παρακολούθηση δημόσιων χώρων σε μεγάλη κλίμακα.

Οι εθνικές αρχές προστασίας δεδομένων, σε συντονισμό με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, μπορούν να παρέχουν καταλόγους περιπτώσεων όπου απαιτείται ΕΑΠΔ. Η ΕΑΠΔ θα πρέπει να πραγματοποιείται πριν από την επεξεργασία και θα πρέπει να θεωρείται ζωντανό εργαλείο και όχι μόνο εφάπαξ άσκηση. Όπου υπάρχουν υπολειπόμενοι κίνδυνοι που δεν μπορούν να μετριαστούν με τα μέτρα που έχουν ληφθεί, πρέπει να συμβουλευθείτε την Αρχή Προστασίας Δεδομένων (ΑΠΔ) πριν ξεκινήσετε την επεξεργασία.

Παραδείγματα

Απαιτείται ΕΑΠΔ: *Τράπεζα ελέγχει τους πελάτες της σε συνάρτηση με βάση δεδομένων αναφοράς για πιστώσεις. Νοσοκομείο πρόκειται να θέσει σε εφαρμογή νέα βάση δεδομένων με πληροφορίες για την υγεία, που θα περιλαμβάνει δεδομένα υγείας των ασθενών. Εταιρεία λεωφορείων πρόκειται να εγκαταστήσει κάμερες μέσα στα οχήματα για να παρακολουθεί τη συμπεριφορά οδηγών και επιβατών.*

Δεν απαιτείται ΕΑΠΔ: *Κοινοτικός γιατρός επεξεργάζεται δεδομένα προσωπικού χαρακτήρα των ασθενών του. Σε αυτή την περίπτωση, δεν απαιτείται ΕΑΠΔ καθώς η επεξεργασία από τους κοινοτικούς γιατρούς δεν γίνεται σε μεγάλη κλίμακα σε περιπτώσεις όπου ο αριθμός ασθενών είναι περιορισμένος.*

Υπεύθυνοι προστασίας δεδομένων (ΥΠΔ) / Data Protection Officers (DPO)

Πρέπει η εταιρεία / ο οργανισμός μου να διαθέτει υπεύθυνο προστασίας δεδομένων (ΥΠΔ);

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 συμπεριφορικής διαφήμισης.

Οι δημόσιες διοικήσεις 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.

Παραδείγματα:

Υποχρεωτικός διορισμός ΥΠΔ: *Ο διορισμός ΥΠΔ είναι υποχρεωτικός για παράδειγμα όταν η εταιρεία ή ο οργανισμός σας είναι:*

- *νοσοκομείο που επεξεργάζεται μεγάλο όγκο ευαίσθητων δεδομένων*
- *εταιρεία παροχής υπηρεσιών ασφάλειας υπεύθυνη για την παρακολούθηση εμπορικών κέντρων και δημόσιων χώρων*
- *μικρή εταιρεία ευρέσεως εξειδικευμένου προσωπικού που καταρτίζει προφίλ φυσικών προσώπων.*

Μη υποχρεωτικός διορισμός ΥΠΔ: *Ο διορισμός ΥΠΔ δεν είναι υποχρεωτικός εάν*

- *είστε τοπικός κοινοτικός γιατρός και επεξεργάζεστε δεδομένα προσωπικού χαρακτήρα των ασθενών σας*
- *έχετε ένα μικρό δικηγορικό γραφείο και επεξεργάζεστε δεδομένα προσωπικού χαρακτήρα των πελατών σας.*

Ποια είναι τα καθήκοντα ενός υπεύθυνου προστασίας δεδομένων (ΥΠΔ);

Ο ΥΠΔ βοηθά τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την εργασία σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων προσωπικού χαρακτήρα. Πιο συγκεκριμένα, ο ΥΠΔ οφείλει:

- να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, καθώς και το προσωπικό που απασχολούν, σχετικά με τις υποχρεώσεις τους σύμφωνα με τη νομοθεσία περί προστασίας δεδομένων
- να παρακολουθεί τη συμμόρφωση 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
- να παρέχει συμβουλές όταν έχει πραγματοποιηθεί ΕΑΠΔ και να παρακολουθεί τα αποτελέσματά της
- να λειτουργεί ως σημείο επαφής για αιτήματα φυσικών προσώπων που αφορούν την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και την άσκηση των δικαιωμάτων τους
- να συνεργάζεται με ΑΠΔ και να λειτουργεί ως σημείο επαφής για ΑΠΔ σχετικά με ζητήματα που αφορούν την επεξεργασία.

