ProLegis

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Περιεχόμενα

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Νομικό πλαίσιο

1.1 Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR ή ΓΚΠΔ)

Άρθρο 35

Εκτίμηση αντικτύπου προστασίας δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

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,

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 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, 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.

7. Η εκτίμηση περιέχει τουλάχιστον:

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.

8. Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

9. Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

10. Όταν η επεξεργασία δυνάμει του άρθρου 6 παράγραφος 1 (γ) ή (ε) έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης, οι παράγραφοι 1 έως 7 δεν εφαρμόζονται, εκτός εάν τα κράτη μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω εκτίμησης πριν από τις δραστηριότητες επεξεργασίας.

11. Όπου 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.

Αιτιολογικές εκθέσεις 89 έως 96:

Το άρθρο 35 του ΓΚΠΔ συνδέεται στενά με τα άρθρα 24, 25 και 32. Η κύρια διαφορά μεταξύ του άρθρου 32 και του άρθρου 35 είναι ότι το άρθρο 32 (ασφάλεια επεξεργασίας δεδομένων) εστιάζει στους κινδύνους που συνδέονται με επιζήμια γεγονότα όπως επιθέσεις, ενώ μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) με βάση το άρθρο 35 επικεντρώνεται κυρίως στους κινδύνους που προκύπτουν από την τακτική επεξεργασία δεδομένων.

Η ΕΑΠΔ αποτελεί σημαντικό εργαλείο για την εφαρμογή της προστασίας των δεδομένων με τεχνολογικά μέσα (προστασία δεδομένων κατά το σχεδιασμό), όπως ορίζεται στο άρθρο 25, παράγραφος 1. Και τα δύο βασίζονται στην αρχή της προφύλαξης, δηλαδή στον εντοπισμό κινδύνων ήδη από τις αρχικές φάσεις σχεδιασμού και στην εξέταση σχετικών αντιμέτρων πριν από την εφαρμογή και έναρξη λειτουργίας οποιωνδήποτε συστημάτων επεξεργασίας δεδομένων.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Η ΕΑΠΔ είναι ένα εργαλείο για τον εντοπισμό και την ανάλυση ανάλογων κινδύνων. Στις περιπτώσεις όπου δεν είναι υποχρεωτική μια ΕΑΠΔ, μια ανάλυση των σχετικών κινδύνων είναι απαραίτητη, για την επαρκή εφαρμογή του άρθρου 25 και του άρθρου 32. Και οι δύο κανονισμοί αναφέρονται ρητά στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Το βάθος και η απαιτούμενη τεκμηρίωση της ανάλυσης κινδύνου που πρέπει να διεξαχθεί εξαρτάται από την πολυπλοκότητα και την επικινδυνότητα της επεξεργασίας. Συνιστάται η παροχή μιας γραπτής τεκμηρίωσης της ανάλυσης κινδύνου.

Η εφαρμογή της αρχής της προστασίας δεδομένων κατά τον σχεδιασμό υπερβαίνει τους κινδύνους που εντοπίζονται εκ των προτέρων σε μια ανάλυση κινδύνου τελευταίας τεχνολογίας και περιλαμβάνει αποφάσεις που λαμβάνονται σε μεταγενέστερο στάδιο ad hoc (αυθαίρετα) από τους προγραμματιστές συστημάτων (τεχνική διασφάλισης ιδιωτικότητας) κατά την εφαρμογή των αρχών της ελαχιστοποίησης των δεδομένων.

Πότε είναι απαραίτητη μια ΕΑΠΔ;

2.1 Βασικά

Μια ΕΑΠΔ πρέπει να εκτελείται πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα που φέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Κατ 'αρχήν, η ΕΑΠΔ πρέπει να διεξάγεται για κάθε μορφή επεξεργασίας δεδομένων, εκτός εάν μπορεί να καθοριστεί εκ των προτέρων ότι τα δικαιώματα και οι ελευθερίες των φυσικών προσώπων δεν επηρεάζονται από μια συγκεκριμένη ενέργεια επεξεργασίας δεδομένων.

Για ποια μορφή επεξεργασίας δεδομένων ένας τέτοιος κίνδυνος πρέπει να υποτεθεί καθορίζεται π.χ. στα σημεία που απαριθμούνται στο άρθρο 35, παράγραφος 3 ή στην αιτιολογική σκέψη 91. Η έμφαση δίδεται στη χρήση των λεγομένων νέων τεχνολογιών, μιας αόριστης νομικής έννοιας που εισήχθη στον ΓΚΠΔ όσον αφορά στην ΕΑΠΔ. Η εκτίμηση κινδύνου όχι μόνο πρέπει να εξετάσει τους υπάρχοντες σχηματισμούς

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

κινδύνου, αλλά και την πιθανότητα μελλοντικών συμβάντων, να προσδιοριστεί σε μια προγνωστική εκτίμηση. Τα αποτελέσματα της εκτίμησης πρέπει να τεκμηριώνονται.

Η τελευταία φράση του άρθρου 35 παράγραφος 1 σε συνδυασμό με την αιτιολογική έκθεση 92 παρέχει μια σημαντική οπτική για την εκτίμηση της ανάγκης μιας ΕΑΠΔ: "Υπάρχουν περιπτώσεις στις οποίες μπορεί να είναι λογικό και οικονομικά σκόπιμο το αντικείμενο μιας εκτίμησης αντικτύπου να μην εφαρμόζεται αποκλειστικά σε ένα συγκεκριμένο έργο, αλλά να διευρύνεται το θεματικό πεδίο εφαρμογής του, για παράδειγμα, εάν δημόσιες αρχές ή δημόσιοι φορείς σκοπεύουν να εγκαθιδρύσουν μια κοινή εφαρμογή ή περιβάλλον επεξεργασίας ή εάν πολλοί ενδιαφερόμενοι φορείς σχεδιάζουν να θεσπίσουν μια κοινή εφαρμογή ή ένα περιβάλλον επεξεργασίας σε έναν επιχειρηματικό τομέα ή κλάδο, ή για μια ευρέως χρησιμοποιούμενη οριζόντια δραστηριότητα.

