HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

Προσωπικά Δεδομένα
στο νέο ρυθμιστικό πλαίσιο

Σεμινάριο E-Themis –Νοέμβριος 2018

Σπύρος Τάσσης, LLM
www.tassis.com
info@tassis.com

HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ

ΥΠΕΥΘΥΝΟΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (DPO)

www.dataprotection.gr

Βασικοί Ορισμοί

- *Υπεύθυνος Επεξεργασίας* (*Controller*)
- *Εκτελών την επεξεργασία* (*Processor*)
- *Υπεύθυνος Προστασίας Δεδομένων* (Data Protection Officer)

Υπεύθυνος Προστασίας Δεδομένων

Ισχύων Ρόλος: Άρθρο 18 παρ. 2 Οδηγίας 95/46/ΕΚ, Κανονισμός 45/2001 (όργανα ΕΕ)

Σπ. Τάσσης

Υπεύθυνος Προστασίας Δεδομένων (DPO)

- **Μέρος του συστήματος Λογοδοσίας**

- **Υποχρεωτικός όταν:**
  α) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα,
  β) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα,
  γ) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών

Υπεύθυνος Προστασίας Δεδομένων (DPO)

- **Μέρος του συστήματος Λογοδοσίας**
- **Εθελοντικός (voluntarily) ως ένδειξη υπεύθυνης διαχείρισης των διαδικασιών και μηχανισμών. Η Ομάδα του Άρθρου 29 ενθαρρύνει τον ορισμό DPO ακόμα και όταν δεν είναι υποχρεωτικός.**
- **Όταν ορισθεί εθελοντικά DPO, τότε θα ισχύουν οι ίδιες απαιτήσεις ως εάν ο ορισμός να ήταν υποχρεωτικός.**

Υπεύθυνος Προστασίας Δεδομένων (DPO)

➢ **Μεγάλη κλίμακα ιδίως (Ομάδα του Άρθρου 29):**

- **Όταν ο αριθμός των ενδιαφερόμενων προσώπων στα οποία αναφέρονται τα δεδομένα - είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού είναι σημαντικός**
- **Όταν ο αριθμός δεδομένων και / ή το φάσμα των διαφορετικών στοιχείων δεδομένων που επεξεργάζονται είναι ευρεία**
- **Η επεξεργασία δεδομένων έχει τα στοιχεία της διάρκειας ή μονιμότητας της δραστηριότητας**
- **Η γεωγραφική έκταση της δραστηριότητας επεξεργασίας είναι μεγάλη (π.χ. επεξεργασία δεδομένων γεωγραφικής θέσης σε πραγματικό χρόνο των πελατών μιας εταιρείας για στατιστικούς σκοπούς ή επεξεργασία δεδομένων για συμπεριφορική διαφήμιση από μια μηχανή αναζήτησης)**

Υπεύθυνος Προστασίας Δεδομένων (DPO)

➢ **Μεγάλη κλίμακα ιδίως (Ομάδα του Άρθρου 29):**

Επεξεργασία δεδομένων ασθενών στο πλαίσιο της συνήθους λειτουργίας ενός νοσοκομείου

Επεξεργασία δεδομένων μετακίνησης φυσικών προσώπων που χρησιμοποιούν το σύστημα δημόσιων μεταφορών μιας πόλης (π.χ. παρακολούθηση μέσω καρτών πολλαπλών διαδρομών)

Επεξεργασία δεδομένων πελατών στο πλαίσιο της συνήθους λειτουργίας μιας ασφαλιστικής εταιρείας ή μιας τράπεζας

- **Επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς συμπεριφορικής διαφήμισης από μηχανή αναζήτησης**
- **Επεξεργασία δεδομένων (περιεχόμενο, κίνηση, θέση) από παρόχους υπηρεσιών τηλεφωνίας ή διαδικτύου**
- **Επεξεργασία σε πραγματικό χρόνο δεδομένων γεωγραφικού εντοπισμού πελατών διεθνούς αλυσίδας ταχυφαγείων για στατιστικούς σκοπούς από εκτελούντα την επεξεργασία που ειδικεύεται στην παροχή τέτοιου είδους υπηρεσιών**

Υπεύθυνος Προστασίας Δεδομένων (DPO)

- **Συνεχής και Συστηματική παρακολούθηση**
- **Διενεργείται σύμφωνα με ένα σύστημα οργανωμένο ή μεθοδικό**
- **Πραγματοποιείται ως μέρος ενός γενικού σχεδίου συλλογής δεδομένων**
- **Διεξάγεται ως μέρος μιας στρατηγικής (royalty cards)**
- **Γίνεται συνεχώς ή σε τακτά χρονικά διαστήματα**

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Βασικές Δραστηριότητες ΥΕ

προοίμιο 97: Στον ιδιωτικό τομέα, οι βασικές δραστηριότητες ενός υπευθύνου επεξεργασίας πρέπει να αφορούν τις κύριες δραστηριότητές του και όχι την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως παρεπόμενη δραστηριότητα.

Δεν θα πρέπει να δίδεται ερμηνεία προς την κατεύθυνση της εξαίρεσης δραστηριοτήτων όταν η επεξεργασία δεδομένων αποτελεί αναπόσπαστο μέρος της δραστηριότητας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Π.χ. Βασική δραστηριότητα ενός νοσοκομείου είναι η παροχή υγειονομικής περίθαλψης, για να παρέχει με ασφαλή και αποτελεσματικό τρόπο την υγειονομική περίθαλψη θα πρέπει να επεξεργάζεται ιατρικά δεδομένα (όπως ιατρικούς φακέλους ασθενών). Άρα η επεξεργασία θα πρέπει να θεωρείται ως μία από τις βασικές δραστηριότητες του νοσοκομείου και άρα οφείλει να ορίσει υπεύθυνο προστασίας δεδομένων.

Υπεύθυνος Προστασίας Δεδομένων (DPO)

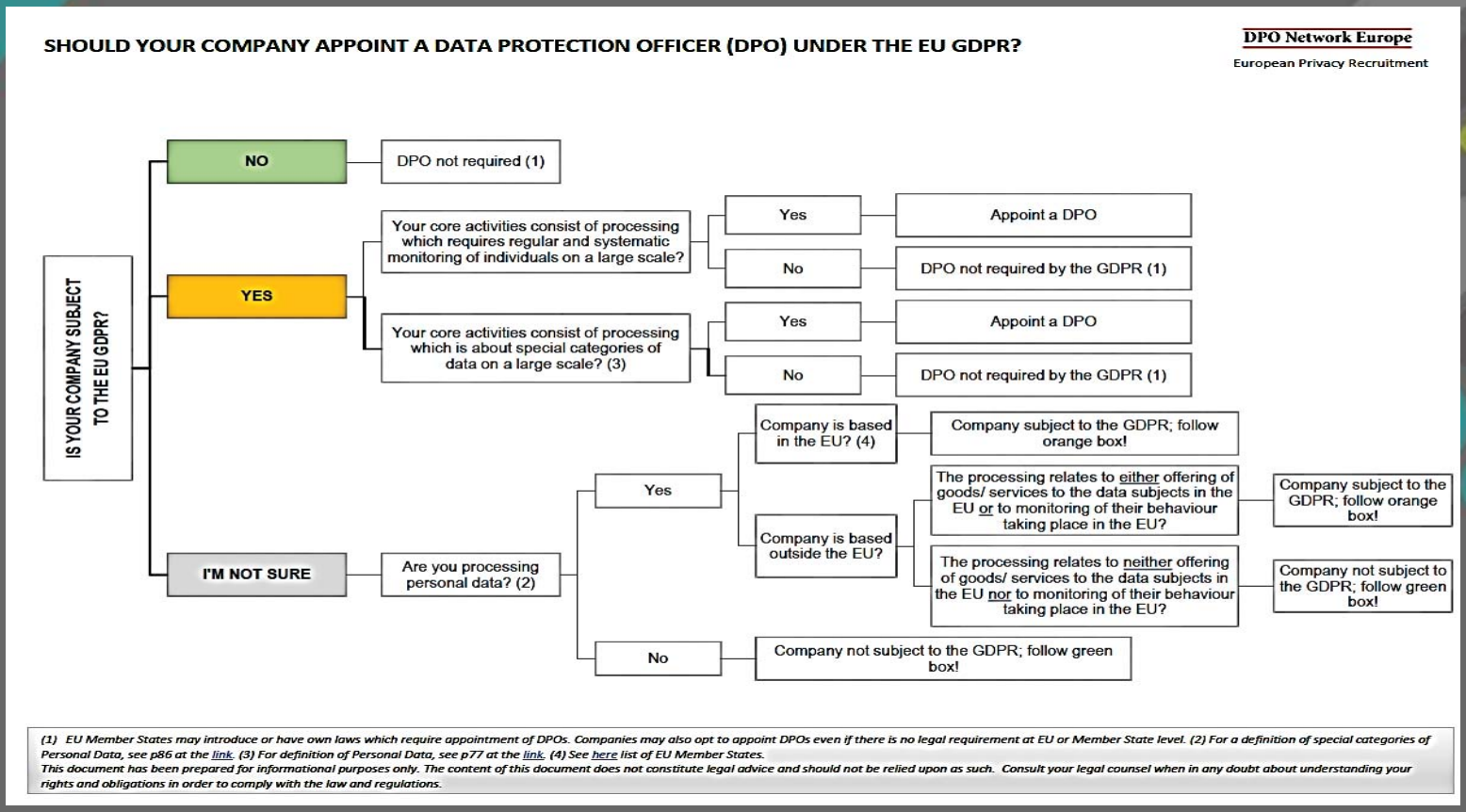
Διορισμός

Σε όμιλο επιχειρήσεων μπορεί να οριστεί ένας DPO

Αρκεί κάθε εγκατάσταση να έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας και σε γλώσσα που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα υποκείμενα των δεδομένων.

Ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές δημόσιες αρχές ή δημόσιους φορείς, λαμβάνοντας υπόψη την οργανωτική δομή και το μέγεθός τους.

Πότε τελικά χρειάζεται μια εταιρεία DPO?
https://www.dponetwork.eu/



Υπεύθυνος Προστασίας Δεδομένων (DPO)

- **Καθήκοντα και Προσόντα DPO**

- **επαγγελματικά προσόντα και ιδίως εμπειρία**
- **εσωτερικός ή εξωτερικός**
- **ενημερώνει και συμβουλεύει**
- **παρακολουθεί τη συμμόρφωση με τον Κανονισμό**

Υπεύθυνος Προστασίας Δεδομένων (DPO)

➢ Καθήκοντα και Προσόντα DPO - Πιστοποίηση;

Η Αρχή συνεδρίασε για θέματα που αφορούν την πιστοποίηση επαγγελματικών προσόντων Υπευθύνων Προστασίας Δεδομένων (Data Protection Officers - DPOs), στο πλαίσιο εκπαιδευτικών προγραμμάτων που πραγματοποιούνται από διάφορους φορείς, και αποφάσισε να εκδώσει την ακόλουθη ανακοίνωση προς ενημέρωση των ενδιαφερομένων: Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαπιστώνει ότι, ενόψει της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) τον Μάϊο του 2018, προσφέρονται αρκετά εκπαιδευτικά προγράμματα/σεμινάρια για τον ρόλο του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO). Στο πλαίσιο της προώθησης των εκπαιδευτικών αυτών προγραμμάτων, υπάρχουν φορείς που υποστηρίζουν ότι η προσφερόμενη εκπαίδευση αποτελεί ένα προπαρασκευαστικό στάδιο που οδηγεί σε κάποιου τύπου πιστοποίηση DPO στην ελληνική επικράτεια. Η Αρχή, με στόχο την ενημέρωση των ενδιαφερομένων, επισημαίνει ότι: • Η δραστηριοποίηση αυτή της αγοράς είναι θετική, αφού συμβάλλει στη μεταφορά γνώσης και ενημέρωσης σε θέματα του ΓΚΠΔ, πρέπει όμως να τεθεί στην ορθή της διάσταση, αποφεύγοντας τη δημιουργία εσφαλμένων εντυπώσεων ως προς τις σχετικές απαιτήσεις του ΓΚΠΔ. • Ο ΓΚΠΔ, που θα τεθεί σε ισχύ τον Μάϊο του 2018, δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO, ούτε καν ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση. • Μέχρι σήμερα κανένας φορέας στην Ελλάδα δεν έχει διαπιστευθεί για να πιστοποιεί τα επαγγελματικά προσόντα/δεξιότητες ενός DPO. Συνεπώς, οι προτεινόμενες πιστοποιήσεις DPO δεν εμπίπτουν στην κατηγορία των υφιστάμενων επίσημων ελληνικών πιστοποιήσεων. • Η ύλη των προσφερόμενων εκπαιδευτικών προγραμμάτων μπορεί μεν να χαρακτηριστεί γενικώς ως συναφής με τον ΓΚΠΔ και τη θέση του DPO, η επιλογή της όμως αποτελεί αποκλειστική ευθύνη των φορέων που τα παρέχουν.

www.dataprotection.gr

Σπ. Τάσσης

Υπεύθυνος Προστασίας Δεδομένων (DPO)

- **Καθήκοντα και Προσόντα DPO**

- **παρέχει συμβουλές, όταν ζητείται, για την εκτίμηση αντικτύπου**
- **συνεργάζεται με την εποπτική αρχή**
- **ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή**
- **λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας**

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Γνώσεις σχετικά με τη λειτουργία του οργανισμού και του τομέα δραστηριοποίησης του

Σημείο επικοινωνίας με την Αρχή

Επικοινωνία με υποκείμενα δεδομένων –> Καταγγελίες/Αιτήματα

Παρακολούθηση συμμόρφωσης

Συνεργασία με εποπτική αρχή

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Συμμετοχή εκτίμηση κινδύνου (DPIA)

Δεν μπορεί να είναι ελεγκτής και ελεγχόμενος ταυτόχρονα. Δεν έχει προσωπική ευθύνη για παραβάσεις. Δεν βρίσκεται στην ιεραρχική δομή.

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Οικονομική αυτοτέλεια

Προσωπική ανεξαρτησία

Εγγυήσεις ανεξαρτησίας

Λειτουργική ανεξαρτησία

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Γνωστοποίηση στην Αρχή – Διοικητικές Κυρώσεις

Σύμβαση – > Σαφής ορισμός καθηκόντων

Ανάκληση – Λόγοι λύσης

Ευθύνη (αστική και ποινική)

Σπ. Τάσσης

Υπεύθυνος Προστασίας Δεδομένων (DPO)

Μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία

Μπορεί να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών

Συνιστάται δε να είναι εγκατεστημένος εντός ΕΕ, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην ΕΕ.

Δεν θα πρέπει να επιτελεί καθήκοντα που θα έρχονται σε σύγκρουση με τον ρόλο του ως DPO βλ. ιδίως γνώμη ομάδας εργασίας α 29 αναλυτικά σελ. 23

«*Αυτό συνεπάγεται συγκεκριμένα ότι ο υπεύθυνος προστασίας δεδομένων δεν μπορεί να κατέχει στους κόλπους του οργανισμού θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Επειδή κάθε οργανισμός έχει διαφορετική οργανωτική δομή, το συγκεκριμένο ζήτημα θα πρέπει να εξετάζεται για κάθε περίπτωση χωριστά.*

Θα μπορούσε να ειπωθεί, με βάση την εμπειρία, ότι θέσεις στις οποίες εντοπίζονται συνήθως συγκρούσεις συμφερόντων στους κόλπους ενός οργανισμού είναι, μεταξύ άλλων, οι θέσεις της ανώτερης διοίκησης (όπως, διευθύνων σύμβουλος, διοικητικός γενικός διευθυντής, οικονομικός διευθυντής, αρχίατρος, προϊστάμενος τμήματος μάρκετινγκ, προϊστάμενος ανθρωπίνων πόρων ή προϊστάμενος τμήματος πληροφορικής), και άλλες θέσεις κατώτερων βαθμίδων της οργανωτικής δομής, εφόσον από τις θέσεις αυτές είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας.»

www.dataprotection.gr

Σπ. Τάσσης

Δημοσίευση και ανακοίνωση των στοιχείων επικοινωνίας DPO

Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων + τα ανακοινώνουν στην εποπτική αρχή.

Στοιχεία επικοινωνίας: ταχυδρομική διεύθυνση, συγκεκριμένος τηλεφωνικός αριθμός ή/και συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου. Θα μπορούσαν να παρέχονται και άλλα μέσα επικοινωνίας, όπως π.χ. Ειδική ανοικτή τηλεφωνική γραμμή ή ειδικό έντυπο επικοινωνίας υπ' όψιν του υπευθύνου προστασίας δεδομένων στον δικτυακό τόπο του οργανισμού.

Όνομα; Δυνάμει του άρθρου 37 παρ. 7 δεν απαιτείται, είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και του υπευθύνου προστασίας δεδομένων να αποφασίζουν εάν η δημοσίευση του ονόματος είναι αναγκαία ή σκόπιμη.

