# Κανόνες GDPR για επιχειρήσεις και οργανισμούς

## Περιεχόμενα

## 1. Εφαρμογή του κανονισμού

Ο 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 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.

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.

Παραπομπές:

Άρθρα 1, 2 και 3 και αιτιολογικές σκέψεις 13, 14, 15, 18, 19 και 21 του ΓΚΠΔ
Βλ. απόφαση του Δικαστηρίου, της 9ης Μαρτίου 2017, Manni, C-398/15, ECLI:EU:C:2017:1971
1 Περίληψη της δικαστικής απόφασης παρατίθεται στην ΕΕ C 144, της 8.5.2017, σ. 6.

## 2. 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.**

Παραπομπές
Άρθρο 4 σημεία 2 και 6 του ΓΚΠΔ

## 3. 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, π.χ. όνομα.επώνυμο@εταιρεία.com·
- αναγνωριστικός αριθμός κάρτας·
- δεδομένα τοποθεσίας (π.χ. η λειτουργία δεδομένων τοποθεσίας σε κινητό τηλέφωνο)*·
- διεύθυνση διαδικτυακού πρωτοκόλλου (IP)·
- αναγνωριστικό 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 εταιρείας·
ηλεκτρονική διεύθυνση του τύπου πληροφορίες@εταιρεία.com·
ανώνυμα δεδομένα.
Παραπομπές
Άρθρο 2, άρθρο 4 σημεία 1 και 5 και αιτιολογικές σκέψεις 14, 15, 26, 27, 29 και 30 του ΓΚΠΔ
WP 01248/07/EL, WP 136 Γνώμη 4/2007 σχετικά με την έννοια του όρου «δεδομένα προσωπικού χαρακτήρα»
Γνώμη 05/2014 της ομάδας εργασίας του άρθρου 29 σχετικά με τις τεχνικές ανωνυμοποίησης

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

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

Παραπομπές
Άρθρα 1 και 2 και αιτιολογικές σκέψεις 1, 2, 14, 18 και 27 του ΓΚΠΔ

1 Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

## 5. 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.

Παραπομπές

Άρθρο 5 παράγραφος 1 και αιτιολογική σκέψη 39 του ΓΚΠΔ

Γνώμη 03/2013 της ομάδας εργασίας του άρθρου 29 σχετικά με τον περιορισμό του σκοπού (WP 203)

## 6. 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».

Παραπομπές
Γνώμη 03/2013 της ομάδας εργασίας του άρθρου 29 σχετικά με τον περιορισμό του σκοπού (WP 203)

## 7. 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.

Παραπομπές
Άρθρο 5 παράγραφος 1 στοιχείο β), άρθρο 6 παράγραφος 4, άρθρο 89 παράγραφος 1 και αιτιολογικές σκέψεις 39 και 50 του ΓΚΠΔ
Γνώμη 03/2013 της ομάδας εργασίας του άρθρου 29 σχετικά με τον περιορισμό του σκοπού (WP 203)

## 8. Πόσα δεδομένα μπορούν να συλλεγούν;

Απάντηση
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.

Παραπομπές
Άρθρο 5 παράγραφος 1 στοιχείο γ) και αιτιολογική σκέψη 39 του ΓΚΠΔ

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

Απάντηση
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).

Παραπομπές
Άρθρο 5 παράγραφος 1 στοιχείο ε) και αιτιολογική σκέψη 39 του ΓΚΠΔ

## 10. 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 (δείτε πλήρη κατάλογο των δικαιωμάτων)·
- 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.

Παραπομπές
Άρθρο 12 παράγραφοι 1, 5 και 7, άρθρα 13 και 14 και αιτιολογικές σκέψεις 58 έως 62 του ΓΚΠΔ
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 σχετικά με ζητήματα διαφάνειας

## 11. Νομικοί Λόγοι Επεξεργασίας Δεδομένων

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).

Παραπομπές
Άρθρο 6 και αιτιολογικές σκέψεις 40 έως 49 του ΓΚΠΔ
Γνώμη 06/2014 της ομάδας εργασίας του άρθρου 29 για την έννοια των έννομων συμφερόντων των υπεύθυνων επεξεργασίας δεδομένων σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ

## 12. 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.

Παραπομπές
Άρθρο 6 και αιτιολογικές σκέψεις 47, 48 και 49 του ΓΚΠΔ
Γνώμη 06/2014 της ομάδας εργασίας του άρθρου 29 για την έννοια των έννομων συμφερόντων των υπεύθυνων επεξεργασίας δεδομένων σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ

## 13. Πότε είναι έγκυρη η συγκατάθεση;

Όταν απαιτείται συγκατάθεση για να υποβληθούν δεδομένα προσωπικού χαρακτήρα σε επεξεργασία, πρέπει να πληρούνται οι ακόλουθες προϋποθέσεις για να είναι έγκυρη η συγκατάθεση:

- η συγκατάθεση πρέπει να δίνεται ελεύθερα·
- η συγκατάθεση πρέπει να δίνεται εν πλήρει επιγνώσει·
- η συγκατάθεση πρέπει να δίνεται για συγκεκριμένο σκοπό·
- όλοι οι λόγοι για την επεξεργασία πρέπει να αναφέρονται με σαφήνεια·
- **η συγκατάθεση πρέπει να είναι ρητή και να δίνεται μέσω θετικής πράξης (π.χ. ηλεκτρονικό πλαίσιο επιλογής το οποίο το άτομο πρέπει να επιλέξει σαφώς στο διαδίκτυο ή υπογραφή σε φόρμα)·**
- η συγκατάθεση πρέπει να χρησιμοποιεί σαφή και απλή γλώσσα και να είναι ξεκάθαρα ορατή·
- παρέχεται δυνατότητα ανάκλησης της συγκατάθεσης και το άτομο ενημερώνεται για το γεγονός αυτό (π.χ. με τη μορφή συνδέσμου κατάργησης εγγραφής στο τέλος ενός ενημερωτικού δελτίου μέσω ηλεκτρονικού μηνύματος).

