ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

17/EL

WP 248 αναθ. 01

Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679.

Εκδόθηκαν στις 4 Απριλίου 2017

Όπως τελικώς αναθεωρήθηκαν και εκδόθηκαν στις 4 Οκτωβρίου 2017

Η παρούσα ομάδα εργασίας συστάθηκε βάσει του άρθρου 29 της οδηγίας 95/46/ΕΚ. Είναι ανεξάρτητο ευρωπαϊκό συμβουλευτικό όργανο για την προστασία 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.

Χρέη γραμματείας της ομάδας ασκεί η Διεύθυνση C (Θεμελιώδη δικαιώματα και ιθαγένεια της Ένωσης) της Ευρωπαϊκής Επιτροπής, Γενική Διεύθυνση Δικαιοσύνης, B-1049 Brussels, Βέλγιο, Γραφείο MO-59 03/075

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

Η ΟΜΑΔΑ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΠΡΟΣΩΠΩΝ ΕΝΑΝΤΙ 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,

ΕΞΕΔΩΣΕ ΤΙΣ ΠΑΡΟΥΣΕΣ ΚΑΤΕΥΘΥΝΤΗΡΙΕΣ ΓΡΑΜΜΕΣ:

Πίνακας περιεχομένων

I. Εισαγωγή

Ο κανονισμός 2016/679[1] (Γενικός Κανονισμός για την Προστασία Δεδομένων – ΓΚΠΔ) θα τεθεί σε εφαρμογή από την 25η Μαΐου 2018. Το άρθρο 35 του ΓΚΠΔ εισάγει την έννοια της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ[2]), όπως και η οδηγία 2016/680[3].

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα[4], με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους. Η ΕΑΠΔ αποτελεί σημαντικό εργαλείο για την πλήρωση της υποχρέωσης λογοδοσίας, καθώς παρέχει συνδρομή στους υπεύθυνους επεξεργασίας όχι μόνον προκειμένου να συμμορφώνονται με τις προδιαγραφές του ΓΚΠΔ, αλλά και για να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για

---

[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).

[2] Ο όρος «εκτίμηση των επιπτώσεων στην ιδιωτική ζωή» είθισται να χρησιμοποιείται σε άλλες περιπτώσεις για να δηλώσει την ίδια έννοια.

[3] Το άρθρο 27 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, επίσης ορίζει ότι η εκτίμηση των επιπτώσεων στην ιδιωτική ζωή είναι αναγκαία όταν «*[ο] τύπος [της] επεξεργασίας [...] είναι πιθανόν να προκαλέσει μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».*

[4] Ο ΓΚΠΔ δεν παρέχει τον επίσημο ορισμό της ΕΑΠΔ, ωστόσο

- το ελάχιστο περιεχόμενό της προσδιορίζεται στο άρθρο 35 παράγραφος 7, ως ακολούθως:
    - «*α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,*
    - *β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,*
    - *γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και*
    - *δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων»·*
- η έννοια και ο ρόλος της αποσαφηνίζονται στην αιτιολογική σκέψη 84, ως ακολούθως: «*Προκειμένου να ενισχυθεί η συμμόρφωση προς τον παρόντα κανονισμό όταν οι πράξεις επεξεργασίας ενδέχεται να έχουν ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας θα πρέπει να ευθύνεται για τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων, ώστε να αξιολογήσει, ιδίως, την προέλευση, τη φύση, την πιθανότητα και τη σοβαρότητα του εν λόγω κινδύνου*».

τη διασφάλιση της συμμόρφωσης προς τον κανονισμό (βλ. επίσης άρθρο 24)[5]. Με άλλα λόγια, **η ΕΑΠΔ είναι μια διαδικασία εμπέδωσης και απόδειξης της συμμόρφωσης.**

Βάσει του ΓΚΠΔ, η μη συμμόρφωση με τις απαιτήσεις ΕΑΠΔ μπορεί να οδηγήσει στην επιβολή προστίμων από την αρμόδια εποπτική αρχή. Η παράλειψη διενέργειας ΕΑΠΔ σε επεξεργασία που υπόκειται σε απαίτηση διενέργειας ΕΑΠΔ (άρθρο 35 παράγραφος 1 και παράγραφοι 3-4), η διενέργεια ΕΑΠΔ με εσφαλμένο τρόπο (άρθρο 35 παράγραφος 2 και παράγραφοι 7-9) ή η μη διαβούλευση με την αρμόδια εποπτική αρχή εφόσον απαιτείται [άρθρο 36 παράγραφος 3 στοιχείο ε)] μπορούν να επιφέρουν διοικητικό πρόστιμο ύψους έως 10 εκατ. ευρώ ή, σε περίπτωση επιχείρησης, έως 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο.

II. Πεδίο εφαρμογής των κατευθυντήριων γραμμών

Οι παρούσες κατευθυντήριες γραμμές έχουν λάβει υπόψη:

- τη δήλωση της ομάδας εργασίας του άρθρου 29 για την προστασία δεδομένων με αριθμό εγγράφου 14/EN WP 218[6]·
- τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για τους υπευθύνους προστασίας δεδομένων, με αριθμό εγγράφου 16/EN WP 243[7]·
- τη γνώμη της ομάδας εργασίας του άρθρου 29 για τον περιορισμό του σκοπού, με αριθμό εγγράφου 13/EN WP 203[8]·
- τα διεθνή πρότυπα[9].

Σύμφωνα με την προσέγγιση βάσει κινδύνου που υιοθετεί ο ΓΚΠΔ, δεν απαιτείται η διενέργεια ΕΑΠΔ σε κάθε πράξη επεξεργασίας. ΕΑΠΔ απαιτείται μόνον όταν η επεξεργασία «*ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*» (άρθρο 35 παράγραφος 1). Για τη διασφάλιση συνεκτικής ερμηνείας των περιπτώσεων στις οποίες απαιτείται η διενέργεια ΕΑΠΔ (άρθρο 35 παράγραφος 3), οι παρούσες κατευθυντήριες γραμμές αποσκοπούν πρωτίστως στο να αποσαφηνίσουν τη συγκεκριμένη έννοια και να θέσουν τα κριτήρια για την

---

[5] Βλέπε επίσης την αιτιολογική σκέψη 84: «*Το αποτέλεσμα της εκτίμησης θα πρέπει να λαμβάνεται υπόψη όταν καθορίζεται ποια μέτρα ενδείκνυται να ληφθούν ώστε να αποδειχθεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύμφωνη με τον παρόντα κανονισμό*».

[6] Δήλωση της ομάδας εργασίας του άρθρου 29 για τον ρόλο μιας προσέγγισης βάσει κινδύνων στα νομικά πλαίσια προστασίας δεδομένων, που εκδόθηκε στις 30 Μαΐου 2014, με αριθμό εγγράφου 14/EN WP 218. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532

[7] Κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για τους υπευθύνους προστασίας δεδομένων, που εκδόθηκαν στις 13 Δεκεμβρίου 2016, με αριθμό εγγράφου 16/EN WP 243. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A

[8] Γνώμη 03/2013 της ομάδας εργασίας του άρθρου 29 για τον περιορισμό του σκοπού, με αριθμό εγγράφου 13/EN WP 203. Εκδόθηκε στις 2 Απριλίου 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[9] Λ.χ. ISO 31000:2009, *Διαχείριση της διακινδύνευσης — Αρχές και οδηγίες,* Διεθνής Οργανισμός Τυποποίησης (ISO)· ISO/IEC 29134 (έργο), *Τεχνολογία Πληροφοριών – Τεχνικές Ασφαλείας – Εκτίμηση επιπτώσεων στην ιδιωτικότητα – Οδηγίες*, Διεθνής Οργανισμός Τυποποίησης (ISO).

κατάρτιση των καταλόγων που θα εγκριθούν από τις Αρχές Προστασίας Δεδομένων (ΑΠΔ) βάσει του άρθρου 35 παράγραφος 4.

Σύμφωνα με το άρθρο 70 παράγραφος 1 στοιχείο ε), το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) θα είναι σε θέση να εκδίδει κατευθυντήριες γραμμές, συστάσεις και βέλτιστες πρακτικές για να ενθαρρύνει τη συνεκτική εφαρμογή του ΓΚΠΔ. Σκοπός του παρόντος εγγράφου είναι να προβλέψει το εν λόγω μελλοντικό έργο του ΕΣΠΔ και, συνεπώς, να αποσαφηνίσει τις συναφείς διατάξεις του ΓΚΠΔ, ώστε να βοηθήσει τους υπεύθυνους επεξεργασίας να συμμορφώνονται με τη νομοθεσία και να παράσχει ασφάλεια δικαίου στους υπεύθυνους επεξεργασίας που απαιτείται να διενεργήσουν ΕΑΠΔ.

Οι παρούσες κατευθυντήριες γραμμές επιδιώκουν επίσης να προαγάγουν την κατάρτιση:

- κοινού καταλόγου της Ευρωπαϊκής Ένωσης με τις πράξεις επεξεργασίας για τις οποίες απαιτείται η διενέργεια ΕΑΠΔ (άρθρο 35 παράγραφος 4)·
- κοινού καταλόγου της ΕΕ με τις πράξεις επεξεργασίας για τις οποίες δεν απαιτείται η διενέργεια ΕΑΠΔ (άρθρο 35 παράγραφος 5)·
- κοινών κριτηρίων για τη μεθοδολογία της διενέργειας ΕΑΠΔ (άρθρο 35 παράγραφος 5)·
- κοινών κριτηρίων για τον καθορισμό των περιπτώσεων διαβούλευσης με την εποπτική αρχή (άρθρο 36 παράγραφος 1)·
- συστάσεων, όπου είναι δυνατό, βάσει της πείρας που έχει αποκτηθεί στα κράτη μέλη της ΕΕ.

III. ΕΑΠΔ: επεξήγηση του κανονισμού

Κατά τις επιταγές του ΓΚΠΔ, οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν ενδεδειγμένα μέτρα για να διασφαλίζουν και να είναι σε θέση να αποδεικνύουν τη συμμόρφωση προς τον ΓΚΠΔ, λαμβάνοντας υπόψη μεταξύ άλλων «τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 24 παράγραφος 1). Η υποχρέωση των υπεύθυνων επεξεργασίας για τη διενέργεια ΕΑΠΔ σε ορισμένες περιστάσεις θα πρέπει να γίνεται αντιληπτή σε σχέση με τη γενική τους υποχρέωση να διαχειρίζονται με ενδεδειγμένο τρόπο τους κινδύνους[10] που ενέχει η επεξεργασία των δεδομένων προσωπικού χαρακτήρα.

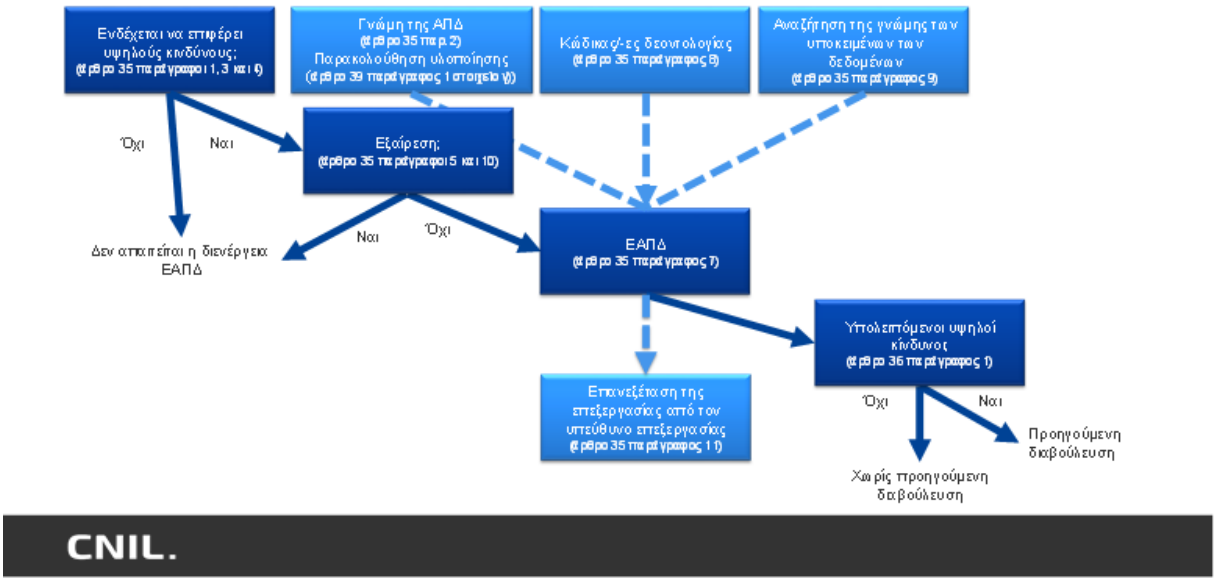
Ως «κίνδυνος» νοείται μια υπόθεση εργασίας που περιγράφει ένα συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης. Από την άλλη, ως «διαχείριση κινδύνου» μπορούν να νοηθούν οι συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού ως προς τον κίνδυνο.