Ο ΥΠΔ πρέπει να εμπλέκεται από τον οργανισμό έγκαιρα. 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.

Τι κανόνες ισχύουν εάν ο οργανισμός μου διαβιβάζει δεδομένα εκτός της ΕΕ;

Στον σημερινό παγκοσμιοποιημένο κόσμο, γίνονται διασυνοριακές διαβιβάσεις μεγάλου όγκου δεδομένων προσωπικού χαρακτήρα, τα οποία ορισμένες φορές αποθηκεύονται σε διακομιστές σε διαφορετικές χώρες. Η **προστασία που προσφέρει ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) συνοδεύει τα δεδομένα**, πράγμα που σημαίνει ότι οι κανόνες για την προστασία των δεδομένων προσωπικού χαρακτήρα εξακολουθούν να ισχύουν ανεξάρτητα από το πού καταλήγουν τα δεδομένα. Αυτό ισχύει επίσης όταν τα δεδομένα διαβιβάζονται σε χώρα που δεν ανήκει στην ΕΕ (τρίτη χώρα).

Ο ΓΚΠΔ παρέχει διαφορετικά εργαλεία που πλαισιώνουν τις διαβιβάσεις δεδομένων από την ΕΕ προς τρίτη χώρα:

- Ορισμένες φορές, μια τρίτη χώρα μπορεί, μέσω απόφασης της Ευρωπαϊκής Επιτροπής («απόφαση επάρκειας»), να κηρυχθεί ως προσφέρουσα επαρκές επίπεδο προστασίας , πράγμα που σημαίνει ότι επιτρέπεται να διαβιβασθούν δεδομένα σε άλλη εταιρεία στην εν λόγω τρίτη χώρα χωρίς να απαιτείται από τον εξαγωγέα δεδομένων να παρέχει περαιτέρω εγγυήσεις ή να υπόκειται σε επιπλέον όρους. Με άλλα λόγια, οι διαβιβάσεις σε μια «επαρκή» τρίτη χώρα εξομοιώνονται με διαβίβαση δεδομένων εντός της ΕΕ.
- Σε περίπτωση που δεν υπάρχει απόφαση επάρκειας, μπορεί να γίνει διαβίβαση με την παροχή κατάλληλων εγγυήσεων και με την προϋπόθεση ότι τα φυσικά πρόσωπα έχουν στη διάθεσή τους εκτελεστά δικαιώματα και πραγματικά ένδικα μέσα. Τέτοιες κατάλληλες εγγυήσεις περιλαμβάνουν τα εξής:
- στην περίπτωση ομίλου επιχειρήσεων ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα, οι εταιρείες μπορούν να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα με βάση τους αποκαλούμενους δεσμευτικούς εταιρικούς κανόνες
- συμβατικές ρυθμίσεις με τον αποδέκτη των δεδομένων προσωπικού χαρακτήρα, μέσω της χρήσης, για παράδειγμα, τυποποιημένων συμβατικών ρητρών που έχουν λάβει την έγκριση της Ευρωπαϊκής Επιτροπής
- την τήρηση ενός κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης παράλληλα με τη λήψη δεσμευτικών και εκτελεστών δεσμεύσεων από τον αποδέκτη σχετικά με την εφαρμογή κατάλληλων εγγυήσεων για την προστασία των δεδομένων που διαβιβάζονται.
- Τέλος, εάν προβλέπεται διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα που δεν υπόκειται σε απόφαση επάρκειας και εάν δεν υπάρχουν κατάλληλες εγγυήσεις, μπορεί να γίνει διαβίβαση με βάση ορισμένες εξαιρέσεις για συγκεκριμένες καταστάσεις, για παράδειγμα, όταν ένα φυσικό πρόσωπο συγκατατέθηκε ρητώς στην προτεινόμενη διαβίβαση αφού του παρασχέθηκαν όλες οι απαραίτητες πληροφορίες σχετικά με τους κινδύνους που αυτή ενέχει.

