

ΠΑΡΑΡΤΗΜΑ ΕΓΓΡΑΦΟΥ ΕΡΓΑΣΙΑΣ WP243 - ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ

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 ΓΚΠΔ.

Ορισμός του υπευθύνου προστασίας δεδομένων (άρθρο 37)

1 Ποιοι οργανισμοί οφείλουν να ορίζουν υπεύθυνο προστασίας δεδομένων; (άρθρο 37 παράγραφος 1)

Ο ΓΚΠΔ θεσπίζει την υποχρέωση ορισμού υπευθύνου προστασίας δεδομένων σε τρεις συγκεκριμένες περιπτώσεις:

- όταν η επεξεργασία διενεργείται από δημόσια αρχή ή δημόσιο φορέα (ανεξάρτητα από το είδος των δεδομένων που υφίστανται επεξεργασία)·
- 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· και
- όταν οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα ή δεδομένων 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, ενδέχεται 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.

Για περισσότερες πληροφορίες, βλ. ενότητα 2.1 των κατευθυντήριων γραμμών.

2 Τι σημαίνει η έννοια «βασικές δραστηριότητες»; (άρθρο 37 παράγραφος 1 στοιχεία β) και γ))

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 ορίζουν 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 συνήθειες δραστηριότητες υποστήριξης ΤΠ. Αυτά είναι αναγκαίες λειτουργίες υποστήριξης της βασικής δραστηριότητας ή του κύριου τομέα δραστηριοποίησης του οργανισμού. Μολονότι οι εν λόγω δραστηριότητες είναι

αναγκαίες ή ουσιώδεις, συνήθως θεωρούνται ως παρεπόμενες λειτουργίες του οργανισμού και όχι ως η βασική του δραστηριότητα.

Για περισσότερες πληροφορίες, βλ. ενότητα 2.1.2 των κατευθυντήριων γραμμών.

3 Τι σημαίνει η έννοια «μεγάλη κλίμακα»; (άρθρο 37 παράγραφος 1 στοιχεία β) και γ))

Ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλη κλίμακα. 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.

Για περισσότερες πληροφορίες, βλ. ενότητα 2.1.3 των κατευθυντήριων γραμμών.

4 Τι σημαίνει η έννοια «τακτική και συστηματική παρακολούθηση»; (άρθρο 37 παράγραφος 1 στοιχείο β))

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.

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.

Παραδείγματα: λειτουργία δικτύου τηλεπικοινωνιών· παροχή υπηρεσιών τηλεπικοινωνιών· επαναστόχευση μηνυμάτων ηλεκτρονικού ταχυδρομείου· διαμόρφωση προφίλ και βαθμολόγηση για σκοπούς εκτίμησης κινδύνου (π.χ. για σκοπούς βαθμολόγησης πιστοληπτικής ικανότητας, προσδιορισμού ασφαλιστρών, 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.

Για περισσότερες πληροφορίες, βλ. ενότητα 2.1.4 των κατευθυντήριων γραμμών.

5 Μπορούν οι οργανισμοί να ορίζουν από κοινού υπεύθυνο προστασίας δεδομένων; Αν ναι, υπό ποιους όρους; (άρθρο 37 παράγραφοι 2 και 3)

Σύμφωνα με τον ΓΚΠΔ, 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 σύμφωνα με τον ΓΚΠΔ. Ο υπεύθυνος προστασίας δεδομένων 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 προσωπική 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.

Για περισσότερες πληροφορίες, βλ. ενότητα 2.3 των κατευθυντήριων γραμμών.

6 Είναι δυνατός ο ορισμός εξωτερικού υπευθύνου προστασίας δεδομένων (άρθρο 37 παράγραφος 6);

Ναι. Σύμφωνα με το άρθρο 37 παράγραφος 6, 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.

Εάν ο υπεύθυνος προστασίας δεδομένων είναι εξωτερικός, τότε ισχύουν όλες οι απαιτήσεις των άρθρων 37 έως 39. Όπως αναφέρεται στις κατευθυντήριες γραμμές, 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 σχετικές απαιτήσεις του ΓΚΠΔ.

Για λόγους νομικής σαφήνειας και καλής οργάνωσης, 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.

Για περισσότερες πληροφορίες, βλ. ενότητες 2.3, 2.4 και 3.5 των κατευθυντήριων γραμμών.

7 Τι επαγγελματικά προσόντα θα πρέπει να έχει ο υπεύθυνος προστασίας δεδομένων (άρθρο 37 παράγραφος 5);

Σύμφωνα με τον ΓΚΠΔ, 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».

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.

Για περισσότερες πληροφορίες, βλ. ενότητα 2.4 των κατευθυντήριων γραμμών.

Θέση του υπευθύνου προστασίας δεδομένων (άρθρο 38)

8 Τι πόροι θα πρέπει να τίθενται στη διάθεση του υπευθύνου προστασίας δεδομένων για την άσκηση των καθηκόντων του;

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».

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 απ' αυτά,
- συνεχή κατάρτιση.

Για περισσότερες πληροφορίες, βλ. ενότητα 3.2 των κατευθυντήριων γραμμών.

9 Ποιες εγγυήσεις απαιτούνται προκειμένου να είναι σε θέση ο υπεύθυνος προστασίας δεδομένων να εκτελεί τα καθήκοντά του με ανεξάρτητο τρόπο (άρθρο 38 παράγραφος 3);

Σύμφωνα με τα αναφερόμενα στην αιτιολογική σκέψη 97, 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.

Για περισσότερες πληροφορίες, βλ. ενότητες 3.3 έως 3.5 των κατευθυντήριων γραμμών.

10 Ποια είναι τα «άλλα καθήκοντα και υποχρεώσεις» του υπευθύνου προστασίας δεδομένων που ενδέχεται να συνεπάγονται σύγκρουση συμφερόντων (άρθρο 38 παράγραφος 6);

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 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.

Για περισσότερες πληροφορίες, βλ. ενότητα 3.5 των κατευθυντήριων γραμμών.

Καθήκοντα του υπευθύνου προστασίας δεδομένων (άρθρο 39)

11 Τι σημαίνει η φράση «παρακολουθεί τη συμμόρφωση» με τον ΓΚΠΔ (άρθρο 39 παράγραφος 1 στοιχείο β);

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, και
- να ενημερώνουν τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, να τους παρέχουν συμβουλές και να εκδίδουν συστάσεις υπ' όψιν τους.

Για περισσότερες πληροφορίες, βλ. ενότητα 4.1 των κατευθυντήριων γραμμών.

12 Ο υπεύθυνος προστασίας δεδομένων φέρει προσωπική ευθύνη για περιπτώσεις μη συμμόρφωσης με τον ΓΚΠΔ;

Όχι, οι υπεύθυνοι προστασίας δεδομένων δεν φέρουν προσωπική ευθύνη για περιπτώσεις 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 τον παρόντα κανονισμό» (άρθρο 24 παράγραφος 1). 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 την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (άρθρο 37 παράγραφος 1 στοιχείο γ) και το αρχείο των δραστηριοτήτων επεξεργασίας (άρθρο 30);

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 τον ΓΚΠΔ.

Για περισσότερες πληροφορίες, βλ. ενότητα 4.2 των κατευθυντήριων γραμμών.

Όσον αφορά το αρχείο των δραστηριοτήτων επεξεργασίας, η τήρησή του 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 το αρχείο των πράξεων επεξεργασίας για τις οποίες είναι υπεύθυνος ο υπεύθυνος επεξεργασίας. 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.

Για περισσότερες πληροφορίες, βλ. ενότητα 4.4 των κατευθυντήριων γραμμών.