Για να δίνεται ελεύθερα η συγκατάθεση, το άτομο πρέπει να έχει ελευθερία επιλογής και πρέπει να μπορεί να αρνηθεί ή να ανακαλέσει τη συγκατάθεση χωρίς να βρεθεί σε μειονεκτική θέση. Η συγκατάθεση δεν δίνεται ελεύθερα εάν, για παράδειγμα, υπάρχει σαφής ανισότητα μεταξύ του ατόμου και της επιχείρησης/οργανισμού (π.χ. σχέση εργοδότη/εργαζομένου) ή όταν μια επιχείρηση ή ένας οργανισμός ζητά συγκατάθεση από άτομα για την επεξεργασία μη απαραίτητων δεδομένων προσωπικού χαρακτήρα ως προαπαιτούμενο για την εκτέλεση σύμβασης ή την παροχή υπηρεσίας.

Για να παραχωρείται η συγκατάθεση εν πλήρει επιγνώσει, πρέπει να παρέχονται στο άτομο οπωσδήποτε οι εξής πληροφορίες:

- η ταυτότητα του οργανισμού που επεξεργάζεται τα δεδομένα·
- οι σκοποί για τους οποίους γίνεται η επεξεργασία των δεδομένων·
- το είδος των δεδομένων που θα υποβληθούν σε επεξεργασία·
- η δυνατότητα ανάκλησης της συγκατάθεσης που έχει δοθεί (π.χ. ύπαρξη συνδέσμου κατάργησης εγγραφής στο τέλος ηλεκτρονικού μηνύματος)·
- όπου είναι απαραίτητο, το γεγονός ότι τα δεδομένα θα χρησιμοποιηθούν μόνο για αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ·
- εάν η συγκατάθεση σχετίζεται με διεθνή διαβίβαση, τους ενδεχόμενους κινδύνους των διαβιβάσεων δεδομένων προς τρίτες χώρες για τις οποίες η Επιτροπή δεν έχει εκδώσει απόφαση επάρκειας και στις οποίες δεν παρέχονται κατάλληλες εγγυήσεις.
- Θυμηθείτε: όταν κάποιος δίνει τη συγκατάθεσή του για την επεξεργασία των δεδομένων του προσωπικού χαρακτήρα, μπορείτε να επεξεργάζεστε τα δεδομένα μόνο για τους σκοπούς για τους οποίους έχει παραχωρηθεί η συγκατάθεση.

Παραδείγματα
Ελεύθερη συγκατάθεση

Είστε αεροπορική εταιρεία και η δήλωση εχεμύθειας που χρησιμοποιείτε αναφέρει ότι τα δεδομένα προσωπικού χαρακτήρα των πελατών μπορεί να υποβληθούν σε επεξεργασία για διαγωνισμό που διοργανώνεται από εσάς με έπαθλο μία δωρεάν πτήση. Οι πελάτες που επέλεξαν το τετραγωνίδιο για να δηλώσουν ότι συμφωνούν να συμμετάσχουν στον διαγωνισμό έχουν δηλώσει με σαφήνεια ότι επιθυμούν να υποβληθούν τα δεδομένα τους προσωπικού χαρακτήρα σε επεξεργασία για τον σκοπό του διαγωνισμού. Υπάρχει συγκατάθεση για την επεξεργασία των δεδομένων για τον σκοπό του διαγωνισμού αλλά όχι για άλλους σκοπούς.

Η συγκατάθεση δεν είναι ελεύθερη

Η εταιρεία ή ο οργανισμός σας προσφέρει υπηρεσίες προβολής ταινιών στο διαδίκτυο. Κατά τη συλλογή των δεδομένων που απαιτούνται για τη σχετική σύμβαση, ζητάτε και επιπλέον δεδομένα, όπως ο γενετήσιος προσανατολισμός ή οι πολιτικές πεποιθήσεις ενός ατόμου. Το εν λόγω άτομο μπορεί να πιστεύει ότι η συγκατάθεσή του για την επεξεργασία αυτού του είδους των δεδομένων είναι απαραίτητη για να έχει πρόσβαση στις ταινίες που ζητά. Η συγκατάθεση στην περίπτωση αυτή δεν δίνεται ελεύθερα, αλλά είναι «συγκατάθεση υπό δέσμευση».

Παραπομπές
Άρθρο 4 σημείο 11, άρθρο 7 και αιτιολογικές σκέψεις 32, 42 και 43 του ΓΚΠΔ
Γνώμη της ομάδας εργασίας του άρθρου 29 σχετικά με τη συγκατάθεση που εγκρίθηκε στις 28 Νοεμβρίου 2017

## 14. 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 περιελάμβανε 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.