Το άρθρο 35 κάνει λόγο για ενδεχόμενο υψηλό κίνδυνο «για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων». Όπως προκύπτει από τη δήλωση της ομάδας εργασίας του άρθρου 29 για την προστασία των δεδομένων αναφορικά με τον ρόλο μιας προσέγγισης βάσει κινδύνου στο νομικό πλαίσιο της προστασίας δεδομένων, η παραπομπή «στα δικαιώματα και στις ελευθερίες» των υποκειμένων των δεδομένων αφορά πρωτίστως τα δικαιώματα προστασίας των δεδομένων και της ιδιωτικής ζωής, ενδέχεται όμως να συμπεριλαμβάνει και άλλα θεμελιώδη δικαιώματα, όπως την ελευθερία του λόγου, την ελευθερία της σκέψης, την ελευθερία κυκλοφορίας, την απαγόρευση των διακρίσεων, το δικαίωμα στην ελευθερία, την ελευθερία συνειδήσεως και θρησκείας.

Σύμφωνα με την προσέγγιση βάσει κινδύνου που υιοθετεί ο ΓΚΠΔ, δεν απαιτείται η διενέργεια ΕΑΠΔ σε κάθε πράξη επεξεργασίας. Αντιθέτως, η διενέργεια ΕΑΠΔ απαιτείται μόνον όταν ένα είδος επεξεργασίας «ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 35 παράγραφος 1). Αυτό καθαυτό γεγονός της μη πλήρωσης των όρων που ενεργοποιούν την υποχρέωση διενέργειας ΕΑΠΔ δεν μειώνει, εντούτοις, τη γενική υποχρέωση των υπεύθυνων επεξεργασίας να εφαρμόζουν μέτρα για την ενδεδειγμένη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στην πράξη, αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να αξιολογούν συνεχώς τους κινδύνους που απορρέουν από τις δραστηριότητες επεξεργασίας τους, για να εξακριβώνουν πότε ένα είδος επεξεργασίας «ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».

[10] Πρέπει να επισημανθεί ότι για τη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, απαιτείται η εξακρίβωση, ανάλυση, εκτίμηση, αξιολόγηση, αντιμετώπιση (λ.χ. μετριασμός...) των κινδύνων και η τακτική τους επανεξέταση. Οι υπεύθυνοι επεξεργασίας δεν μπορούν να απεκδύονται την αρμοδιότητά τους μέσω της κάλυψης των κινδύνων με ασφαλιστικές συμβάσεις.

Το ακόλουθο γράφημα απεικονίζει τις βασικές αρχές που διέπουν την ΕΑΠΔ κατά τον ΓΚΠΔ:



CNIL.

A. Τι αφορά η ΕΑΠΔ; Μία επιμέρους πράξη επεξεργασίας ή ένα σύνολο παρόμοιων πράξεων επεξεργασίας.

Μια ΕΑΠΔ μπορεί να αφορά μία επιμέρους πράξη επεξεργασίας δεδομένων. Ωστόσο, το άρθρο 35 παράγραφος 1 ορίζει ότι «*σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους*». Με την αιτιολογική σκέψη 92 προστίθεται ότι «*Υπάρχουν περιπτώσεις στις οποίες ενδέχεται να είναι λογικό και οικονομικό το αντικείμενο μιας εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων να υπερβαίνει ένα μεμονωμένο σχέδιο, για παράδειγμα εάν δημόσιες αρχές ή φορείς σκοπεύουν να εγκαθιδρύσουν μια κοινή εφαρμογή ή πλατφόρμα επεξεργασίας ή εάν περισσότεροι υπεύθυνοι επεξεργασίας σχεδιάζουν να θεσπίσουν μια κοινή εφαρμογή ή ένα περιβάλλον επεξεργασίας σε ένα βιομηχανικό τομέα ή κλάδο ή για μια ευρέως χρησιμοποιούμενη οριζόντια δραστηριότητα*».

Μία επιμέρους ΕΑΠΔ θα μπορούσε να χρησιμοποιηθεί για την αξιολόγηση περισσότερων πράξεων επεξεργασίας που είναι παρόμοιες ως προς τη φύση, το πεδίο εφαρμογής, το πλαίσιο, τον σκοπό και τους κινδύνους. Πράγματι, σκοπός της ΕΑΠΔ είναι η συστηματική μελέτη νέων καταστάσεων που θα μπορούσαν να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, και δεν απαιτείται η διενέργεια ΕΑΠΔ σε περιπτώσεις που έχουν ήδη εξεταστεί (δηλαδή, πράξεις επεξεργασίας που έχουν υλοποιηθεί σε συγκεκριμένο πλαίσιο και για συγκεκριμένο σκοπό). Κάτι τέτοιο θα μπορούσε να ισχύει σε περιπτώσεις όπου χρησιμοποιούνται παρόμοιες τεχνολογίες για τη συλλογή ομοειδών δεδομένων για τον ίδιο σκοπό. Για παράδειγμα, ένα σύνολο αρχών της τοπικής αυτοδιοίκησης που εγκαθιστούν παρόμοια συστήματα κλειστού κυκλώματος τηλεόρασης (CCTV) θα μπορούσαν να διενεργήσουν μία μόνο ΕΑΠΔ που να καλύπτει την επεξεργασία από τους εν λόγω ξεχωριστούς υπεύθυνους επεξεργασίας, ή ένας σιδηροδρομικός φορέας (ένας μόνο υπεύθυνος επεξεργασίας) θα μπορούσε να καλύπτει τη βιντεοεπιτήρηση σε όλους τους σιδηροδρομικούς σταθμούς της αρμοδιότητάς του με μία μόνο ΕΑΠΔ. Το ίδιο μπορεί επίσης να ισχύει σε παρόμοιες πράξεις επεξεργασίας που τελούνται από διάφορους υπεύθυνους επεξεργασίας. Στις περιπτώσεις αυτές, θα πρέπει να διαμοιράζεται ή να καθίσταται δημοσίως προσβάσιμη μια

πρότυπη ΕΑΠΔ, ενώ πρέπει να υλοποιούνται τα μέτρα που περιγράφονται στην ΕΑΠΔ και να παρέχεται αιτιολόγηση για τη διενέργεια μίας μόνο ΕΑΠΔ.

Σε πράξη επεξεργασίας στην οποία συμπράττουν από κοινού υπεύθυνοι επεξεργασίας, πρέπει να προσδιορίζονται επακριβώς οι υποχρεώσεις που αντιστοιχούν στον καθένα. Στην ΕΑΠΔ τους θα πρέπει να ορίζεται το μέρος που είναι αρμόδιο για τα διάφορα μέτρα που έχουν σχεδιαστεί για την αντιμετώπιση των κινδύνων και τη διαφύλαξη των δικαιωμάτων και των ελευθεριών των υποκειμένων των δεδομένων. Κάθε υπεύθυνος επεξεργασίας θα πρέπει να διατυπώνει τις ανάγκες του και να ανταλλάσσει χρήσιμες πληροφορίες χωρίς να θέτει σε κίνδυνο απόρρητες πληροφορίες (π.χ.: προστασία εμπορικού απορρήτου, διανοητικής ιδιοκτησίας, εμπιστευτικών επιχειρηματικών πληροφοριών) ούτε να γνωστοποιεί τρωτά σημεία.

Μια ΕΑΠΔ μπορεί επίσης να χρησιμεύσει στην εκτίμηση του αντικτύπου ενός τεχνολογικού προϊόντος σχετικά με την προστασία των δεδομένων, για παράδειγμα ενός στοιχείου υλισμικού ή λογισμικού, όταν αυτό ενδέχεται να χρησιμοποιηθεί από διαφορετικούς υπεύθυνους επεξεργασίας για την υλοποίηση διαφορετικών πράξεων επεξεργασίας. Εννοείται πως ο υπεύθυνος επεξεργασίας που κάνει χρήση του προϊόντος παραμένει υποχρεωμένος να διενεργήσει τη δική του ΕΑΠΔ ως προς τη συγκεκριμένη εφαρμογή, ωστόσο, εάν ενδείκνυται, αυτή μπορεί να τεκμηριωθεί με χρήση της ΕΑΠΔ που έχει καταρτίσει ο πάροχος του προϊόντος. Ενδεικτικό παράδειγμα θα μπορούσε να είναι η σχέση μεταξύ κατασκευαστών ευφυών μετρητών και υπηρεσιών κοινής ωφελείας. Κάθε πάροχος προϊόντος ή εκτελών την επεξεργασία θα πρέπει να ανταλλάσσει χρήσιμες πληροφορίες χωρίς να θέτει σε κίνδυνο το απόρρητο ή να επιφέρει κινδύνους ασφάλειας γνωστοποιώντας τρωτά σημεία.

Β. Ποιες πράξεις επεξεργασίας υπόκεινται σε απαίτηση διενέργειας ΕΑΠΔ; Εκτός από εξαιρέσεις, κάθε πράξη επεξεργασίας που «*ενδέχεται να επιφέρει υψηλό κίνδυνο*».

Η παρούσα ενότητα περιγράφει τις περιπτώσεις που είναι υποχρεωτική η διενέργεια ΕΑΠΔ και τις περιπτώσεις που δεν είναι αναγκαία η διενέργεια ΕΑΠΔ.

Εφόσον η πράξη επεξεργασίας δεν εμπίπτει σε εξαίρεση (ΙΙΙ.Β.α), η διενέργεια ΕΑΠΔ απαιτείται όποτε μια πράξη επεξεργασίας «*ενδέχεται να επιφέρει υψηλό κίνδυνο*» (ΙΙΙ.Β.β).

α) Πότε είναι υποχρεωτική η διενέργεια ΕΑΠΔ; Όταν η επεξεργασία «*ενδέχεται να επιφέρει υψηλό κίνδυνο*».

Ο ΓΚΠΔ δεν προϋποθέτει τη διενέργεια ΕΑΠΔ για κάθε πράξη επεξεργασίας η οποία ενδέχεται να συνεπάγεται κινδύνους για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η διενέργεια ΕΑΠΔ είναι υποχρεωτική μόνο όταν η επεξεργασία «*ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*» (άρθρο 35 παράγραφος 1, το οποίο επεξηγείται από το άρθρο 35 παράγραφος 3 και συμπληρώνεται από το άρθρο 35 παράγραφος 4). Τούτο ισχύει ιδίως σε περίπτωση που εισάγεται μια νέα τεχνολογία επεξεργασίας δεδομένων[11].

Οσάκις δεν είναι σαφές κατά πόσον απαιτείται η διενέργεια ΕΑΠΔ, η ομάδα εργασίας του άρθρου 29 συνιστά να διενεργείται ΕΑΠΔ, καθώς σε κάθε περίπτωση αποτελεί χρήσιμο εργαλείο για τους υπεύθυνους επεξεργασίας προκειμένου να συμμορφώνονται με τη νομοθεσία για την προστασία των δεδομένων.