2.2 Περιπτώσεις στις οποίες η ΕΑΠΔ είναι επιτακτική

Το άρθρο 35 παρ. 3 απαριθμεί τις υποχρεωτικές περιπτώσεις για μια ΕΑΠΔ:

α) συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο ·

β) μεγάλης κλίμακας επεξεργασία 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 ·

γ) συστηματική παρακολούθηση ενός δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

2.2.1. Περαιτέρω σκέψεις σχετικά με την ανάγκη διενέργειας μιας ΕΑΠΔ

Η αιτιολογική έκθεση 91 απαριθμεί περαιτέρω υποθέσεις που απαιτούν μια ΕΑΠΔ:

Πράξεις επεξεργασίας

α) οι οποίες ενδέχεται να περιλαμβάνουν μεγάλο αριθμό ατόμων, ή / και υψηλό επίπεδο κινδύνου ή / και χρήση τεχνολογίας ευρείας κλίμακας σύμφωνα με τις σύγχρονες τεχνολογίες ·

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

β) οι οποίες συνεπάγονται υψηλό επίπεδο κινδύνου και δυσχεραίνουν τα υποκείμενα των δεδομένων στην άσκηση των δικαιωμάτων τους ·

γ) στις οποίες δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία ενόψει της λήψης αποφάσεων σχετικά με συγκεκριμένα φυσικά πρόσωπα έπειτα από οποιαδήποτε συστηματική και εκτενή αξιολόγηση των προσωπικών πτυχών που αφορούν φυσικά πρόσωπα, και βασίζονται στην κατάρτιση προφίλ βάσει των εν λόγω δεδομένων ή έπειτα από επεξεργασία συγκεκριμένων κατηγοριών προσωπικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα ή συναφή μέτρα ασφαλείας ·

δ) οι οποίες συνεπάγονται υψηλό επίπεδο κινδύνου, διότι εμποδίζουν τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση ·

ε) οι οποίες παρουσιάζουν υψηλό κίνδυνο επειδή πραγματοποιούνται συστηματικά σε μεγάλη κλίμακα.

2.2.2. Διενέργεια μιας ΕΑΠΔ για πολλά παρόμοια συστήματα επεξεργασίας δεδομένων

Το άρθρο 35 παρ. 1 δηλώνει ότι μία και μόνο ΕΑΠΔ μπορεί να διενεργείται για συστήματα επεξεργασίας με παρόμοιο επίπεδο κινδύνου. Κατά την εκτίμηση ανάλογων περιπτώσεων πρέπει να λαμβάνεται υπόψη ο συνολικός σκοπός της επεξεργασίας δεδομένων σε κάθε μεμονωμένη περίπτωση. Η αιτιολογική έκθεση 92 αναφέρει ότι, λαμβάνοντας υπόψη το οικονομικό κόστος, η ΕΑΠΔ μπορεί να έχει ένα ευρύτερο θεματικό πεδίο, παρέχοντας στα μέλη σε συγκεκριμένο τομέα ή κλάδο την ευκαιρία να καλύψουν εφαρμογές ή περιβάλλοντα επεξεργασίας ή ευρέως χρησιμοποιούμενες οριζόντιες δραστηριότητες με μια ενιαία ατομική ΕΑΠΔ.

2.2.3. Θετικοί και αρνητικοί κατάλογοι για την ΕΑΠΔ

Μπορεί να υποτεθεί ότι οι εποπτικές αρχές θα δημοσιεύσουν θετικούς / αρνητικούς καταλόγους για να καθοδηγήσουν την απόφαση σχετικά με το εάν απαιτείται μια ΕΑΠΔ σε μια συγκεκριμένη περίπτωση. Οι κατάλογοι αυτοί θα καθορίσουν μορφές επεξεργασίας που απαιτούν ΕΑΠΔ («θετικοί κατάλογοι») και περιπτώσεις όπου δεν απαιτείται ΕΑΠΔ («αρνητικοί»). Οι δύο κατάλογοι πρέπει να διαβιβάζονται από τα εθνικά εποπτικές αρχές στο Ευρωπαϊκό Συμβούλιο για την προστασία των δεδομένων, στο πλαίσιο του καθεστώτος συνοχής των κανονιστικών ρυθμίσεων (άρθρο 35, παρ. 4), ώστε να επιτευχθεί καλύτερη εναρμόνιση σε ολόκληρη την ΕΕ.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Πρέπει να σημειωθεί ότι η ομάδα εργασίας του άρθρου 29 (WP29) συνιστά τη διενέργεια μιας ΕΑΠΔ και στις περιπτώσεις, όπου δεν καθίσταται σαφές αν απαιτείται ΕΑΠΔ ώστε να συμβάλει στην εκπλήρωση των νομικών απαιτήσεων για την ορθή προστασία των δεδομένων.

2.3 Χρόνος διενέργειας της ΕΑΠΔ

Ο χρόνος και η μέθοδος εφαρμογής μιας ΕΑΠΔ οφείλουν να καθορίζονται από τον υπεύθυνο επεξεργασίας. Προβλέπονται νομικές κυρώσεις για την αδυναμία εκτέλεσης μιας ΕΑΠΔ. Συνιστάται να ξεκινά η προετοιμασία για την ΕΑΠΔ κατά το πιο πρώιμο δυνατό στάδιο ενός έργου. Κάθε τμήμα ή τα σχετικά μέλη του προσωπικού που εμπλέκονται στην επεξεργασία δεδομένων πρέπει να ξεκινήσουν τις σχετικές διαδικασίες. Προτείνεται κατάρτιση για την ευαισθητοποίηση σχετικά με την ανάγκη για ΕΑΠΔ στο πλαίσιο του οργανισμού.

Η λήψη μέτρων για την ελαχιστοποίηση του κινδύνου σε πρώιμο στάδιο κάθε έργου, που περιλαμβάνει την επεξεργασία δεδομένων, μπορεί να συμβάλει στη διατήρηση των γραφειοκρατικών προσπαθειών σε σχετικά χαμηλό επίπεδο.