Παραπομπές
Άρθρο 4 σημείο 11, άρθρο 7 και αιτιολογική σκέψη 171 του ΓΚΠΔ
Γνώμη της ομάδας εργασίας του άρθρου 29 σχετικά με τη συγκατάθεση που εγκρίθηκε στις 28 Νοεμβρίου 2017

## 15. 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.

Παραπομπές
Άρθρο 7 και αιτιολογικές σκέψεις 32, 33, 42, 43 και 58 του ΓΚΠΔ

Γνώμη 15/2011 της ομάδας εργασίας του άρθρου 29 σχετικά με τον ορισμό της συγκατάθεσης (θα ενημερωθεί με τη γνώμη που εγκρίθηκε στις 28 Νοεμβρίου 2017)

## 16. Πώς λαμβάνεται συγκατάθεση για επεξεργασία όσον αφορά επιστημονική έρευνα;

Επιτρέπεται κάποιος βαθμός ευελιξίας όσον αφορά τον βαθμό του προσδιορισμού και του επιπέδου λεπτομέρειας της συγκατάθεσης στο πλαίσιο της επιστημονικής έρευνας. Κατά τη συλλογή δεδομένων προσωπικού χαρακτήρα, οι ερευνητές ενδέχεται να μην μπορούν να προσδιορίσουν πλήρως τους σκοπούς της επεξεργασίας τους. Σε αυτές τις περιπτώσεις μπορούν να ζητήσουν από τα άτομα να δώσουν τη συγκατάθεσή τους για ορισμένα πεδία επιστημονικής έρευνας ή τμήματα ερευνητικών έργων. Εν πάση περιπτώσει, η συγκατάθεση πρέπει να διατηρεί τα βασικά στοιχεία της, πράγμα που σημαίνει ότι πρέπει να δίνεται ελεύθερα, εν πλήρει επιγνώσει, να παρέχεται με σαφή θετική ενέργεια και να είναι συγκεκριμένη στον βαθμό που επιτρέπει η εκάστοτε έρευνα. Οι ερευνητές πρέπει να βεβαιωθούν ότι συμμορφώνονται επίσης με τα πρότυπα δεοντολογίας και μεθοδολογίας που απαιτούνται στο πεδίο τους.

## 17. 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.

Παραπομπές
Άρθρο 4 σημεία 13, 14 και 15, άρθρο 9 και αιτιολογικές σκέψεις 51 έως 56 του ΓΚΠΔ

Παράδειγμα
Ομάδα ερευνητών επιθυμεί να μελετήσει μια συγκεκριμένη μορφή καρκίνου αλλά τα μέλη της γνωρίζουν τις πιθανές επιπτώσεις για άλλες μορφές καρκίνου. Σε αυτήν την περίπτωση μπορούν να ζητήσουν τη συγκατάθεση ενός ατόμου για επεξεργασία δεδομένων που σχετίζονται με την έρευνα για τον καρκίνο.

Παραπομπή
Αιτιολογική σκέψη 33 του ΓΚΠΔ

## 18. Υπό ποιες προϋποθέσεις μπορεί η εταιρεία μου/ο οργανισμός μου να επεξεργάζεται ευαίσθητα δεδομένα; (**)

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.

**Παραπομπές**

**Άρθρο 9 και αιτιολογικές σκέψεις 51-56 του ΓΚΠΔ**

## 19. Υπάρχουν συγκεκριμένες εγγυήσεις για δεδομένα παιδιών;

Η εταιρεία ή ο οργανισμός σας μπορεί να επεξεργαστεί δεδομένα προσωπικού χαρακτήρα ενός παιδιού βάσει συγκατάθεσης εφόσον έχει λάβει τη ρητή συγκατάθεση του γονιού ή κηδεμόνα τους μέχρι μια συγκεκριμένη ηλικία. Το όριο ηλικίας για τη λήψη γονικής συγκατάθεσης ποικίλλει από τα 13 έως τα 16 έτη, ανάλογα με την ηλικία που καθορίζεται εν προκειμένω σε κάθε κράτος μέλος της ΕΕ. Για περισσότερες πληροφορίες, απευθυνθείτε στην εθνική σας αρχή προστασίας δεδομένων.

Πρέπει να καταβάλλονται φιλότιμες προσπάθειες, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία, για να επαληθεύεται ότι η συγκατάθεση δίνεται πράγματι σύμφωνα με τη νομοθεσία. Αυτό σημαίνει ότι η εταιρεία ή ο οργανισμός σας πρέπει να εφαρμόσει μέτρα επαλήθευσης της ηλικίας (π.χ. ερωτήσεις ελέγχου, ενέργειες στον ιστότοπο).

Πρέπει να λαμβάνεται συγκατάθεση από τον γονιό ή τον κηδεμόνα εάν ο οργανισμός σας δραστηριοποιείται σε ιστότοπους κοινωνικής δικτύωσης που παρέχουν δωρεάν παιχνίδια σε παιδιά ή οικογενειακή ασφάλιση, για παράδειγμα.