[11] Βλέπε τις αιτιολογικές σκέψεις 89, 91 και το άρθρο 35 παράγραφοι 1 και 3 για περαιτέρω παραδείγματα.

Ακόμη και εάν υπό άλλες συνθήκες θα ήταν αναγκαία η διενέργεια ΕΑΠΔ, το άρθρο 35 παράγραφος 3 παραθέτει ορισμένες ενδεικτικές περιπτώσεις που μια πράξη επεξεργασίας «*ενδέχεται να επιφέρει υψηλό κίνδυνο*»:

- «*α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο*[12],»
- *β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10*[13]*, ή*
- *γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα*».

Όπως υποδεικνύει ο όρος «*ιδίως*» στην εναρκτήρια πρόταση του άρθρου 35 παράγραφος 3 του ΓΚΠΔ, ο κατάλογος αυτός είναι ενδεικτικός. Ενδέχεται να υπάρχουν πράξεις επεξεργασίας «υψηλού κινδύνου» που δεν περιλαμβάνονται στον εν λόγω κατάλογο, όμως ενέχουν ανάλογα υψηλούς κινδύνους. Οι εν λόγω πράξεις επεξεργασίας θα πρέπει ομοίως να υπόκεινται σε ΕΑΠΔ. Για τον λόγο αυτό, τα κριτήρια που παρατίθενται στη συνέχεια ενίοτε δεν αρκούνται σε μια απλή εξήγηση του τι θα έπρεπε να εννοείται με τα τρία παραδείγματα του άρθρου 35 παράγραφος 3 του ΓΚΠΔ.

Για την παροχή πιο συνεκτικού συνόλου πράξεων επεξεργασίας που απαιτούν τη διενέργεια ΕΑΠΔ λόγω του υψηλού κινδύνου που ενέχουν, λαμβανομένων υπόψη των ειδικών στοιχείων του άρθρου 35 παράγραφος 1 και του άρθρου 35 παράγραφος 3 στοιχεία α) έως γ), του καταλόγου που πρέπει να εγκριθεί σε εθνικό επίπεδο σύμφωνα με το άρθρο 35 παράγραφος 4 και τις αιτιολογικές σκέψεις 71, 75 και 91, καθώς και των λοιπών παραπομπών του ΓΚΠΔ σε πράξη επεξεργασίας που *«ενδέχεται να επιφέρει υψηλό κίνδυνο»*[14], θα πρέπει να ληφθούν υπόψη τα ακόλουθα εννέα κριτήρια.

1. Αξιολόγηση ή βαθμολόγηση, περιλαμβανομένης της κατάρτισης προφίλ και προβλέψεων, ιδίως *«πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων»* (αιτιολογικές σκέψεις 71 και 91). Σχετικό παράδειγμα θα μπορούσε να είναι η περίπτωση που ένα χρηματοπιστωτικό ίδρυμα ελέγχει τους πελάτες του σε σχέση με μια βάση δεδομένων πιστοληπτικής ικανότητας ή μια βάση δεδομένων για την καταπολέμηση της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και της χρηματοδότησης της τρομοκρατίας (ΚΞΧ/ΧΤ) ή μια βάση δεδομένων για εγκλήματα απάτης, ή η περίπτωση που μια εταιρεία βιοτεχνολογίας παρέχει απευθείας στους καταναλωτές γενετικές δοκιμές για να εκτιμήσει και να προβλέψει τους κινδύνους νόσου/υγείας ή η περίπτωση που μια εταιρεία δημιουργεί συμπεριφορικά προφίλ ή προφίλ εμπορικής προώθησης βάσει της χρήσης ή πλοήγησης στον δικτυακό της τόπο.

---

[12] Βλέπε αιτιολογική σκέψη 71: «*ιδίως την ανάλυση ή πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ*».

[13] Βλέπε αιτιολογική σκέψη 75: «*όταν υπόκεινται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα και γίνεται επεξεργασία γενετικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας*».

[14] Βλέπε λ.χ. αιτιολογικές σκέψεις 75, 76, 92, 116.

2. Λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο: επεξεργασία που αποσκοπεί στη λήψη αποφάσεων που αφορούν υποκείμενα δεδομένων και παράγουν «*έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο*» ή που «*ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο*» [άρθρο 35 παράγραφος 3 στοιχείο α)]. Για παράδειγμα, η επεξεργασία μπορεί να οδηγήσει σε αποκλεισμό ή σε διακρίσεις σε βάρος των φυσικών προσώπων. Επεξεργασία με μικρό ή μηδαμινό αντίκτυπο στα φυσικά πρόσωπα δεν πληροί τους όρους του συγκεκριμένου κριτηρίου. Περαιτέρω επεξηγήσεις των εν λόγω εννοιών θα περιλαμβάνονται στις επερχόμενες κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για την κατάρτιση προφίλ.
3. Συστηματική παρακολούθηση: επεξεργασία για την παρατήρηση, την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, περιλαμβανομένων των δεδομένων που συλλέγονται μέσω δικτύων ή «*συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου*» [άρθρο 35 παράγραφος 3 στοιχείο γ)][15]. Αυτό το είδος παρακολούθησης αποτελεί κριτήριο, διότι τα δεδομένα προσωπικού χαρακτήρα μπορεί να συλλέγονται σε περιστάσεις κατά τις οποίες τα υποκείμενα των δεδομένων ενδέχεται να μην έχουν επίγνωση του ποιος συλλέγει τα δεδομένα τους και του πώς θα χρησιμοποιηθούν. Επιπρόσθετα, τα φυσικά πρόσωπα ενδεχομένως να είναι αδύνατο να αποφύγουν την εν λόγω επεξεργασία των δεδομένων τους σε δημόσιο/-ους (ή δημοσίως προσβάσιμο/-ους) χώρο/-ους.
4. Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα: σε αυτά περιλαμβάνονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 (για παράδειγμα, πληροφορίες για τα πολιτικά φρονήματα φυσικών προσώπων), καθώς και δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες ή αδικήματα, όπως ορίζονται στο άρθρο 10. Σχετικό παράδειγμα θα μπορούσαν να είναι τα ιατρικά αρχεία ασθενών που τηρεί ένα γενικό νοσοκομείο ή τα προσωπικά στοιχεία παραβατών που τηρεί ένας πράκτορας ιδιωτικών ερευνών. Εκτός από τις εν λόγω διατάξεις του ΓΚΠΔ, ορισμένες κατηγορίες δεδομένων μπορεί να θεωρηθεί ότι αυξάνουν τον δυνητικό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Τα εν λόγω δεδομένα προσωπικού χαρακτήρα θεωρούνται ευαίσθητα (όπως κοινώς νοείται ο εν λόγω όρος), επειδή συνδέονται με οικιακές δραστηριότητες και δραστηριότητες του ιδιωτικού βίου (όπως, οι ηλεκτρονικές επικοινωνίες, των οποίων θα πρέπει να διαφυλάττεται η εμπιστευτικότητα) ή επειδή επηρεάζουν την άσκηση ενός θεμελιώδους δικαιώματος (όπως δεδομένα τοποθεσίας με τη συλλογή των οποίων διαμφισβητείται η ελευθερία κυκλοφορίας) ή επειδή η παραβίασή τους σαφώς επηρεάζει σημαντικά την καθημερινή ζωή του υποκειμένου των δεδομένων (όπως τα οικονομικά δεδομένα που θα μπορούσαν να χρησιμοποιηθούν σε τέλεση απάτης πληρωμών). Εν προκειμένω, σημασία μπορεί να έχει και το κατά πόσον τα δεδομένα έχουν δημοσιοποιηθεί από το υποκείμενο των δεδομένων ή από τρίτα πρόσωπα. Ο δημόσιος χαρακτήρας των δεδομένων προσωπικού χαρακτήρα μπορεί να εξετάζεται ως παράμετρος για

[15] Η ομάδα εργασίας του άρθρου 29 αποδίδει στον όρο «*συστηματική*» μία ή περισσότερες από τις ακόλουθες έννοιες (βλέπε τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για τους υπευθύνους προστασίας δεδομένων, με αριθμό εγγράφου 16/EN WP 243):

- λαμβάνει χώρα σύμφωνα με ένα σύστημα·
- είναι προκαθορισμένη, οργανωμένη ή μεθοδική·
- υλοποιείται στο πλαίσιο γενικού σχεδίου συλλογής δεδομένων·
- διενεργείται στο πλαίσιο στρατηγικής.

Η ομάδα εργασίας του άρθρου 29 ερμηνεύει τον όρο «*δημοσίως προσβάσιμος χώρος*» ως κάθε χώρο που είναι ανοικτός στο κοινό, όπως μια πλατεία, ένα εμπορικό κέντρο, ένας δρόμος, μια αγορά, ένας σιδηροδρομικός σταθμός ή μια δημόσια βιβλιοθήκη.

να εκτιμηθεί αν τα δεδομένα αναμενόταν να χρησιμοποιηθούν περαιτέρω για συγκεκριμένους σκοπούς. Στο παρόν κριτήριο μπορεί επίσης να περιλαμβάνονται δεδομένα όπως προσωπικά έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) που προσφέρει δυνατότητες τήρησης σημειώσεων, και πολύ προσωπικές πληροφορίες που περιλαμβάνονται σε εφαρμογές καταγραφής βίου («life-logging»).

5. Δεδομένα μεγάλης κλίμακας επεξεργασίας: ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλης κλίμακας επεξεργασία, ωστόσο η αιτιολογική σκέψη 91 παρέχει ορισμένες κατευθύνσεις. Σε κάθε περίπτωση, η ομάδα εργασίας του άρθρου 29 συνιστά να λαμβάνονται συγκεκριμένα υπόψη οι ακόλουθες παράμετροι κατά τον προσδιορισμό του κατά πόσον η επεξεργασία τελείται σε μεγάλη κλίμακα[16]:

   α. ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού·

   β. ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία·

   γ. η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων·

   δ. το γεωγραφικό εύρος της δραστηριότητας επεξεργασίας.

6. Η αντιστοίχιση ή ο συνδυασμός συνόλων δεδομένων που απορρέουν, για παράδειγμα, από δύο ή περισσότερες πράξεις επεξεργασίας δεδομένων που υλοποιούνται για διαφορετικούς σκοπούς και/ή από διαφορετικούς υπεύθυνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων[17].
7. Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων (αιτιολογική σκέψη 75): η επεξεργασία του εν λόγω τύπου δεδομένων αποτελεί κριτήριο λόγω της αυξημένα άνισης σχέσης ισχύος μεταξύ των υποκειμένων των δεδομένων και του υπεύθυνου επεξεργασίας, με την έννοια ότι τα φυσικά πρόσωπα ενδέχεται να μην είναι σε θέση να συναινέσουν ή να εναντιωθούν με ευκολία στην επεξεργασία των δεδομένων τους ή να ασκήσουν τα δικαιώματά τους. Στα ευάλωτα υποκείμενα δεδομένων ενδέχεται να περιλαμβάνονται παιδιά (τα οποία μπορεί να θεωρηθεί ότι δεν είναι σε θέση να εναντιωθούν ή να συναινέσουν μετά λόγου γνώσης ή συνειδητά στην επεξεργασία των δεδομένων τους), εργαζόμενοι, πιο ευάλωτα τμήματα του πληθυσμού που χρήζουν ειδικής προστασίας (ψυχικά νοσούντες, αιτούντες άσυλο ή ηλικιωμένοι, ασθενείς κ.ο.κ.), και σε κάθε περίπτωση που εξακριβώνεται άνιση σχέση μεταξύ της θέσης του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας.
8. Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης κ.ο.κ. Ο ΓΚΠΔ καθιστά σαφές (άρθρο 35 παράγραφος 1 και αιτιολογικές σκέψεις 89 και 91) ότι η χρήση νέων τεχνολογιών, που ορίζονται «*σύμφωνα με τα υφιστάμενα επίπεδα τεχνολογικής γνώσης*» (αιτιολογική σκέψη 91), μπορεί να

[16] Βλέπε τις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για τους υπευθύνους προστασίας δεδομένων, με αριθμό εγγράφου 16/EN WP 243.