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, η γνωστοποίηση στην εποπτική αρχή και στο υποκείμενο των δεδομένων περιλαμβάνει μεταξύ άλλων και το όνομα του υπεύθυνου προστασίας δεδομένων.

Δημοσίευση και ανακοίνωση των στοιχείων επικοινωνίας DPO

Η Ομάδα του άρθρου 29 συνιστά ως ορθή πρακτική τη γνωστοποίηση από τον οργανισμό του ονόματος και των στοιχείων επικοινωνίας του υπεύθυνου προστασίας δεδομένων στους υπαλλήλους του

π.χ. Δημοσιεύοντας το όνομα και τα στοιχεία στο ενδοδίκτυό του, στον εσωτερικό τηλεφωνικό κατάλογο, στα οργανογράμματά του.

Διαχείριση Κινδύνου

- **Οργανωτικό (ανεπαρκείς διαδικασίες, μη ασφαλή συστήματα και ελλιπής οργάνωση της επίβλεψης τους)**
- **Ανθρώπινο (ελλιπής εκπαίδευση του προσωπικού που τα χειρίζεται). Είναι εκπληκτικό το πόσα περιστατικά ασφαλείας οφείλονται στον ανθρώπινο παράγοντα.**

Αρχή της Λογοδοσίας

Ανάλυση κινδύνου –> Διενέργεια DPIA

Ως «κίνδυνος» νοείται μια υπόθεση εργασίας που περιγράφει ένα συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης.

Ως «διαχείριση κινδύνου» μπορούν να νοηθούν οι συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού ως προς τον κίνδυνο.

Εκτίμηση Αντικτύπου -> Συμμετοχή DPO

Άρθρο 35 - κατηγορίες επεξεργασίας που (ιδίως) απαιτούν Εκτίμηση Αντικτύπου

- **συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ,**

- **μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 (ευαίσθητα) ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10**

- **συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.**

Η εποπτική αρχή εκδίδει κατάλογο πράξεων επεξεργασίας που υπόκεινται

Αρχή της Λογοδοσίας

Άρθρο 32 ΓΚ – Ασφάλεια της επεξεργασίας

«Λαμβάνοντας υπόψη … ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέσα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων»

Confidentiality – Εμπιστευτικότητα

Integrity- Ακεραιότητα

Availability – Διαθεσιμότητα

Resiliency - Ανθεκτικότητα

Αρχή της Λογοδοσίας

Πολιτική Ασφαλείας

- **Ενημέρωση (awareness)**
- **Πορεία προς την συμμόρφωση (inventory - gap analysis - roadmap)**
- **Ανάλυση κινδύνου και εκτίμηση αντικτύπου**
- **Πολιτικές και Διαδικασίες**
- **Σαφής καταγραφή των διαδικασιών και αρμοδιοτήτων (Εσωτερική Πολιτική Προστασίας Δεδομένων)**
- **Όχι <u>εφησυχασμός</u>.**

Ευχαριστώ

Σπύρος Τάσσης
www.tassis.com
info@tassis.com

HADPP ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ
www.dataprotection.gr

ΟΜΑΔΑ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΤΟΥ ΑΡΘΡΟΥ 29

16/EL
WP 243 rev.01

Κατευθυντήριες γραμμές σχετικά με τους υπεύθυνους προστασίας δεδομένων

Εγκρίθηκε στις 13 Δεκεμβρίου 2016

Όπως αναθεωρήθηκε τελευταία και εγκρίθηκε στις 5 Απριλίου 2017

Η εν λόγω ομάδα συστάθηκε δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ. Είναι ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για θέματα προστασίας των δεδομένων και της ιδιωτικής ζωής. Τα καθήκοντά της περιγράφονται στο άρθρο 30 της οδηγίας 95/46/ΕΚ και στο άρθρο 15 της οδηγίας 2002/58/ΕΚ.

Η γραμματειακή υποστήριξη παρέχεται από τη Διεύθυνση Γ (Θεμελιώδη δικαιώματα και κράτος δικαίου) της Ευρωπαϊκής Επιτροπής, Γενική Διεύθυνση Δικαιοσύνης και Καταναλωτών, Β-1049 Βρυξέλλες, Βέλγιο, γραφείο αριθ. MO59 05/35

Δικτυακός τόπος: http://ec.europa.eu/justice/data-protection/index_en.htm

Η ΟΜΑΔΑ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΩΝ ΈΝΑΝΤΙ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

που συστάθηκε με την οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995,

έχοντας υπόψη τα άρθρα 29 και 30 της οδηγίας,

έχοντας υπόψη τον εσωτερικό κανονισμό της ομάδας,

ΕΞΕΔΩΣΕ ΤΙΣ ΠΑΡΟΥΣΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

Πίνακας περιεχομένων

1 Εισαγωγή

Ο γενικός κανονισμός για την προστασία δεδομένων («ΓΚΠΔ»)[1], που αναμένεται να τεθεί σε ισχύ στις 25 Μαΐου 2018, παρέχει ένα εκσυγχρονισμένο πλαίσιο συμμόρφωσης για την προστασία των δεδομένων στην Ευρώπη με βάση τη λογοδοσία. Στο επίκεντρο αυτού του νέου νομικού πλαισίου θα βρίσκονται για πολλούς οργανισμούς οι υπεύθυνοι προστασίας δεδομένων, οι οποίοι θα διευκολύνουν τη συμμόρφωση με τις διατάξεις του ΓΚΠΔ.

Σύμφωνα με τον ΓΚΠΔ, ορισμένοι υπεύθυνοι επεξεργασίας και εκτελούντες την επεξεργασία υποχρεούνται να ορίσουν υπεύθυνο προστασίας δεδομένων[2]. Η υποχρέωση αυτή ισχύει για όλες τις δημόσιες αρχές και φορείς (ανεξαρτήτως του είδους δεδομένων που επεξεργάζονται), καθώς και για άλλους οργανισμούς που έχουν ως κύρια δραστηριότητα τη συστηματική παρακολούθηση φυσικών προσώπων σε μεγάλη κλίμακα, ή την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα σε μεγάλη κλίμακα.

Ενδέχεται, πάντως, να υπάρξουν οργανισμοί που θα κρίνουν σκόπιμο να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, ακόμη και σε περιπτώσεις στις οποίες ο ΓΚΠΔ δεν απαιτεί ρητώς τον ορισμό υπευθύνου προστασίας δεδομένων. Η ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 («ομάδα του άρθρου 29») ενθαρρύνει τέτοιου είδους εθελοντικές ενέργειες.

Η έννοια του υπευθύνου προστασίας δεδομένων δεν είναι καινούργια. Αν και η οδηγία 95/46/ΕΚ[3] δεν επέβαλλε σε κανέναν οργανισμό την υποχρέωση να ορίσει υπεύθυνο προστασίας δεδομένων, η συγκεκριμένη πρακτική αναπτύχθηκε παρόλα αυτά σε αρκετά κράτη μέλη στο πέρασμα του χρόνου.

Πριν από την έγκριση του ΓΚΠΔ, η ομάδα του άρθρου 29 ήταν της γνώμης ότι ο υπεύθυνος προστασίας δεδομένων συνιστά ακρογωνιαίο λίθο της λογοδοσίας και ότι ο ορισμός του μπορεί να διευκολύνει τη συμμόρφωση και επιπλέον να αποτελέσει ανταγωνιστικό πλεονέκτημα για τις

[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). Ο ΓΚΠΔ παρουσιάζει ενδιαφέρον για τον ΕΟΧ και θα τεθεί σε εφαρμογή μετά την ενσωμάτωσή του στη συμφωνία ΕΟΧ.

[2] Ο ορισμός υπευθύνου προστασίας δεδομένων είναι επίσης υποχρεωτικός για τις αρμόδιες αρχές δυνάμει του άρθρου 32 της οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου (ΕΕ L 119 της 4.5.2016, σ. 89–131), και δυνάμει εθνικών εκτελεστικών νομοθετικών διατάξεων. Παρότι οι εν λόγω κατευθυντήριες γραμμές αφορούν συγκεκριμένα τους υπεύθυνους προστασίας δεδομένων του κανονισμού ΓΚΠΔ, ισχύουν και για τους υπεύθυνους προστασίας δεδομένων της οδηγίας 2016/680, όσον αφορά τις παρεμφερείς διατάξεις των δύο νομοθετικών πράξεων.

[3] Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 281 της 23.11.1995, σ. 31).

επιχειρήσεις[4]. Εκτός από τον διευκολυντικό ρόλο που έχουν σε επίπεδο συμμόρφωσης μέσω της εφαρμογής εργαλείων λογοδοσίας (όπως διευκόλυνση διενέργειας εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων και διενέργεια ή διευκόλυνση διενέργειας ελέγχων), οι υπεύθυνοι προστασίας δεδομένων ενεργούν και ως μεσολαβητές μεταξύ των διαφόρων ενδιαφερομένων (π.χ., εποπτικές αρχές, υποκείμενα των δεδομένων και επιχειρησιακές μονάδες του ίδιου οργανισμού).

Οι υπεύθυνοι προστασίας δεδομένων δεν φέρουν προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης με τον ΓΚΠΔ. Ο ΓΚΠΔ καθιστά σαφές ότι είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τις διατάξεις του (άρθρο 24 παράγραφος 1). Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Ο ρόλος του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία είναι επίσης καθοριστικός όσον αφορά την αποτελεσματική εκτέλεση των καθηκόντων του υπευθύνου προστασίας δεδομένων. Ο ορισμός υπευθύνου προστασίας δεδομένων είναι μεν το πρώτο βήμα, όμως πρέπει επιπλέον να του δοθούν επαρκής αυτονομία και πόροι για να είναι σε θέση να ασκήσει αποτελεσματικά τα καθήκοντά του.

Ο ΓΚΠΔ αναγνωρίζει τον υπεύθυνο προστασίας δεδομένων ως καίρια συνιστώσα του νέου συστήματος διακυβέρνησης δεδομένων και θεσπίζει τις προϋποθέσεις για τον ορισμό, τη θέση και τα καθήκοντά του. Οι παρούσες κατευθυντήριες γραμμές επιδιώκουν να αποσαφηνίσουν τις σχετικές διατάξεις του ΓΚΠΔ ώστε αφενός να βοηθήσουν τους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να συμμορφωθούν με τη νομοθεσία, και αφετέρου να συνδράμουν τους υπεύθυνους προστασίας δεδομένων στην άσκηση του ρόλου τους. Οι κατευθυντήριες γραμμές παρέχουν επίσης συστάσεις για βέλτιστες πρακτικές, με βάση την εμπειρία που έχουν αποκτήσει στον συγκεκριμένο τομέα ορισμένα κράτη μέλη. Η ομάδα του άρθρου 29 θα παρακολουθεί την εφαρμογή των εν λόγω κατευθυντήριων γραμμών και ενδέχεται επίσης να τις συμπληρώνει και να τις εμπλουτίζει κατά περίπτωση.

2 Ορισμός υπευθύνου προστασίας δεδομένων

2.1. Υποχρεωτικός ορισμός

Σύμφωνα με το άρθρο 37 παράγραφος 1 του ΓΚΠΔ, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός σε τρεις συγκεκριμένες περιπτώσεις[5]:

α) όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα[6]·
β) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα· ή

[4] Βλ. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

[5] Σημειώνεται ότι, σύμφωνα με το άρθρο 37 παράγραφος 4, το δίκαιο της Ένωσης ή των κρατών μελών είναι δυνατό να επιβάλλει τον ορισμό υπευθύνου προστασίας δεδομένων και σε άλλες περιπτώσεις.

[6] Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα. Βλ. άρθρο 32 της οδηγίας (ΕΕ) 2016/680.

γ) όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων[7] ή[8] δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα[9].

Στις ακόλουθες υποενότητες, η ομάδα του άρθρου 29 παρέχει καθοδήγηση σχετικά με τα κριτήρια και την ορολογία που χρησιμοποιείται στο άρθρο 37 παράγραφος 1.

Εκτός από τις περιπτώσεις όπου είναι προφανές ότι ένας οργανισμός δεν υποχρεούται να ορίσει υπεύθυνο προστασίας δεδομένων, η ομάδα του άρθρου 29 συνιστά στους υπεύθυνους επεξεργασίας και τους εκτελούντες την επεξεργασία να καταγράφουν την εσωτερική ανάλυση που διενεργούν προκειμένου να προσδιορίσουν αν πρέπει ή όχι να διοριστεί υπεύθυνος προστασίας δεδομένων, ώστε να μπορούν να αποδείξουν ότι λήφθηκαν δεόντως υπόψη οι σχετικοί παράγοντες[10]. Η εν λόγω ανάλυση αποτελεί μέρος της απαιτούμενης τεκμηρίωσης δυνάμει της αρχής της λογοδοσίας. Μπορεί να ζητηθεί από την εποπτική αρχή και θα πρέπει να επικαιροποιείται όταν κρίνεται απαραίτητο, για παράδειγμα αν οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία αναλαμβάνουν νέες δραστηριότητες ή παρέχουν νέες υπηρεσίες που εμπίπτουν ενδεχομένως στις περιπτώσεις του άρθρου 37 παράγραφος 1.

Όταν ένας οργανισμός ορίζει υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι απαιτήσεις των άρθρων 37 έως 39 ως εάν ο ορισμός να ήταν υποχρεωτικός.

Οι οργανισμοί που δεν υποχρεούνται, βάσει της νομοθεσίας, να ορίσουν υπεύθυνο προστασίας δεδομένων και που δεν επιθυμούν να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση μπορούν κάλλιστα να απασχολούν υπαλλήλους ή εξωτερικούς συμβούλους επιφορτισμένους με καθήκοντα σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα. Σ' αυτές τις περιπτώσεις, είναι σημαντικό να διασφαλίζεται ότι δεν υπάρχει σύγχυση ως προς τον τίτλο, το καθεστώς, τη θέση και τα καθήκοντα των εν λόγω υπαλλήλων ή συμβούλων. Θα πρέπει, επομένως, να διευκρινίζεται, τόσο στο πλαίσιο της ενδοεταιρικής επικοινωνίας, όσο και στις αρχές προστασίας δεδομένων, τα υποκείμενα των δεδομένων και το ευρύ κοινό, ότι ο εν λόγω υπάλληλος ή σύμβουλος δεν φέρει τον τίτλο του «υπευθύνου προστασίας δεδομένων». [11]

Ο ορισμός, υποχρεωτικός ή εθελοντικός, του υπευθύνου προστασίας δεδομένων γίνεται για όλες τις πράξεις επεξεργασίας που διενεργούνται από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.

---

[7] Σύμφωνα με το άρθρο 9, στις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα περιλαμβάνονται εκείνα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

[8] Στο άρθρο 37 παράγραφος 1 στοιχείο γ) χρησιμοποιείται η λέξη «*και*». Βλ. ενότητα 2.1.5 ακολούθως για διευκρινίσεις σχετικά με τη χρήση του «*ή*» αντί του «*και*».

[9] Άρθρο 10.

[10] Βλέπε άρθρο 24 παράγραφος 1.

[11] Αυτό ισχύει και για τους υπεύθυνους προστασίας της ιδιωτικής ζωής ή άλλους επαγγελματίες στον τομέα της προστασίας της ιδιωτικής ζωής που απασχολούνται ήδη σε ορισμένες εταιρείες, οι οποίοι δεν πληρούν ενδεχομένως σε όλες τις περιπτώσεις τα κριτήρια του ΓΚΠΔ, για παράδειγμα ως προς τους διαθέσιμους πόρους ή τις εγγυήσεις περί ανεξαρτησίας· εάν δεν πληρούν τα κριτήρια του ΓΚΠΔ, δεν μπορούν να θεωρούνται ως υπεύθυνοι προστασίας δεδομένων ούτε να φέρουν τον συγκεκριμένο τίτλο.

2.1.1 «ΔΗΜΟΣΙΑ ΑΡΧΗ Η ΔΗΜΟΣΙΟΣ ΦΟΡΕΑΣ»

Ο ΓΚΠΔ δεν ορίζει τι συνιστά «*δημόσια αρχή ή δημόσιο φορέα»*. Η ομάδα του άρθρου 29 εκτιμά ότι η έννοια αυτή πρέπει να προσδιορίζεται από τα εθνικά δίκαια. Συνεπώς, δημόσιες αρχές και δημόσιοι φορείς είναι μεν, μεταξύ άλλων, οι εθνικές, περιφερειακές και τοπικές αρχές, όμως στη συγκεκριμένη έννοια, δυνάμει των ισχυουσών διατάξεων των εθνικών δικαίων, περιλαμβάνονται κατά κανόνα και διάφοροι άλλοι φορείς δημοσίου δικαίου[12]. Σ' αυτές τις περιπτώσεις, ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός.