Μια ΕΑΠΔ μπορεί να καθοδηγήσει την αναζήτηση κατάλληλων λύσεων και να συμβάλει στην αποτελεσματική και έγκαιρη εφαρμογή των απαιτήσεων προστασίας δεδομένων - όπως προαναφέρθηκε- μέσω κατάλληλων τεχνολογικών λύσεων (προστασία δεδομένων κατά το σχεδιασμό) και της επιλογής προεπιλεγμένων ρυθμίσεων για την προστασία των δεδομένων.

Παρέχοντας ολοκληρωμένες και εντατικές προετοιμασίες, η ΕΑΠΔ θα καθοδηγήσει ένα σχεδιαζόμενο πρόγραμμα από το στάδιο των αρχικών ιδεών μέχρι την τελική επιχειρησιακή εφαρμογή του και αποδεικνύει τον επαναληπτικό χαρακτήρα της διαδικασίας ΕΑΠΔ.

Το αν μια ΕΑΠΔ απαιτήθηκε για πράξεις επεξεργασίας που έλαβαν χώρα πριν από τη γενική εφαρμογή του ΓΚΠΔ (25 Μαΐου 2018) συνιστά ανοικτό ερώτημα. Λαμβάνοντας υπόψη την κυριολεκτική διατύπωση («πριν από»), απαιτείται μια ΕΑΠΔ μόνο για τις πράξεις που άρχισαν μετά τις 25 Μαΐου 2018 ή που υφίστανται σημαντικές μεταβολές μετά την ημερομηνία αυτή.

Δεδομένου ότι σε αυτές τις περιπτώσεις το σύστημα επεξεργασίας δεδομένων λειτουργεί ήδη, δεν είναι δυνατός ο προκαταρκτικός έλεγχος. Επιπλέον, αυτές οι ενέργειες δεν υπάρχουν σε ένα μη καθοριζόμενο χώρο (αν υποτεθεί ότι έχουν ληφθεί

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

υπόψη όλοι οι νομικοί κανονισμοί και οι απαιτήσεις υποβολής εκθέσεων του προηγουμένου νομικού πλαισίου).

Παρόλα αυτά, η Ομάδα Εργασίας 29 συνιστά θερμά την εφαρμογή της ΕΑΠΔ για συστήματα επεξεργασίας που ήδη τελούν εν λειτουργία, προκειμένου να αποφευχθούν νομικές ανακρίβειες και ακόμη και νομικές κυρώσεις.

2.4 Επανεξέταση της ΕΑΠΔ

Μετά τη διενέργεια μιας ΕΑΠΔ, η εφαρμογή των προτεινόμενων μέτρων πρέπει να επανεξετασθεί, εάν κρίνεται απαραίτητο. Ενδέχεται να είναι αναγκαία η επανεξέταση της επεξεργασίας δεδομένων για τον εντοπισμό τυχόν νέων στοιχείων των κινδύνων που σχετίζονται με την επεξεργασία των δεδομένων. Η αιτιολογική έκθεση 89 αναφέρει ότι μπορεί να χρειαστεί μια αναθεώρηση της ΕΑΠΔ σε εύθετο χρόνο μετά από μια πρώτη εκτίμηση. Κατά τη διενέργεια μιας ΕΑΠΔ, ένα χρονικό πλαίσιο για ελέγχους ρουτίνας ή μελλοντικές ανανεώσεις πρέπει να συμπεριληφθεί στην τεκμηρίωση.

Οι τεχνολογικές εξελίξεις, η νέα νομοθετική ρύθμιση και οι αλλαγές στις ρουτίνες επεξεργασίας πρέπει να εξεταστούν. Εάν προκύψει κίνδυνος, πρέπει να διενεργηθεί μια νέα ΕΑΠΔ.

Το καθήκον διενέργειας μια ΕΑΠΔ αποτελεί μέρος των υποχρεώσεων του υπευθύνου επεξεργασίας δεδομένων, που τεκμηριώνει τη λογοδοσία τους. Η τεκμηρίωση και η έκθεση δε θα πρέπει να παρέχουν μόνο πληροφορίες σχετικά με την ΕΑΠΔ που διενεργήθηκε αλλά επίσης να αναφέρουν τους λόγους για τους οποίους δε διενεργήθηκε μια πλήρης ΕΑΠΔ ή τερματίστηκε μια ΕΑΠΔ αφού εντοπίστηκαν υψηλοί κίνδυνοι για τα υποκείμενα των δεδομένων.

2.5 Διαβούλευση με την αρχή προστασίας δεδομένων σύμφωνα με το άρθρο 36 του ΓΚΠΔ

Ο υπεύθυνος της επεξεργασίας δεδομένων πρέπει να συμβουλευθεί την Αρχή Προστασίας Δεδομένων (DPA) σε περίπτωση που η ΕΑΠΔ αποκαλύπτει σημαντικούς κινδύνους και ο υπεύθυνος επεξεργασίας δε γνωρίζει τον τρόπο με τον οποίο μπορεί να λάβει οποιαδήποτε διορθωτικά μέτρα για τον μετριασμό των εν λόγω κινδύνων. Η ΑΠΔ οφείλει να απαντήσει σε αυτή την αίτηση διαβούλευσης εντός δεκατεσσάρων εβδομάδων. Για σύνθετα και καινοτόμα έργα, συνιστάται να ξεκινήσει μια ΕΑΠΔ το συντομότερο δυνατό, ώστε οποιαδήποτε πρόταση της ΑΠΔ να μπορεί να εξεταστεί κατά την εφαρμογή του σχεδίου του έργου.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.Ποιος είναι υπεύθυνος για τη διενέργεια μιας ΕΑΠΔ;

3.1Βάση

Η ευθύνη για τη διεξαγωγή μιας ΕΑΠΔ είναι του υπευθύνου επεξεργασίας- στην περίπτωση αυτή της τοπικής δημόσιας αρχής. Αρχικά, η πρόταση της Επιτροπής ανέθετε την ευθύνη για την ΕΑΠΔ στον εκτελούντα την επεξεργασία δεδομένων που ενεργούσε με εντολή του υπευθύνου επεξεργασίας. Αντίθετα, η αιτιολογική έκθεση 95 απλώς απαιτεί από τον εκτελούντα την επεξεργασία να επικουρεί τον υπεύθυνο επεξεργασίας όταν είναι απαραίτητο και κατόπιν αιτήσεως, στη διασφάλιση της τήρησης των υποχρεώσεων που απορρέουν από την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων.