[17] Βλέπε την εξήγηση στη γνώμη της ομάδας εργασίας του άρθρου 29 για τον περιορισμό του σκοπού, με αριθμό εγγράφου 13/EN WP 203, σ. 24.

καταστήσει αναγκαία τη διενέργεια ΕΑΠΔ. Και τούτο διότι η χρήση μιας τέτοιας τεχνολογίας μπορεί να περιλαμβάνει νέες μορφές συλλογής και χρήσης δεδομένων, πιθανώς με υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Πράγματι, οι προσωπικές και κοινωνικές επιπτώσεις από τη χρήση μιας νέας τεχνολογίας ενδέχεται να είναι άγνωστες. Η διενέργεια ΕΑΠΔ θα βοηθήσει τον υπεύθυνο επεξεργασίας να κατανοήσει και να αντιμετωπίσει τους εν λόγω κινδύνους. Για παράδειγμα, συγκεκριμένες εφαρμογές του «διαδικτύου των πραγμάτων» θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην καθημερινή ζωή και την ιδιωτική ζωή των φυσικών προσώπων· και, ως εκ τούτου, απαιτείται η διενέργεια σχετικής ΕΑΠΔ.

9. Όταν η επεξεργασία αυτή καθαυτήν *«εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση»* (άρθρο 22 και αιτιολογική σκέψη 91). Εδώ περιλαμβάνονται πράξεις επεξεργασίας που έχουν σκοπό να επιτρέψουν, να τροποποιήσουν ή να αρνηθούν στα υποκείμενα των δεδομένων την πρόσβαση σε υπηρεσία ή τη σύναψη σύμβασης. Σχετικό παράδειγμα είναι η περίπτωση που μια τράπεζα ελέγχει τους πελάτες της χρησιμοποιώντας μια βάση δεδομένων πιστοληπτικής ικανότητας για να αποφασίσει αν θα τους χορηγήσει δάνειο ή όχι.

Στις περισσότερες περιπτώσεις, ο υπεύθυνος επεξεργασίας μπορεί να θεωρεί ότι σε μια επεξεργασία που πληροί δύο κριτήρια θα απαιτούνταν η διενέργεια ΕΑΠΔ. Εν γένει, η ομάδα εργασίας του άρθρου 29 θεωρεί ότι όσο περισσότερα κριτήρια πληρούνται με την επεξεργασία, τόσο πιθανότερο είναι να τίθενται σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων και, ως εκ τούτου, να απαιτείται η διενέργεια ΕΑΠΔ, ανεξάρτητα από τα προβλεπόμενα μέτρα του υπεύθυνου επεξεργασίας.

Ωστόσο, σε ορισμένες περιπτώσεις, **ο υπεύθυνος επεξεργασίας μπορεί να θεωρήσει ότι σε επεξεργασία στην οποία πληρούται μόνο ένα από τα εν λόγω κριτήρια απαιτείται η διενέργεια ΕΑΠΔ**.

Τα ακόλουθα παραδείγματα δείχνουν τον τρόπο με τον οποίο θα πρέπει να χρησιμοποιούνται τα κριτήρια προκειμένου να εκτιμηθεί κατά πόσον για μια πράξη επεξεργασίας απαιτείται η διενέργεια ΕΑΠΔ:

Παραδείγματα πράξεων επεξεργασίας	**Πιθανά συναφή κριτήρια**	**Ενδέχεται να απαιτείται διενέργεια ΕΑΠΔ;**
Νοσοκομείο που επεξεργάζεται τα γενετικά δεδομένα και τα δεδομένα υγείας των ασθενών του (πληροφοριακό σύστημα του νοσοκομείου).	- Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων. - Δεδομένα μεγάλης κλίμακας επεξεργασίας.	Ναι
Χρήση συστήματος βιντεοσκόπησης για την παρακολούθηση της οδικής συμπεριφοράς σε αυτοκινητοδρόμους. Ο υπεύθυνος επεξεργασίας σκοπεύει να χρησιμοποιεί έξυπνο σύστημα	- Συστηματική παρακολούθηση. - Καινοτόμος χρήση ή εφαρμογή τεχνολογικών ή οργανωτικών λύσεων.	

Παραδείγματα πράξεων επεξεργασίας	Πιθανά συναφή κριτήρια	Ενδέχεται να απαιτείται διενέργεια ΕΑΠΔ;
ανάλυσης βίντεο για να απομονώνει τα οχήματα και να αναγνωρίζει αυτόματα τις πινακίδες τους.		
Εταιρεία που παρακολουθεί συστηματικά τις δραστηριότητες των εργαζομένων της, καθώς και τον σταθμό εργασίας τους, τη δραστηριότητά τους στο διαδίκτυο κ.ο.κ.	- Συστηματική παρακολούθηση. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.	
Συλλογή δημόσιων δεδομένων στα μέσα κοινωνικής δικτύωσης για την κατάρτιση προφίλ.	- Αξιολόγηση ή βαθμολόγηση. - Δεδομένα μεγάλης κλίμακας επεξεργασίας. - Αντιστοίχιση ή συνδυασμός συνόλων δεδομένων. - Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα:	
Οργανισμός που δημιουργεί εθνική βάση δεδομένων αξιολόγησης της πιστοληπτικής ικανότητας ή υποθέσεων απάτης.	- Αξιολόγηση ή βαθμολόγηση. - Λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο. - Τα υποκείμενα των δεδομένων εμποδίζονται να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση. - Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα:	
Αποθήκευση για λόγους αρχείου ψευδωνυμοποιημένων ευαίσθητων δεδομένων προσωπικού χαρακτήρα που αφορούν ευάλωτα υποκείμενα δεδομένων σε ερευνητικά έργα ή κλινικές δοκιμές.	- Ευαίσθητα δεδομένα. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων. - Τα υποκείμενα των δεδομένων εμποδίζονται να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση.	
Μια επεξεργασία «δεδομένων προσωπικού χαρακτήρα ασθενών ή πελατών ιδιώτη ιατρού, άλλου επαγγελματία του τομέα της υγείας ή δικηγόρου» (αιτιολογική σκέψη 91).	- Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.	Όχι
Ηλεκτρονικό περιοδικό που χρησιμοποιεί κατάλογο ηλεκτρονικών διευθύνσεων για να αποστέλλει γενικές ημερήσιες συνόψεις στους συνδρομητές του.	- Δεδομένα μεγάλης κλίμακας επεξεργασίας.	
Δικτυακός τόπος ηλεκτρονικού εμπορίου που διαφημίζει ανταλλακτικά αυτοκινήτων-αντικών και περιλαμβάνει περιορισμένη κατάρτιση προφίλ	- Αξιολόγηση ή βαθμολόγηση.	

Παραδείγματα πράξεων επεξεργασίας	Πιθανά συναφή κριτήρια	Ενδέχεται να απαιτείται διενέργεια ΕΑΠΔ;
βάσει των αντικειμένων που έχουν προβληθεί ή αγοραστεί στον δικτυακό του τόπο.		

Αντιθέτως, μια πράξη επεξεργασίας που ενδεχομένως αντιστοιχεί στις ανωτέρω αναφερόμενες περιπτώσεις κατά τον υπεύθυνο επεξεργασίας μπορεί να θεωρείται ότι εξακολουθεί να μην «ενδέχεται να επιφέρει υψηλό κίνδυνο». Στις εν λόγω περιπτώσεις, ο υπεύθυνος επεξεργασίας θα πρέπει να δικαιολογεί και να τεκμηριώνει τους λόγους μη διενέργειας ΕΑΠΔ και να περιλαμβάνει/καταγράφει τις απόψεις του υπεύθυνου προστασίας δεδομένων.

Επιπρόσθετα, στο πλαίσιο της αρχής της λογοδοσίας, κάθε υπεύθυνος επεξεργασίας «*τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος*», στο οποίο περιλαμβάνονται μεταξύ άλλων οι σκοποί της επεξεργασίας, περιγραφή των κατηγοριών των δεδομένων και των αποδεκτών των δεδομένων και «*όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που αναφέρονται στο άρθρο 32 παράγραφος 1*» (άρθρο 30 παράγραφος 1) και πρέπει να αξιολογεί αν η επεξεργασία ενδέχεται να επιφέρει υψηλό κίνδυνο, ακόμη και αν τελικά αποφασίσει να μη διενεργήσει ΕΑΠΔ.

Σημείωση: οι εποπτικές αρχές απαιτείται να καταρτίζουν, να δημοσιοποιούν και να ανακοινώνουν στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) κατάλογο με τις πράξεις επεξεργασίας που υπόκεινται στην απαίτηση για τη διενέργεια ΕΑΠΔ (άρθρο 35 παράγραφος 4)[18]. Τα κριτήρια που ορίζονται ανωτέρω μπορούν να συνδράμουν τις εποπτικές αρχές στην κατάρτιση του εν λόγω καταλόγου, με την προσθήκη πιο εξειδικευμένου περιεχομένου εν καιρώ, εφόσον ενδείκνυται. Για παράδειγμα, η επεξεργασία οποιουδήποτε τύπου βιομετρικών δεδομένων ή δεδομένων παιδιών θα μπορούσε επίσης να θεωρηθεί συναφής για την κατάρτιση καταλόγου δυνάμει του άρθρου 35 παράγραφος 4.

β) Σε ποιες περιπτώσεις δεν απαιτείται η διενέργεια ΕΑΠΔ; Όταν η επεξεργασία δεν «*ενδέχεται να επιφέρει υψηλό κίνδυνο*» ή διατίθεται παρόμοια ΕΑΠΔ ή έχει εγκριθεί πριν από τον Μάιο του 2018 ή διαθέτει νομική βάση ή περιλαμβάνεται στον κατάλογο των πράξεων επεξεργασίας για τις οποίες δεν απαιτείται η διενέργεια ΕΑΠΔ.

Η ομάδα εργασίας του άρθρου 29 θεωρεί ότι η ΕΑΠΔ δεν απαιτείται στις ακόλουθες περιπτώσεις:

- **όταν η επεξεργασία δεν «*ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*»** (άρθρο 35 παράγραφος 1)·
- **όταν η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας παρουσιάζουν πολλές ομοιότητες με την επεξεργασία για την οποία έχει διενεργηθεί**

[18] Στο πλαίσιο αυτό, «*η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση*» (άρθρο 35 παράγραφος 6).