Η εκπλήρωση δημόσιου καθήκοντος και η άσκηση δημόσιας εξουσίας[13] είναι δυνατή όχι μόνο από δημόσιες αρχές ή δημόσιους φορείς, αλλά και από άλλα φυσικά ή νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου, σε διάφορους τομείς που απορρέουν από τους εθνικούς κανονισμούς κάθε κράτους μέλους, όπως οι υπηρεσίες δημόσιων μεταφορών, η ύδρευση και η παροχή ενέργειας, οι οδικές υποδομές, η δημόσια ραδιοτηλεόραση, η κατασκευή εργατικών κατοικιών, ή πειθαρχικά όργανα για νομοθετικά κατοχυρωμένα επαγγέλματα.

Στις περιπτώσεις αυτές, τα υποκείμενα των δεδομένων είναι πιθανό να βρεθούν σε θέση που ομοιάζει πολύ με την επεξεργασία των δεδομένων τους από δημόσια αρχή ή δημόσιο φορέα. Συγκεκριμένα, είναι δυνατή η επεξεργασία δεδομένων για παρόμοιους σκοπούς και, ομοίως, τα φυσικά πρόσωπα έχουν συνήθως ελάχιστη ή καμία δυνατότητα επιλογής ως προς το εάν και το πώς θα υποβληθούν σε επεξεργασία τα δεδομένα τους. Είναι πιθανό, επομένως, να απαιτείται η πρόσθετη προστασία που παρέχει ο ορισμός υπευθύνου προστασίας δεδομένων.

Μολονότι δεν προβλέπεται σχετική υποχρέωση σε τέτοιες περιπτώσεις, η ομάδα του άρθρου 29 συνιστά, ως ορθή πρακτική, στους οργανισμούς ιδιωτικού δικαίου που εκπληρώνουν δημόσια καθήκοντα ή ασκούν δημόσια εξουσία να ορίζουν υπεύθυνο προστασίας δεδομένων. Η δραστηριότητα του εν λόγω υπευθύνου προστασίας δεδομένων καλύπτει όλες τις πράξεις επεξεργασίας που διενεργούνται, περιλαμβανομένων εκείνων που δεν σχετίζονται με την εκπλήρωση δημόσιου καθήκοντος ή την άσκηση επίσημης αρμοδιότητας (π.χ., τη διαχείριση βάσης δεδομένων υπαλλήλων).

[12] Βλ., π.χ., τους ορισμούς του «*φορέα του δημόσιου τομέα*» και του «*οργανισμού δημοσίου δικαίου*» στο άρθρο 2 παράγραφοι 1 και 2 της οδηγίας 2003/98/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 17ης Νοεμβρίου 2003, για την περαιτέρω χρήση πληροφοριών του δημόσιου τομέα (ΕΕ L 345 της 31.12.2003, σ. 90).
[13] Άρθρο 6 παράγραφος 1 στοιχείο ε).

2.1.2 «ΒΑΣΙΚΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ»

Το άρθρο 37 παράγραφος 1 στοιχεία β) και γ) του ΓΚΠΔ αναφέρεται στις «*βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία*». Στην αιτιολογική σκέψη 97 διευκρινίζεται ότι οι βασικές δραστηριότητες ενός υπευθύνου επεξεργασίας αφορούν «*τις κύριες δραστηριότητές του και όχι την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως παρεπόμενη δραστηριότητα*». Ως «βασικές δραστηριότητες» μπορούν να θεωρηθούν οι καίριες πράξεις που είναι αναγκαίες για την επίτευξη των στόχων του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

Στις «βασικές δραστηριότητες» δεν θα πρέπει, πάντως, να δίδεται ερμηνεία προς την κατεύθυνση της εξαίρεσης δραστηριοτήτων όταν η επεξεργασία δεδομένων αποτελεί αναπόσπαστο μέρος της δραστηριότητας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Για παράδειγμα, η βασική δραστηριότητα ενός νοσοκομείου είναι η παροχή υγειονομικής περίθαλψης. Το νοσοκομείο, όμως, δεν μπορεί να παρέχει υγειονομική περίθαλψη με ασφαλή και αποτελεσματικό τρόπο εάν δεν επεξεργάζεται ιατρικά δεδομένα, όπως τους ιατρικούς φακέλους των ασθενών. Η επεξεργασία των εν λόγω δεδομένων θα πρέπει να θεωρείται, επομένως, ως μία από τις βασικές δραστηριότητες κάθε νοσοκομείου. Κατά συνέπεια, τα νοσοκομεία οφείλουν να ορίζουν υπεύθυνο προστασίας δεδομένων.

Άλλο παράδειγμα είναι οι ιδιωτικές εταιρείες ασφαλείας που αναλαμβάνουν τη φύλαξη ιδιωτικών εμπορικών κέντρων και δημόσιων χώρων. Η βασική δραστηριότητα των εν λόγω εταιρειών είναι η φύλαξη, η οποία είναι άρρηκτα συνδεδεμένη με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Κατά συνέπεια, και αυτές οι εταιρείες οφείλουν να ορίσουν υπεύθυνο προστασίας δεδομένων.

Από την άλλη πλευρά, όλοι οι οργανισμοί επιτελούν ορισμένες δραστηριότητες όπως, π.χ., καταβάλλουν τους μισθούς των υπαλλήλων τους ή αναπτύσσουν συνήθεις δραστηριότητες υποστήριξης ΤΠ. Αυτά είναι παραδείγματα αναγκαίων λειτουργιών υποστήριξης της βασικής δραστηριότητας ή του κύριου τομέα δραστηριότητας του οργανισμού. Μολονότι οι εν λόγω δραστηριότητες είναι αναγκαίες ή ουσιώδεις, θεωρούνται κατά κανόνα ως παρεπόμενες λειτουργίες του οργανισμού και όχι ως η βασική του δραστηριότητα.

2.1.3 «ΜΕΓΑΛΗ ΚΛΙΜΑΚΑ»

Σύμφωνα με το άρθρο 37 παράγραφος 1 στοιχεία β) και γ), για να ενεργοποιηθεί η υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να διενεργείται σε μεγάλη κλίμακα. Ο ΓΚΠΔ δεν ορίζει τι συνιστά επεξεργασία μεγάλης κλίμακας. Παρόλα αυτά στην αιτιολογική σκέψη 91 παρέχονται κάποιες οδηγίες για το συγκεκριμένο θέμα[14].

Είναι γεγονός ότι δεν είναι δυνατό να προσδιοριστεί με ακρίβεια ούτε η ποσότητα των δεδομένων που υποβάλλονται σε επεξεργασία ούτε το πλήθος των εμπλεκόμενων φυσικών προσώπων, ώστε να δοθεί ένας αριθμός που να ισχύει σε όλες τις περιπτώσεις. Δεν αποκλείεται, πάντως, να αναπτυχθεί με τον καιρό τυποποιημένη πρακτική για τον ακριβέστερο προσδιορισμό, με πιο συγκεκριμένους και/ή ποσοτικούς όρους, του τι συνιστά «*μεγάλη κλίμακα*» σε σχέση με ορισμένους τύπους συνήθων δραστηριοτήτων επεξεργασίας. Η ομάδα του άρθρου 29 σκοπεύει μάλιστα να συμβάλει προς την κατεύθυνση αυτή μέσω της ανταλλαγής και της δημοσιοποίησης παραδειγμάτων των κατώτατων ορίων που εφαρμόστηκαν σε διάφορες περιπτώσεις για τον ορισμό υπευθύνου προστασίας δεδομένων.

Σε κάθε περίπτωση, η ομάδα του άρθρου 29 συνιστά να λαμβάνονται συγκεκριμένα υπόψη οι ακόλουθοι παράγοντες όταν επιχειρείται να προσδιοριστεί εάν η επεξεργασία διενεργείται σε μεγάλη κλίμακα ή όχι:

- ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού,
- ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία,
- η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων,
- η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

[14] Σύμφωνα με την εν λόγω αιτιολογική σκέψη, στην έννοια της «μεγάλης κλίμακας» εμπίπτουν συγκεκριμένα «*πράξεις επεξεργασίας μεγάλης κλίμακας που στοχεύουν στην επεξεργασία σημαντικής ποσότητας δεδομένων προσωπικού χαρακτήρα σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, οι οποίες θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανόν να έχουν ως αποτέλεσμα υψηλό κίνδυνο*». Από την άλλη πλευρά, η αιτιολογική σκέψη προβλέπει ρητά ότι «*η επεξεργασία δεδομένων προσωπικού χαρακτήρα δεν θα πρέπει να θεωρείται ότι είναι μεγάλης κλίμακας, εάν η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα ασθενών ή πελατών ιδιώτη ιατρού, άλλου επαγγελματία του τομέα της υγείας ή δικηγόρου*». Είναι σημαντικό να ληφθεί υπόψη ότι, ενώ στην αιτιολογική σκέψη παρατίθενται παραδείγματα που αφορούν τα δύο άκρα (επεξεργασία από ιδιώτη ιατρό έναντι επεξεργασίας δεδομένων σε εθνικό επίπεδο ή σε ολόκληρη την Ευρώπη), μεταξύ των δύο αυτών άκρων, υπάρχει μια μεγάλη γκρίζα ζώνη. Θα πρέπει να ληφθεί υπόψη επιπλέον ότι η συγκεκριμένη αιτιολογική σκέψη αναφέρεται στις εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων. Αυτό σημαίνει ότι ορισμένα στοιχεία μπορεί να αφορούν συγκεκριμένα το εν λόγω πλαίσιο και δεν ισχύουν απαραιτήτως κατά τον ίδιο ακριβώς τρόπο για τον ορισμό υπευθύνου προστασίας δεδομένων.

Παραδείγματα επεξεργασίας σε μεγάλη κλίμακα είναι, μεταξύ άλλων, τα ακόλουθα:

- η επεξεργασία δεδομένων ασθενών στο πλαίσιο της συνήθους λειτουργίας ενός νοσοκομείου,
- η επεξεργασία δεδομένων μετακίνησης φυσικών προσώπων που χρησιμοποιούν το σύστημα δημόσιων μεταφορών μιας πόλης (π.χ., παρακολούθηση μέσω καρτών πολλαπλών διαδρομών),
- η επεξεργασία σε πραγματικό χρόνο δεδομένων γεωγραφικού εντοπισμού πελατών διεθνούς αλυσίδας ταχυφαγείων για στατιστικούς σκοπούς από εκτελούντα την επεξεργασία που ειδικεύεται στην παροχή τέτοιου είδους υπηρεσιών,
- η επεξεργασία δεδομένων πελατών στο πλαίσιο της συνήθους λειτουργίας μιας ασφαλιστικής εταιρείας ή μιας τράπεζας,
- η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς συμπεριφορικής διαφήμισης από μηχανή αναζήτησης,
- η επεξεργασία δεδομένων (περιεχόμενο, κίνηση, θέση) από παρόχους υπηρεσιών τηλεφωνίας ή διαδικτύου.

Παραδείγματα που δεν συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων, τα ακόλουθα:

- η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό,
- η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

2.1.4 «ΤΑΚΤΙΚΗ ΚΑΙ ΣΥΣΤΗΜΑΤΙΚΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗ»

Η έννοια της τακτικής και συστηματικής παρακολούθησης των υποκειμένων των δεδομένων δεν ορίζεται μεν στον ΓΚΠΔ, όμως στην αιτιολογική σκέψη 24[15] αναφέρεται η έννοια της «*παρακολούθησης της συμπεριφοράς των υποκειμένων των δεδομένων*» στην οποία περιλαμβάνονται ξεκάθαρα όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, μεταξύ άλλων, και για σκοπούς συμπεριφορικής διαφήμισης.

Η έννοια της παρακολούθησης δεν περιορίζεται, πάντως, στο επιγραμμικό περιβάλλον και η επιγραμμική παρακολούθηση θα πρέπει να θεωρείται ως ένα μόνο παράδειγμα παρακολούθησης της συμπεριφοράς των υποκειμένων των δεδομένων[16].

Η ομάδα του άρθρου 29 δίδει στο επίθετο «τακτική» μία ή περισσότερες από τις ακόλουθες ερμηνείες:

---

[15] *«Για τον καθορισμό του κατά πόσον μια δραστηριότητα επεξεργασίας μπορεί να θεωρηθεί ότι παρακολουθεί τη συμπεριφορά υποκειμένου των δεδομένων, θα πρέπει να εξακριβωθεί κατά πόσον φυσικά πρόσωπα παρακολουθούνται στο Διαδίκτυο, συμπεριλαμβανομένης της δυνητικής μετέπειτα χρήσης τεχνικών επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες συνίστανται στη διαμόρφωση του "προφίλ" ενός φυσικού προσώπου, ιδίως με σκοπό να ληφθούν αποφάσεις που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του».*

[16] Σημειώνεται ότι η αιτιολογική σκέψη 24 αφορά συγκεκριμένα την εξωεδαφική εφαρμογή του ΓΚΠΔ. Επιπλέον, υπάρχει διαφορά ανάμεσα στη διατύπωση «*παρακολούθηση της συμπεριφοράς τους*» (άρθρο 3 παράγραφος 2 στοιχείο β)) και στη διατύπωση *«τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων»* (άρθρο 37 παράγραφος 1 στοιχείο β)), γεγονός που θα μπορούσε συνεπώς να υποδηλώνει ότι πρόκειται για διαφορετική έννοια.

- λαμβάνουσα χώρα σε συνεχή βάση ή σε συγκεκριμένα χρονικά διαστήματα για συγκεκριμένη χρονική περίοδο,
- λαμβάνουσα χώρα τακτικά ή κατ' επανάληψη σε σταθερές χρονικές στιγμές,
- λαμβάνουσα χώρα αδιαλείπτως ή περιοδικά.

Η ομάδα του άρθρου 29 δίδει στο επίθετο «συστηματική» μία ή περισσότερες από τις ακόλουθες ερμηνείες:

- λαμβάνουσα χώρα σύμφωνα με κάποιο σύστημα,
- προκαθορισμένη, οργανωμένη ή μεθοδική,
- λαμβάνουσα χώρα στο πλαίσιο γενικότερου σχεδίου για τη συλλογή δεδομένων,
- διενεργούμενη στο πλαίσιο στρατηγικής.

Παραδείγματα δραστηριοτήτων που συνιστούν ενδεχομένως τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων: λειτουργία δικτύου τηλεπικοινωνιών· παροχή υπηρεσιών τηλεπικοινωνιών· επαναστόχευση μηνυμάτων ηλεκτρονικού ταχυδρομείου· δραστηριότητες μάρκετινγκ βάσει δεδομένων· διαμόρφωση προφίλ και βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (π.χ. για σκοπούς βαθμολόγησης πιστοληπτικής ικανότητας, προσδιορισμού ασφαλίστρων, καταπολέμησης της απάτης, εντοπισμού πρακτικών νομιμοποίησης εσόδων από εγκληματικές δραστηριότητες)· εντοπισμός θέσης, για παράδειγμα, μέσω εφαρμογών για κινητά τηλέφωνα· προγράμματα επιβράβευσης αφοσιωμένων πελατών· συμπεριφορική διαφήμιση· παρακολούθηση δεδομένων σχετικά με την ευεξία, τη φυσική κατάσταση και την υγεία μέσω φορέσιμων συσκευών· τηλεόραση κλειστού κυκλώματος· συνδεδεμένες συσκευές, π.χ. έξυπνες συσκευές μέτρησης, έξυπνα αυτοκίνητα, οικιακός αυτοματισμός κ.λπ.

2.1.5 ΕΙΔΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΔΕΔΟΜΕΝΑ ΠΟΥ ΑΦΟΡΟΥΝ ΠΟΙΝΙΚΕΣ ΚΑΤΑΔΙΚΕΣ ΚΑΙ ΑΔΙΚΗΜΑΤΑ

Το άρθρο 37 παράγραφος 1 στοιχείο γ) πραγματεύεται την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10. Μολονότι στη διάταξη χρησιμοποιείται η λέξη «και», δεν υφίσταται κάποιος λόγος σε επίπεδο πολιτικής για να πρέπει να ισχύουν ταυτόχρονα τα δύο κριτήρια. Επομένως, όταν διαβάζεται το κείμενο, θα πρέπει να γίνεται αντιληπτό με διαζευκτικό τρόπο, ήτοι ως εάν να έγραφε «ή» αντί για «και».

2.2. Υπεύθυνος προστασίας δεδομένων του εκτελούντος την επεξεργασία

Το άρθρο 37 σχετικά με τον ορισμό του υπευθύνου προστασίας δεδομένων ισχύει τόσο για τους υπεύθυνους επεξεργασίας[17] όσο και για τους εκτελούντες την επεξεργασία[18]. Ανάλογα με το ποιος πληροί τα κριτήρια περί υποχρεωτικού ορισμού, σε κάποιες περιπτώσεις η υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων βαρύνει μόνο τον υπεύθυνο επεξεργασίας ή μόνο τον εκτελούντα την επεξεργασία, ενώ σε άλλες περιπτώσεις αμφότερους τον υπεύθυνο επεξεργασίας και τον δικό του εκτελούντα την επεξεργασία (στην πορεία θα πρέπει να συνεργάζονται όλοι μεταξύ τους).