Επομένως, στην πράξη θα είναι σκόπιμο να ζητηθεί συμβατικά από έναν εκτελούντα την επεξεργασία, εάν είναι διαθέσιμος και ήδη επιλεγμένος, να εμπλακεί και να υποστηρίξει ενεργά όλη τη διαδικασία ΕΑΠΔ. Αυτό είναι πέραν του άρθρου 28, παράγραφος 3 (στ), το οποίο προβλέπει ότι η σύμβαση για την επεξεργασία (ή άλλο νομικό όργανο) πρέπει να προβλέπει ότι ο εκτελών την επεξεργασία, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και των πληροφοριών που έχει στη διάθεσή του, θα διασφαλίσει τη συμμόρφωση προς τα άρθρα 32 έως 36. Συχνά, μόνο ο εκτελών την επεξεργασία θα έχει τις απαραίτητες πληροφορίες για να εκτιμήσει τις αντίστοιχες πτυχές της επεξεργασίας. Κατά την εκτίμηση, θα πρέπει να λαμβάνεται υπόψη ο κίνδυνος αποκάλυψης των εμπορικών και επιχειρηματικών απορρήτων. Και πάλι συνιστάται αντίστοιχος συμβατικός κανονισμός. Εάν προβλέπεται επεξεργασία δεδομένων από κοινού, η ΕΑΠΔ, σύμφωνα με το άρθρο 35, παρ. 1, εδάφιο 2, μπορεί επίσης να διενεργείται από έναν από τους υπευθύνους επεξεργασίας - κάτι το οποίο δεν απαλλάσσει τους υπολοίπους υπευθύνους επεξεργασίας από τις ευθύνες.

3.2 Συμμετοχή στην ΕΑΠΔ

Η ΕΑΠΔ πρέπει να οργανώνεται ως έργο και ως εκ τούτου θα πρέπει να εξοπλίζεται με τα απαραίτητα υλικά και ανθρώπινα μέσα από ένα αντίστοιχο υψηλό επίπεδο διοίκησης. Κατά την κατάρτιση της ομάδας του έργου πρέπει να δοθεί ιδιαίτερη προσοχή στην πολυπλοκότητα του έργου, στις απαιτούμενες εξειδικευμένες γνώσεις και στις απαιτούμενες γνώσεις σχετικά με το συγκεκριμένο έργο και το περιβάλλον του. Στην πράξη, μπορούν να συγκεντρωθούν μια ομάδα δικηγόρων, IT staff, CISO, υπεύθυνος προστασίας δεδομένων, το τμήμα που έχει αιτηθεί επεξεργασίας («κάτοχος δεδομένων») κ.λπ.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Ιδιαίτερη προσοχή δίνεται στη διασφάλιση της αποφυγής συγκρούσεων συμφερόντων. Συνεπώς, όσοι θα ασχοληθούν με την επεξεργασία δεδομένων στο μέλλον δε θα πρέπει να θεωρούνται ανεξάρτητοι, αλλά από την άλλη πλευρά μπορούν να παράσχουν πολύτιμες πληροφορίες για τον σχεδιασμό της εκτίμησης αντικτύπου ιδιωτικότητας. Η υλοποίηση μπορεί να γίνει από εσωτερική ομάδα καθώς και από εξωτερικά τρίτα μέρη. Ιδανικά, θα πρέπει να συμμετέχει ένας ανεξάρτητος φορέας.

Ο υπεύθυνος επεξεργασίας οφείλει να ζητήσει τη συμβουλή του Υπευθύνου Προστασίας Δεδομένων. Σύμφωνα με το άρθρο 39, παράγραφος 1 (γ), οι συμβουλές σχετικά με την ΕΑΠΔ και ο έλεγχος της εφαρμογής της περιλαμβάνονται μεταξύ των υποχρεωτικών καθηκόντων του ΥΠΔ, αλλά μόνο κατόπιν αιτήματος και όχι σε ηγετική θέση.

Συνεπώς, ο υπεύθυνος επεξεργασίας υποχρεούται να λαμβάνει τις συμβουλές του Υπευθύνου Προστασίας Δεδομένων. Το χρονικό σημείο και ο βαθμός στον οποίον ο υπεύθυνος προστασίας δεδομένων πρέπει να συμμετάσχει στη διαδικασία, συνιστούν απόφαση του υπευθύνου επεξεργασίας. Μια μεταγενέστερη επανεξέταση της τελικής έκθεσης θα ήταν επίσης επιθυμητή. Στην πράξη, συνιστάται θερμά η έγκαιρη συμμετοχή του υπευθύνου προστασίας δεδομένων, λόγω της εμπειρίας του.

Ανάλογα με τον οργανισμό του υπευθύνου επεξεργασίας, συνιστάται να εγκρίνεται η ΕΑΠΔ σε επίπεδο διαχείρισης ή από τον αντίστοιχο εξουσιοδοτημένο φορέα.

4. Πώς διενεργείται μια ΕΑΠΔ

4.1 Βάση

Πρέπει να επισημανθεί ότι ο ΓΚΠΔ δεν προβλέπει συγκεκριμένη μορφή ή συγκεκριμένη μέθοδο για τον σχεδιασμό μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, κάτι το οποίο επί του παρόντος συζητείται εντατικά σε εθνικό και ευρωπαϊκό επίπεδο. Η WP 29 δηλώνει ότι μπορούν να χρησιμοποιηθούν διαφορετικές επιλογές σχεδιασμού για να υποστηριχθεί η εφαρμογή των διατάξεων του ΓΚΠΔ και παραπέμπει σε παραδείγματα υφισταμένων (γενικών ή τομεακών) μοντέλων επεξεργασίας ΕΑΠΔ στο παράρτημα 1.1

[1] WP29, WP 248, 15: Διαφορετικές μεθοδολογίες (βλ. Παράρτημα 1 για παραδείγματα μεθόδων εκτίμησης αντίκτυπου προστασίας δεδομένων και ιδιωτικότητας) θα μπορούσαν να χρησιμοποιηθούν για την υποστηρίξουν την εφαρμογή των βασικών απαιτήσεων που ορίζονται στο ΓΚΠΔ (Παράρτημα 1).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.2 Εφαρμογή μιας ΕΑΠΔ