ΕΑΠΔ. Στις εν λόγω περιπτώσεις, μπορούν να χρησιμοποιούνται τα αποτελέσματα της ΕΑΠΔ στις παρόμοιες επεξεργασίες (άρθρο 35 παράγραφος 1[19])·

- όταν οι πράξεις επεξεργασίας έχουν ελεγχθεί από εποπτική αρχή πριν από τον Μάιο του 2018 υπό συγκεκριμένους όρους που παραμένουν αμετάβλητοι [20] (βλέπε ΙΙΙ.Γ)·
- **όταν η πράξη επεξεργασίας,** δυνάμει του άρθρου 6 παράγραφος 1 στοιχείο γ) ή ε), **έχει νομική βάση** στο δίκαιο της Ένωσης ή στο δίκαιο κράτους μέλους, όταν το εν λόγω δίκαιο ρυθμίζει τη συγκεκριμένη πράξη επεξεργασίας **και έχει διενεργηθεί ήδη ΕΑΠΔ** στο πλαίσιο της θέσπισης της εν λόγω νομικής βάσης (άρθρο 35 παράγραφος 10)[21], εκτός αν τα κράτη μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω ΕΑΠΔ πριν από τις δραστηριότητες επεξεργασίας·
- **όταν η επεξεργασία περιλαμβάνεται στον προαιρετικό κατάλογο (που καταρτίζεται από την εποπτική αρχή) των πράξεων επεξεργασίας** για τις οποίες δεν απαιτείται η διενέργεια ΕΑΠΔ (άρθρο 35 παράγραφος 5). Ο εν λόγω κατάλογος μπορεί να περιλαμβάνει δραστηριότητες επεξεργασίας που πληρούν τους όρους που έχει θέσει η εν λόγω αρχή, ιδίως μέσω κατευθυντήριων γραμμών, ειδικών αποφάσεων ή εγκρίσεων, κανόνων συμμόρφωσης κ.ο.κ. (π.χ. στη Γαλλία, εγκρίσεις, εξαιρέσεις, απλοποιημένοι κανόνες, δέσμες συμμόρφωσης...). Στις περιπτώσεις αυτές, και με τον όρο της εκ νέου αξιολόγησης από την αρμόδια εποπτική αρχή, δεν απαιτείται η διενέργεια ΕΑΠΔ, παρά μόνον εάν η επεξεργασία εμπίπτει αυστηρά στο πεδίο εφαρμογής της συναφούς διαδικασίας που παρατίθεται στον κατάλογο και παραμένει σε πλήρη συμμόρφωση με όλες τις συναφείς απαιτήσεις του ΓΚΠΔ.

Γ. Τι ισχύει για τις ήδη υφιστάμενες πράξεις επεξεργασίας; Η διενέργεια ΕΑΠΔ απαιτείται σε ορισμένες περιστάσεις.

Η απαίτηση διενέργειας ΕΑΠΔ ισχύει σε υφιστάμενες πράξεις επεξεργασίας που ενδέχεται να επιφέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και στις οποίες έχει επέλθει μεταβολή των κινδύνων, λαμβανομένης υπόψη της φύσης, του πεδίου εφαρμογής, του πλαισίου και των σκοπών της επεξεργασίας.

Δεν απαιτείται ΕΑΠΔ σε πράξεις επεξεργασίας που έχουν ελεγχθεί από εποπτική αρχή ή τον υπεύθυνο υπάλληλο προστασίας δεδομένων, σύμφωνα με το άρθρο 20 της οδηγίας 95/46/ΕΚ, και υλοποιούνται χωρίς καμία μεταβολή από τον προηγούμενο έλεγχο. Πράγματι, «*Οι αποφάσεις της Επιτροπής και οι εγκρίσεις εποπτικών αρχών που εκδόθηκαν βάσει της οδηγίας 95/46/ΕΚ παραμένουν σε ισχύ μέχρι την τροποποίηση, αντικατάσταση ή κατάργησή τους*» (αιτιολογική σκέψη 171).

Εξ αντιδιαστολής, τούτο σημαίνει ότι κάθε επεξεργασία δεδομένων στην οποία έχουν μεταβληθεί οι όροι υλοποίησης (πεδίο εφαρμογής, σκοπός, δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί,

[19] «*Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους*».

[20] «*Οι αποφάσεις της Επιτροπής και οι εγκρίσεις εποπτικών αρχών που εκδόθηκαν βάσει της οδηγίας 95/46/ΕΚ παραμένουν σε ισχύ μέχρι την τροποποίηση, αντικατάσταση ή κατάργησή τους*» (αιτιολογική σκέψη 171).

[21] Όταν διενεργείται ΕΑΠΔ στο στάδιο της επεξεργασίας της νομοθεσίας που παρέχει τη νομική βάση της επεξεργασίας, ενδέχεται να απαιτείται επανεξέταση πριν από την εφαρμογή της, διότι η ψηφισθείσα νομοθεσία ενδέχεται να διαφέρει από τη νομοθετική πρόταση με τρόπο που να επηρεάζει ζητήματα προστασίας των δεδομένων και της ιδιωτικής ζωής. Επιπλέον, μπορεί να μη διατίθενται επαρκή τεχνικά στοιχεία που αφορούν την πραγματική επεξεργασία κατά τον χρόνο θέσπισης της νομοθεσίας, ακόμη και αν αυτή συνοδευόταν από ΕΑΠΔ. Στις εν λόγω περιπτώσεις, ενδέχεται να παραμένει αναγκαία η διενέργεια συγκεκριμένης ΕΑΠΔ πριν από τη διενέργεια των δραστηριοτήτων επεξεργασίας.

ταυτότητα των υπεύθυνων επεξεργασίας ή των αποδεκτών, περίοδος τήρησης των δεδομένων, τεχνικά και οργανωτικά μέτρα κ.ο.κ.) από τον τελευταίο έλεγχο της εποπτικής αρχής ή του υπευθύνου υπαλλήλου προστασίας δεδομένων και ενδέχεται να επιφέρει υψηλό κίνδυνο θα πρέπει να υπόκειται σε διενέργεια ΕΑΠΔ.

Επιπλέον, ΕΑΠΔ θα μπορούσε να απαιτείται σε περίπτωση μεταβολής των κινδύνων που συνεπάγονται οι πράξεις επεξεργασίας[22], για παράδειγμα επειδή χρησιμοποιείται πλέον μια νέα τεχνολογία ή επειδή τα δεδομένα προσωπικού χαρακτήρα χρησιμοποιούνται για διαφορετικό σκοπό. Οι πράξεις επεξεργασίας δεδομένων μπορούν να εξελίσσονται ταχέως και να προκύπτουν νέα τρωτά σημεία. Ως εκ τούτου, θα πρέπει να σημειωθεί ότι η επανεξέταση της ΕΑΠΔ δεν είναι μόνο χρήσιμη για τη συνεχή βελτίωση, αλλά και κρίσιμη για τη μη υπονόμευση του επιπέδου προστασίας δεδομένων σε ένα περιβάλλον που μεταβάλλεται με την πάροδο του χρόνου. Η ΕΑΠΔ μπορεί επίσης να καταστεί αναγκαία επειδή έχει μεταβληθεί το οργανωτικό ή κοινωνικό πλαίσιο της δραστηριότητας επεξεργασίας, για παράδειγμα επειδή τα αποτελέσματα συγκεκριμένων αυτοματοποιημένων αποφάσεων έχουν γίνει πιο σημαντικά ή νέες κατηγορίες υποκειμένων δεδομένων έχουν γίνει ευάλωτες σε διακρίσεις. Καθένα από τα παραπάνω παραδείγματα θα μπορούσε να αποτελεί στοιχείο που οδηγεί σε μεταβολή του κινδύνου που συνεπάγεται η οικεία δραστηριότητα επεξεργασίας.

Αντιστρόφως, συγκεκριμένες μεταβολές θα μπορούσαν επίσης να μειώνουν τον κίνδυνο. Για παράδειγμα, μια πράξη επεξεργασίας θα μπορούσε να εξελιχθεί με τρόπο που οι αποφάσεις να πάψουν να είναι αυτοματοποιημένες ή αν μια δραστηριότητα παρακολούθησης παύει πλέον να είναι συστηματική. Στην περίπτωση αυτή, η επανεξέταση της ανάλυσης κινδύνου που έχει διενεργηθεί μπορεί να αποδείξει ότι πλέον δεν απαιτείται η διενέργεια ΕΑΠΔ.

Ως ορθή πρακτική, **μια ΕΑΠΔ θα πρέπει να επανεξετάζεται συνεχώς και να επαναξιολογείται τακτικά**. Ως εκ τούτου, ακόμη και αν μια ΕΑΠΔ δεν είναι αναγκαία στις 25 Μαΐου 2018, ο υπεύθυνος επεξεργασίας θα υποχρεωθεί, στον ενδεδειγμένο χρόνο, να διενεργήσει μια τέτοια εκτίμηση στο πλαίσιο των γενικών υποχρεώσεων λογοδοσίας που υπέχει.

Δ. Πώς πρέπει να διενεργείται η ΕΑΠΔ;

α) Πότε θα πρέπει να διενεργείται η ΕΑΠΔ; Πριν από την επεξεργασία.

Η ΕΑΠΔ θα πρέπει να διενεργείται «*πριν από την επεξεργασία*» (άρθρο 35 παράγραφος 1 και άρθρο 35 παράγραφος 10, αιτιολογικές σκέψεις 90 και 93)[23]. Τούτο συνάδει με τις αρχές της εξ ορισμού και της εκ σχεδιασμού προστασίας των δεδομένων (άρθρο 25 και αιτιολογική σκέψη 78). Η ΕΑΠΔ θα πρέπει να αντιμετωπίζεται ως εργαλείο που βοηθά στη λήψη αποφάσεων σε σχέση με την επεξεργασία.

Η ΕΑΠΔ θα πρέπει να ξεκινά το νωρίτερο δυνατό στον σχεδιασμό της πράξης επεξεργασίας, ακόμη και αν ορισμένες πράξεις επεξεργασίας παραμένουν άγνωστες. Η επικαιροποίηση της ΕΑΠΔ καθ' όλον τον κύκλο ζωής του έργου θα διασφαλίζει ότι λαμβάνονται υπόψη η προστασία δεδομένων και η

[22] Ως προς το πλαίσιο, τα δεδομένα που έχουν συλλεχθεί, τους σκοπούς, τη λειτουργία, τα δεδομένα προσωπικού χαρακτήρα που τίθενται σε επεξεργασία, τους αποδέκτες, τους συνδυασμούς δεδομένων, τους κινδύνους (τα υποστηρικτικά περιουσιακά στοιχεία, τις πηγές των κινδύνων, τις πιθανές επιπτώσεις, τους επαπειλούμενους κινδύνους κ.ο.κ.), τα μέτρα ασφαλείας και τις διεθνείς διαβιβάσεις.

[23] Εκτός εάν υφίσταται ήδη επεξεργασία που έχει ελεγχθεί προηγουμένως από την Εποπτική Αρχή, οπότε η ΕΑΠΔ θα πρέπει να διενεργηθεί πριν από την επέλευση σημαντικών μεταβολών.

ιδιωτική ζωή και θα ενθαρρύνει τη δημιουργία λύσεων που προάγουν τη συμμόρφωση. Μπορεί επίσης να απαιτείται η επανάληψη επιμέρους βημάτων της αξιολόγησης καθώς προχωρά η διαδικασία ανάπτυξης, διότι η επιλογή συγκεκριμένων τεχνικών ή οργανωτικών μέτρων μπορεί να επηρεάσει τη σοβαρότητα ή την πιθανότητα επέλευσης των κινδύνων που ενέχει η επεξεργασία.

Το γεγονός ότι η ΕΑΠΔ ενδέχεται να χρειαστεί επικαιροποίηση μετά την έναρξη της επεξεργασίας δεν αποτελεί βάσιμη αιτία για την αναβολή ή την παράλειψη διενέργειας ΕΑΠΔ. Η ΕΑΠΔ είναι μια διαρκής διαδικασία, ειδικά όταν η πράξη επεξεργασίας είναι δυναμική και υπόκειται σε διαρκείς μεταβολές. **Η ΕΑΠΔ αποτελεί διαρκή διαδικασία και όχι πράξη που διενεργείται άπαξ.**

β) Ποιος οφείλει να διενεργεί την ΕΑΠΔ; Ο υπεύθυνος επεξεργασίας, με τον ΥΠΔ και τους εκτελούντες την επεξεργασία.

Ο υπεύθυνος επεξεργασίας είναι αρμόδιος για τη διασφάλιση της διενέργειας της ΕΑΠΔ (άρθρο 35 παράγραφος 2). Η διενέργεια της ΕΑΠΔ μπορεί να πραγματοποιηθεί από άλλο πρόσωπο, εντός ή εκτός του οργανισμού, ωστόσο ο υπεύθυνος επεξεργασίας παραμένει ο τελικός υπεύθυνος για το εν λόγω καθήκον.