Εάν ο οργανισμός σας απευθύνεται σε παιδιά, πρέπει να διασφαλίσετε ότι οποιαδήποτε πληροφορία και επικοινωνία που απευθύνεται σε ένα παιδί είναι εύκολα προσβάσιμη και σε σαφή και απλή γλώσσα η οποία είναι ευνόητη για ένα παιδί.

Οι υπηρεσίες πρόληψης ή παροχής συμβουλών που προσφέρονται άμεσα σε παιδιά δεν απαιτούν γονική άδεια, καθώς στόχο έχουν να προστατεύσουν τα μείζονα συμφέροντα του παιδιού.

Παραπομπές
Άρθρα 8 και 12 και αιτιολογικές σκέψεις 38 και 58 του ΓΚΠΔ

## 20. 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 περιελάμβανε 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/ΕΚ1).**

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.

Παραπομπές
Άρθρο 4 σημείο 10 και άρθρα 5, 6, 14 και 21 του ΓΚΠΔ
Γνώμη της ομάδας εργασίας του άρθρου 29 σχετικά με ζητήματα διαφάνειας
Κανόνες της οδηγίας για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες 2002/58/ΕΚ σχετικά με την εμπορική προώθηση, ιδίως άρθρο 13
1 Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) (ΕΕ L 201 της 31.7.2002, σ. 37).

## 21. 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 ΤΠ, συμπεριλαμβανομένης της αποθήκευσης σε νέφος.** 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 ΤΠ 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.

Παραπομπές
Παραπομπές: Άρθρο 4 σημεία 7 και 8, άρθρα 24, 26, 28 και 29 και αιτιολογικές σκέψεις 74, 79 και 81 του ΓΚΠΔ
Γνώμη 1/2010 της ομάδας εργασίας του άρθρου 29 σχετικά με την έννοια του «υπεύθυνου επεξεργασίας» και του «εκτελούντος την επεξεργασία» (WP 169)

## 22. 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.

Παραπομπές
Άρθρο 28 και αιτιολογική σκέψη 81 του ΓΚΠΔ

## 23. 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.

Παραπομπή
Κεφάλαιο IV του ΓΚΠΔ

## 24. 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.

Παραπομπές
Άρθρο 25 και αιτιολογική σκέψη 78 του ΓΚΠΔ

## 25. 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 ΑΠΔ 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 ΑΠΔ 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 ΑΠΔ και τα φυσικά πρόσωπα ανάλογα με τα δεδομένα που είχαν υποβληθεί σε επεξεργασία από τον εκτελούντα την επεξεργασία.

Παραπομπές
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 σχετικά με την ειδοποίηση για παραβίαση δεδομένων προσωπικού χαρακτήρα σύμφωνα με τον κανονισμό (ΕΕ) 2016/679, 3 Οκτωβρίου 2017 (WP 250)
Άρθρο 4 σημείο 12, άρθρα 33 και 34 και αιτιολογικές σκέψεις 85 έως 88 του ΓΚΠΔ

## 26. Πότε πρέπει να γίνεται εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ); (**)

Απάντηση
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 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.**

Παραπομπές
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 για την εκτίμηση αντίκτυπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και τον προσδιορισμό των περιπτώσεων στις οποίες η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού (ΕΕ) 2016/679, 4 Απριλίου 2017
Άρθρα 35 και 36 και αιτιολογικές σκέψεις 89 έως 96 του ΓΚΠΔ

## 27. 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.

Παραπομπές
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 σχετικά με τους υπεύθυνους προστασίας δεδομένων, 5 Απριλίου 2017 (WP 243)
Άρθρα 37, 38 και 39 και αιτιολογική σκέψη 97 του ΓΚΠΔ

## 28. 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.

Παραπομπή
Άρθρα 37, 38 και 39 και αιτιολογική σκέψη 97 του ΓΚΠΔ

## 29. 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.

Παραπομπές

Κεφάλαιο V, άρθρα 44 έως 50 και αιτιολογικές σκέψεις 101 έως 116 του ΓΚΠΔ

Τελευταία έγγραφα εργασίας της ομάδας εργασίας του άρθρου 29 σχετικά με τις διεθνείς διαβιβάσεις
Έγγραφο εργασίας σχετικά με τα κριτήρια αναφοράς για την επάρκεια (ενημέρωση του πρώτου κεφαλαίου του εγγράφου WP 12), WP 254
Έγγραφο εργασίας το οποίο καταρτίζει πίνακα με τα στοιχεία και τις αρχές που πρέπει να περιλαμβάνονται στους δεσμευτικούς εταιρικούς κανόνες, WP 256
Έγγραφο εργασίας το οποίο καταρτίζει πίνακα με τα στοιχεία και τις αρχές που πρέπει να περιλαμβάνονται στους δεσμευτικούς εταιρικούς κανόνες για τον εκτελούντα την επεξεργασία, WP 257
Για αναφορά δείτε επίσης την ανακοίνωση της Ευρωπαϊκής Επιτροπής «Ανταλλαγή και προστασία των δεδομένων προσωπικού χαρακτήρα σε έναν παγκοσμιοποιημένο κόσμο»1, 10 Ιανουαρίου 2017
1 COM(2017)7 final

## 30. 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 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 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.