Παράδειγμα: *Είστε γαλλική εταιρεία που σκοπεύει να επεκτείνει τις υπηρεσίες της στη Νότια Αμερική, και πιο συγκεκριμένα στην Αργεντινή, την Ουρουγουάη και τη Βραζιλία. Το πρώτο βήμα που θα πρέπει να κάνετε είναι να ελέγξετε αν οι εν λόγω τρίτες χώρες υπόκεινται σε απόφαση επάρκειας. Πράγματι, η Αργεντινή και η Ουρουγουάη έχουν κηρυχθεί επαρκείς. Επομένως, θα μπορείτε να διαβιβάσετε δεδομένα προσωπικού χαρακτήρα σε αυτές τις δύο τρίτες χώρες χωρίς πρόσθετες εγγυήσεις, ενώ για τις διαβιβάσεις προς τη Βραζιλία, για την οποία δεν έχει εκδοθεί απόφαση επάρκειας, πρέπει να πλαισιώσετε τις διαβιβάσεις σας με την παροχή κατάλληλων εγγυήσεων.*

Πώς μπορώ να αποδείξω ότι ο οργανισμός μου συμμορφώνεται με τον ΓΚΠΔ;

Η αρχή της **λογοδοσίας** συνιστά ακρογωνιαίο λίθο του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ). Σύμφωνα με τον ΓΚΠΔ, επιχειρήσεις και οργανισμοί οφείλουν να συμμορφώνονται με όλες τις αρχές προστασίας δεδομένων καθώς και να αποδεικνύουν τη συμμόρφωση αυτή. Ο ΓΚΠΔ παρέχει στις επιχειρήσεις και

τους οργανισμούς μια σειρά εργαλείων για να τα βοηθά να αποδεικνύουν τη λογοδοσία, ορισμένα εκ των οποίων πρέπει να τίθενται σε εφαρμογή υποχρεωτικά.

Για παράδειγμα, σε ορισμένες περιπτώσεις ο διορισμός ΥΠΔ ή η διεξαγωγή εκτιμήσεων αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) μπορεί να είναι υποχρεωτικά. Οι υπεύθυνοι επεξεργασίας δεδομένων μπορούν να επιλέξουν να χρησιμοποιήσουν άλλα εργαλεία, π.χ. κώδικες δεοντολογίας και μηχανισμούς πιστοποίησης, για την απόδειξη της συμμόρφωσης με τις αρχές προστασίας δεδομένων.

Μπορείτε να τηρείτε **έναν κώδικα δεοντολογίας** που έχει καταρτισθεί από επιχειρηματική ένωση η οποία έχει εγκριθεί από μια Αρχή Προστασίας Δεδομένων (ΑΠΔ). Ένας κώδικας δεοντολογίας μπορεί να τεθεί σε ισχύ σε όλη την ΕΕ μέσω εκτελεστικής πράξης της Επιτροπής.

Μπορείτε να τηρείτε έναν **μηχανισμό πιστοποίησης** που εφαρμόζεται από έναν από τους φορείς πιστοποίησης που έχουν λάβει διαπίστευση από Αρχή Προστασίας Δεδομένων (ΑΠΔ) ή εθνικό οργανισμό διαπίστευσης ή και τα δύο, όπως ορίζεται στη νομοθεσία κάθε κράτους μέλους της ΕΕ.

Τόσο οι κώδικες δεοντολογίας όσο και η πιστοποίηση είναι προαιρετικά μέσα και για αυτόν τον λόγο εξαρτάται από την εταιρεία ή τον οργανισμό σας να αποφασίσει εάν θα τηρεί έναν συγκεκριμένο κώδικα δεοντολογίας ή εάν θα ζητήσει πιστοποίηση. Παρόλο που η εταιρεία ή ο οργανισμός σας οφείλει και πάλι να τηρεί και να συμμορφώνεται με τον ΓΚΠΔ, η τήρηση τέτοιων μέσων μπορεί να λαμβάνεται υπόψη στην περίπτωση λήψης μέτρου επιβολής του νόμου εναντίον σας για παραβίαση του ΓΚΠΔ.