Ο υπεύθυνος επεξεργασίας πρέπει επίσης να ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων (ΥΠΔ), εφόσον έχει οριστεί (άρθρο 35 παράγραφος 2) και η γνώμη αυτή, καθώς και οι αποφάσεις του υπεύθυνου επεξεργασίας, θα πρέπει να τεκμηριώνονται στην ΕΑΠΔ. Ο ΥΠΔ θα πρέπει επίσης να παρακολουθεί την υλοποίηση της ΕΑΠΔ [άρθρο 39 παράγραφος 1 στοιχείο γ)]. Περαιτέρω καθοδήγηση παρέχεται στις κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 για τους υπευθύνους προστασίας δεδομένων, με αριθμό εγγράφου 16/EN WP 243.

Εάν η επεξεργασία εν όλω ή εν μέρει υλοποιείται από έναν εκτελούντα την επεξεργασία, **ο εκτελών την επεξεργασία θα πρέπει να συνδράμει τον υπεύθυνο επεξεργασίας στη διενέργεια της ΕΑΠΔ** και να παράσχει κάθε αναγκαία πληροφορία [σύμφωνα με το άρθρο 28 παράγραφος 3 στοιχείο στ)].

Ο υπεύθυνος επεξεργασίας οφείλει, «*όποτε ενδείκνυται*», να «*ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους*» (άρθρο 35 παράγραφος 9). Η ομάδα εργασίας του άρθρου 29 θεωρεί ότι:

- οι εν λόγω γνώμες θα μπορούσαν να ζητηθούν με διάφορα μέσα, ανάλογα με το πλαίσιο (π.χ. με γενική μελέτη που σχετίζεται με τον σκοπό και τα μέσα της πράξης επεξεργασίας, με ερώτημα προς τους εκπροσώπους των εργαζομένων ή με συνήθεις έρευνες που αποστέλλονται στους μελλοντικούς πελάτες του υπεύθυνου επεξεργασίας) διασφαλίζοντας ότι ο υπεύθυνος επεξεργασίας έχει νόμιμη βάση επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που διακυβεύονται όταν ζητούνται οι εν λόγω γνώμες. Παρά ταύτα, θα πρέπει να σημειωθεί ότι η συναίνεση στην επεξεργασία προφανώς δεν αποτελεί μέσο αναζήτησης της γνώμης των υποκειμένων των δεδομένων·
- εάν η τελική απόφαση του υπεύθυνου επεξεργασίας διαφέρει από τη γνώμη των υποκειμένων των δεδομένων, τότε θα πρέπει να τεκμηριώνει τους λόγους για τους οποίους αποφάσισε να συνεχίσει ή όχι·
- ο υπεύθυνος επεξεργασίας θα πρέπει επίσης να τεκμηριώνει τον λόγο για τον οποίο δεν ζήτησε τη γνώμη των υποκειμένων των δεδομένων, εφόσον αποφασίζει ότι δεν ενδείκνυται, για παράδειγμα εάν κάτι τέτοιο θα διακινδύνευε την εμπιστευτικότητα των επιχειρηματικών σχεδίων της εταιρείας ή θα ήταν δυσανάλογο ή μη εφαρμόσιμο.

Τέλος, συνιστά ορθή πρακτική ο καθορισμός και η τεκμηρίωση άλλων ειδικών ρόλων και αρμοδιοτήτων, ανάλογα με την εσωτερική πολιτική, τις διαδικασίες και τους κανόνες, π.χ.:

- όποτε συγκεκριμένες επιχειρηματικές μονάδες προτείνουν τη διενέργεια ΕΑΠΔ, τότε θα πρέπει να εισφέρουν δεδομένα στην ΕΑΠΔ και να μετέχουν στη διαδικασία επικύρωσής της·
- όποτε ενδείκνυται, συνιστάται να ζητείται η γνώμη ανεξάρτητων εμπειρογνωμόνων από διαφορετικά επαγγέλματα[24] (από δικηγόρους, ειδικούς τεχνολογίας πληροφοριών, εμπειρογνώμονες σε θέματα ασφαλείας, δεοντολογίας, κοινωνιολόγους κ.ο.κ.).
- οι ρόλοι και οι αρμοδιότητες των εκτελούντων την επεξεργασία πρέπει να ορίζονται συμβατικά· και η ΕΑΠΔ πρέπει να διενεργείται με τη συνδρομή του εκτελούντος την επεξεργασία, λαμβανομένης υπόψη της φύσης της επεξεργασίας και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία [άρθρο 28 παράγραφος 3 στοιχείο στ)]·
- ο υπεύθυνος ασφάλειας πληροφοριών (ΥΑΠ), εφόσον έχει οριστεί, καθώς και ο υπεύθυνος προστασίας δεδομένων (ΥΠΔ) θα μπορούσαν να προτείνουν τη διενέργεια ΕΑΠΔ από τον υπεύθυνο επεξεργασίας σε συγκεκριμένη πράξη επεξεργασίας και θα πρέπει να συνδράμουν τους ενδιαφερόμενους παράγοντες στη μεθοδολογία, να συνδράμουν στην αξιολόγηση της ποιότητας της εκτίμησης κινδύνου και στον καθορισμό του κατά πόσον ο υπολειπόμενος κίνδυνος είναι αποδεκτός και στην ανάπτυξη ειδικής γνώσης σε σχέση με το πλαίσιο του υπεύθυνου επεξεργασίας·
- ο υπεύθυνος ασφάλειας πληροφοριών (ΥΑΠ), εφόσον έχει οριστεί, και/ή το τμήμα τεχνολογίας πληροφοριών, θα πρέπει να παράσχουν συνδρομή στον υπεύθυνο επεξεργασίας και θα μπορούσαν να προτείνουν τη διενέργεια ΕΑΠΔ σε συγκεκριμένη πράξη επεξεργασίας ανάλογα με τις λειτουργικές ανάγκες ή τις ανάγκες ασφαλείας.

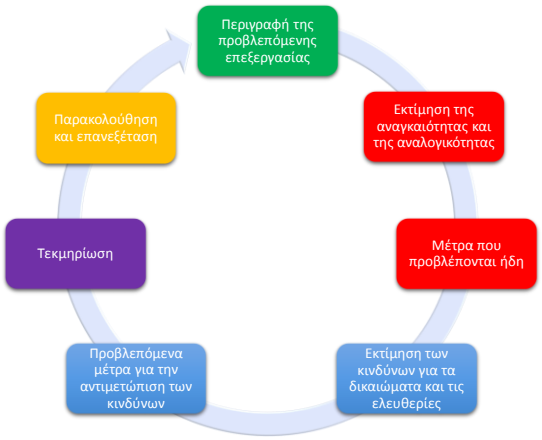
γ) Με ποια μεθοδολογία πρέπει να διενεργείται μια ΕΑΠΔ; Με διάφορες μεθοδολογίες, αλλά με κοινά κριτήρια.

[24] *Συστάσεις για ένα πλαίσιο εκτίμησης επιπτώσεων στην ιδιωτική ζωή για την Ευρωπαϊκή Ένωση, Παραδοτέο Δ3:* http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

Ο ΓΚΠΔ ορίζει το ελάχιστο περιεχόμενο της ΕΑΠΔ (άρθρο 35 παράγραφος 7 και αιτιολογικές σκέψεις 84 και 90):

- «*περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας*»·
- «*εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας*»·
- «*εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων*»·
- «*τα προβλεπόμενα μέτρα:*
    - «*αντιμετώπισης των κινδύνων*»·
    - «*απόδειξης της συμμόρφωσης με τον παρόντα κανονισμό*».

Το ακόλουθο γράφημα απεικονίζει τη γενική επαναλαμβανόμενη διαδικασία που πρέπει να ακολουθείται για τη διενέργεια ΕΑΠΔ[25]:



Κατά την εκτίμηση του αντικτύπου μιας πράξης επεξεργασίας δεδομένων πρέπει να λαμβάνεται υπόψη (άρθρο 35 παράγραφος 8) η συμμόρφωση με έναν κώδικα δεοντολογίας (άρθρο 40). Τούτο μπορεί επίσης να χρησιμεύσει στην απόδειξη ότι έχουν επιλεγεί ή ληφθεί τα κατάλληλα μέτρα, με τον όρο ότι ο κώδικας δεοντολογίας ενδείκνυται για την πράξη επεξεργασίας. Θα πρέπει επίσης να λαμβάνονται υπόψη οι πιστοποιήσεις, οι σφραγίδες και τα σήματα [προστασίας των δεδομένων] για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία (άρθρο 42) με τον ΓΚΠΔ, καθώς και οι δεσμευτικοί εταιρικοί κανόνες (BCR).

Όλες οι συναφείς απαιτήσεις που περιέχει ο ΓΚΠΔ παρέχουν ένα ευρύ, γενικό πλαίσιο για τον σχεδιασμό και την υλοποίηση ΕΑΠΔ. Η πρακτική υλοποίηση μιας ΕΑΠΔ θα εξαρτηθεί από την

[25] Θα πρέπει να τονιστεί ότι η διαδικασία που απεικονίζεται στο παρόν είναι επαναλαμβανόμενη: στην πράξη, ενδέχεται κάθε στάδιο να επαναλαμβάνεται περισσότερες φορές πριν από την ολοκλήρωση της ΕΑΠΔ.

πλήρωση των απαιτήσεων του ΓΚΠΔ, οι οποίες μπορεί να συμπληρωθούν με πιο αναλυτικές πρακτικές οδηγίες. Ως εκ τούτου, η υλοποίηση ΕΑΠΔ είναι κλιμακώσιμη. Τούτο σημαίνει ότι ακόμη και ένας μικρής εμβέλειας υπεύθυνος επεξεργασίας μπορεί να σχεδιάσει και να διενεργήσει ΕΑΠΔ πρόσφορη για τις πράξεις επεξεργασίας του.

Η αιτιολογική σκέψη 90 του ΓΚΠΔ παραθέτει μια σειρά στοιχείων της ΕΑΠΔ που αλληλεπικαλύπτονται με τα πλήρως καθορισμένα στοιχεία της διαχείρισης κινδύνων (λ.χ. ISO 31000[26]). Με όρους διαχείρισης κινδύνου, μια ΕΑΠΔ αποσκοπεί στη «διαχείριση των κινδύνων» για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, με χρήση των ακόλουθων διαδικασιών, μέσω:

- του καθορισμού του πλαισίου: «*λαμβάνοντας υπόψη τη φύση, την έκταση, το πλαίσιο και τους σκοπούς της επεξεργασίας και τις πηγές του κινδύνου*»·
- της εκτίμησης των κινδύνων: «*ώστε να εκτιμήσει την ιδιαίτερη πιθανότητα και τη σοβαρότητα του υψηλού κινδύνου*»·
- της αντιμετώπισης των κινδύνων: «*που μετριάζουν αυτόν τον κίνδυνο*» και «*διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα*» και «*αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό*».

Σημείωση: Η ΕΑΠΔ κατά τον ΓΚΠΔ αποτελεί εργαλείο διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, υιοθετεί τη δική τους οπτική, όπως ισχύει σε ορισμένους τομείς (π.χ. κοινωνική ασφάλεια). Αντιθέτως, σε άλλους τομείς η διαχείριση των κινδύνων (π.χ. ασφάλεια πληροφοριών) επικεντρώνεται στην οργανωτική διάρθρωση.

Ο ΓΚΠΔ παρέχει ευελιξία στους υπεύθυνους επεξεργασίας για τον καθορισμό της ακριβούς δομής και της μορφής της ΕΑΠΔ, προκειμένου αυτή να εξυπηρετεί τις υφιστάμενες πρακτικές εργασίας. Υπάρχουν πολυάριθμες καθιερωμένες διαδικασίες, εντός της ΕΕ και παγκοσμίως, που λαμβάνουν υπόψη τα στοιχεία που περιγράφονται στην αιτιολογική σκέψη 90. Ωστόσο, ανεξαρτήτως της μορφής που θα λάβει, η ΕΑΠΔ θα πρέπει να αποτελεί μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους.