Παραπομπές
Άρθρα 24, 40 έως 43 και 83 και αιτιολογικές σκέψεις 98, 99, 100, 148, 150 και 151 του ΓΚΠΔ

## 31. 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.

Παραπομπές
Άρθρα 12 και 15 έως 22 και αιτιολογικές σκέψεις 59 και 63 έως 71 του ΓΚΠΔ

## 32. Σε ποια δεδομένα προσωπικού χαρακτήρα και πληροφορίες μπορεί να έχει πρόσβαση ένα φυσικό πρόσωπο κατόπιν αιτήματος;

Όταν κάποιος υποβάλει αίτημα για πρόσβαση στα δεδομένα του προσωπικού χαρακτήρα, η εταιρεία ή ο οργανισμός σας πρέπει:

- ✓ να επιβεβαιώσει εάν υποβάλλει ή όχι σε επεξεργασία δεδομένα προσωπικού χαρακτήρα που αφορούν το συγκεκριμένο πρόσωπο·
- ✓ να παράσχει στο εν λόγω πρόσωπο αντίγραφο των δεδομένων προσωπικού χαρακτήρα που διαθέτει σχετικά με αυτό·
- ✓ να παράσχει πληροφορίες σχετικά με την επεξεργασία (π.χ. σκοποί, κατηγορίες δεδομένων προσωπικού χαρακτήρα, αποδέκτες κ.λπ.).
- ✓ Η εταιρεία ή ο οργανισμός σας πρέπει να παρέχει στα άτομα αντίγραφο των δεδομένων τους προσωπικού χαρακτήρα δωρεάν. Παρόλα αυτά, για περαιτέρω αντίγραφα μπορεί να χρεωθεί εύλογο τέλος.

Η άσκηση του δικαιώματος πρόσβασης είναι στενά συνδεδεμένη με την άσκηση του δικαιώματος φορητότητας των δεδομένων, και τούτο για να μπορεί το άτομο να διαβιβάζει τα δεδομένα του σε άλλον οργανισμό.

Είναι σημαντικό, στη δήλωση εχεμύθειας της εταιρείας ή του οργανισμού σας, να γίνεται σαφής διάκριση μεταξύ των δύο δικαιωμάτων. Επομένως, πρέπει να αναφέρονται εν συντομία και τα δύο δικαιώματα χωριστά.

Παράδειγμα
Η εταιρεία ή ο οργανισμός σας παρέχει ηλεκτρονική υπηρεσία κοινωνικής δικτύωσης όπου φυσικά πρόσωπα μπορούν να ανταλλάσσουν μηνύματα και φωτογραφίες. Ένας χρήστης ζητά να αποκτήσει πρόσβαση στα δεδομένα του προσωπικού χαρακτήρα και να ελέγξει τι δεδομένα προσωπικού χαρακτήρα που τον αφορούν υποβάλλονται σε επεξεργασία από την εταιρεία ή τον οργανισμό σας. Η εταιρεία ή ο οργανισμός σας πρέπει να επιβεβαιώσει ότι όντως επεξεργάζεται δεδομένα προσωπικού χαρακτήρα που τον αφορούν και να του παράσχει αντίγραφο (π.χ. του ονοματεπωνύμου του, των στοιχείων επικοινωνίας, των μηνυμάτων και των φωτογραφιών που ανταλλάχθηκαν). Πρέπει επίσης να του παράσχει πληροφορίες σχετικά με την επεξεργασία, οι οποίες συνήθως περιλαμβάνονται στη δήλωση εχεμύθειας της υπηρεσίας σας.

Παραπομπές
Άρθρο 15 και αιτιολογικές σκέψεις 63 και 64 του ΓΚΠΔ

## 33. Πρέπει πάντα να διαγράφουμε δεδομένα προσωπικού χαρακτήρα εάν ένα άτομο το ζητά;

Ο Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΓΚΠΔ) δίνει στα άτομα το δικαίωμα να ζητούν τη διαγραφή των δεδομένων τους και οι οργανισμοί υποχρεούνται να το πράξουν, εκτός από τις ακόλουθες περιπτώσεις:

- ⇨ τα δεδομένα προσωπικού χαρακτήρα που κατέχει η εταιρεία ή ο οργανισμός σας είναι απαραίτητα για την άσκηση του δικαιώματος της ελευθερίας έκφρασης·
- ⇨ όταν νομική υποχρέωση επιβάλλει τη διατήρηση των δεδομένων·
- ⇨ για λόγους δημοσίου συμφέροντος (π.χ. δημόσια υγεία, σκοποί επιστημονικής, στατιστικής ή ιστορικής έρευνας).

Εάν η εταιρεία ή ο οργανισμός σας έχει επεξεργαστεί δεδομένα παράνομα, πρέπει να τα διαγράψει. Η διαγραφή είναι υποχρεωτική επίσης στην περίπτωση ατόμου του οποίου συλλέχθηκαν δεδομένα προσωπικού χαρακτήρα όταν ήταν ακόμα ανήλικος.

Όσον αφορά το δικαίωμα στη λήθη στο διαδίκτυο, οι οργανισμοί καλούνται να λαμβάνουν εύλογα μέτρα (π.χ. τεχνικά μέτρα) για να ενημερώνουν άλλους ιστότοπους ότι ένα συγκεκριμένο άτομο έχει ζητήσει τη διαγραφή των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

Τα δεδομένα μπορούν επίσης να φυλάσσονται εάν έχουν υποβληθεί σε κατάλληλη διαδικασία ανωνυμοποίησης.