Συνεπώς, ο υπεύθυνος επεξεργασίας είναι βασικά ελεύθερος όσον αφορά στον τρόπο διενέργειας της επεξεργασίας ΕΑΠΔ και μπορεί να την προσαρμόσει στις υπάρχουσες εσωτερικές διαδικασίες, υπό την προϋπόθεση ότι η τοπική δημόσια αρχή λαμβάνει υπόψη τις τέσσερις απαιτήσεις που περιέχονται στο άρθρο 35 παράγραφος 7 του ΓΚΠΔ (α) έως (δ) ως ελάχιστες απαιτήσεις μιας ΕΑΠΔ, την οποία περιγράφει λεπτομερέστερα η ομάδα εργασίας του άρθρου 29 και λαμβάνει επιπλέον υπόψη το σημείο "τα ενδιαφερόμενα μέρη εμπλέκονται" (βλ. άρθρο 35 παρ. 2) και την άποψη των υποκειμένων των δεδομένων [βλ. άρθρο 35 παρ. 9]):

α) στη συστηματική περιγραφή των προβλεπομένων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

β) στην εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

γ) στην εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

δ) στα προβλεπόμενα μέτρα για την αντιμετώπιση των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων ασφαλείας και των μηχανισμών για την προστασία των δεδομένων προσωπικού χαρακτήρα και για την απόδειξη της συμμόρφωσης με τον παρόντα Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερομένων προσώπων.

4.3. Ελάχιστο περιεχόμενο μιας ΕΑΠΔ

Το άρθρο 35, παρ. 7, (α) έως (δ) του ΓΚΠΔ σε συνδυασμό με τις αιτιολογικές εκθέσεις 84 και 90 ορίζει ως ελάχιστα τα εξής:

α) συστηματική περιγραφή των προβλεπομένων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ·

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των διεργασιών επεξεργασίας σε συνάρτηση με τους σκοπούς ·

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

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, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων ασφαλείας και των μηχανισμών για την προστασία των δεδομένων προσωπικού χαρακτήρα και για την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερομένων προσώπων.

Τα σημεία (γ) και (δ) συνιστούν εκφάνσεις της λεγόμενης "προσέγγισης με βάση τον κίνδυνο" του ΓΚΠΔ και αφορούν όχι μόνο στην εφαρμογή της ΕΑΠΔ αλλά και στο πλαίσιο των άρθρων 24, 25 και 32 του ΓΚΠΔ. Με άλλα λόγια, η ΕΑΠΔ είναι ένα συγκεκριμένο παράδειγμα της προσέγγισης που βασίζεται στον κίνδυνο για την επεξεργασία δεδομένων, για τα δεδομένα -εν ολίγοις- που αναμένεται να συνεπάγονται υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ζητεί εκτενέστερη εκτίμηση κινδύνου και θεραπεία. Κατ 'αρχήν, όμως, οποιοσδήποτε άλλος έλεγχος παραδοχής της επεξεργασίας δεδομένων είναι εγγενής σε μια τέτοια εκτίμηση κινδύνου, συμπεριλαμβανομένων των κατάλληλων τεχνικών και οργανωτικών μέτρων που ελαχιστοποιούν τον κίνδυνο, πριν από την εφαρμογή τους (βλέπε μόνο το άρθρο 24 (1) του ΓΚΠΔ).

4.4 Η επεξεργασία ΕΑΠΔ

Η ΕΑΠΔ θα πρέπει να θεωρηθεί ως μια επεξεργασία (όχι μόνο ως μια έκθεση) που οφείλει να ξεκινήσει το συντομότερο δυνατόν προκειμένου να επηρεάσει το σχεδιασμό του αντικειμένου («έργου»). Ως εκ τούτου, η εκτίμηση αντικτύπου διαφέρει επίσης από έναν έλεγχο που αποτιμά ένα έργο εκ των υστέρων και συνήθως έρχεται πολύ αργά για να «απομακρύνει» τις ανάγκες προστασίας δεδομένων που πρέπει να παραγάγει η ΕΑΠΔ.

Υπάρχουν πολλές προτάσεις για την εφαρμογή μιας επεξεργασίας ΕΑΠΔ, οι οποίες κατά τον ένα ή τον άλλο τρόπο είναι παρόμοιες με τα αποτελέσματα της μελέτης PIAF (2012)2, η οποία απεικόνιζε τις μεθοδολογίες εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα σε επτά χώρες (συμπεριλαμβανομένης της κατάρτισης συστάσεων «Βέλτιστης Πρακτικής» και βασικών στοιχείων μιας διαδικασίας εκτίμησης αντικτύπου

[2] De Hert / Kloza / Wright (Hrsg), PIAF, Συστάσεις για ένα πλαίσιο εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα για την Ευρωπαϊκή Ένωση, Παραδοτέο D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf. Διαθέσιμο στο http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

σχετικά με την ιδιωτικότητα) για την Ευρωπαϊκή Επιτροπή, μεταξύ άλλων. Τα ακόλουθα βασικά στοιχεία εντοπίστηκαν:

1. Προσδιορισμός εάν απαιτείται PIA (πρωταρχική ανάλυση).

2. Προσδιορισμός της ομάδας PIA και καθορισμός όρων αναφοράς.

3. Περιγραφή του προτεινόμενου σχεδίου [και προσδιορισμός των ενδιαφερομένων].

4. Ανάλυση των ροών πληροφόρησης και άλλων αντικτύπων σχετικά με την ιδιωτικότητα.

5. Διαβούλευση με τους ενδιαφερομένους.

6. Διαχείριση κινδύνων [Προσδιορισμός κινδύνων και πιθανών λύσεων].

7. Έλεγχος συμμόρφωσης με το νόμο.

8. Διατύπωση συστάσεων.

9. Προετοιμασία και δημοσίευση της έκθεσης [π.χ. στην ιστοσελίδα του οργανισμού].

10. Εφαρμογή των συστάσεων.

11. Εξωτερική επισκόπηση ή / και έλεγχος [τρίτων].

12. Επανεξέταση της PIA εάν το σχετικό έργο αλλάξει [Ενημέρωση της PIA εάν υπάρχουν αλλαγές στο έργο].