Διαφορετικές μεθοδολογίες (βλέπε Παράρτημα 1 για παραδείγματα μεθοδολογίας για την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και την ιδιωτική ζωή) θα μπορούσαν να χρησιμοποιηθούν για να συνδράμουν στην υλοποίηση των βασικών απαιτήσεων που θέτει ο ΓΚΠΔ. Έχουν προσδιοριστεί ορισμένα κοινά κριτήρια ώστε να επιτρέπεται στους υπεύθυνους επεξεργασίας να υιοθετούν διαφορετικές προσεγγίσεις, συμμορφούμενοι παράλληλα με τον ΓΚΠΔ (βλέπε Παράρτημα 2). Τα εν λόγω κριτήρια αποσαφηνίζουν τις βασικές απαιτήσεις του κανονισμού και παρέχουν επαρκές έδαφος για τη χρήση διαφορετικών μορφών υλοποίησης. Τα εν λόγω κριτήρια μπορούν να χρησιμοποιηθούν για την απόδειξη ότι μια συγκεκριμένη μεθοδολογία ΕΑΠΔ πληροί τα απαιτούμενα πρότυπα που θέτει ο ΓΚΠΔ. **Ο υπεύθυνος επεξεργασίας είναι αρμόδιος να επιλέξει τη μεθοδολογία, η οποία όμως θα πρέπει να συνάδει με τα κριτήρια του Παραρτήματος 2.**

Η ομάδα εργασίας του άρθρου 29 ενθαρρύνει τη δημιουργία πλαισίων για τομεακά εξειδικευμένες ΕΑΠΔ, διότι μπορεί να χρησιμοποιηθεί ειδική τομεακή γνώση, με την έννοια ότι η ΕΑΠΔ μπορεί να εξετάσει τα ιδιαίτερα χαρακτηριστικά ενός είδους πράξης επεξεργασίας (π.χ.: συγκεκριμένα είδη

[26] Διαδικασίες διαχείρισης κινδύνων: επικοινωνία και διαβούλευση, ορισμός του πλαισίου, εκτίμηση κινδύνου, αντιμετώπιση κινδύνων, παρακολούθηση και επανεξέταση (βλέπε όρους και ορισμούς και πίνακα περιεχομένων, στην προεπισκόπηση του ISO 31000: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

δεδομένων, εταιρικά περιουσιακά στοιχεία, πιθανό αντίκτυπο, απειλές, μέτρα). Αυτό σημαίνει ότι η ΕΑΠΔ μπορεί να εξετάσει τα ζητήματα που εγείρονται σε ορισμένο οικονομικό τομέα, ή κατά τη χρήση συγκεκριμένων τεχνολογιών ή τη διενέργεια συγκεκριμένων ειδών πράξεων επεξεργασίας.

Τέλος, όποτε απαιτείται, «*ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας*» (άρθρο 35 παράγραφος 11[27]).

δ) Είναι υποχρεωτική η δημοσίευση της ΕΑΠΔ; Όχι, ωστόσο η δημοσίευση μιας σύνοψης θα μπορούσε να προαγάγει την εμπιστοσύνη, ενώ η πλήρης ΕΑΠΔ πρέπει να ανακοινωθεί στην εποπτική αρχή εφόσον έχει προηγηθεί διαβούλευση ή το ζητεί η ΑΠΔ.

Η δημοσίευση της ΕΑΠΔ δεν συνιστά νομική απαίτηση του ΓΚΠΔ και αποτελεί απόφαση του υπεύθυνου επεξεργασίας. Ωστόσο, οι υπεύθυνοι επεξεργασίας θα πρέπει να εξετάζουν το ενδεχόμενο δημοσίευσης τουλάχιστον αποσπασμάτων αυτής, όπως σύνοψη ή συμπέρασμα της ΕΑΠΔ τους.

Ο σκοπός της διαδικασίας αυτής θα ήταν η προαγωγή της εμπιστοσύνης στις πράξεις επεξεργασίας του υπεύθυνου επεξεργασίας και η απόδειξη της διαφάνειας και της πλήρωσης της υποχρέωσης λογοδοσίας. Είναι ιδιαίτερα ορθή πρακτική η δημοσίευση της ΕΑΠΔ σε πράξη επεξεργασίας που επηρεάζει το κοινό. Κάτι τέτοιο θα μπορούσε να ισχύει ιδιαίτερα σε περίπτωση διενέργειας ΕΑΠΔ από δημόσια αρχή.

Η δημοσιευμένη ΕΑΠΔ δεν χρειάζεται να περιλαμβάνει την πλήρη εκτίμηση, ιδίως όταν η ΕΑΠΔ θα μπορούσε να εκθέτει συγκεκριμένες πληροφορίες που αφορούν τους κινδύνους ασφαλείας για τον υπεύθυνο επεξεργασίας ή να αποκαλύπτει εμπορικά απόρρητα ή εμπορικά ευαίσθητες πληροφορίες. Στις περιπτώσεις αυτές, η δημοσιευμένη έκδοση θα μπορούσε να απαρτίζεται απλώς από μια σύνοψη των κύριων ευρημάτων της ΕΑΠΔ ή απλώς από μια δήλωση ότι έχει διενεργηθεί ΕΑΠΔ.

Επιπλέον, όποτε η ΕΑΠΔ αποκαλύπτει υψηλούς υπολειπόμενους κινδύνους, ο υπεύθυνος επεξεργασίας θα πρέπει να ζητά προηγούμενη διαβούλευση με την εποπτική αρχή για την επεξεργασία (άρθρο 36 παράγραφος 1). Σε αυτή την περίπτωση, πρέπει να παρέχεται η πλήρης ΕΑΠΔ [άρθρο 36 παράγραφος 3 στοιχείο ε)]. Η εποπτική αρχή μπορεί να παρέχει συμβουλές[28] και δεν θα διαρρεύσει εμπορικά απόρρητα ούτε θα αποκαλύψει τρωτά σημεία στην ασφάλεια, βάσει των αρχών που ισχύουν σε κάθε κράτος μέλος για τη δημόσια πρόσβαση στα επίσημα έγγραφα.

Γ. Πότε πρέπει να ζητείται η γνώμη της εποπτικής αρχής; Όταν οι υπολειπόμενοι κίνδυνοι είναι υψηλοί.

Όπως εξηγήθηκε ανωτέρω:

- η διενέργεια ΕΑΠΔ απαιτείται όταν μια πράξη επεξεργασίας «*ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων*» (άρθρο 35 παράγραφος 1, βλέπε ΙΙΙ.Β.α). Παραδείγματος χάριν, η επεξεργασία δεδομένων υγείας σε μεγάλη κλίμακα

[27] Το άρθρο 35 παράγραφος 10 ρητά αποκλείει μόνον την εφαρμογή του άρθρου 35 παράγραφοι 1 έως 7.

[28] Έγγραφες συμβουλές προς τον υπεύθυνο επεξεργασίας απαιτούνται μόνο στην περίπτωση που η εποπτική αρχή φρονεί ότι η σκοπούμενη επεξεργασία δεν συνάδει με τον κανονισμό, κατά το άρθρο 36 παράγραφος 2.

θεωρείται ότι ενδέχεται να επιφέρει υψηλό κίνδυνο και υπόκειται σε απαίτηση διενέργειας ΕΑΠΔ·

- οπότε, ο υπεύθυνος επεξεργασίας ευθύνεται για την εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και τον προσδιορισμό των προβλεπόμενων μέτρων[29] για τη μείωση αυτών σε αποδεκτό επίπεδο και για την απόδειξη της συμμόρφωσης προς τον ΓΚΠΔ (άρθρο 35 παράγραφος 7, βλέπε ΙΙΙ.Γ.γ). Ένα παράδειγμα που αφορά την αποθήκευση δεδομένων προσωπικού χαρακτήρα σε φορητούς υπολογιστές θα μπορούσε να είναι η χρήση κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας (αποτελεσματική πλήρης κρυπτογράφηση δίσκου, ισχυρή διαχείριση κλειδιών, κατάλληλος έλεγχος πρόσβασης, ασφαλή εφεδρικά αντίγραφα κ.ο.κ.) πλέον των υφιστάμενων πολιτικών (ειδοποίηση, συναίνεση, δικαίωμα πρόσβασης, δικαίωμα εναντίωσης κ.ο.κ.).

Στο παραπάνω παράδειγμα με τους φορητούς υπολογιστές, εάν ο υπεύθυνος επεξεργασίας θεωρήσει ότι οι κίνδυνοι έχουν μειωθεί σημαντικά και κατά τα διαλαμβανόμενα στο άρθρο 36 παράγραφος 1 και τις αιτιολογικές σκέψεις 84 και 94, η επεξεργασία μπορεί να συνεχιστεί χωρίς διαβούλευση με την εποπτική αρχή. Σε περίπτωση που οι εξακριβωθέντες κίνδυνοι δεν μπορούν να αντιμετωπιστούν επαρκώς από τον υπεύθυνο επεξεργασίας (δηλαδή, οι υπολειπόμενοι κίνδυνοι εξακολουθούν να είναι υψηλοί), ο υπεύθυνος επεξεργασίας πρέπει να ζητήσει τη γνώμη της εποπτικής αρχής.

Ένα παράδειγμα μη αποδεκτού υψηλού υπολειπόμενου κινδύνου περιλαμβάνει περιπτώσεις που τα υποκείμενα των δεδομένων μπορεί να υποστούν σημαντικές, ή ακόμη και μη αναστρέψιμες, επιπτώσεις τις οποίες ενδέχεται να μην ξεπεράσουν (π.χ.: αθέμιτη πρόσβαση σε δεδομένα που ενέχει απειλή για τη ζωή των υποκειμένων των δεδομένων, απόλυση, οικονομική διακινδύνευση) και/ή όταν καθίσταται προφανές ότι θα επέλθει ο κίνδυνος (π.χ.: όταν δεν είναι δυνατή η μείωση του αριθμού των προσώπων που έχουν πρόσβαση στα δεδομένα λόγω των τρόπων διαμοιρασμού, χρήσης ή διανομής ή όταν δεν καλύπτεται ένα ήδη γνωστό τρωτό σημείο).

Όποτε ο υπεύθυνος επεξεργασίας δεν μπορεί να βρει επαρκή μέτρα για τη μείωση των κινδύνων σε αποδεκτό επίπεδο (δηλαδή οι υπολειπόμενοι κίνδυνοι παραμένουν υψηλοί) απαιτείται διαβούλευση με την εποπτική αρχή[30].

Επιπλέον, ο υπεύθυνος επεξεργασίας θα πρέπει να διαβουλεύεται με την εποπτική αρχή οποτεδήποτε το δίκαιο του κράτους μέλους απαιτεί από τους υπευθύνους επεξεργασίας να διαβουλεύονται και/ή να λαμβάνουν προηγούμενη έγκριση από την εποπτική αρχή σε σχέση με την επεξεργασία από υπεύθυνο επεξεργασίας για την εκτέλεση καθήκοντος που ασκείται από τον εν λόγω υπεύθυνο προς το δημόσιο συμφέρον, περιλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία (άρθρο 36 παράγραφος 5).

[29] Περιλαμβάνεται ο συνυπολογισμός της υφιστάμενης καθοδήγησης από το ΕΣΠΔ και τις εποπτικές αρχές, και ο συνυπολογισμός των τεχνολογικών εξελίξεων και του κόστους εφαρμογής, όπως προβλέπεται στο άρθρο 35 παράγραφος 1.