Παράδειγμα: *Ο γενικός ασφαλιστικός φορέας στο κράτος μέλος της ΕΕ στο οποίο εδρεύει η εταιρεία ή ο οργανισμός σας διαθέτει κώδικα δεοντολογίας που έχει εγκριθεί από την εποπτική αρχή. Ορισμένες ανταγωνίστριες ασφαλιστικές εταιρείες έχουν υιοθετήσει τον εν λόγω κώδικα. Παρόλο που η τήρηση του κώδικα είναι προαιρετική, συμβάλλει στην απόδειξη της συμμόρφωσης με τον ΓΚΠΔ.*

Δικαιώματα για τους πολίτες

Μάθετε αναλυτικά πώς προστατεύονται τα δεδομένα προσωπικού χαρακτήρα που σας αφορούν, τα δικαιώματα που σας βοηθούν να επανακτήσετε τον έλεγχο των δεδομένων σας και τι να κάνετε εάν τα πράγματα πάνε στραβά.

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_el

Ποια είναι τα δικαιώματα μου στα δεδομένα μου;

Στα δεδομένα προσωπικού χαρακτήρα που αφορούν το πρόσωπο σας και συλλέγει μια εταιρία/οργανισμός, έχετε το δικαίωμα:

- **να ενημερώνεστε** σχετικά με την επεξεργασία των δεδομένων σας προσωπικού χαρακτήρα
- **να αποκτάτε πρόσβαση** στα δεδομένα προσωπικού χαρακτήρα που σας αφορούν
- να ζητάτε τη **διόρθωση** εσφαλμένων, ανακριβών ή ελλιπών δεδομένων προσωπικού χαρακτήρα
- να υποβάλετε αίτημα για τη διαγραφή **δεδομένων** προσωπικού χαρακτήρα όταν δεν είναι πλέον απαραίτητα ή εάν η επεξεργασία είναι παράνομη
- **να εναντιωθείτε** στην επεξεργασία των δεδομένων σας προσωπικού χαρακτήρα για σκοπούς εμπορικής προώθησης ή για λόγους που σχετίζονται με την ιδιαίτερη κατάστασή σας
- να υποβάλετε αίτημα για **περιορισμό** της επεξεργασίας των δεδομένων σας προσωπικού χαρακτήρα σε συγκεκριμένες περιπτώσεις
- να λαμβάνετε τα δεδομένα σας προσωπικού χαρακτήρα σε μορφότυπο αναγνώσιμο από μηχάνημα και να τα αποστέλλετε σε άλλον υπεύθυνο επεξεργασίας («**φορητότητα δεδομένων**»)
- να υποβάλετε αίτημα έτσι ώστε αποφάσεις που βασίζονται σε **αυτοματοποιημένη επεξεργασία**, σας αφορούν ή σας επηρεάζουν σε σημαντικό βαθμό και βασίζονται στα δεδομένα σας προσωπικού χαρακτήρα, να γίνονται από φυσικά πρόσωπα και όχι μόνο από υπολογιστές. Έχετε επίσης το δικαίωμα σε αυτήν την περίπτωση να εκφράσετε την άποψή σας και να προσβάλετε την απόφαση.

Για την άσκηση των δικαιωμάτων σας θα πρέπει να επικοινωνήσετε με την εταιρεία ή τον οργανισμό που επεξεργάζεται τα δεδομένα σας προσωπικού χαρακτήρα, που εν προκειμένω καλείται επίσης «υπεύθυνος επεξεργασίας». Εάν η εταιρεία ή ο οργανισμός διαθέτει έναν υπεύθυνο προστασίας δεδομένων (ΥΠΔ), μπορείτε να υποβάλετε το αίτημά σας σε αυτόν. Η εταιρεία ή ο οργανισμός πρέπει να απαντά στα αιτήματά σας χωρίς αδικαιολόγητη καθυστέρηση και **τουλάχιστον εντός ενός μήνα.** Εάν δεν σκοπεύει να συμμορφωθεί με το αίτημά σας, πρέπει να δηλώσει τον λόγο. Μπορεί να σας ζητηθεί να παράσχετε πληροφορίες για να επιβεβαιώσετε την ταυτότητά σας (για παράδειγμα να πατήσετε έναν σύνδεσμο επαλήθευσης, συμπληρώνοντας ένα όνομα χρήστη ή έναν κωδικό πρόσβασης) για να ασκήσετε τα δικαιώματά σας.