Παραδείγματα
Τα δεδομένα δεν πρέπει να διαγραφούν

Η εταιρεία ή ο οργανισμός σας έχει μια ηλεκτρονική εφημερίδα. Ένας από τους δημοσιογράφους σας δημοσιεύει ένα άρθρο σχετικά με το πώς ένας πολιτικός είχε κάνει νομιμοποίηση εσόδων από παράνομες δραστηριότητες σε υπεράκτιες τράπεζες. Ο πολιτικός ζητά να αφαιρεθεί το άρθρο γιατί υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα που τον αφορούν. Δεδομένου ότι τα δεδομένα προσωπικού χαρακτήρα χρησιμοποιούνται με σκοπό την άσκηση του δικαιώματος της ελευθερίας έκφρασης, η εταιρεία ή ο οργανισμός σας δεν υποχρεούται καταρχήν να τα διαγράψει. Ωστόσο, αυτό εξαρτάται από την ισχύουσα εθνική νομοθεσία.

Τα δεδομένα πρέπει να διαγραφούν

Η εταιρεία ή ο οργανισμός σας είναι ιδιοκτήτης μιας πλατφόρμας κοινωνικής δικτύωσης. Ένας ανήλικος ανεβάζει φωτογραφίες. Ωστόσο, μερικά χρόνια αργότερα αποφασίζει ότι οι εν λόγω φωτογραφίες είναι ενδεχομένως επιβλαβείς για τις επαγγελματικές του προοπτικές. Καθώς το άτομο ήταν ανήλικος τη στιγμή της μεταφόρτωσης, η εταιρεία ή ο οργανισμός σας υποχρεούται να διαγράψει τις εν λόγω φωτογραφίες. Επιπλέον, εάν οι φωτογραφίες έχουν υποβληθεί σε επεξεργασία σε άλλους ιστότοπους, πρέπει να λάβει εύλογα μέτρα για να τους ενημερώσει ότι έχει υποβληθεί αίτημα διαγραφής των φωτογραφιών.

Παραπομπές
Άρθρο 17 και αιτιολογικές σκέψεις 65 και 66 του ΓΚΠΔ
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 σχετικά με την εφαρμογή της απόφασης του Δικαστηρίου, της 13ης Μαΐου 2014, **Google Spain** και **Google**, C-131/12, ECLI:EU:C:2014:317 (WP 225)

## 34. Τι γίνεται εάν κάποιος αντιτίθεται στην επεξεργασία των δεδομένων του προσωπικού χαρακτήρα από την εταιρεία μου;

Τα φυσικά πρόσωπα έχουν το δικαίωμα να αρνηθούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα για συγκεκριμένους λόγους. Το εάν υφίσταται μια τέτοια κατάσταση πρέπει να εξετάζεται με γνώμονα τα δεδομένα κάθε περίπτωσης.

Τα άτομα μπορούν να εναντιωθούν μόνο στις περιπτώσεις όπου δημόσια διοίκηση επεξεργάζεται τα δεδομένα στο πλαίσιο των δημόσιων καθηκόντων της ή όταν εταιρεία επεξεργάζεται τα δεδομένα βάσει των έννομων συμφερόντων της. Σε τέτοιες περιπτώσεις, η εταιρεία ή ο οργανισμός σας δεν μπορεί πλέον να επεξεργάζεται τα δεδομένα εκτός εάν αποδεικνύει ότι η επεξεργασία είναι αναγκαία για λόγους που υπερισχύουν των δικαιωμάτων και των ελευθεριών του ατόμου ή εάν τα δεδομένα απαιτούνται για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων.

**Τα άτομα έχουν επίσης το δικαίωμα να αντιταχθούν οποιαδήποτε στιγμή στην επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης. Ως άμεση εμπορική προώθηση νοείται, σύμφωνα με τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, οποιαδήποτε ενέργεια εταιρείας με σκοπό την προώθηση διαφημιστικού υλικού ή υλικού εμπορικής προώθησης που απευθύνεται σε συγκεκριμένα άτομα. Η εταιρεία ή ο οργανισμός σας πρέπει να ενημερώνει τα άτομα, στη δήλωση εχεμύθειας ή το αργότερο την πρώτη φορά που επικοινωνεί μαζί τους, ότι θα χρησιμοποιεί τα δεδομένα τους προσωπικού χαρακτήρα για άμεση εμπορική προώθηση και ότι έχουν δικαίωμα να αντιταχθούν χωρίς χρέωση. Αν ένα άτομο αντιταχθεί στην επεξεργασία για σκοπούς άμεσης εμπορικής προώθησης, η εταιρεία ή ο οργανισμός σας δεν μπορεί πλέον να επεξεργάζεται τα δεδομένα του προσωπικού χαρακτήρα για τέτοιους σκοπούς.**

Παράδειγμα
Στον ασφαλιστικό τομέα, πολύ συχνά τα δεδομένα προσωπικού χαρακτήρα είναι απαραίτητα για την υποστήριξη νομικών αξιώσεων στην περίπτωση μέτρων καταπολέμησης της απάτης ή της νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Σε αυτές τις περιπτώσεις, οι ασφαλιστικές εταιρείες μπορεί να αρνηθούν να δεχθούν το αίτημα ενός ατόμου για τη μη επεξεργασία των δεδομένων του με βάση λόγους που υπερισχύουν των δικαιωμάτων και των ελευθεριών του ατόμου.