Είναι σημαντικό να τονιστεί ότι ακόμη κι αν ο υπεύθυνος επεξεργασίας πληροί τα κριτήρια περί υποχρεωτικού ορισμού, ο δικός του εκτελών την επεξεργασία δεν υποχρεούται απαραιτήτως να ορίσει υπεύθυνο προστασίας δεδομένων. Αυτό, ωστόσο, θα μπορούσε να αποτελέσει ορθή πρακτική.

Παραδείγματα:

- Μικρή οικογενειακή επιχείρηση που δραστηριοποιείται στον τομέα της διανομής οικιακών συσκευών σε μία πόλη χρησιμοποιεί τις υπηρεσίες εκτελούντος την επεξεργασία του οποίου η βασική δραστηριότητα είναι η παροχή υπηρεσιών ανάλυσης δικτυακών τόπων και υποστήριξης στον τομέα της στοχευμένης διαφήμισης και εμπορικής προώθησης. Οι δραστηριότητες της οικογενειακής επιχείρησης και οι πελάτες της δεν συνιστούν επεξεργασία δεδομένων σε «μεγάλη κλίμακα», δεδομένου του μικρού αριθμού πελατών και των σχετικά περιορισμένων δραστηριοτήτων. Αντιθέτως, οι δραστηριότητες του εκτελούντος την επεξεργασία, ο οποίος έχει πολλούς πελάτες σαν αυτή τη μικρή επιχείρηση, συνιστούν επεξεργασία μεγάλης κλίμακας, αν ληφθούν υπόψη συνολικά. Ο εκτελών την επεξεργασία πρέπει, επομένως, να ορίσει υπεύθυνο προστασίας δεδομένων σύμφωνα με το άρθρο 37 παράγραφος 1 στοιχείο β). Ταυτόχρονα, η ίδια η οικογενειακή επιχείρηση δεν βαρύνεται με την υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων.

- Κατασκευαστική εταιρεία μεσαίου μεγέθους αναθέτει υπεργολαβικά την παροχή υπηρεσιών επαγγελματικής υγείας σε εξωτερικό εκτελούντα την επεξεργασία, ο οποίος έχει πολλούς παρόμοιους πελάτες. Ο εκτελών την επεξεργασία οφείλει να ορίσει υπεύθυνο προστασίας δεδομένων σύμφωνα με το άρθρο 37 παράγραφος 1 στοιχείο γ) εφόσον η επεξεργασία είναι μεγάλης κλίμακας. Ο κατασκευαστής, αντίθετα, δεν βαρύνεται απαραιτήτως με την υποχρέωση να ορίσει υπεύθυνο προστασίας δεδομένων.

Ο υπεύθυνος προστασίας δεδομένων που ορίζεται από εκτελούντα την επεξεργασία επιβλέπει επιπλέον τις δραστηριότητες που αναπτύσσει ο οργανισμός του εκτελούντος την επεξεργασία όταν ενεργεί αυτοδικαίως ως υπεύθυνος επεξεργασίας (π.χ., ανθρώπινο δυναμικό, πληροφορική, εφοδιαστική).

2.3. Ορισμός ενός μόνο υπευθύνου προστασίας δεδομένων για πολλούς οργανισμούς

[17] Σύμφωνα με τον ορισμό του άρθρου 4 παράγραφος 7, ως υπεύθυνος επεξεργασίας νοείται το πρόσωπο ή ο φορέας που καθορίζει τους σκοπούς και τον τρόπο της επεξεργασίας.

[18] Σύμφωνα με τον ορισμό του άρθρου 4 παράγραφος 8, ως εκτελών την επεξεργασία νοείται το πρόσωπο ή ο φορέας που επεξεργάζεται δεδομένα για λογαριασμό του υπευθύνου της επεξεργασίας.

Σύμφωνα με το άρθρο 37 παράγραφος 2, όμιλος επιχειρήσεων μπορεί να διορίσει έναν μόνο υπεύθυνο προστασίας δεδομένων, υπό την προϋπόθεση ότι «*κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων*». Η έννοια της προσβασιμότητας αναφέρεται στα καθήκοντα του υπευθύνου προστασίας δεδομένων ως σημείου επικοινωνίας με τα υποκείμενα των δεδομένων[19], την εποπτική αρχή[20], αλλά και στο εσωτερικό του ίδιου του οργανισμού, δεδομένου ότι ένα από τα καθήκοντα του υπευθύνου προστασίας δεδομένων είναι να *«ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό»*[21].

Προκειμένου να διασφαλιστεί η πρόσβαση στον υπεύθυνο προστασίας δεδομένων, είτε αυτός είναι εσωτερικός είτε εξωτερικός, είναι σημαντικό τα στοιχεία επικοινωνίας του να είναι διαθέσιμα σύμφωνα με τις απαιτήσεις του ΓΚΠΔ[22].

Ο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, πρέπει να είναι σε θέση να επικοινωνεί με τα υποκείμενα των δεδομένων[23] και να συνεργάζεται[24] με τις ενδιαφερόμενες εποπτικές αρχές με αποτελεσματικό τρόπο. Αυτό σημαίνει επίσης ότι η επικοινωνία πρέπει να γίνεται στη γλώσσα ή στις γλώσσες που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων. Η διαθεσιμότητα του υπευθύνου προστασίας δεδομένων (είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας) είναι καθοριστικής σημασίας για τη διασφάλιση της δυνατότητας επικοινωνίας των υποκειμένων των δεδομένων μαζί του.

Σύμφωνα με το άρθρο 37 παράγραφος 3, ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές δημόσιες αρχές ή δημόσιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους. Τα ίδια ισχύουν και σε σχέση με τους πόρους και την επικοινωνία. Δεδομένου ότι ο υπεύθυνος προστασίας δεδομένων είναι επιφορτισμένος με ποικίλα καθήκοντα, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πρέπει να διασφαλίζουν ότι ένας μόνο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, δύναται να επιτελεί αποτελεσματικά όλα τα καθήκοντα παρά το γεγονός ότι έχει οριστεί για πολλές δημόσιες αρχές και δημόσιους φορείς.

---

[19] Άρθρο 38 παράγραφος 4: «*Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος κανονισμού*».

[20] Άρθρο 39 παράγραφος 1 στοιχείο ε): «*ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα*».

[21] Άρθρο 39 παράγραφος 1 στοιχείο α).

[22] Βλέπε επίσης ενότητα 2.6 κατωτέρω.

[23] Άρθρο 12 παράγραφος 1: *«Ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία που αναφέρεται στα άρθρα 13 και 14 και κάθε ανακοίνωση στο πλαίσιο των άρθρων 15 έως 22 και του άρθρου 34 σχετικά με την επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά.»*

[24] Άρθρο 39 παράγραφος 1 στοιχείο δ)*: «συνεργάζεται με την εποπτική αρχή»*

2.4. Προσβασιμότητα και τοποθεσία του υπευθύνου προστασίας δεδομένων

Σύμφωνα με το τμήμα 4 του ΓΚΠΔ, η προσβασιμότητα στον υπεύθυνο προστασίας δεδομένων θα πρέπει να είναι αποτελεσματική.

Για τη διασφάλιση της προσβασιμότητας στον υπεύθυνο προστασίας δεδομένων, η ομάδα του άρθρου 29 συνιστά να είναι εγκατεστημένος ο τελευταίος εντός Ευρωπαϊκής Ένωσης, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην Ευρωπαϊκή Ένωση.

Δεν αποκλείεται, πάντως, σε κάποιες περιπτώσεις στις οποίες ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν είναι εγκατεστημένοι εντός Ευρωπαϊκής Ένωσης[25], ο υπεύθυνος προστασίας δεδομένων να είναι σε θέση να εκτελεί τις δραστηριότητές του αποτελεσματικότερα εάν είναι εγκατεστημένος εκτός ΕΕ.

2.5. Εμπειρογνωμοσύνη και δεξιότητες του υπευθύνου προστασίας δεδομένων

Σύμφωνα με το άρθρο 37 παράγραφος 5, ο υπεύθυνος προστασίας δεδομένων «*διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39*». Στην αιτιολογική σκέψη 97 αναφέρεται ότι το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία.

- **Επίπεδο εμπειρογνωμοσύνης**

Αν και το απαιτούμενο επίπεδο εμπειρογνωμοσύνης δεν καθορίζεται αυστηρά, σε κάθε περίπτωση πρέπει να είναι ανάλογο της ευαισθησίας, της πολυπλοκότητας και της ποσότητας των δεδομένων που επεξεργάζεται ο οργανισμός. Για παράδειγμα, όταν μια δραστηριότητα επεξεργασίας δεδομένων είναι ιδιαίτερα πολύπλοκη, ή όταν εμπλέκεται μεγάλος όγκος ευαίσθητων δεδομένων, ο υπεύθυνος προστασίας δεδομένων είναι πιθανό να χρειάζεται υψηλότερο επίπεδο εμπειρογνωμοσύνης και υποστήριξης. Διαφορά υπάρχει επίσης και όταν ο οργανισμός διαβιβάζει συστηματικά δεδομένα προσωπικού χαρακτήρα εκτός της Ευρωπαϊκής Ένωσης ή όταν οι διαβιβάσεις αυτές είναι περιστασιακές. Ο υπεύθυνος προστασίας δεδομένων θα πρέπει επομένως να επιλέγεται προσεκτικά, λαμβάνοντας δεόντως υπόψη τα ζητήματα προστασίας δεδομένων που ανακύπτουν στο εσωτερικό του οργανισμού.

- **Επαγγελματικά προσόντα**

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

[25] Βλ. άρθρο 3 του ΓΚΠΔ σχετικά με το εδαφικό πεδίο εφαρμογής.

επίσης οι εποπτικές αρχές να προωθούν ανά τακτά χρονικά διαστήματα κατάλληλα προγράμματα κατάρτισης για τους υπεύθυνους προστασίας δεδομένων.

Χρήσιμη θεωρείται δε η γνώση του τομέα δραστηριότητας καθώς και του οργανισμού του υπευθύνου επεξεργασίας. Ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει καλή γνώση των πράξεων επεξεργασίας που διενεργούνται, καθώς και των συστημάτων πληροφορικής, και των αναγκών του υπευθύνου επεξεργασίας σε επίπεδο ασφάλειας και προστασίας των δεδομένων.

Στην περίπτωση δημόσιας αρχής ή δημόσιου φορέα, ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει επιπλέον καλή γνώση των διοικητικών κανόνων και διαδικασιών του οργανισμού.

- **Ικανότητα εκπλήρωσης των καθηκόντων**

Η ικανότητα εκπλήρωσης των καθηκόντων που βαρύνουν τον υπεύθυνο προστασίας δεδομένων θα πρέπει να ερμηνεύεται τόσο σε σχέση με τις προσωπικές ικανότητες και γνώσεις του, όσο και με τη θέση που κατέχει εντός του οργανισμού. Στις προσωπικές ικανότητες θα πρέπει να περιλαμβάνονται, μεταξύ άλλων, η ακεραιότητα και το υψηλό αίσθημα επαγγελματικής δεοντολογίας, ενώ πρωταρχικό μέλημα του υπευθύνου προστασίας δεδομένων θα πρέπει να είναι η μέγιστη δυνατή συμμόρφωση με τον ΓΚΠΔ. Ο υπεύθυνος προστασίας δεδομένων διαδραματίζει καίριο ρόλο στην ανάπτυξη νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού και συμβάλλει στην εφαρμογή ουσιωδών στοιχείων του ΓΚΠΔ, όπως οι αρχές της επεξεργασίας δεδομένων[26], τα δικαιώματα των υποκειμένων των δεδομένων[27], η προστασία των δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού[28], τα αρχεία των δραστηριοτήτων επεξεργασίας[29], η ασφάλεια των δεδομένων προσωπικού χαρακτήρα[30], και η γνωστοποίηση και ανακοίνωση παραβίασης δεδομένων[31].

- **Υπεύθυνος προστασίας δεδομένων με σύμβαση παροχής υπηρεσιών**

Τα καθήκοντα του υπευθύνου προστασίας δεδομένων είναι δυνατό επίσης να ασκηθούν βάσει σύμβασης παροχής υπηρεσιών η οποία συνάπτεται με φυσικό πρόσωπο ή οργανισμό εκτός του οργανισμού του υπευθύνου επεξεργασίας/εκτελούντος την επεξεργασία. Στην τελευταία αυτή περίπτωση, είναι σημαντικό κάθε μέλος του οργανισμού που ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων να πληροί όλες τις ισχύουσες απαιτήσεις του τμήματος 4 του ΓΚΠΔ (π.χ., είναι σημαντικό να μην έχει κανείς σύγκρουση συμφερόντων). Εξίσου σημαντικό είναι να προστατεύονται από τις διατάξεις του ΓΚΠΔ όλα τα προαναφερόμενα μέλη (π.χ., όχι καταχρηστική καταγγελία της σύμβασης παροχής υπηρεσιών για την άσκηση δραστηριοτήτων που εμπίπτουν στην ιδιότητα του υπευθύνου προστασίας δεδομένων, ούτε καταχρηστική απόλυση οποιουδήποτε μέλους του οργανισμού το οποίο ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων). Παράλληλα, θα μπορούσαν να συνδυαστούν οι προσωπικές δεξιότητες και τα δυνατά σημεία διαφόρων επιμέρους ατόμων έτσι ώστε τα εν λόγω άτομα, συνεργαζόμενα ως ομάδα, να είναι σε θέση να εξυπηρετούν αποτελεσματικότερα τους πελάτες τους.

[26] Κεφάλαιο II.
[27] Κεφάλαιο III.
[28] Άρθρο 25.
[29] Άρθρο 30.
[30] Άρθρο 32.
[31] Άρθρα 33 και 34.

Για λόγους νομικής σαφήνειας, καλής οργάνωσης και αποφυγής των συγκρούσεων συμφερόντων για τα μέλη της ομάδας, συνιστάται να υπάρχει σαφής καταμερισμός των καθηκόντων στους κόλπους της ομάδας του υπευθύνου προστασίας δεδομένων και να ορίζεται ένα μόνο άτομο ως επικεφαλής επικοινωνίας και υπεύθυνος για κάθε πελάτη. Σκόπιμο θα ήταν γενικώς επίσης να αναφέρονται αναλυτικά τα ανωτέρω στη σύμβαση παροχής υπηρεσιών.

2.6. Δημοσίευση και ανακοίνωση των στοιχείων επικοινωνίας του υπευθύνου προστασίας δεδομένων

Σύμφωνα με το άρθρο 37 παράγραφος 7 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία:

- δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και
- ανακοινώνουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων στις οικείες εποπτικές αρχές.

Ο στόχος αυτών των απαιτήσεων είναι να διασφαλιστεί η εύκολη και απευθείας επικοινωνία των υποκειμένων των δεδομένων (τόσο εντός όσο και εκτός του οργανισμού) και των εποπτικών αρχών με τον υπεύθυνο προστασίας δεδομένων χωρίς να απαιτείται επικοινωνία με άλλο τμήμα του οργανισμού. Εξίσου σημαντική είναι και η παράμετρος της εμπιστευτικότητας: για παράδειγμα, οι εργαζόμενοι μπορεί να διστάζουν να υποβάλουν καταγγελία στον υπεύθυνο προστασίας δεδομένων αν δεν διασφαλίζεται το απόρρητο των επικοινωνιών τους.
Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους (άρθρο 38 παράγραφος 5).

Στα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων θα πρέπει να περιλαμβάνονται πληροφορίες που διευκολύνουν την επικοινωνία των υποκειμένων των δεδομένων και των εποπτικών αρχών μαζί του (ταχυδρομική διεύθυνση, συγκεκριμένος τηλεφωνικός αριθμός και/ή συγκεκριμένη διεύθυνση ηλεκτρονικού ταχυδρομείου). Εφόσον ενδείκνυται, για σκοπούς επικοινωνίας με το κοινό, θα μπορούσαν να παρέχονται και άλλα μέσα επικοινωνίας όπως, π.χ., ειδική ανοικτή τηλεφωνική γραμμή ή ειδικό έντυπο επικοινωνίας υπ' όψιν του υπευθύνου προστασίας δεδομένων στον δικτυακό τόπο του οργανισμού.

Το άρθρο 37 παράγραφος 7 δεν απαιτεί τη συμπερίληψη του ονόματος του υπευθύνου προστασίας δεδομένων στα στοιχεία επικοινωνίας που δημοσιεύονται. Μολονότι η δημοσίευση του ονόματος θα μπορούσε να αποτελέσει ορθή πρακτική, είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία και του υπευθύνου προστασίας δεδομένων να αποφασίζουν εάν είναι αναγκαία ή σκόπιμη, ανάλογα με τις ιδιαιτερότητες κάθε περίπτωσης[32].