Τα εν λόγω δικαιώματα ισχύουν **σε ολόκληρη την ΕΕ**, ανεξάρτητα από το πού γίνεται η επεξεργασία των δεδομένων και πού έχει έδρα η εταιρεία. Τα εν λόγω δικαιώματα ισχύουν επίσης όταν αγοράζετε αγαθά και υπηρεσίες από εταιρείες που έχουν την έδρα τους εκτός της ΕΕ αλλά δραστηριοποιούνται στην ΕΕ.

Πώς θα πρέπει να ζητείται η συγκατάθεσή μου;

Ένα αίτημα συγκατάθεσης πρέπει να υποβάλλεται με **σαφή και συνοπτικό** τρόπο, με διατύπωση που να είναι εύκολα κατανοητή και να είναι **σαφώς διακριτό** από άλλες πληροφορίες όπως όροι και προϋποθέσεις. Το αίτημα πρέπει να προσδιορίζει **τη χρήση που θα γίνει στα δεδομένα σας προσωπικού χαρακτήρα** και να περιλαμβάνει τα **στοιχεία επικοινωνίας** της εταιρείας που επεξεργάζεται τα δεδομένα. Η συγκατάθεση πρέπει να **δίνεται ελεύθερα**, **να είναι συγκεκριμένη**, **εν επιγνώσει** και αδιαμφισβήτητη. Ο όρος «εν επιγνώσει» σημαίνει ότι πρέπει να έχετε ενημερωθεί σχετικά με την επεξεργασία των δεδομένων σας προσωπικού χαρακτήρα, καθώς και οπωσδήποτε σχετικά με τα εξής:

- την ταυτότητα του οργανισμού που επεξεργάζεται τα δεδομένα
- τους σκοπούς για τους οποίους γίνεται η επεξεργασία των δεδομένων
- το είδος των δεδομένων που θα υποβληθούν σε επεξεργασία
- τη δυνατότητα ανάκλησης της συγκατάθεσης (π.χ. με την αποστολή ηλεκτρονικού μηνύματος για ανάκληση της συγκατάθεσης)
- όπου είναι απαραίτητο, το γεγονός ότι τα δεδομένα θα χρησιμοποιηθούν μόνο για αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ
- το κατά πόσον η συγκατάθεση σχετίζεται με διεθνή διαβίβαση των δεδομένων σας, τους ενδεχόμενους κινδύνους των διαβιβάσεων δεδομένων προς χώρες εκτός της ΕΕ εάν δεν υπάρχει για τις χώρες αυτές απόφαση της Επιτροπής περί επάρκειας και δεν προβλέπονται κατάλληλες εγγυήσεις.

Παραδείγματα

Δεν απαιτείται συγκατάθεση σύμφωνα με τη νομοθεσία:

Εγγράφεστε σε ωδείο για να παρακολουθήσετε μαθήματα πιάνου. Η φόρμα εγγραφής περιέχει ένα μακροσκελές έγγραφο με μικρή γραμματοσειρά στο οποίο χρησιμοποιούνται εξειδικευμένοι νομικοί και τεχνικοί όροι, το οποίο περιλαμβάνει τη δυνατότητα να διαβιβάσει το ωδείο τα προσωπικά στοιχεία σας σε λιανέμπορους που πωλούν μουσικά όργανα. Το ωδείο παραβιάζει τη νομοθεσία, καθώς η συγκατάθεσή σας σχετικά με τη λήψη υλικού εμπορικής προώθησης (πιθανώς από λιανέμπορους μουσικών οργάνων) δεν σας ζητήθηκε όπως ορίζεται από τη νομοθεσία.

Ανοίγετε έναν τραπεζικό λογαριασμό στο διαδίκτυο και θέλετε να επιβεβαιώσετε το αίτημά σας. Εμφανίζεται μια σελίδα με δύο πλαίσια επιλογής στα οποία αναγράφεται «Αποδέχομαι τους όρους και τις προϋποθέσεις» και «Συμφωνώ ότι η απόφαση σχετικά με το εάν πληρώ τις προϋποθέσεις για πιστωτική κάρτα βασίζεται μόνο στην κατάρτιση προφίλ χωρίς καμία ανθρώπινη παρέμβαση». Και τα δύο πλαίσια επιλογής είναι ενεργοποιημένα (επιλεγμένα) από προεπιλογή. Πρέπει να απενεργοποιήσετε το πλαίσιο επιλογής εάν δεν θέλετε να υπόκεισθε σε απόφαση σχετικά με το εάν πληροίτε τις προϋποθέσεις για πιστωτική κάρτα μόνο βάσει κατάρτισης προφίλ. Ακόμα και εάν δεν απενεργοποιήσετε το πλαίσιο επιλογής, η τράπεζα δεν θα έχει λάβει έγκυρη συγκατάθεση, καθώς τα προεπιλεγμένα πλαίσια δεν θεωρούνται έγκυρη συγκατάθεση σύμφωνα με τον ΓΚΠΔ.