Παραπομπές
Άρθρο 21 και αιτιολογικές σκέψεις 69 και 70 του ΓΚΠΔ
Γνώμη 06/2014 της ομάδας εργασίας του άρθρου 29 για την έννοια των έννομων συμφερόντων των υπεύθυνων επεξεργασίας δεδομένων σύμφωνα με το άρθρο 7 της οδηγίας 95/46/ΕΚ

## 35. Μπορούν τα άτομα να ζητούν τη διαβίβαση των δεδομένων τους σε άλλον οργανισμό;

Ναι, τα φυσικά πρόσωπα έχουν το δικαίωμα στη φορητότητα των δεδομένων, δηλαδή να λαμβάνουν από την εταιρεία/τον οργανισμό σας τα δεδομένα προσωπικού χαρακτήρα που σας παρείχαν, σε δομημένο μορφότυπο αναγνώσιμο από μηχάνημα, και να τα διαβιβάζουν σε άλλη εταιρεία/οργανισμό. Το δικαίωμα μπορεί να ασκείται μόνο στις περιπτώσεις όπου τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν στο πλαίσιο σύμβασης ή βάσει συγκατάθεσης και τα εν λόγω δεδομένα υποβάλλονται σε επεξεργασία με αυτόματα μέσα.

Παράδειγμα
Ένας ασθενής ιδιωτικής κλινικής στο Βέλγιο μεταφέρεται σε άλλη κλινική στη Γερμανία και. ζητά από τη βελγική κλινική, η οποία διατηρεί ηλεκτρονικά αρχεία για αυτόν, να του παράσχει τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν σε δομημένο μορφότυπο αναγνώσιμο από μηχάνημα για να μπορέσει να τα διαβιβάσει στους σχετικούς επαγγελματίες υγείας στη Γερμανία. **Η βελγική κλινική θα πρέπει να του διαθέσει τα δεδομένα προσωπικού χαρακτήρα σε ανοικτό μορφότυπο** (π.χ. XML, JSON, CSV κ.λπ.) που χρησιμοποιείται συνήθως. Κατά την επιλογή του μορφοτύπου των δεδομένων, ο οργανισμός θα πρέπει να λάβει υπόψη πώς αυτός ενδέχεται να επηρεάσει ή να παρεμποδίσει το δικαίωμα του ατόμου για εκ νέου χρήση των δεδομένων. **Για παράδειγμα, η παροχή σε ένα άτομο των αρχείων του σε έκδοση PDF μπορεί να μην διασφαλίζει επαρκώς ότι τα δεδομένα προσωπικού χαρακτήρα θα μπορούν να επαναχρησιμοποιηθούν εύκολα.**

Παραπομπές
Άρθρο 20 και αιτιολογική σκέψη 68
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 σχετικά με τη φορητότητα των δεδομένων

## 36. Υπάρχουν περιορισμοί όσον αφορά τη χρήση αυτοματοποιημένης λήψης αποφάσεων;

Ναι, τα φυσικά πρόσωπα δεν θα πρέπει να υπόκεινται σε απόφαση που βασίζεται μόνο σε αυτοματοποιημένη επεξεργασία (όπως οι αλγόριθμοι) και η οποία να είναι νομικά δεσμευτική ή να τους επηρεάζει σε σημαντικό βαθμό.

Μια απόφαση μπορεί να θεωρείται ότι παράγει έννομα αποτελέσματα όταν επηρεάζονται τα νομικά δικαιώματα ή το νομικό καθεστώς του φυσικού προσώπου (π.χ. το δικαίωμα ψήφου του). Επιπλέον, η επεξεργασία μπορεί να επηρεάσει σε σημαντικό βαθμό ένα άτομο εάν επηρεάζει την προσωπική του κατάσταση, τη συμπεριφορά του ή τις επιλογές του (για παράδειγμα, αυτόματη επεξεργασία μπορεί να οδηγήσει στην απόρριψη ηλεκτρονικής αίτησης πίστωσης).

Η χρήση αυτοματοποιημένης επεξεργασίας για τη λήψη απόφασης επιτρέπεται μόνο στις εξής περιπτώσεις:

είναι απαραίτητη η απόφαση με βάση τον αλγόριθμο (δηλ. δεν θα πρέπει να υπάρχει κανένας άλλος τρόπος να επιτευχθεί ο ίδιος στόχος) για τη σύναψη ή την εκτέλεση σύμβασης με το άτομο το οποίου τα δεδομένα υποβάλλονται σε επεξεργασία μέσω του αλγόριθμου (π.χ. ηλεκτρονική αίτηση δανείου)·
συγκεκριμένος νόμος (της ΕΕ ή εθνικός) επιτρέπει τη χρήση αλγορίθμων και παρέχει κατάλληλες εγγυήσεις για την προστασία των δικαιωμάτων, των ελευθεριών και των έννομων συμφερόντων του ατόμου (π.χ. κανονισμοί κατά της φοροδιαφυγής)·
το άτομο έχει δώσει ρητή συγκατάθεση σε απόφαση που βασίζεται στον αλγόριθμο.
Ωστόσο, η απόφαση που λαμβάνεται πρέπει να προστατεύει τα δικαιώματα, τις ελευθερίες και τα έννομα συμφέροντα του ατόμου, θέτοντας σε εφαρμογή κατάλληλες εγγυήσεις. Με εξαίρεση τις περιπτώσεις όπου μια τέτοια λήψη απόφασης βασίζεται σε νόμο, το άτομο πρέπει να ενημερωθεί οπωσδήποτε σχετικά με τα εξής: **i)** τη λογική της διαδικασίας λήψης αποφάσεων, **ii)** το δικαίωμά του να αξιώσει ανθρώπινη παρέμβαση, **iii)** τις ενδεχόμενες συνέπειες της επεξεργασίας, και **iv)** το δικαίωμά του να προσβάλει την απόφαση. Επομένως, η εταιρεία ή ο οργανισμός σας πρέπει να προβεί στις απαραίτητες διαδικαστικές ρυθμίσεις έτσι ώστε να επιτρέψει στο άτομο να εκφράσει την άποψή του και να προσβάλει την απόφαση.