Η ανακοίνωση, πάντως, του ονόματος του υπευθύνου προστασίας δεδομένων στην εποπτική αρχή είναι καίριας σημασίας προκειμένου ο υπεύθυνος προστασίας δεδομένων να ενεργεί ως σημείο επικοινωνίας ανάμεσα στον οργανισμό και την εποπτική αρχή (άρθρο 39 παράγραφος 1 στοιχείο ε)).

[32] Σημειώνεται ότι το άρθρο 33 παράγραφος 3 στοιχείο β), στο οποίο παρατίθενται αναλυτικά οι πληροφορίες που πρέπει να παρέχονται στην εποπτική αρχή και στα υποκείμενα των δεδομένων σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, σε αντίθεση με το άρθρο 37 στοιχείο 7, απαιτεί επιπλέον ρητώς να ανακοινώνεται το όνομα (και όχι μόνο τα στοιχεία επικοινωνίας) του υπευθύνου προστασίας δεδομένων.

Η ομάδα του άρθρου 29 συνιστά επίσης, ως ορθή πρακτική, να γνωστοποιεί ο οργανισμός το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων στους υπαλλήλους του, δημοσιεύοντάς τα, για παράδειγμα, στο ενδοδίκτυό του, στον εσωτερικό τηλεφωνικό κατάλογο και στα οργανογράμματά του.

3 Θέση του υπευθύνου προστασίας δεδομένων

3.1. Συμμετοχή του υπευθύνου προστασίας δεδομένων σε όλα τα ζητήματα που σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα

Σύμφωνα με το άρθρο 38 του ΓΚΠΔ, ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων *«συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα»*.

Η όσο το δυνατόν νωρίτερη συμμετοχή του υπευθύνου προστασίας δεδομένων, ή της ομάδας του, σε όλα τα ζητήματα που σχετίζονται με την προστασία των δεδομένων είναι καίριας σημασίας. Όσον αφορά τις εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων, ο ΓΚΠΔ προβλέπει ρητώς την έγκαιρη συμμετοχή του υπευθύνου προστασίας δεδομένων και προσδιορίζει ότι ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων κατά τη διενέργεια εκτιμήσεων αντικτύπου σχετικά με την προστασία των δεδομένων[33]. Η ενημέρωση του υπευθύνου προστασίας δεδομένων και η διαβούλευση μαζί του από το αρχικό κιόλας στάδιο θα διευκολύνουν τη συμμόρφωση με τον ΓΚΠΔ και θα προωθήσουν την προσέγγιση της προστασίας της ιδιωτικής ζωής ήδη από το στάδιο του σχεδιασμού. Θα πρέπει, επομένως, να αποτελούν συνήθη διαδικασία στο πλαίσιο της διακυβέρνησης του οργανισμού. Σημαντικό είναι επίσης ο υπεύθυνος προστασίας δεδομένων να αντιμετωπίζεται ως συνομιλητής στους κόλπους του οργανισμού και να συμμετέχει στις ομάδες εργασίας που ασχολούνται με δραστηριότητες επεξεργασίας δεδομένων εντός του οργανισμού.

Συνεπώς, ο οργανισμός θα πρέπει να διασφαλίζει, για παράδειγμα, τα ακόλουθα:

- να καλείται ο υπεύθυνος προστασίας δεδομένων να συμμετέχει τακτικά στις συσκέψεις των ανώτερων και μεσαίων στελεχών της διοίκησης·
- να είναι παρών όταν λαμβάνονται αποφάσεις που έχουν επιπτώσεις στην προστασία δεδομένων. Όλες οι σχετικές πληροφορίες πρέπει να διαβιβάζονται εγκαίρως στον υπεύθυνο προστασίας δεδομένων ώστε να είναι σε θέση να παράσχει κατάλληλες συμβουλές·
- να δίδεται πάντοτε η δέουσα βαρύτητα στη γνώμη του υπευθύνου προστασίας δεδομένων. Σε περίπτωση διαφωνίας, η ομάδα του άρθρου 29 συνιστά, ως ορθή πρακτική, να καταγράφονται οι λόγοι για τους οποίους δεν ακολουθήθηκαν οι συμβουλές του υπευθύνου προστασίας δεδομένων·
- να ζητείται απαραιτήτως άμεσα η γνώμη του υπευθύνου προστασίας δεδομένων σε περίπτωση παραβίασης δεδομένων ή άλλου σχετικού συμβάντος.

Κατά περίπτωση, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία θα μπορούσαν επίσης να αναπτύξουν κατευθυντήριες γραμμές ή προγράμματα για την προστασία των δεδομένων όπου θα

[33] Άρθρο 35 παράγραφος 2.

αναφέρεται συγκεκριμένα σε ποιες περιπτώσεις πρέπει να ζητείται η γνώμη του υπευθύνου προστασίας δεδομένων.

3.2. Απαραίτητοι πόροι

Σύμφωνα με το άρθρο 38 παράγραφος 2 του ΓΚΠΔ, ο οργανισμός στηρίζει τον υπεύθυνο προστασίας δεδομένων του *«παρέχοντας απαραίτητους πόρους για την άσκηση των καθηκόντων [του] και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του».* Ειδικότερα, πρέπει να λαμβάνονται υπόψη τα ακόλουθα στοιχεία:

- Ενεργή στήριξη του υπευθύνου προστασίας δεδομένων από τα ανώτερα διοικητικά στελέχη (π.χ. σε επίπεδο διοικητικού συμβουλίου).
- Επάρκεια χρόνου ώστε να μπορούν οι υπεύθυνοι προστασίας δεδομένων να επιτελούν τα καθήκοντά τους. Αυτό είναι ιδιαίτερα σημαντικό όταν ο ορισθείς εσωτερικός υπεύθυνος προστασίας δεδομένων τελεί υπό καθεστώς μερικής απασχόλησης ή όταν ο εξωτερικός υπεύθυνος προστασίας δεδομένων ασχολείται με την προστασία των δεδομένων επιπλέον των λοιπών καθηκόντων που επιτελεί. Ειδάλλως, οι αντικρουόμενες προτεραιότητες του υπευθύνου προστασίας δεδομένων ενδέχεται να έχουν ως συνέπεια την παραμέληση των καθηκόντων του. Η εξασφάλιση επαρκούς χρόνου είναι μείζονος σημασίας προκειμένου να μπορεί ο υπεύθυνος προστασίας δεδομένων να ασχολείται απερίσπαστος με τα καθήκοντά του. Συνιστά ορθή πρακτική να ορίζεται συγκεκριμένο ποσοστό χρόνου ενασχόλησης με τα καθήκοντα του υπευθύνου προστασίας δεδομένων όταν δεν επιτελούνται υπό καθεστώς πλήρους απασχόλησης. Ορθές πρακτικές είναι επίσης ο καθορισμός του χρόνου που απαιτείται για την επιτέλεση των καθηκόντων του υπευθύνου προστασίας δεδομένων, η ιεράρχηση των εν λόγω καθηκόντων κατά σειρά προτεραιότητας και ο προσδιορισμός του χρόνου που χρειάζεται ο υπεύθυνος προστασίας δεδομένων (ή ο οργανισμός) για να καταρτίσει σχέδιο εργασίας.
- Προσήκουσα στήριξη σε επίπεδο οικονομικών πόρων, υποδομών (χώροι, εγκαταστάσεις, εξοπλισμός) και προσωπικού, κατά περίπτωση.
- Επίσημη ανακοίνωση του ορισμού του υπευθύνου προστασίας δεδομένων σε όλο το προσωπικό ώστε να διασφαλιστεί ότι η ύπαρξη και τα καθήκοντά του είναι γνωστά σε όλον τον οργανισμό.
- Απαραίτητη πρόσβαση σε άλλα τμήματα, όπως το τμήμα ανθρωπίνων πόρων, το τμήμα ασφάλειας, το νομικό τμήμα, το τμήμα πληροφορικής κ.λπ., ώστε οι υπεύθυνοι προστασίας δεδομένων να μπορούν να λαμβάνουν ουσιαστική στήριξη, συνδρομή και πληροφόρηση απ' αυτά.
- Συνεχής κατάρτιση. Πρέπει να δίδεται στους υπεύθυνους προστασίας δεδομένων η ευκαιρία να παρακολουθούν τις εξελίξεις στον τομέα της προστασίας των δεδομένων. Ο στόχος θα πρέπει να είναι η διαρκής βελτίωση του επιπέδου εμπειρογνωσίας των υπευθύνων προστασίας δεδομένων. Θα πρέπει να ενθαρρύνονται να συμμετέχουν σε σεμινάρια κατάρτισης για την προστασία των δεδομένων και σε άλλες μορφές επαγγελματικής επιμόρφωσης, όπως συμμετοχή σε φόρα συζήτησης με θέμα την προστασία της ιδιωτικής ζωής, εργαστήρια κ.λπ.
- Αναλόγως του μεγέθους και της δομής του οργανισμού, μπορεί ενδεχομένως να απαιτείται η σύσταση ομάδας υπευθύνου προστασίας δεδομένων (να υπάρχει δηλαδή υπεύθυνος προστασίας δεδομένων με δικό του προσωπικό). Σε τέτοιες περιπτώσεις, θα πρέπει να καθορίζεται με σαφήνεια η εσωτερική δομή της ομάδας, καθώς και τα καθήκοντα και οι

αρμοδιότητες των επιμέρους μελών της. Ομοίως, όταν τα καθήκοντα του υπευθύνου προστασίας δεδομένων ασκούνται από εξωτερικό πάροχο υπηρεσιών, η αποτελεσματική άσκησή τους είναι δυνατό να εξασφαλιστεί με τη σύσταση ομάδας στους κόλπους της εν λόγω οντότητας, τα μέλη της οποίας συνεργάζονται μεταξύ τους υπό την ευθύνη ατόμου το οποίο έχει οριστεί επικεφαλής επικοινωνίας για κάθε πελάτη.

Γενικώς, όσο πιο περίπλοκες και/ή ευαίσθητες είναι οι πράξεις επεξεργασίας, τόσο περισσότεροι πόροι πρέπει να διατίθενται στον υπεύθυνο προστασίας δεδομένων. Ο υπεύθυνος προστασίας δεδομένων πρέπει να μπορεί να ασκεί αποτελεσματικά τα καθήκοντά του και να έχει στη διάθεσή του επαρκείς πόρους σε σχέση με τη διενεργούμενη επεξεργασία δεδομένων.

3.3. Εντολές και «*εκτέλεση των υποχρεώσεων και των καθηκόντων με ανεξάρτητο τρόπο*»

Το άρθρο 38 παράγραφος 3 θεσπίζει ορισμένες βασικές εγγυήσεις ώστε να διασφαλίζεται ότι οι υπεύθυνοι προστασίας δεδομένων είναι σε θέση να εκτελούν τα καθήκοντά τους με επαρκή βαθμό αυτονομίας στους κόλπους του οργανισμού όπου απασχολούνται. Συγκεκριμένα, οι υπεύθυνοι επεξεργασίας/εκτελούντες την επεξεργασία οφείλουν να διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων «*δεν λαμβάνει εντολές για την άσκηση των [...] καθηκόντων [του]*.» Στην αιτιολογική σκέψη 97 αναφέρεται επιπροσθέτως ότι οι υπεύθυνοι προστασίας δεδομένων, «*ανεξάρτητα από το κατά πόσον είναι υπάλληλοι του υπευθύνου επεξεργασίας, θα πρέπει να είναι σε θέση να εκτελούν τις υποχρεώσεις και τα καθήκοντά τους με ανεξάρτητο τρόπο*».

Αυτό σημαίνει ότι, κατά την άσκηση των καθηκόντων τους που απορρέουν από το άρθρο 39, οι υπεύθυνοι προστασίας δεδομένων δεν πρέπει να λαμβάνουν εντολές για το πώς θα χειριστούν την εκάστοτε υπόθεση όπως, π.χ. τι αποτέλεσμα θα πρέπει να επιτευχθεί, πώς πρέπει να γίνει η διερεύνηση μιας καταγγελίας ή εάν θα ζητηθεί ή όχι η γνώμη της εποπτικής αρχής. Επιπλέον, δεν πρέπει να λαμβάνουν εντολές προκειμένου να υιοθετήσουν συγκεκριμένη στάση για ένα ζήτημα σε σχέση με τη νομοθεσία περί προστασίας των δεδομένων όπως, π.χ., να ερμηνεύσουν με συγκεκριμένο τρόπο τη νομοθεσία.

Η διασφάλιση της αυτονομίας των υπεύθυνων προστασίας δεδομένων δεν σημαίνει, πάντως, ότι αποκτούν εξουσίες λήψης αποφάσεων καθ' υπέρβαση των καθηκόντων τους, όπως αυτά ορίζονται στο άρθρο 39.

Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι αυτός που εξακολουθεί να φέρει την ευθύνη της συμμόρφωσης με το δίκαιο περί προστασίας των δεδομένων και πρέπει να είναι σε θέση να αποδείξει την εν λόγω συμμόρφωση[34]. Αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία λαμβάνει αποφάσεις που έρχονται σε σύγκρουση με τον ΓΚΠΔ και με τις συμβουλές του υπευθύνου προστασίας δεδομένων, τότε ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει τη δυνατότητα να γνωστοποιήσει την αντίθετη γνώμη του στο ανώτατο διοικητικό επίπεδο του οργανισμού και στους υπεύθυνους λήψης των αποφάσεων. Σχετικά με το συγκεκριμένο θέμα, το άρθρο 38 παράγραφος 3 προβλέπει ότι ο υπεύθυνος προστασίας δεδομένων «*λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία*». Με την απευθείας λογοδοσία διασφαλίζεται η πλήρης ενημέρωση της ανώτερης διοίκησης (π.χ., διοικητικό συμβούλιο) για τις συμβουλές και τις συστάσεις που διατυπώνει ο υπεύθυνος προστασίας δεδομένων στο πλαίσιο του

[34] Άρθρο 5 παράγραφος 2.

καθήκοντός του να ενημερώνει και να συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία. Άλλο παράδειγμα απευθείας λογοδοσίας είναι η κατάρτιση ετήσιας έκθεσης δραστηριοτήτων από τον υπεύθυνο προστασίας δεδομένων και η υποβολή της στο ανώτατο διοικητικό επίπεδο.

3.4. Απόλυση ή επιβολή κυρώσεων για λόγους που σχετίζονται με την επιτέλεση των καθηκόντων του υπευθύνου προστασίας δεδομένων

Σύμφωνα με το άρθρο 38 παράγραφος 3, ο υπεύθυνος προστασίας δεδομένων *«δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του»*.

Η εν λόγω απαίτηση ενισχύει την αυτονομία των υπευθύνων προστασίας δεδομένων και βοηθάει να διασφαλιστεί ότι ενεργούν ανεξάρτητα και ότι απολαύουν επαρκούς προστασίας κατά την επιτέλεση των καθηκόντων τους που σχετίζονται με θέματα προστασίας των δεδομένων.

Ο ΓΚΠΔ απαγορεύει την επιβολή κυρώσεων μόνο στην περίπτωση που αυτές επιβάλλονται απλώς επειδή ο υπεύθυνος προστασίας δεδομένων επιτέλεσε τα καθήκοντά του που απορρέουν από τη συγκεκριμένη ιδιότητα. Για παράδειγμα, ο υπεύθυνος προστασίας δεδομένων εκτιμά ότι μια συγκεκριμένη επεξεργασία ενδέχεται να συνεπάγεται υψηλό κίνδυνο και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία να διενεργήσει εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων, όμως ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν συμφωνεί με την άποψη του υπευθύνου προστασίας δεδομένων. Σε μια τέτοια περίπτωση, ο υπεύθυνος προστασίας δεδομένων δεν μπορεί να απολυθεί απλώς επειδή παρείχε τη συγκεκριμένη συμβουλή.

Οι κυρώσεις είναι δυνατό να έχουν διάφορες μορφές και να είναι άμεσες ή έμμεσες. Μπορεί, π.χ., ο υπεύθυνος προστασίας δεδομένων να μην πάρει ποτέ προαγωγή ή να την πάρει με μεγάλη καθυστέρηση. Μπορεί ακόμη να υπονομευτεί η εξέλιξη της σταδιοδρομίας του ή να μην του χορηγούνται παροχές που λαμβάνουν άλλοι εργαζόμενοι. Δεν είναι ανάγκη οι εν λόγω κυρώσεις να επιβάλλονται πράγματι. Αρκεί απλώς η απειλή της επιβολής τους, εφόσον χρησιμοποιούνται προκειμένου να τιμωρηθεί ο υπεύθυνος προστασίας δεδομένων για λόγους που σχετίζονται με τις δραστηριότητες τις οποίες εκτελεί υπό τη συγκεκριμένη ιδιότητα.