[30] Σημείωση: «*Η ψευδωνυμοποίηση και η κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα*» (καθώς και η ελαχιστοποίηση των δεδομένων, οι μηχανισμοί επιτήρησης κ.ο.κ.) δεν συνιστούν κατ' ανάγκη ενδεδειγμένα μέτρα. Είναι μόνο παραδείγματα. Τα ενδεδειγμένα μέτρα εξαρτώνται από το ειδικό πλαίσιο και τους κινδύνους κάθε πράξης επεξεργασίας.

Θα πρέπει, ωστόσο, να αναφερθεί ότι ανεξαρτήτως του κατά πόσον απαιτείται ή όχι διαβούλευση με την εποπτική αρχή βάσει του επιπέδου του υπολειπόμενου κινδύνου, οι υποχρεώσεις τήρησης αρχείου της ΕΑΠΔ και επικαιροποίησης της ΕΑΠΔ σε εύθετο χρόνο παραμένουν.

IV. Συμπεράσματα και συστάσεις

Οι ΕΑΠΔ αποτελούν ένα χρήσιμο μέσο που διαθέτουν οι υπεύθυνοι επεξεργασίας για να εφαρμόζουν συστήματα επεξεργασίας δεδομένων που συμμορφώνονται με τον ΓΚΠΔ και μπορεί να είναι υποχρεωτικές για ορισμένα είδη πράξεων επεξεργασίας. Είναι κλιμακώσιμες και μπορούν να λάβουν διαφορετικές μορφές, ωστόσο ο ΓΚΠΔ θέτει τις βασικές απαιτήσεις μιας αποτελεσματικής ΕΑΠΔ. Οι υπεύθυνοι επεξεργασίας θα πρέπει να αντιμετωπίζουν την ΕΑΠΔ ως χρήσιμη και θετική δραστηριότητα που παρέχει συνδρομή στη νομική τους συμμόρφωση.

Το άρθρο 24 παράγραφος 1 ορίζει τη βασική αρμοδιότητα του υπεύθυνου επεξεργασίας με όρους συμμόρφωσης με τον ΓΚΠΔ: «*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*».

Η διενέργεια ΕΑΠΔ αποτελεί ουσιώδες μέρος της συμμόρφωσης με τον κανονισμό, όποτε σχεδιάζεται ή υλοποιείται επεξεργασία δεδομένων με υψηλό κίνδυνο. Αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας θα πρέπει να χρησιμοποιούν τα κριτήρια που ορίζονται στο παρόν έγγραφο για να καθορίζουν το κατά πόσον πρέπει να διενεργηθεί ΕΑΠΔ ή όχι. Η εσωτερική πολιτική του υπεύθυνου επεξεργασίας θα μπορούσε να επεκτείνει τον κατάλογο αυτό πέρα από τις νομικές απαιτήσεις του ΓΚΠΔ, κάτι που θα μπορούσε να ενισχύσει την πίστη και την εμπιστοσύνη των υποκειμένων των δεδομένων και άλλων υπεύθυνων επεξεργασίας.

Σε περίπτωση σχεδιασμού επεξεργασίας που ενέχει υψηλό κίνδυνο, ο υπεύθυνος επεξεργασίας οφείλει:

- να επιλέξει μια μεθοδολογία ΕΑΠΔ (παραδείγματα παρατίθενται στο Παράρτημα 1) που πληροί τα κριτήρια του Παραρτήματος 2 ή να ορίσει και να εφαρμόσει μια συστηματική διαδικασία ΕΑΠΔ που:
  - να πληροί τα κριτήρια του Παραρτήματος 2·
  - να είναι ενσωματωμένη στις υφιστάμενες διαδικασίες σχεδιασμού, ανάπτυξης, μεταβολής και επανεξέτασης κινδύνων και λειτουργίας σύμφωνα με τις εσωτερικές διαδικασίες, το πλαίσιο και τη νοοτροπία·
  - να περιλαμβάνει τα ενδεδειγμένα ενδιαφερόμενα μέρη και να ορίζει σαφώς τις αρμοδιότητές τους (υπεύθυνος επεξεργασίας, ΥΠΔ, υποκείμενα δεδομένων ή οι εκπρόσωποί τους, επιχειρηματικές δραστηριότητες, τεχνική εξυπηρέτηση, εκτελούντες την επεξεργασία, υπεύθυνοι ασφαλείας πληροφοριών κ.ο.κ.)·
- εφόσον απαιτείται, να υποβάλει την έκθεση της ΕΑΠΔ στην αρμόδια εποπτική αρχή·
- να ζητεί τη γνώμη της εποπτικής αρχής σε περίπτωση που δεν έχουν κατορθώσει να καθορίσουν επαρκή μέτρα για τον μετριασμό του υψηλού κινδύνου·
- να επανεξετάζει σε περιοδική βάση την ΕΑΠΔ και την επεξεργασία που αξιολογεί, τουλάχιστον όταν έχει μεταβληθεί ο κίνδυνος που θέτει η πράξη επεξεργασίας·
- να τεκμηριώνει τις ληφθείσες αποφάσεις.

Παράρτημα 1 – Παραδείγματα υφιστάμενων πλαισίων ΕΑΠΔ της ΕΕ

Ο ΓΚΠΔ δεν προσδιορίζει ποια διαδικασία ΕΑΠΔ πρέπει να ακολουθηθεί, αλλά αντιθέτως επιτρέπει στους υπεύθυνους επεξεργασίας να εισάγουν ένα πλαίσιο που συμπληρώνει τις υφιστάμενες πρακτικές εργασίας τους, με τον όρο ότι λαμβάνει υπόψη τα στοιχεία που περιγράφονται στο άρθρο 35 παράγραφος 7. Το εν λόγω πλαίσιο μπορεί να είναι προσαρμοσμένο στις ανάγκες του υπεύθυνου επεξεργασίας ή κοινό σε συγκεκριμένο κλάδο. Στα ήδη δημοσιευμένα πλαίσια που έχουν καταρτιστεί από τις ΑΠΔ της ΕΕ και στα ειδικά τομεακά πλαίσια περιλαμβάνονται (ενδεικτικά):

Παραδείγματα γενικών πλαισίων της ΕΕ:

- DE (Γερμανία): Πρότυπο Μοντέλο Προστασίας Δεδομένων, V.I.0 – Δοκιμαστική έκδοση, 2016[31].
  https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf
- ES (Ισπανία): *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014.
  https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR (Γαλλία): *Εκτίμηση Επιπτώσεων στην Ιδιωτικότητα (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015.
  https://www.cnil.fr/fr/node/15798
- HB: *Κώδικας πρακτικής για τη διενέργεια εκτίμησης επιπτώσεων στην ιδιωτικότητα*, Γραφείο Επιτρόπου Πληροφοριών (ICO), 2014.
  https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

Παραδείγματα ειδικών τομεακών πλαισίων στην ΕΕ:

- Πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID [32].
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης[33]

---

[31] Ομόφωνα αναγνωρισμένο και επιβεβαιωμένο (με αποχή της Βαυαρίας) από την 92η Συνδιάσκεψη των Ανεξάρτητων Αρχών προστασίας δεδομένων της ομοσπονδίας και των ομόσπονδων κρατιδίων (Bund und die Länder) στο Kühlungsborn, στις 9-10 Νοεμβρίου 2016.

[32] Βλέπε επίσης:

- Σύσταση της Επιτροπής, της 12ης Μαΐου 2009, για την εφαρμογή αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων στις εφαρμογές που υποστηρίζονται από ραδιοσυχνική αναγνώριση.
  https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
- Γνώμη 9/2011 σχετικά με την αναθεωρημένη πρόταση του κλάδου για ένα πλαίσιο εκπόνησης εκτιμήσεων των επιπτώσεων στην προστασία της ιδιωτικής ζωής και των δεδομένων για τις εφαρμογές RFID.
  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_el.pdf

[33] Βλέπε επίσης τη γνώμη 07/2013 σχετικά με το υπόδειγμα για την εκτίμηση των επιπτώσεων της προστασίας δεδομένων όσον αφορά τα ευφυή δίκτυα και τα ευφυή συστήματα μέτρησης («υπόδειγμα ΕΕΠΔ») το οποίο εκπόνησε η ομάδα εμπειρογνωμόνων 2 της ομάδας ειδικών καθηκόντων της Επιτροπής για τα ευφυή ηλεκτρικά

http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Ένα διεθνές πρότυπο θα παρέχει επίσης κατευθυντήριες γραμμές για τις μεθοδολογίες που χρησιμοποιούνται στη διενέργεια ΕΑΠΔ (ISO/IEC 29134[34]).

δίκτυα. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_el.pdf

[34] ISO/IEC 29134 (έργο), *Τεχνολογία Πληροφοριών – Τεχνικές Ασφαλείας – Εκτίμηση επιπτώσεων στην ιδιωτικότητα – Οδηγίες*, Διεθνής Οργανισμός Τυποποίησης (ISO).

Παράρτημα 2 – Κριτήρια για μια αποδεκτή ΕΑΠΔ

Η ομάδα εργασίας του άρθρου 29 προτείνει τα ακόλουθα κριτήρια, τα οποία οι υπεύθυνοι επεξεργασίας μπορούν να χρησιμοποιούν για να αξιολογούν κατά πόσο μια ΕΑΠΔ ή μια μεθοδολογία διενέργειας ΕΑΠΔ είναι επαρκώς περιεκτική προκειμένου να συμμορφώνεται με τον ΓΚΠΔ:

- ☐ παρέχεται συστηματική περιγραφή των πράξεων επεξεργασίας [άρθρο 35 παράγραφος 7 στοιχείο α)]:
  - ☐ λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)·
  - ☐ καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα·
  - ☐ παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας·
  - ☐ προσδιορίζονται τα στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)·
  - ☐ λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 παράγραφος 8)·
- ☐ εκτιμώνται η αναγκαιότητα και η αναλογικότητα [άρθρο 35 παράγραφος 7 στοιχείο β)]·
  - ☐ καθορίζονται τα προβλεπόμενα μέτρα συμμόρφωσης με τον κανονισμό [άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90], λαμβάνοντας υπόψη:
    - ☐ τα μέτρα που κατατείνουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:
      - ☐ καθορισμένων, ρητών και νόμιμων σκοπών [άρθρο 5 παράγραφος 1 στοιχείο β)]·
      - ☐ της νομιμότητας της επεξεργασίας (άρθρο 6)·
      - ☐ κατάλληλων, συναφών και περιορισμένων στα αναγκαία δεδομένων [άρθρο 5 παράγραφος 1 στοιχείο γ)]·
      - ☐ της περιορισμένης διάρκειας αποθήκευσης [άρθρο 5 παράγραφος 1 στοιχείο ε)]·
    - ☐ μέτρα που συμβάλλουν στη διαφύλαξη των δικαιωμάτων των υποκειμένων των δεδομένων:
      - ☐ πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14):
      - ☐ δικαίωμα πρόσβασης και δικαίωμα στη φορητότητα των δεδομένων (άρθρα 15 και 20)·
      - ☐ δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19)·
      - ☐ δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21)·
      - ☐ σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28)·
      - ☐ διασφαλίζονται οι περιστάσεις που περιβάλλουν τη διεθνή διαβίβαση ή τις διεθνείς διαβιβάσεις (Κεφάλαιο V)·
      - ☐ προηγούμενη διαβούλευση (άρθρο 36).
- ☐ τελούν υπό διαχείριση οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων [άρθρο 35 παράγραφος 7 στοιχείο γ)]:
  - ☐ έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (πρβλ. αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων·
    - ☐ έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)·
    - ☐ εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων·

- ☐ εξακριβώνονται απειλές που θα μπορούσαν να επιφέρουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων·
- ☐ εκτιμώνται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90)·

☐ καθορίζονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90)·

☐ <u>συμμετέχουν τα ενδιαφερόμενα μέρη</u>:

☐ ζητείται η γνώμη του ΥΠΔ (άρθρο 35 παράγραφος 2)·

☐ ζητείται η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους, όταν ενδείκνυται (άρθρο 35 παράγραφος 9).