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

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.

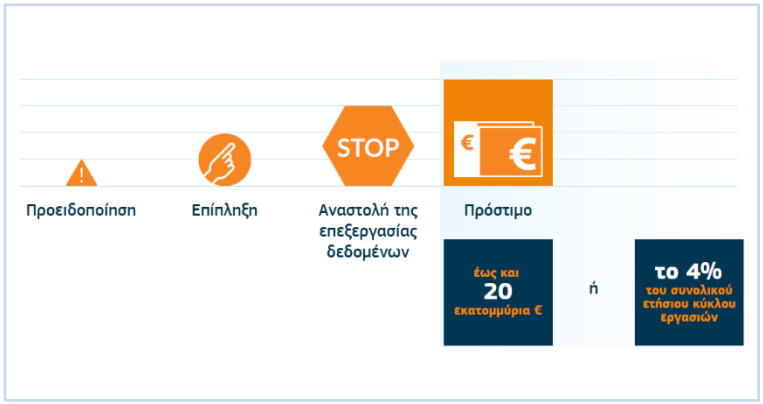
Παράδειγμα: *Ένα φυσικό πρόσωπο που απέκτησε πρόσβαση σε όλα του τα δεδομένα προσωπικού χαρακτήρα τον περασμένο μήνα υποβάλλει ξανά το ίδιο αίτημα για πρόσβαση στα ίδια δεδομένα. Μπορείτε είτε να το ενημερώσετε ότι απορρίπτετε το αίτημά του είτε να απαιτήσετε την καταβολή εύλογου τέλους.*

Επιβολή της νομοθεσίας και κυρώσεις

Τι γίνεται σε περίπτωση μη συμμόρφωσης της εταιρείας ή του οργανισμού σας με τους κανόνες προστασίας δεδομένων;

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) παρέχει μια σειρά επιλογών στις αρχές προστασίας δεδομένων σε περίπτωση μη συμμόρφωσης με τους κανόνες προστασίας δεδομένων:

- εάν η παράβαση είναι απλώς πιθανή, μπορεί να εκδοθεί **προειδοποίηση**
- εάν η παράβαση είναι διαπιστωμένη, ενδέχεται να επιβληθεί μεταξύ άλλων:
  - **επίπληξη**,
  - **προσωρινή ή οριστική απαγόρευση της επεξεργασίας** και
  - **πρόστιμο** μέγιστου ύψους 20 εκατομμυρίων ευρώ ή ίσο με το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών της επιχείρησης.



Πρέπει να επισημανθεί ότι σε περίπτωση παράβασης, η Αρχή Προστασίας Δεδομένων (ΑΠΔ) μπορεί να επιβάλει χρηματικό πρόστιμο, αντί ή επιπλέον της επίπληξης ή/και της απαγόρευσης της επεξεργασίας.

Η Αρχή Προστασίας Δεδομένων (ΑΠΔ) πρέπει να διασφαλίζει ότι τα πρόστιμα που επιβάλλονται σε κάθε ατομική περίπτωση είναι **αποτελεσματικά, αναλογικά και αποτρεπτικά**. Στο πλαίσιο αυτό, λαμβάνει υπόψη διάφορους παράγοντες, π.χ. τη φύση, τη σοβαρότητα και τη διάρκεια της παράβασης, το αν η παράβαση ήταν εσκεμμένη ή προήλθε από αμέλεια, τυχόν μέτρα που έχουν ληφθεί για τον μετριασμό της ζημίας που υπέστησαν φυσικά πρόσωπα, τον βαθμό συνεργασίας του οργανισμού κ.λπ.