Σύμφωνα με τους συνήθεις κανόνες διοίκησης και όπως ισχύει για οποιονδήποτε υπάλληλο ή ανάδοχο δυνάμει των διατάξεων του εφαρμοστέου εθνικού δικαίου περί συμβάσεων, καθώς και του εφαρμοστέου εθνικού εργατικού και ποινικού δικαίου, που διέπουν τους υπαλλήλους και τους αναδόχους, ο υπεύθυνος προστασίας δεδομένων μπορεί κάλλιστα να απολυθεί νομίμως για λόγους που δεν σχετίζονται με την επιτέλεση των καθηκόντων που απορρέουν από τη συγκεκριμένη ιδιότητα (π.χ., σε περίπτωση κλοπής, σωματικής, ψυχολογικής ή σεξουαλικής παρενόχλησης ή συναφούς σοβαρού παραπτώματος).

Στο πλαίσιο αυτό, θα πρέπει να σημειωθεί ότι ο ΓΚΠΔ δεν προσδιορίζει με ποιους τρόπους και σε ποιες περιπτώσεις μπορεί να απολυθεί ο υπεύθυνος προστασίας δεδομένων ή να αντικατασταθεί από άλλο πρόσωπο. Όσο πιο στέρεα είναι, πάντως, η σύμβαση του υπευθύνου προστασίας δεδομένων, και όσες περισσότερες εγγυήσεις παρέχονται κατά της καταχρηστικής απόλυσης, τόσο αυξάνουν οι

πιθανότητες να μπορεί να ενεργεί με ανεξάρτητο τρόπο. Επομένως, η ομάδα του άρθρου 29 επιδοκιμάζει θερμά τυχόν προσπάθειες των οργανισμών προς αυτήν την κατεύθυνση.

3.5. Συγκρούσεις συμφερόντων

Σύμφωνα με το άρθρο 38 παράγραφος 6, οι υπεύθυνοι προστασίας δεδομένων μπορούν να επιτελούν «*και άλλα καθήκοντα και υποχρεώσεις*». Ο οργανισμός υποχρεούται, πάντως, να διασφαλίζει ότι «*τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων*».

Η απουσία σύγκρουσης συμφερόντων συνδέεται στενά με την απαίτηση της επιτέλεσης των καθηκόντων με ανεξάρτητο τρόπο. Μολονότι οι υπεύθυνοι προστασίας δεδομένων επιτρέπεται να επιτελούν και άλλα καθήκοντα, η ανάθεση σ' αυτούς άλλων καθηκόντων και υποχρεώσεων είναι δυνατή μόνο υπό την προϋπόθεση ότι δεν προκύπτουν συγκρούσεις συμφερόντων. Αυτό συνεπάγεται συγκεκριμένα ότι ο υπεύθυνος προστασίας δεδομένων δεν μπορεί να κατέχει στους κόλπους του οργανισμού θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Επειδή κάθε οργανισμός έχει διαφορετική οργανωτική δομή, το συγκεκριμένο ζήτημα θα πρέπει να εξετάζεται για κάθε περίπτωση χωριστά.

Θα μπορούσε να ειπωθεί, με βάση την εμπειρία, ότι θέσεις στις οποίες εντοπίζονται συνήθως συγκρούσεις συμφερόντων στους κόλπους ενός οργανισμού είναι, μεταξύ άλλων, οι θέσεις της ανώτερης διοίκησης (όπως, διευθύνων σύμβουλος, διοικητικός γενικός διευθυντής, οικονομικός διευθυντής, αρχίατρος, προϊστάμενος τμήματος μάρκετινγκ, προϊστάμενος ανθρωπίνων πόρων ή προϊστάμενος τμήματος πληροφορικής), και άλλες θέσεις κατώτερων βαθμίδων της οργανωτικής δομής, εφόσον από τις θέσεις αυτές είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας. Σύγκρουση συμφερόντων μπορεί επίσης να προκύψει, π.χ., σε περίπτωση που ζητηθεί από εξωτερικό υπεύθυνο προστασίας δεδομένων να εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ενώπιον των δικαστηρίων σε υποθέσεις που σχετίζονται με ζητήματα προστασίας των δεδομένων.

Αναλόγως των δραστηριοτήτων, του μεγέθους και της δομής του οργανισμού, τα ακόλουθα μπορούν να αποτελέσουν ορθές πρακτικές για τους υπεύθυνους επεξεργασίας ή τους εκτελούντες την επεξεργασία:

- να εντοπίζουν τις θέσεις που είναι ενδεχομένως ασύμβατες με τα καθήκοντα του υπευθύνου προστασίας δεδομένων,
- να καταρτίζουν εσωτερικό κανονισμό για τον συγκεκριμένο σκοπό, με γνώμονα την αποτροπή των συγκρούσεων συμφερόντων,
- να περιλαμβάνουν μια πιο γενική εξήγηση των συγκρούσεων συμφερόντων,
- να ανακοινώνουν ότι δεν υφίσταται σύγκρουση συμφερόντων για τον υπεύθυνο προστασίας δεδομένων που έχουν ορίσει όσον αφορά την άσκηση των καθηκόντων του υπό τη συγκεκριμένη ιδιότητα, ως έναν τρόπο ενίσχυσης της ευαισθητοποίησης γύρω από τη συγκεκριμένη απαίτηση,
- να συμπεριλαμβάνουν στον εσωτερικό κανονισμό του οργανισμού εγγυήσεις και να διασφαλίζουν ότι η ανακοίνωση για την πλήρωση της θέσης του υπευθύνου προστασίας δεδομένων ή η σύμβαση παροχής υπηρεσιών είναι επαρκώς ακριβείς και λεπτομερείς ώστε να αποτρέπονται οι συγκρούσεις συμφερόντων. Στο πλαίσιο αυτό, θα πρέπει να σημειωθεί ότι οι

συγκρούσεις συμφερόντων μπορούν να λάβουν διάφορες μορφές ανάλογα με το εάν ο προσληφθείς υπεύθυνος προστασίας δεδομένων είναι εσωτερικός ή εξωτερικός.

4 Καθήκοντα του υπευθύνου προστασίας δεδομένων

4.1. Παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ

Σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχείο β), οι υπεύθυνοι προστασίας δεδομένων έχουν, μεταξύ άλλων, το καθήκον να παρακολουθούν τη συμμόρφωση με τον ΓΚΠΔ. Στην αιτιολογική σκέψη 97 διευκρινίζεται περαιτέρω ότι ο υπεύθυνος προστασίας δεδομένων «*θα πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον παρόντα κανονισμό*».

Στο πλαίσιο των καθηκόντων παρακολούθησης της συμμόρφωσης, οι υπεύθυνοι προστασίας δεδομένων μπορούν συγκεκριμένα:

- να συλλέγουν πληροφορίες με σκοπό τον προσδιορισμό δραστηριοτήτων επεξεργασίας,
- να αναλύουν και να ελέγχουν τη συμμόρφωση των δραστηριοτήτων επεξεργασίας,
- να ενημερώνουν τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, να τους παρέχουν συμβουλές και να εκδίδουν συστάσεις υπ' όψιν τους.

Το γεγονός ότι είναι επιφορτισμένος με το καθήκον της παρακολούθησης της συμμόρφωσης δεν σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων φέρει προσωπική ευθύνη σε περίπτωση μη συμμόρφωσης. Ο ΓΚΠΔ καθιστά σαφές ότι υπεύθυνος να « *εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό*» (άρθρο 24 παράγραφος 1) είναι ο υπεύθυνος επεξεργασίας, και όχι ο υπεύθυνος προστασίας δεδομένων. Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων είναι εταιρική ευθύνη του υπευθύνου επεξεργασίας, και όχι του υπευθύνου προστασίας δεδομένων.

4.2. Ρόλος του υπευθύνου προστασίας δεδομένων στην εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων

Σύμφωνα με το άρθρο 35 παράγραφος 1, είναι καθήκον του υπευθύνου επεξεργασίας, και όχι του υπευθύνου προστασίας δεδομένων, να διενεργεί εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Ο υπεύθυνος προστασίας δεδομένων μπορεί, πάντως, να διαδραματίσει πολύ σημαντικό και χρήσιμο ρόλο στο πλαίσιο αυτό παρέχοντας συνδρομή στον υπεύθυνο επεξεργασίας. Σύμφωνα με το άρθρο 35 παράγραφος 2, το οποίο ακολουθεί την αρχή της προστασίας των δεδομένων ήδη από τον σχεδιασμό, ο υπεύθυνος επεξεργασίας «*ζητεί τη γνώμη*» του υπευθύνου προστασίας δεδομένων κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, ενώ, σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχείο γ), ο υπεύθυνος προστασίας δεδομένων έχει, μεταξύ άλλων, το καθήκον να «*παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35*».

Η ομάδα του άρθρου 29 συνιστά να ζητεί ο υπεύθυνος επεξεργασίας τη γνώμη του υπευθύνου προστασίας δεδομένων για ζητήματα όπως, ενδεικτικά, τα ακόλουθα [35]:

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

Αν ο υπεύθυνος επεξεργασίας διαφωνεί με τις συμβουλές του υπευθύνου προστασίας δεδομένων, τότε στα έγγραφα της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων θα πρέπει να καταγραφούν γραπτώς οι λόγοι για τους οποίους δεν λήφθηκαν υπόψη οι συμβουλές[36].

Η ομάδα του άρθρου 29 συνιστά περαιτέρω ο υπεύθυνος επεξεργασίας να περιγράφει συνοπτικά αλλά με σαφήνεια , για παράδειγμα στη σύμβαση του υπευθύνου προστασίας δεδομένων, αλλά και στις πληροφορίες που παρέχονται στους υπαλλήλους, τη διοίκηση (και άλλους ενδιαφερόμενους, κατά περίπτωση), τα ακριβή καθήκοντα του υπευθύνου προστασίας δεδομένων και το πεδίο εφαρμογής τους, συγκεκριμένα δε σε σχέση με τη διενέργεια της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων.

4.3. Συνεργασία με την εποπτική αρχή και λειτουργία σημείου επικοινωνίας

Σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχεία δ) και ε), ο υπεύθυνος προστασίας δεδομένων θα πρέπει να «*συνεργάζεται με την εποπτική αρχή*» και να «*ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα*».

Τα εν λόγω καθήκοντα αναφέρονται ουσιαστικά στον «μεσολαβητικό» ρόλο του υπευθύνου προστασίας δεδομένων που αναφέρεται στην εισαγωγή των παρουσών κατευθυντήριων γραμμών. Ο

---

[35] Στο άρθρο 39 παράγραφος 1 απαριθμούνται τα καθήκοντα του υπευθύνου προστασίας δεδομένων και αναφέρεται συγκεκριμένα ότι ο υπεύθυνος προστασίας δεδομένων έχει «*τουλάχιστον*» τα ακόλουθα καθήκοντα. Συνεπώς, ο υπεύθυνος επεξεργασίας μπορεί κάλλιστα να αναθέτει στον υπεύθυνο προστασίας δεδομένων και άλλα καθήκοντα πέραν αυτών που αναφέρονται ρητώς στο άρθρο 39 παράγραφος 1, ή να τα εξειδικεύει περαιτέρω.

[36] Το άρθρο 24 παράγραφος 1 ορίζει τα εξής: «*Λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει* ***και να μπορεί να αποδεικνύει*** *ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο*».

υπεύθυνος προστασίας δεδομένων ενεργεί ως σημείο επικοινωνίας προκειμένου να διευκολύνει την πρόσβαση της εποπτικής αρχής στα έγγραφα και τις πληροφορίες που σχετίζονται με την επιτέλεση των καθηκόντων του άρθρου 57, καθώς και με την άσκηση των εξουσιών έρευνας και των διορθωτικών, αδειοδοτικών και συμβουλευτικών εξουσιών του άρθρου 58. Όπως προαναφέρεται, ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους (άρθρο 38 παράγραφος 5). Η υποχρέωση τήρησης του απορρήτου/της εμπιστευτικότητας δεν σημαίνει, πάντως, ότι ο υπεύθυνος προστασίας δεδομένων απαγορεύεται να επικοινωνήσει με την εποπτική αρχή και να της ζητήσει συμβουλές. Σύμφωνα με το άρθρο 39 παράγραφος 1 στοιχείο ε), ο υπεύθυνος προστασίας δεδομένων μπορεί να πραγματοποιεί διαβουλεύσεις με την εποπτική αρχή, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

4.4. Προσέγγιση με βάση την επικινδυνότητα

Σύμφωνα με το άρθρο 39 παράγραφος 2, ο υπεύθυνος προστασίας δεδομένων «*λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας*».

Το εν λόγω άρθρο υπενθυμίζει ουσιαστικά μια γενική αρχή της κοινής λογικής, η οποία σχετίζεται ενδεχομένως με πολλές πτυχές των καθημερινών εργασιών που επιτελεί ο υπεύθυνος προστασίας δεδομένων. Απαιτεί, κατ' ουσίαν, από τους υπεύθυνους προστασίας δεδομένων να ιεραρχούν τις δραστηριότητές τους κατά σειρά προτεραιότητας και να επικεντρώνονται στα ζητήματα που εγκυμονούν σοβαρότερους κινδύνους για την προστασία των δεδομένων. Αυτό δεν σημαίνει μεν ότι θα πρέπει να παραμελούν την παρακολούθηση της συμμόρφωσης των πράξεων επεξεργασίας δεδομένων που παρουσιάζουν συγκριτικά χαμηλότερο επίπεδο κινδύνου, υποδεικνύει όμως ότι θα πρέπει να εστιάζουν πρώτιστα στους τομείς υψηλού κινδύνου.

Αυτή η επιλεκτική και ρεαλιστική προσέγγιση θα βοηθήσει λογικά τους υπεύθυνους προστασίας δεδομένων να συμβουλεύουν τον υπεύθυνο επεξεργασίας ποια μεθοδολογία να χρησιμοποιήσει κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, σε ποιους τομείς θα πρέπει να διενεργηθεί εσωτερικός ή εξωτερικός έλεγχος για την προστασία των δεδομένων, ποιες δραστηριότητες εσωτερικής κατάρτισης θα πρέπει να παρασχεθούν στο προσωπικό ή στα διοικητικά στελέχη που είναι υπεύθυνα για δραστηριότητες επεξεργασίας δεδομένων, και σε ποιες πράξεις επεξεργασίας θα πρέπει να διαθέσει περισσότερο χρόνο και πόρους.

4.5. Ρόλος του υπευθύνου προστασίας δεδομένων στην τήρηση αρχείων

Σύμφωνα με το άρθρο 30 παράγραφοι 1 και 2, υπεύθυνος να «*τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος*» ή να *«τηρεί αρχείο όλων των κατηγοριών δραστηριοτήτων επεξεργασίας που διεξάγονται εκ μέρους του υπευθύνου επεξεργασίας»* είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία, και όχι ο υπεύθυνος προστασίας δεδομένων.

Στην πράξη, συνήθως οι υπεύθυνοι προστασίας δεδομένων δημιουργούν καταλόγους και τηρούν μητρώο των πράξεων επεξεργασίας με βάση τις πληροφορίες που λαμβάνουν από τα διάφορα τμήματα του οργανισμού τους που είναι υπεύθυνα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η πρακτική αυτή έχει καθιερωθεί από πολλά ισχύοντα επί του παρόντος εθνικά δίκαια

καθώς και από τους κανόνες περί προστασίας των δεδομένων που διέπουν τα θεσμικά όργανα και οργανισμούς της ΕΕ[37].

Στο άρθρο 39 παράγραφος 1 απαριθμούνται τα καθήκοντα που πρέπει να έχει κατ' ελάχιστον ο υπεύθυνος προστασίας δεδομένων. Συνεπώς, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί κάλλιστα να αναθέτει στον υπεύθυνο προστασίας δεδομένων το καθήκον να τηρεί αρχείο των πράξεων επεξεργασίας για τις οποίες είναι αρμόδιος ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Το εν λόγω αρχείο θα πρέπει να θεωρείται ως ένα από τα εργαλεία που επιτρέπουν στον υπεύθυνο προστασίας δεδομένων να επιτελεί δύο από τα καθήκοντά του, ήτοι την παρακολούθηση της συμμόρφωσης, και την ενημέρωση και παροχή συμβουλών στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.

Σε κάθε περίπτωση, το αρχείο που επιβάλλεται να τηρείται δυνάμει του άρθρου 30 θα πρέπει να αντιμετωπίζεται ως εργαλείο που επιτρέπει στον υπεύθυνο επεξεργασίας και την εποπτική αρχή, κατόπιν αιτήματος, να έχουν μια επισκόπηση όλων των δραστηριοτήτων επεξεργασίας δεδομένων προσωπικού χαρακτήρα που επιτελεί ένας οργανισμός. Αποτελεί επομένως προϋπόθεση συμμόρφωσης και, κατά συνέπεια, αποτελεσματικό μέτρο λογοδοσίας.

[37] Άρθρο 24 παράγραφος 1 στοιχείο δ) του κανονισμού (ΕΚ) αριθ. 45/2001.