Τέλος, θα πρέπει να επιδεικνύεται ιδιαίτερη προσοχή εάν ο αλγόριθμος χρησιμοποιεί ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα. Η αυτοματοποιημένη λήψη αποφάσεων επιτρέπεται μόνο στις ακόλουθες περιπτώσεις:

το άτομο έχει δώσει ρητή συγκατάθεσή·
η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος με βάση τη νομοθεσία της ΕΕ ή εθνική νομοθεσία.
Επιπλέον, εάν το άτομο είναι παιδί, θα πρέπει να αποφεύγεται η λήψη αποφάσεων οι οποίες είναι αποκλειστικά αυτοματοποιημένες και οι οποίες

παράγουν έννομα ή άλλα εξίσου σημαντικά αποτελέσματα για το παιδί, καθώς τα παιδιά συνιστούν μια πιο ευπαθή ομάδα της κοινωνίας.

Παράδειγμα
Η εταιρεία ή ο οργανισμός σας είναι ηλεκτρονική τράπεζα που προσφέρει δάνεια. Οι πελάτες εισάγουν τα δεδομένα τους και ένας αλγόριθμός παράγει αποτελέσματα σχετικά με το αν θα πρέπει ή όχι να προσφερθεί στον πελάτη δάνειο και το προτεινόμενο επιτόκιο. Η εταιρεία ή ο οργανισμός σας θα πρέπει να ελέγξει την εν λόγω απόφαση πριν την ανακοινώσει στον υποψήφιο πελάτη και να τον ενημερώσει ότι μπορεί να εκφράσει τη γνώμη του και ενδεχομένως να προσβάλει την απόφαση, λαμβάνοντας υπόψη ότι το άτομο έχει το δικαίωμα να μην υπόκειται σε απόφαση στηριζόμενη σε αλγόριθμους.

Παραπομπές
Άρθρο 4 σημείο 4, άρθρο 22 και αιτιολογικές σκέψεις 71 και 72 του ΓΚΠΔ
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 για την αυτοματοποιημένη ατομική λήψη απόφασης και την κατάρτιση προφίλ για τους σκοπούς του κανονισμού (ΕΕ) 2016/679 (WP 251)

## 37. 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 ΑΠΔ μπορεί να επιβάλει χρηματικό πρόστιμο, αντί ή επιπλέον της επίπληξης ή/και της απαγόρευσης της επεξεργασίας.

**Η 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 ΤΠ; Πόσο καιρό οι υποδομές ΤΠ 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.

Παραπομπές
Άρθρα 58, 60, 83 και 84 και αιτιολογικές σκέψεις 129, 148, 150 και 151 του ΓΚΠΔ
Κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 για την εφαρμογή και τον ορισμό διοικητικών προστίμων για τους σκοπούς του κανονισμού (ΕΕ) 2016/679, 3 Οκτωβρίου 2017

## 38. 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.

Παραπομπή
Άρθρο 82 και αιτιολογικές σκέψεις 146 και 147 του ΓΚΠΔ

*Σημείωση: Όλο το υλικό του εγγράφου, οι διατυπώσεις, οι νομικές παραπομπές κλπ* ***προέρχεται, έχει ως πηγή και αποτελεί πνευματική ιδιοκτησία της ιστοσελίδας της Ευρωπαϊκής Επιτροπής στην Ελληνική της έκδοση****. Η Ευρωπαϊκή Επιτροπή διατηρεί αυτόν τον ιστότοπο για να διευκολύνει την πρόσβαση του κοινού σε πληροφορίες σχετικά με τις πρωτοβουλίες της και, εν γένει, τις πολιτικές της Ευρωπαϊκής Ένωσης. Οι πληροφορίες που περιλαμβάνονται: Είναι γενικού μόνο χαρακτήρα και δεν αφορούν συγκεκριμένες περιστάσεις σχετικά με οποιοδήποτε φυσικό ή νομικό πρόσωπο. Δεν είναι απαραίτητα ολοκληρωμένες, πλήρεις, ακριβείς ή επικαιροποιημένες. Δεν αποτελούν επαγγελματικές ή νομικές συμβουλές (αν χρειάζεστε συγκεκριμένες συμβουλές, πρέπει πάντοτε να απευθύνεστε σε ειδικευμένους επαγγελματίες).*