Παράδειγμα

Μια εταιρεία πουλάει είδη σπιτιού στο διαδίκτυο. Μέσω του ιστοτόπου της οι καταναλωτές μπορούν να αγοράζουν ηλεκτρικές συσκευές κουζίνας, τραπέζια, καρέκλες και άλλα είδη σπιτιού εισάγοντας τα στοιχεία του τραπεζικού τους λογαριασμού. Ο ιστότοπος δέχτηκε κυβερνοεπίθεση που είχε ως αποτέλεσμα να αποκτηθεί πρόσβαση στα προσωπικά στοιχεία από τον υπεύθυνο της επίθεσης. Σε αυτήν την περίπτωση, η μη λήψη κατάλληλων τεχνικών μέτρων από την εταιρεία φαίνεται να είναι η αιτία της απώλειας των δεδομένων.

Σε αυτή την περίπτωση, η εποπτική αρχή θα πρέπει να λάβει υπόψη διάφορους παράγοντες πριν τη λήψη απόφασης σχετικά με το ποιο διορθωτικό εργαλείο πρέπει να χρησιμοποιηθεί. Τέτοιοι παράγοντες είναι οι εξής: Πόσο σοβαρή ήταν η ανεπάρκεια στο σύστημα τεχνολογίας πληροφοριών; Πόσο καιρό οι υποδομές τεχνολογίας πληροφοριών ήταν εκτεθειμένες σε έναν τέτοιο κίνδυνο; Έγιναν στο παρελθόν δοκιμές για την πρόληψη μιας τέτοιας επίθεσης; Τα δεδομένα πόσων πελατών κλάπηκαν/κοινολογήθηκαν; Τι είδους ήταν τα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν και συμπεριλαμβάνονταν σε αυτά ευαίσθητα δεδομένα; Όλοι αυτοί και άλλοι παράγοντες θα ληφθούν υπόψη από την εποπτική αρχή.

Μπορεί η εταιρεία μου/ο οργανισμός μου να φέρει ευθύνη για ζημιές;

Τα φυσικά πρόσωπα μπορούν να ζητήσουν αποζημίωση εάν μια εταιρεία ή ένας οργανισμός έχει παραβιάσει τον Γενικό Κανονισμό για την Προστασία των Δεδομένων (ΓΚΠΔ) και έχουν υποστεί υλική ζημία (π.χ. οικονομική απώλεια) ή μη υλική ζημία (π.χ. δυσφήμιση ή ψυχική οδύνη). Ο ΓΚΠΔ διασφαλίζει ότι θα τους καταβληθεί αποζημίωση, ανεξάρτητα από τον αριθμό των οργανισμών που συμμετείχαν στην επεξεργασία των δεδομένων τους. Το άτομο που έχει υποστεί ζημία μπορεί να αξιώσει αποζημίωση είτε άμεσα από τον οργανισμό είτε ενώπιον των αρμόδιων εθνικών δικαστηρίων. Η διαδικασία μπορεί να κινηθεί ενώπιον των δικαστηρίων του κράτους μέλους της ΕΕ όπου ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διαθέτει επαγγελματική εγκατάσταση ή όπου διαμένει (δηλαδή έχει τη συνήθη κατοικία του) ο πολίτης που ζητά αποζημίωση.

Το περιεχόμενο που εμπεριέχεται σε αυτό το έντυπο
έχει προέλθει από τον ιστότοπο της Ευρωπαϊκής Επιτροπής

πηγές και περισσότερες πληροφορίες:

Μάθετε περισσότερα στην σελίδα της Ευρωπαϊκής Επιτροπής σχετικά με την μεταρρύθμιση των κανόνων προστασίας δεδομένων της ΕΕ στον παρακάτω σύνδεσμο:
https://ec.europa.eu/info/law/law-topic/data-protection/reform_el

Ακολουθήστε τον διαδραστικό οδηγό ενημέρωσης στον παρακάτω σύνδεσμο:
http://ec.europa.eu/justice/smedataprotect/index_el.htm

Η πολιτική χρήσης εγγράφων της Ευρωπαϊκής Επιτροπής διέπεται από την απόφαση 2011/833/ΕΕ (ΕΕ L 330 της 14.12.2011, σ. 39)

επιμέλεια περιεχομένου:
Θεόδωρος Κεντιστός

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