5 ΠΑΡΑΡΤΗΜΑ - ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ ΣΧΕΤΙΚΑ ΜΕ ΤΟΥΣ ΥΠΕΥΘΥΝΟΥΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ: ΤΙ ΠΡΕΠΕΙ ΝΑ ΓΝΩΡΙΖΕΤΕ

Στόχος του παρόντος παραρτήματος είναι να δώσει απαντήσεις, με απλό και ευανάγνωστο τρόπο, σε βασικά ερωτήματα που μπορεί να έχουν οι οργανισμοί σε σχέση με τις νέες απαιτήσεις περί ορισμού υπευθύνου προστασίας δεδομένων τις οποίες θεσπίζει ο γενικός κανονισμός για την προστασία δεδομένων (ΓΚΠΔ).

Ορισμός του υπευθύνου προστασίας δεδομένων

1 Ποιοι οργανισμοί πρέπει να ορίζουν υπεύθυνο προστασίας δεδομένων;

Ο ορισμός υπευθύνου προστασίας δεδομένων είναι υποχρεωτικός:

- εάν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (ανεξάρτητα από το είδος των δεδομένων που υφίστανται επεξεργασία),
- εάν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα,
- εάν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Σημειώνεται ότι το δίκαιο της Ένωσης ή των κρατών μελών είναι δυνατό να επιβάλλει τον ορισμό υπευθύνου προστασίας δεδομένων και σε άλλες περιπτώσεις. Τέλος, ακόμη κι αν ο ορισμός υπευθύνου προστασίας δεδομένων δεν είναι υποχρεωτικός, ενδέχεται να υπάρξουν οργανισμοί που θα κρίνουν σκόπιμο να ορίσουν υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση. Η ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα του άρθρου 29 («ομάδα του άρθρου 29») ενθαρρύνει τέτοιου είδους εθελοντικές ενέργειες. Όταν ένας οργανισμός ορίζει υπεύθυνο προστασίας δεδομένων σε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι ίδιες απαιτήσεις ως εάν ο ορισμός να ήταν υποχρεωτικός.

Πηγή: Άρθρο 37 παράγραφος 1 του ΓΚΠΔ

2 Τι σημαίνει «βασικές δραστηριότητες»;

Ως «βασικές δραστηριότητες» μπορούν να θεωρηθούν οι καίριες πράξεις για την επίτευξη των στόχων του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Σ' αυτές συμπεριλαμβάνονται επίσης όλες οι δραστηριότητες που επιτελούνται όταν η επεξεργασία δεδομένων αποτελεί αναπόσπαστο μέρος της δραστηριότητας του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία. Για παράδειγμα, η επεξεργασία ιατρικών δεδομένων, όπως οι ιατρικοί φάκελοι ασθενών, θα πρέπει να θεωρείται ως μία από τις βασικές δραστηριότητες κάθε νοσοκομείου. Κατά συνέπεια, τα νοσοκομεία οφείλουν να ορίσουν υπεύθυνο προστασίας δεδομένων.

Από την άλλη πλευρά, όλοι οι οργανισμοί επιτελούν ορισμένες υποστηρικτικές δραστηριότητες όπως, π.χ., καταβάλλουν τους μισθούς των υπαλλήλων τους ή αναπτύσσουν συνήθεις δραστηριότητες υποστήριξης ΤΠ. Αυτά είναι παραδείγματα αναγκαίων λειτουργιών υποστήριξης της βασικής δραστηριότητας ή του κύριου τομέα δραστηριότητας του οργανισμού. Μολονότι οι εν λόγω δραστηριότητες είναι αναγκαίες ή ουσιώδεις, θεωρούνται κατά κανόνα ως παρεπόμενες λειτουργίες του οργανισμού και όχι ως η βασική του δραστηριότητα.

Πηγή: Άρθρο 37 παράγραφος 1 στοιχεία β) και γ) του ΓΚΠΔ

3 Τι σημαίνει «μεγάλη κλίμακα»;

Ο ΓΚΠΔ δεν ορίζει τι συνιστά επεξεργασία μεγάλης κλίμακας. Η ομάδα του άρθρου 29 συνιστά να λαμβάνονται συγκεκριμένα υπόψη οι ακόλουθοι παράγοντες όταν επιχειρείται να προσδιοριστεί εάν η επεξεργασία διενεργείται σε μεγάλη κλίμακα ή όχι:

- ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού,
- ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υφίστανται επεξεργασία,
- η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων,
- η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Παραδείγματα επεξεργασίας σε μεγάλη κλίμακα είναι, μεταξύ άλλων, τα ακόλουθα:

- η επεξεργασία δεδομένων ασθενών στο πλαίσιο της συνήθους λειτουργίας ενός νοσοκομείου,
- η επεξεργασία δεδομένων μετακίνησης φυσικών προσώπων που χρησιμοποιούν το σύστημα δημόσιων μεταφορών μιας πόλης (π.χ., παρακολούθηση μέσω καρτών πολλαπλών διαδρομών),
- η επεξεργασία σε πραγματικό χρόνο δεδομένων γεωγραφικού εντοπισμού πελατών διεθνούς αλυσίδας ταχυφαγείων για στατιστικούς σκοπούς από εκτελούντα την επεξεργασία που ειδικεύεται σε τέτοιου είδους δραστηριότητες,
- η επεξεργασία δεδομένων πελατών στο πλαίσιο της συνήθους λειτουργίας μιας ασφαλιστικής εταιρείας ή μιας τράπεζας,
- η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς συμπεριφορικής διαφήμισης από μηχανή αναζήτησης,
- η επεξεργασία δεδομένων (περιεχόμενο, κίνηση, θέση) από παρόχους υπηρεσιών τηλεφωνίας ή διαδικτύου.

Παραδείγματα που δεν συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων, τα ακόλουθα:

- η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό,
- η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

Πηγή: Άρθρο 37 παράγραφος 1 στοιχεία β) και γ) του ΓΚΠΔ

4 Τι σημαίνει «τακτική και συστηματική παρακολούθηση»;

Η έννοια της τακτικής και συστηματικής παρακολούθησης των υποκειμένων των δεδομένων δεν ορίζεται μεν στον ΓΚΠΔ, όμως περιλαμβάνει ξεκάθαρα όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, μεταξύ άλλων, και για σκοπούς συμπεριφορικής διαφήμισης. Η έννοια της παρακολούθησης δεν περιορίζεται, πάντως, στο επιγραμμικό περιβάλλον.

Παραδείγματα δραστηριοτήτων που συνιστούν ενδεχομένως τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων: λειτουργία δικτύου τηλεπικοινωνιών· παροχή υπηρεσιών τηλεπικοινωνιών· επαναστόχευση μηνυμάτων ηλεκτρονικού ταχυδρομείου· δραστηριότητες μάρκετινγκ βάσει δεδομένων· διαμόρφωση προφίλ και βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (π.χ., για σκοπούς βαθμολόγησης πιστοληπτικής ικανότητας, προσδιορισμού ασφαλίστρων, καταπολέμησης της απάτης, εντοπισμού πρακτικών νομιμοποίησης εσόδων από

εγκληματικές δραστηριότητες)· εντοπισμός θέσης, για παράδειγμα, μέσω εφαρμογών για κινητά τηλέφωνα· προγράμματα επιβράβευσης αφοσιωμένων πελατών· συμπεριφορική διαφήμιση· παρακολούθηση δεδομένων σχετικά με την ευεξία, τη φυσική κατάσταση και την υγεία μέσω φορέσιμων συσκευών· τηλεόραση κλειστού κυκλώματος· συνδεδεμένες συσκευές, π.χ. έξυπνες συσκευές μέτρησης, έξυπνα αυτοκίνητα, οικιακός αυτοματισμός κ.λπ.

Η ομάδα του άρθρου 29 δίδει στο επίθετο «τακτική» μία ή περισσότερες από τις ακόλουθες ερμηνείες:

- συνεχής ή ανά συγκεκριμένα χρονικά διαστήματα για συγκεκριμένη χρονική περίοδο,
- λαμβάνουσα χώρα τακτικά ή κατ' επανάληψη σε σταθερές χρονικές στιγμές,
- λαμβάνουσα χώρα αδιαλείπτως ή περιοδικά.

Η ομάδα του άρθρου 29 δίδει στο επίθετο «συστηματική» μία ή περισσότερες από τις ακόλουθες ερμηνείες:

- λαμβάνουσα χώρα σύμφωνα με κάποιο σύστημα,
- προκαθορισμένη, οργανωμένη ή μεθοδική,
- λαμβάνουσα χώρα στο πλαίσιο γενικότερου σχεδίου για τη συλλογή δεδομένων,
- διενεργούμενη στο πλαίσιο στρατηγικής.

Πηγή: Άρθρο 37 παράγραφος 1 στοιχείο β) του ΓΚΠΔ

5 Μπορούν οι οργανισμοί να ορίζουν από κοινού υπεύθυνο προστασίας δεδομένων; Αν ναι, υπό ποιους όρους;

Ναι. Όμιλος επιχειρήσεων μπορεί να διορίσει έναν μόνο υπεύθυνο προστασίας δεδομένων, υπό την προϋπόθεση ότι «*κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων*». Η έννοια της προσβασιμότητας αναφέρεται στα καθήκοντα του υπευθύνου προστασίας δεδομένων ως σημείου επικοινωνίας με τα υποκείμενα των δεδομένων, την εποπτική αρχή, αλλά και στο εσωτερικό του ίδιου του οργανισμού. Προκειμένου να διασφαλιστεί η πρόσβαση στον υπεύθυνο προστασίας δεδομένων, είτε αυτός είναι εσωτερικός είτε εξωτερικός, είναι σημαντικό τα στοιχεία επικοινωνίας του να είναι διαθέσιμα. Ο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, πρέπει να είναι σε θέση να επικοινωνεί με τα υποκείμενα των δεδομένων και να συνεργάζεται με τις ενδιαφερόμενες εποπτικές αρχές με αποτελεσματικό τρόπο. Αυτό σημαίνει ότι η επικοινωνία πρέπει να γίνεται στη γλώσσα ή στις γλώσσες που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων. Η διαθεσιμότητα του υπευθύνου προστασίας δεδομένων (είτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας) είναι καθοριστικής σημασίας για τη διασφάλιση της δυνατότητας επικοινωνίας των υποκειμένων των δεδομένων μαζί του.

Ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές δημόσιες αρχές ή δημόσιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους. Τα ίδια ισχύουν και σε σχέση με τους πόρους και την επικοινωνία. Δεδομένου ότι ο υπεύθυνος προστασίας δεδομένων είναι επιφορτισμένος με ποικίλα καθήκοντα, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πρέπει να διασφαλίζουν ότι ένας μόνο υπεύθυνος προστασίας δεδομένων, συνεπικουρούμενος από ομάδα εφόσον απαιτείται, δύναται να επιτελεί αποτελεσματικά όλα τα καθήκοντα παρά το γεγονός ότι έχει οριστεί για πολλές δημόσιες αρχές και φορείς.

Πηγή: Άρθρο 37 παράγραφοι 2 και 3 του ΓΚΠΔ

6 Πού θα πρέπει να είναι εγκατεστημένος ο υπεύθυνος προστασίας δεδομένων;

Για τη διασφάλιση της προσβασιμότητας στον υπεύθυνο προστασίας δεδομένων, η ομάδα του άρθρου 29 συνιστά να είναι εγκατεστημένος ο τελευταίος εντός Ευρωπαϊκής Ένωσης, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι ή όχι εγκατεστημένοι στην Ευρωπαϊκή Ένωση. Δεν αποκλείεται, πάντως, σε κάποιες περιπτώσεις στις οποίες ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν είναι εγκατεστημένοι εντός Ευρωπαϊκής Ένωσης, ο υπεύθυνος προστασίας δεδομένων να είναι σε θέση να εκτελεί τις δραστηριότητές του αποτελεσματικότερα εάν είναι εγκατεστημένος εκτός ΕΕ.

7 Είναι δυνατός ο ορισμός εξωτερικού υπευθύνου προστασίας δεδομένων;

Ναι. Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών. Αυτό σημαίνει ότι ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι εξωτερικός, και σ' αυτήν την περίπτωση, τα καθήκοντά του μπορούν να ασκηθούν βάσει σύμβασης παροχής υπηρεσιών η οποία συνάπτεται με φυσικό πρόσωπο ή οργανισμό.

Όταν τα καθήκοντα του υπευθύνου προστασίας δεδομένων ασκούνται από εξωτερικό πάροχο υπηρεσιών, η αποτελεσματική άσκησή τους είναι δυνατό να εξασφαλιστεί με τη σύσταση ομάδας στους κόλπους της εν λόγω οντότητας, τα μέλη της οποίας συνεργάζονται μεταξύ τους υπό την ευθύνη ατόμου το οποίο έχει οριστεί επικεφαλής επικοινωνίας και «υπεύθυνος» για κάθε πελάτη. Σ' αυτήν την περίπτωση, είναι σημαντικό κάθε μέλος του εξωτερικού οργανισμού που ασκεί καθήκοντα υπευθύνου προστασίας δεδομένων να πληροί όλες τις ισχύουσες απαιτήσεις του ΓΚΠΔ.

Για λόγους νομικής σαφήνειας, καλής οργάνωσης και αποφυγής των συγκρούσεων συμφερόντων για τα μέλη της ομάδας, οι κατευθυντήριες γραμμές συνιστούν να υπάρχει, στη σύμβαση παροχής υπηρεσιών, σαφής καταμερισμός των καθηκόντων στους κόλπους της ομάδας του εξωτερικού υπευθύνου προστασίας δεδομένων και να ορίζεται ένα μόνο άτομο ως επικεφαλής επικοινωνίας και υπεύθυνος για κάθε πελάτη.

Πηγή: Άρθρο 37 παράγραφος 6 του ΓΚΠΔ

8 Τι επαγγελματικά προσόντα θα πρέπει να έχει ο υπεύθυνος προστασίας δεδομένων;

Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων του.

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

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

- εμπειρογνωσία στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, τόσο σε εθνικό όσο και σε ευρωπαϊκό επίπεδο, καθώς και άριστη γνώση του ΓΚΠΔ,
- γνώση των πράξεων επεξεργασίας που διενεργούνται,
- γνώση του τομέα των τεχνολογιών πληροφοριών και της ασφάλειας δεδομένων,
- γνώση του τομέα δραστηριότητας και του οργανισμού,
- ικανότητα ανάπτυξης νοοτροπίας προστασίας των δεδομένων στους κόλπους του οργανισμού.

Πηγή: Άρθρο 37 παράγραφος 5 του ΓΚΠΔ

Θέση του υπευθύνου προστασίας δεδομένων

9 Τι πόρους θα πρέπει να θέτει στη διάθεση του υπευθύνου προστασίας δεδομένων ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία;

Ο υπεύθυνος προστασίας δεδομένων πρέπει να έχει στη διάθεσή του τους απαραίτητους πόρους για την άσκηση των καθηκόντων του.

Αναλόγως της φύσης των πράξεων επεξεργασίας και των δραστηριοτήτων και του μεγέθους του οργανισμού, ο υπεύθυνος προστασίας δεδομένων θα πρέπει να έχει στη διάθεσή του τους ακόλουθους πόρους:

- ενεργή στήριξη του υπευθύνου προστασίας δεδομένων από τα ανώτερα διοικητικά στελέχη,
- επάρκεια χρόνου ώστε να μπορούν οι υπεύθυνοι προστασίας δεδομένων να επιτελούν τα καθήκοντά τους,
- προσήκουσα στήριξη σε επίπεδο οικονομικών πόρων, υποδομών (χώροι, εγκαταστάσεις, εξοπλισμός) και προσωπικού, κατά περίπτωση,
- επίσημη ανακοίνωση του ορισμού του υπευθύνου προστασίας δεδομένων σε όλο το προσωπικό,
- πρόσβαση σε άλλα τμήματα του οργανισμού, ώστε οι υπεύθυνοι προστασίας δεδομένων να μπορούν να λαμβάνουν ουσιαστική στήριξη, συνδρομή ή πληροφόρηση από αυτά,

- συνεχή κατάρτιση.

Πηγή: Άρθρο 38 παράγραφος 2 του ΓΚΠΔ

10 Ποιες εγγυήσεις απαιτούνται προκειμένου να είναι σε θέση ο υπεύθυνος προστασίας δεδομένων να εκτελεί τα καθήκοντά του με ανεξάρτητο τρόπο; Τι σημαίνει «σύγκρουση συμφερόντων»;

Υπάρχουν διάφορες εγγυήσεις προκειμένου ο υπεύθυνος προστασίας δεδομένων να είναι σε θέση να εκτελεί τα καθήκοντά του με ανεξάρτητο τρόπο:

- να μην δίνουν οι υπεύθυνοι επεξεργασίας ή οι εκτελούντες την επεξεργασία εντολές στον υπεύθυνο προστασίας δεδομένων σχετικά με την άσκηση των καθηκόντων του,
- να μην απολύει ο υπεύθυνος επεξεργασίας τον υπεύθυνο προστασίας δεδομένων ή να μην του επιβάλλει κυρώσεις για λόγους σχετικούς με την άσκηση των καθηκόντων του,
- να μην υπάρχουν συγκρούσεις συμφερόντων με πιθανά άλλα καθήκοντα και υποχρεώσεις.