Το μοντέλο ΕΑΠΔ για έξυπνα δίκτυα και συστήματα έξυπνης μέτρησης, το οποίο αναφέρεται ρητώς στη σύσταση 2014/724/ΕΕ της Ευρωπαϊκής Επιτροπής, προβλέπει τα ακόλουθα βήματα:3

1. Βήμα 1 Προ-αξιολόγηση και κριτήρια που καθορίζουν την ανάγκη διενέργειας μιας ΕΑΠΔ

2. Βήμα 2 Έναρξη

[3] Σύσταση 2014/724 / ΕΕ της Επιτροπής, της 10ης Οκτωβρίου 2014, σχετικά με το πρότυπο ετίμησης αντικτύπου σχετικά με την προστασία δεδομένων για το Έξυπνο Δίκτυο και τα Έξυπνα Συστήματα Μέτρησης, ABL L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Βήμα 3: Προσδιορισμός, χαρακτηρισμός και περιγραφή των συστημάτων έξυπνου δικτύου / εφαρμογών που επεξεργάζονται προσωπικά δεδομένα

4. Βήμα 4: Προσδιορισμός των σχετικών κινδύνων

5. Βήμα 5 Εκτίμηση κινδύνου σχετικά με την προστασία δεδομένων

6. Βήμα 6 Προσδιορισμός και σύσταση ελέγχων και υπολειπόμενοι κίνδυνοι

7. Βήμα 7 Τεκμηρίωση και σύνταξη της έκθεσης ΕΑΠΔ

8. Βήμα 8 Επισκόπηση και συντήρηση

Το νέο πρότυπο ISO / IEC 29134 παρέχει κατευθυντήριες γραμμές για μια διαδικασία διενέργειας αντικτύπου σχετικά με την ιδιωτικότητα και για τη δομή και το περιεχόμενο μιας έκθεσης PIA. Η διαδικασία χωρίζεται στις ακόλουθες τέσσερις υπο-κατηγορίες:

1. Πρωταρχική ανάλυση

2. Προετοιμασία της PIA

3. Εκτέλεση του PIA

4. Επικαιροποίηση της PIA

Σε ποια και σε πόσα μέρη χωρίζεται μια διαδικασία ΕΑΠΔ είναι μάλλον θέμα προτίμησης, περαιτέρω προτάσεις κυμαίνονται για παράδειγμα από τρεις ή τέσσερις φάσεις σε έξι έως επτά στάδια. Περισσότερο σημαντική είναι η κατανόηση της δομής και η επεξεργασία της διαδικασίας, η οποία λαμβάνει ιδίως υπόψη τις απαιτήσεις του άρθρου 35 (7) του ΓΚΠΔ και τις συστάσεις της Ομάδας Εργασίας του άρθρου 29.

4.5 Συμπερίληψη των υποκειμένων των δεδομένων και των εκπροσώπων τους

Σύμφωνα με το άρθρο 35 παράγραφος 9, ο υπεύθυνος επεξεργασίας θα ζητήσει, κατά περίπτωση, τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους σχετικά με την προβλεπόμενη διαδικασία, με την επιφύλαξη της προστασίας του εμπορικού ή του δημοσίου συμφέροντος ή της ασφάλειας των διεργασιών επεξεργασίας. Η συμπερίληψη της φράσης «κατά περίπτωση» στο πλαίσιο των τριμερών διαπραγματεύσεων δεν καθιστά σαφείς τις συγκεκριμένες συνθήκες υπό τις οποίες απαιτείται η παρουσία του ενδιαφερομένου ή του εκπροσώπου του και σε ποιες περιπτώσεις (επιτρεπτές) μπορεί αυτή να αγνοηθεί.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Η μορφή με την οποία ζητείται η γνωμοδότηση είναι ασαφής και η WP29 αναγνωρίζει διαφορετικούς τρόπους, όπως τη διεξαγωγή μελέτης (εσωτερικής ή εξωτερικής), επίσημων συνεντεύξεων με εκπροσώπους του προσωπικού ή συνδικάτων και την υποβολή ερωτηματολογίου σε μελλοντικούς πελάτες του υπευθύνου επεξεργασίας. Από την ίδια τη διατύπωση μπορεί να αντληθεί μόνο η άποψη (στην αρχική εκδοχή των κρατών μελών «της γνωμοδότησης»), αλλά όχι η υποχρέωση να λαμβάνεται υπόψη ή ακόμη και μια (νέα) απαίτηση συγκατάθεσης (πέραν του νόμου για τον Κανονισμό Εργασίας / Labour Constitution Act (ArbVG)) του συμβουλίου εργαζομένων ως εκπροσώπου των ενδιαφερομένων. Ο υπεύθυνος επεξεργασίας, ωστόσο, θα πρέπει να ασχοληθεί με τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους και θα πρέπει να τις λάβει υπόψη κατά την εκτίμηση αντικτύπου. Το αν οι οργανισμοί προστασίας καταναλωτών μπορούν επίσης να συμπεριληφθούν στον όρο «εκπρόσωπος» είναι αμφιλεγόμενο στη βιβλιογραφία.4

Εν πάση περιπτώσει, η υποχρέωση διαβούλευσης με ρητή δήλωση δεν θίγει την προστασία εμπορικών ή δημοσίων συμφερόντων ή την ασφάλεια των πράξεων επεξεργασίας. Συνεπώς, ο υπεύθυνος επεξεργασίας μπορεί να περιορίσει ή να αρνηθεί σε μεγάλο βαθμό την υποχρέωση ενημέρωσης των ενδιαφερομένων προσώπων ή των εκπροσώπων σχετικά με την προβλεπόμενη διαδικασία σύμφωνα με το άρθρο 35 (9) (η οποία, στην τελευταία περίπτωση, θα οδηγήσει στο να μην είναι δυνατή η συμμετοχή εκ των προτέρων υπό την έννοια του άρθρου 35 (9), δεδομένου ότι η ύπαρξη επαρκών πληροφοριών αποτελεί απαραίτητη προϋπόθεση για τη γνώμη των ενδιαφερομένων ή των εκπροσώπων τους).