Τα άλλα καθήκοντα και υποχρεώσεις του υπευθύνου προστασίας δεδομένων δεν πρέπει να συνεπάγονται σύγκρουση συμφερόντων. Αυτό σημαίνει, καταρχάς, ότι ο υπεύθυνος προστασίας δεδομένων δεν μπορεί να κατέχει στους κόλπους του οργανισμού θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Επειδή κάθε οργανισμός έχει διαφορετική οργανωτική δομή, το συγκεκριμένο ζήτημα θα πρέπει να εξετάζεται για κάθε περίπτωση χωριστά.

Θα μπορούσε να ειπωθεί, με βάση την εμπειρία, ότι θέσεις στις οποίες εντοπίζονται συνήθως συγκρούσεις συμφερόντων στους κόλπους ενός οργανισμού είναι, μεταξύ άλλων, οι θέσεις της ανώτερης διοίκησης (όπως, διευθύνων σύμβουλος, διοικητικός γενικός διευθυντής, οικονομικός διευθυντής, αρχίατρος, προϊστάμενος τμήματος μάρκετινγκ, προϊστάμενος ανθρωπίνων πόρων ή προϊστάμενος τμήματος πληροφορικής), και άλλες θέσεις κατώτερων βαθμίδων της οργανωτικής δομής, εφόσον από τις θέσεις αυτές είναι δυνατός ο καθορισμός των σκοπών και των μέσων της επεξεργασίας. Σύγκρουση συμφερόντων μπορεί επίσης να προκύψει, π.χ., σε περίπτωση που ζητηθεί από εξωτερικό υπεύθυνο προστασίας δεδομένων να εκπροσωπεί τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ενώπιον των δικαστηρίων σε υποθέσεις που σχετίζονται με ζητήματα προστασίας των δεδομένων.

Πηγή: Άρθρο 38 παράγραφοι 3 και 6 του ΓΚΠΔ

11 Τι σημαίνει «παρακολούθηση συμμόρφωσης»;

Στο πλαίσιο των καθηκόντων παρακολούθησης της συμμόρφωσης, οι υπεύθυνοι προστασίας δεδομένων μπορούν συγκεκριμένα:

- να συλλέγουν πληροφορίες με σκοπό τον προσδιορισμό δραστηριοτήτων επεξεργασίας,
- να αναλύουν και να ελέγχουν τη συμμόρφωση των δραστηριοτήτων επεξεργασίας,
- να ενημερώνουν τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, να τους παρέχουν συμβουλές και να εκδίδουν συστάσεις υπ' όψιν τους.

Πηγή: Άρθρο 39 παράγραφος 1 στοιχείο β) του ΓΚΠΔ

12 Ο υπεύθυνος προστασίας δεδομένων φέρει προσωπική ευθύνη για περιπτώσεις μη συμμόρφωσης με τις απαιτήσεις περί προστασίας των δεδομένων;

Όχι. Οι υπεύθυνοι προστασίας δεδομένων δεν φέρουν προσωπική ευθύνη για περιπτώσεις μη συμμόρφωσης με τις απαιτήσεις περί προστασίας των δεδομένων. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Η συμμόρφωση με τους κανόνες προστασίας των δεδομένων είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

13 Ποιος είναι ο ρόλος του υπευθύνου προστασίας δεδομένων όσον αφορά τις εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων και τα αρχεία των δραστηριοτήτων επεξεργασίας;

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

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

Όσον αφορά τα αρχεία των δραστηριοτήτων επεξεργασίας, η τήρησή τους είναι ευθύνη του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, και όχι του υπευθύνου προστασίας δεδομένων. Πάντως, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί κάλλιστα να αναθέτει στον υπεύθυνο προστασίας δεδομένων το καθήκον να τηρεί τα αρχεία των πράξεων επεξεργασίας για τις οποίες είναι υπεύθυνος ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Τα εν λόγω αρχεία θα πρέπει να θεωρούνται ως ένα από τα εργαλεία που επιτρέπουν στον υπεύθυνο προστασίας δεδομένων να επιτελεί δύο από τα καθήκοντά του, ήτοι την παρακολούθηση της συμμόρφωσης, και την ενημέρωση και παροχή συμβουλών στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία.

Πηγή: Άρθρο 39 παράγραφος 1 στοιχείο γ) και άρθρο 30 του ΓΚΠΔ

Βρυξέλλες, 13 Δεκεμβρίου 2016

Για την ομάδα του άρθρου 29,
Η πρόεδρος

Isabelle FALQUE-PIERROTIN

Όπως αναθεωρήθηκε τελευταία και εγκρίθηκε στις 5 Απριλίου 2017

Για την ομάδα του άρθρου 29,
Η πρόεδρος

Isabelle FALQUE-PIERROTIN

ΑΝΑΡΤΗΣΗ ΑΠΟ ΤΗΝ ΙΣΤΟΣΕΛΙΔΑ ΤΗΣ ΑΠΔΠΧ

Εισαγωγή

Ο **Υπεύθυνος Προστασίας Δεδομένων (DPO)διευκολύνει** τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τις διατάξεις του ΓΚΠΔ και **μεσολαβεί** μεταξύ των διαφόρων ενδιαφερομένων (π.χ. εποπτικές αρχές, υποκείμενα των δεδομένων).**Ο ρόλος του είναι συμβουλευτικός (όχι αποφασιστικός)**και δε φέρει προσωπική ευθύνη για τη μη συμμόρφωση με τον Κανονισμό. Υπεύθυνος να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον ΓΚΠΔ είναι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Προβλέπονται συγκεκριμένα καθήκοντα του DPO και αντίστοιχες υποχρεώσεις του εργοδότη του. Παράβαση των σχετικών με τον DPOδιατάξεων επιφέρει κυρώσεις (βλ. άρθρα 37-38 και 83 σε συνδυασμό με αιτιολογική σκέψη 97 του ΓΚΠΔ).

Συχνές Ερωτήσεις

1. Ποιοι οργανισμοί πρέπει να ορίζουνDPO;

Ο ορισμός DPO είναι υποχρεωτικός όταν:

- Η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (συμπεριλαμβανομένων και φυσικών ή νομικών προσώπων δημοσίου ή ιδιωτικού δικαίου που ασκούν δημόσια εξουσία).Εξαιρούνται τα δικαστήρια όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα.
- Απαιτείται τακτική και συστηματική παρακολούθηση τωνυποκειμένων των δεδομένων σε μεγάλη κλίμακα (π.χ. ασφαλιστικές ή τραπεζικές υπηρεσίες,υπηρεσίες τηλεφωνίας ή διαδικτύου,παροχή υπηρεσιών ασφαλείας,όλες οι μορφές παρακολούθησης και διαμόρφωσης «προφίλ» στο διαδίκτυο, όπως για σκοπούς συμπεριφορικής διαφήμισης).
- Διενεργείται μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων (π.χ. στο πλαίσιο παροχής υπηρεσιών υγείας από νοσοκομεία)ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα.

Για τον προσδιορισμό της μεγάλης κλίμακας επεξεργασίας πρέπει να λαμβάνονται υπόψη: α) ο αριθμός των εμπλεκομένων υποκειμένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του πληθυσμού, β) ο όγκος και το εύρος των δεδομένων, γ) η διάρκεια ή ο μόνιμος χαρακτήρας της επεξεργασίας, δ) η γεωγραφική έκταση της επεξεργασίας. Παραδείγματα που **δεν** συνιστούν επεξεργασία μεγάλης κλίμακας είναι, μεταξύ άλλων,η επεξεργασία δεδομένων ασθενών από ιδιώτη ιατρό και η επεξεργασία δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα από ιδιώτη δικηγόρο.

2. Δεν υποχρεούμαι, αλλά επιθυμώ να ορίσω DPOστην επιχείρησή μου.Τι ισχύει σε αυτή την περίπτωση;

Κάθε οργανισμός μπορεί να ορίσειDPO. Ακόμη και στις περιπτώσεις που ο ορισμός DPOδεν είναι υποχρεωτικός, ενθαρρύνονται τέτοιου είδους εθελοντικές ενέργειες. Όταν ένας οργανισμός ορίζει DPOσε εθελοντική βάση, σε σχέση με τον ορισμό, τη θέση και τα καθήκοντά του θα ισχύουν οι ίδιες απαιτήσεις ως εάν ο ορισμός να ήταν υποχρεωτικός (βλ. ερώτηση 5).

3. Μπορεί να οριστείένας DPOγια περισσότερους φορείς ή οργανισμούς;

Ναι. Όμιλος επιχειρήσεων ή περισσότεροι δημόσιοι φορείς,λαμβάνοντας υπόψη το μέγεθος και την οργανωτική τους δομή, μπορούν να ορίσουν έναν μόνοDPO,υπό την προϋπόθεση **να είναι διαθέσιμος και εύκολα προσβάσιμος** σε κάθε εγκατάσταση ή φορέαείτε με φυσική παρουσία στις ίδιες εγκαταστάσεις με τους υπαλλήλους, είτε μέσω ανοικτής τηλεφωνικής γραμμής ή άλλου ασφαλούς μέσου επικοινωνίας και σε γλώσσα που χρησιμοποιούν οι ενδιαφερόμενες εποπτικές αρχές και τα οικεία υποκείμενα των δεδομένων.

4. Ποια είναι τα καθήκοντα του DPO;

Ο DPOπροάγει την κουλτούρα της προστασίας προσωπικών δεδομένων εντός του οργανισμού ή φορέα. Τα ελάχιστα καθήκοντα του DPO είναι τα ακόλουθα:

- Να ενημερώνει και να συμβουλεύει τον οργανισμό και τους υπαλλήλους του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό και άλλες διατάξεις περί προστασίας δεδομένων.
- Να παρακολουθεί την εσωτερική συμμόρφωση με τον Κανονισμό και άλλες διατάξειςπερί προστασίας δεδομένων(π.χ. προσδιορισμός και διαχείριση δραστηριοτήτων επεξεργασίας, εκπαίδευση προσωπικού, διενέργεια εσωτερικών ελέγχων).
- Να παρέχει συμβουλές για την εκτίμηση αντικτύπου και να παρακολουθεί την υλοποίησήτης.
- Να είναι το πρώτο σημείο επαφής για τις εποπτικές αρχές και τα υποκείμενα των δεδομένων (εργαζόμενοι, πελάτες κ.λπ.).
- Να συνεργάζεται με την εποπτική αρχή.

5. Ποιες είναι οι υποχρεώσεις του εργοδότη ενός DPO;

Ο εργοδότης υποχρεούται να δημοσιεύσει τα στοιχεία επικοινωνίας του DPOκαι να τα ανακοινώσει στην εποπτική αρχή. Επίσης, οφείλει να διασφαλίζει ότι ο DPO:

- Συμμετέχει σε όλα τα ζητήματα σχετικά με την προστασία προσωπικών δεδομένων (π.χ. παρουσία σε συσκέψεις ανώτερων και μεσαίων στελεχών της διοίκησης και κατά τη λήψη αποφάσεων, καταγραφή λόγων διαφωνίας με τις συμβουλές του, έγκαιρη διαβίβαση πληροφοριών για παροχή γνώμης, άμεση λήψη γνώμης σε περίπτωση περιστατικού παραβίασης).
- Έχει ελεύθερη πρόσβαση σε δεδομένα και πράξεις επεξεργασίας
- Έχει στη διάθεσή του τους απαραίτητους πόρους για την εκπλήρωση των καθηκόντων του (π.χ. ενεργή στήριξη από τα ανώτερα διοικητικά στελέχη, οικονομικοί πόροι, υποδομές, συνεχής κατάρτιση).

- Εκπληρώνει τα καθήκοντά του με ανεξάρτητο τρόπο (δεν λαμβάνει εντολές για την άσκηση των καθηκόντων του) και δεν απολύεται ούτε υφίσταται κυρώσεις επειδή επιτέλεσε τα καθήκοντά του.
- Λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του εργοδότη.
- Όταν ασκεί πρόσθετα καθήκοντα, αυτά να μην συνεπάγονται σύγκρουση συμφερόντων(π.χ. δεν μπορεί να κατέχει θέση από την οποία μπορεί να καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας, όπως θέσεις ανώτερης διοίκησης).
- Δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του.

6. Ο DPO είναι υπάλληλος ήεξωτερικός συνεργάτης;

Είτε το ένα είτε το άλλο. Ο DPOμπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία (εσωτερικός υπεύθυνος προστασίας δεδομένων) ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών (εξωτερικός συνεργάτης). Σε κάθε περίπτωση, μπορεί να συνεπικουρείται από ομάδα, εφόσον απαιτείται. Συνιστάται δε να είναι εγκατεστημένος εντός ΕΕ, ανεξάρτητα από το εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασίαείναι ή όχι εγκατεστημένοι στην ΕΕ.

7. Τι επαγγελματικά προσόντα θα πρέπει να έχει ο DPO; Προβλέπεται σχετική πιστοποίηση;

Ο DPOδιορίζεται ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων του. Το αναγκαίο επίπεδο εμπειρογνωσίας θα πρέπει να καθορίζεται ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που υφίστανται επεξεργασία. Παράλληλα, ο DPOπρέπει να έχει γνώση του τομέα δραστηριότητας του οργανισμού ή φορέα στον οποίο απασχολείται αλλά και των τεχνολογιών πληροφορίας και ασφάλειας των δεδομένων.

Ο Κανονισμός δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO, ούτε καν ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση (βλ. την υπ' αριθμ. πρωτ.Γ/ΕΞ/6007/09-08-2017 **Ανακοίνωση** και τη **Γνωμοδότηση 7/2017** της Αρχής).

Για περισσότερες λεπτομέρειες και σχετικές διευκρινίσεις, βλ. **Κατευθυντήριες γραμμές**της ΟΕ του άρθρου 29 σχετικά με τους Υπεύθυνους Προστασίας Δεδομένων και **Παράρτημα** αυτών (στα αγγλικά).

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΑΝΑΚΟΙΝΩΣΗ

Αθήνα, 9-8-2017

Αρ. πρωτ.: Γ/ΕΞ/6007

Η Αρχή συνεδρίασε για θέματα που αφορούν την πιστοποίηση επαγγελματικών προσόντων Υπευθύνων Προστασίας Δεδομένων (Data Protection Officers - DPOs), στο πλαίσιο εκπαιδευτικών προγραμμάτων που πραγματοποιούνται από διάφορους φορείς, και αποφάσισε να εκδώσει την ακόλουθη ανακοίνωση προς ενημέρωση των ενδιαφερομένων:

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαπιστώνει ότι, ενόψει της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) τον Μάϊο του 2018, προσφέρονται αρκετά εκπαιδευτικά προγράμματα/σεμινάρια για τον ρόλο του Υπευθύνου Προστασίας Δεδομένων (Data Protection Officer - DPO). Στο πλαίσιο της προώθησης των εκπαιδευτικών αυτών προγραμμάτων, υπάρχουν φορείς που υποστηρίζουν ότι η προσφερόμενη εκπαίδευση αποτελεί ένα προπαρασκευαστικό στάδιο που οδηγεί σε κάποιου τύπου πιστοποίηση DPO στην ελληνική επικράτεια.

Η Αρχή, με στόχο την ενημέρωση των ενδιαφερομένων, επισημαίνει ότι:

- Η δραστηριοποίηση αυτή της αγοράς είναι θετική, αφού συμβάλλει στη μεταφορά γνώσης και ενημέρωσης σε θέματα του ΓΚΠΔ, πρέπει όμως να τεθεί στην ορθή της διάσταση, αποφεύγοντας τη δημιουργία εσφαλμένων εντυπώσεων ως προς τις σχετικές απαιτήσεις του ΓΚΠΔ.
- Ο ΓΚΠΔ, που θα τεθεί σε ισχύ τον Μάϊο του 2018, δεν θέτει κάποια υποχρεωτική απαίτηση για πιστοποίηση του DPO, ούτε καν ενθαρρύνει σχετική πιστοποίηση σε προαιρετική βάση.
- Μέχρι σήμερα κανένας φορέας στην Ελλάδα δεν έχει διαπιστευθεί για να πιστοποιεί τα επαγγελματικά προσόντα/δεξιότητες ενός DPO. Συνεπώς, οι προτεινόμενες πιστοποιήσεις DPO δεν εμπίπτουν στην κατηγορία των υφιστάμενων επίσημων ελληνικών πιστοποιήσεων.
- Η ύλη των προσφερόμενων εκπαιδευτικών προγραμμάτων μπορεί μεν να χαρακτηριστεί γενικώς ως συναφής με τον ΓΚΠΔ και τη θέση του DPO, η επιλογή της όμως αποτελεί αποκλειστική ευθύνη των φορέων που τα παρέχουν.