Για την εφαρμογή της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, συνιστάται να τεκμηριώνεται στην έκθεση για αποδεικτικούς λόγους για ποιο λόγο έχει ληφθεί περιορισμένη άποψη σχετικά με το περιεχόμενο ή δεν έχει ληφθεί καμία ή για ποιο λόγο δεν έχει ληφθεί γνώμη ή έχει ληφθεί και έχει εξεταστεί μόνο εν μέρει.

4.6. Η έκθεση σχετικά με την εφαρμογή εκτίμησης αντικτύπου για την προστασία της ιδιωτικότητας

Θα πρέπει να σημειωθεί σε αυτό το σημείο ότι η έκθεση ΕΑΠΔ δεν είναι ο πραγματικός στόχος μιας ΕΑΠΔ, αλλά ένα «μέσο για τον τελικό σκοπό» , μια τεκμηρίωση της

4 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

διαδικασίας (εσωτερική και εξωτερική). Η υποβολή εκθέσεων δεν πρέπει να υποτιμάται - τεκμηριώνει την υλοποίηση και τα αποτελέσματα και μια απλή Η "PR DPIA report" πρέπει να αποφεύγεται για λόγους συμμόρφωσης. Η έκθεση μπορεί επίσης να χρησιμεύσει ως οδηγός και κατάλογος ελέγχου κατά τη διενέργεια της ΕΑΠΔ.

Το Άρθρο 35 του ΓΚΠΔ δεν περιέχει, απροσδόκητα κατά κάποιο τρόπο , καμία ρητή απαίτηση για την εκπόνηση έκθεσης σχετικά με τη διενέργεια της ΕΑΠΔ. Ωστόσο, το γεγονός ότι υπάρχει υποχρέωση τεκμηρίωσης από πλευράς υπευθύνου επεξεργασίας είναι αναμφισβήτητο και ακολουθεί σιωπηρά το άρθρο 35 παρ. 7 του ΓΚΠΔ καθώς και το άρθρο 5 παρ. 2 του ΓΚΠΔ (λογοδοσία) σε συνδυασμό με το άρθρο 24 παρ. 1 του ΓΚΠΔ και το άρθρο 36 (3) (ε) (που απαιτεί από τον επιβλέποντα να παράσχει "την εκτίμηση αντικτύπου προστασίας δεδομένων που αναφέρεται στο άρθρο 35"). Επίσης, η επανεξέταση που απαιτείται από το άρθρο 35 παρ. 11 για να εκτιμηθεί κατά πόσον η επεξεργασία διενεργείται σύμφωνα με την ΕΑΠΔ απαιτεί να διατηρηθούν τα αποτελέσματα της εκτίμησης αντικτύπου. Επιπλέον, η υποβολή εκθέσεων σχετικά με τις ΑΠΔ είναι σύμφωνη με την παγκόσμια ορθή πρακτική σε αυτόν τον τομέα (βλ. Το τμήμα IV.1 κατωτέρω), η οποία βασίζεται στην ΕΑΠΔ που προβλέπεται στο άρθρο 35 του ΓΚΠΔ.

Συνιστάται η συνοδευτική διαδικασία ΕΑΠΔ με τεκμηρίωση υπό την έννοια του «ζωντανού εγγράφου», αρχίζοντας με την τεκμηρίωση της πρωταρχικής ανάλυσης, σε περίπτωση που δεν είναι απαραίτητη η διενέργεια μιας ΕΑΠΔ. Ακόμη και αν αυτή η ανάλυση δείξει ότι δεν απαιτείται ΕΑΠΔ και η διαδικασία ανασταλεί, ο υπεύθυνος επεξεργασίας θα είναι υπεύθυνος για τη λογοδοσία και τα αποδεικτικά στοιχεία της. Η γραπτή αυτή τεκμηρίωση μπορεί να υποβληθεί στον επόπτη σε οποιαδήποτε μελλοντική διαδικασία και θα ανιχνεύει εσωτερικές θεωρήσεις και εκτιμήσεις.

Όσον αφορά στο περιεχόμενο, η έκθεση ΕΑΠΔ καθορίζει ουσιαστικά τη διαδικασία (συμπεριλαμβανομένης της παρουσίασης των γεγονότων με την έννοια της συστηματικής περιγραφής ολόκληρου του αντικειμένου της δοκιμής - «στόχος της αξιολόγησης») και τα αποτελέσματα της διενέργειας ΕΑΠΔ. Όπως και στην περίπτωση της ίδιας της διενέργειας ΕΑΠΔ, ο ΓΚΠΔ δεν προβλέπει ειδικούς κανόνες για το σχεδιασμό μιας έκθεσης ΕΑΠΔ. Ωστόσο, ως ελάχιστο περιεχόμενο, τα κριτήρια που απαριθμούνται στην Ομάδα Εργασίας του Άρθρου 29 για την προστασία δεδομένων στο Παράρτημα 2 WP 248, τα οποία βασίζονται ουσιαστικά στο Άρθρο 35 παρ. 7, είναι προκαθορισμένα. Το ISO / IEC 29134 συνιστά τα ακόλουθα περιεχόμενα της έκθεσης εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα, με έμφαση στην εκτίμηση των κινδύνων:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Σχετικές απαιτήσεις ιδιωτικότητας

2. Περιγραφή του πεδίου εφαρμογής

3. Περιγραφή των χρησιμοποιουμένων κριτηρίων κινδύνου

4. Συμμετέχοντες στην υλοποίηση

5. Διαβουλεύσεις με τους ενδιαφερομένους

Αυτό υποστηρίζεται επίσης από την αιτιολογική έκθεση 90, η οποία αναφέρει, μεταξύ άλλων, τα εξής: «Η εκτίμηση αντικτύπου πρέπει να περιλαμβάνει ιδίως τα προβλεπόμενα μέτρα, εγγυήσεις και μηχανισμούς που μετριάζουν αυτόν τον κίνδυνο, διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα και αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό».

Στην αναλυτική μελέτη PIAF, το ελάχιστο περιεχόμενο μιας έκθεσης ΑΠΔ έχει ως εξής:5

1. Εισαγωγή και πληροφορίες σχετικά με το ποιος έχει αναλάβει την ΕΑΠΔ, τα στοιχεία επικοινωνίας της και πού θα βρεθούν περισσότερες πληροφορίες και άλλες πηγές βοήθειας και συμβουλών

2. Περιγραφή του έργου, των ροών πληροφοριών και των αντικτύπων σχετικά με την ιδιωτικότητα

3. Αποτελέσματα της διαβούλευσης με τα ενδιαφερόμενα μέρη

4. Περιγραφή των φάσεων εκτίμησης κινδύνων και μετριασμού των κινδύνων, συμπεριλαμβανομένων των εναλλακτικών λύσεων που εξετάζονται

5. Ανάλυση της συμμόρφωσης με το νόμο

6. Συστάσεις

7. Παραρτήματα, εάν είναι απαραίτητο

Εάν είναι διαθέσιμη η έκθεση ή το τελικό σχέδιο, μπορεί να προκύψει το ερώτημα σχετικά με το τι πρέπει να γίνει με τον υπεύθυνο (εσωτερικά), κυρίως εάν και από ποιον

[5] De Hert / Kloza / Wright (Hrsg), PIAF, Συστάσεις για ένα πλαίσιο εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα για την Ευρωπαϊκή Ένωση, Παραδοτέο D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf. Διαθέσιμο στο http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

πρόκειται να «εγκριθεί» - ένα πρακτικά σημαντικό σημείο το οποίο παραμένει ασαφές στον ΓΚΠΔ. Το ICO ορίζει ρητώς στον Κώδικα Πρακτικής του τα εξής: «να εξασφαλισθεί η κατάλληλη υπογραφή στο πλαίσιο του οργανισμού». Δεδομένου ότι ο υπεύθυνος πρέπει να διενεργήσει την ΕΑΠΔ, προκύπτει ότι οι αρμόδιοι εκπρόσωποι του υπευθύνου προσώπου εμπλέκονται στην ΕΑΠΔ και έχουν επίσης την τελική ευθύνη. Οι υπεύθυνοι διαχείρισης θα έχουν συνήθως την τελική ευθύνη λήψης αποφάσεων σχετικά με το θέμα και τη φύση του έργου ΕΑΠΔ. Ως ελάχιστη παραλλαγή, ο υπεύθυνος διαχείρισης έργου ή υπεύθυνος προστασίας δεδομένων οφείλουν να αναφέρουν στο «ανώτατο επίπεδο διαχείρισης», όπως προβλέπεται στο άρθρο 38 (3) του ΓΚΠΔ.

Ο ΓΚΠΔ δεν έχει καμία υποχρέωση δημοσίευσης της ΕΑΠΔ, αλλά η WP29 συνιστά τη δημοσίευσή της (τουλάχιστον εν μέρει) προκειμένου να αυξηθεί η εμπιστοσύνη στην επεξεργασία δεδομένων και να προωθηθεί η διαφάνεια. Συγκεκριμένα, η δημοσίευση ενθαρρύνεται σε περιπτώσεις όπου ένα μέρος του κοινού θα επηρεαστεί από την (προγραμματισμένη) διαδικασία.

5. Συμπεράσματα και πρακτικές συμβουλές

Ειδικότερα, οι ρυθμιστικοί οργανισμοί με επαρκείς πόρους έχουν αναπτύξει τις δικές τους προσεγγίσεις για την εκτίμηση αντικτύπου σχετικά με την ιδιωτικότητα κατά τη διάρκεια των ετών. Σύμφωνα με την τωρινή προοπτική, αναμένεται ότι οι αρχές προστασίας δεδομένων που έχουν ήδη αναπτύξει το δικό τους μοντέλο θα το προτιμήσουν ή θα το διαδώσουν, κυρίως επειδή η γνώση της αντίστοιχης εποπτικής αρχής σχετικά με τις δικές τους συστάσεις θα είναι πιο σαφής. Το περιεχόμενο των επί του παρόντος διαθέσιμων μοντέλων εθνικών εποπτικών αρχών (από κράτη μέλη της ΕΕ) συχνά προηγείται του ΓΚΠΔ και δεν έχει προσαρμοστεί (ακόμη) συστηματικά στις απαιτήσεις ή την ορολογία του ΓΚΠΔ.

Πάντως, ο ICO πρόσθεσε τον Κώδικα Πρακτικής ΑΠΔ (2014) στην (αξιοπρόσεκτη) έκθεση σχετικά με «μεγάλα δεδομένα, τεχνητή νοημοσύνη, μηχανική μάθηση και προστασία δεδομένων» στις απαιτήσεις και την ορολογία του ΓΚΠΔ, κάτι που αναμένεται και από τις άλλες αρχές προστασίας δεδομένων. Επίσης, αναμένεται να φανεί εάν το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (Άρθρο 68) θα παράσχει κατευθυντήριες γραμμές, συστάσεις ή / και βέλτιστες πρακτικές για την ΕΑΠΔ σύμφωνα με το Άρθρο 70 (1) (ε).

Συστάσεις με μια ματιά:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Τεκμηρίωση όλων των αποφάσεων, ιδίως γιατί δεν έχει διενεργηθεί ΕΑΠΔ (εάν είναι εφαρμόσιμη)

Σε περίπτωση αμφιβολίας, πραγματοποιήστε μια ΕΑΠΔ

Συμμετοχή εσωτερικών και εξωτερικών ενδιαφερομένων

Χρήση των προτύπων, των βέλτιστων πρακτικών και, ανάλογα με την περίπτωση, των παρόμοιων ΕΑΠΔ που έχουν ήδη τεθεί σε ισχύ

Δημοσίευση της ΕΑΠΔ

α) Ειδικά από τις δημόσιες αρχές

β) Δημιουργεί και αυξάνει την εμπιστοσύνη στην ιδιωτική ζωή.

6. Εξωτερικές πηγές και σύνδεσμοι

6.1. Βιβλία και άρθρα

Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

De Hert, Paul/Kloza, Dariusz/Wright, David, Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf

Wright, David/De Hert, Paul (Ed.), Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012

De Hert/Kloza/Wright (Ed.), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Martini in Paal/Pauly (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2 Αρχεία Working Party Άρθρου 29

Artikel-29-Working Party, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

6.3. Διαδικτυακοί σύνδεσμοι

Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/

ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).