ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Διπλωματική Διατριβή με θέμα:

Μεθοδολογίες Εκπόνησης Εκτίμησης Αντικτύπου: Μία επισκόπηση

Δεσποτίδη Χαρίκλεια

Επιβλέπων Καθηγητής:

Γκρίτζαλης Στέφανος

ΠΕΙΡΑΙΑΣ

ΦΕΒΡΟΥΑΡΙΟΣ 2023

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μεθοδολογίες Εκπόνησης Εκτίμησης Αντικτύπου: Μία επισκόπηση

Δεσποτίδη Χαρίκλεια
Α.Μ.: MTE2006

ΠΕΡΙΛΗΨΗ

Ο ΓΚΠΔ απαιτεί την αξιολόγηση και τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA) για την επεξεργασία δεδομένων προσωπικού χαρακτήρα που μπορεί να οδηγήσει σε υψηλό κίνδυνο και αντίκτυπο για τα υποκείμενα των δεδομένων. Η τεκμηρίωση αυτής της διαδικασίας απαιτεί πληροφορίες σχετικά με τις δραστηριότητες επεξεργασίας, τις οντότητες και τους ρόλους τους, τους κινδύνους, τους μετριασμούς και τις επιπτώσεις που προκύπτουν, και τις διαβουλεύσεις. Οι μέθοδοι αξιολόγησης των επιπτώσεων στην ιδιωτικότητα καθοδηγούν την εφαρμογή των αρχών της προστασίας της ιδιωτικότητας από τον σχεδιασμό και προβλέπονται στον Γενικό Κανονισμό της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων. Καθώς η εφαρμογή μιας εκτίμησης αντικτύπου εξακολουθεί να αποτελεί ένα περίπλοκο έργο για τους οργανισμούς, η παρούσα εργασία παρέχει μια κριτική επισκόπηση και αξιολόγηση των γενικών μεθόδων DPIA που προτείνονται από σχετικές έρευνες, τις Αρχές Προστασίας Δεδομένων και τους Οργανισμούς Τυποποίησης. Το πλαίσιο αξιολόγησης βασίζεται σε ένα ολοκληρωμένο σύνολο κριτηρίων που προέκυψαν μέσω συστηματικής ανάλυσης της σχετικής βιβλιογραφίας, ενώ εντοπίζονται επίσης στοιχεία των μεθόδων PIA που χρήζουν περαιτέρω υποστήριξης ή αποσαφήνισης, καθώς και ζητήματα που παραμένουν ακόμη ανοικτά, όπως η ανάγκη εφαρμογής υποστηρικτικών εργαλείων.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Εκτίμηση αντικτύπου στην ιδιωτική ζωή (DPIA), κίνδυνοι για την ιδιωτική ζωή, κριτήρια αξιολόγησης, ΓΚΠΔ, μεθοδολογία, επεξεργασία

ABSTRACT

The GDPR requires a data protection impact assessment (DPIA) to be carried out for the processing of personal data that may result in a high risk and impact for data subjects. Documenting this process requires information on processing activities, entities and their roles, risks, mitigations, and impacts arising, and consultations. Privacy impact assessment methods guide the application of privacy principles by design and are provided for in the EU General Data Protection Regulation. As the implementation of an impact assessment is still a complex task for organizations, this paper provides a critical review and evaluation of generic DPIA methods proposed by relevant research, data protection authorities and standardization agencies. The evaluation framework is based on a comprehensive set of criteria derived through a systematic analysis of the relevant literature and identifies elements of PIA methods that need further support or clarification, as well as issues that remain open, such as the need to implement supporting tools.

KEYWORDS: Privacy impact assessment (DPIA), privacy risks, assessment criteria, GDPR, methodology, processing

ΕΥΧΑΡΙΣΤΙΕΣ

Για τη διεκπεραίωση της παρούσας εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της παρούσας εργασίας κ.Στέφανο Γκρίτζαλη του τμήματος Ψηφιακών Συστημάτων του Πανεπιστήμιου Πειραιά για την υποστήριξη και την καθοδήγηση του κατά την διάρκεια εκπόνησης της διπλωματικής εργασίας. Ακόμα,θα ήθελα να ευχαριστήσω το σύνολο των καθηγητών του Προγράμματος.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια και τους φίλους μου, για την ενθάρρυνση και την συμπαράσταση τους.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

1. Εισαγωγή

Η Εκτίμηση Αντικτύπου στην Ιδιωτικότητα (Privacy Impact Assessment, PIA) είναι ένα σύστημα έγκαιρης προειδοποίησης Early Warning System [1]:

- για την αποτίμηση των δυνητικών επιπτώσεων στην ιδιωτικότητα από διαδικασίες, πληροφοριακά συστήματα, προγράμματα, τμήματα λογισμικού, συσκευές, ή άλλες συνιστώσες που επεξεργάζονται αναγνωριστικά στοιχεία ταυτότητας PII (Personally Identifiable Information) και
- για τη λήψη των αναγκαίων μέτρων για την αντιμετώπιση της επικινδυνότητας ιδιωτικότητας (Privacy risk), μετά από διαβούλευση με δικαιούχους.

Πιο συγκεκριμένα, η αναφορά της Εκτίμησης Αντικτύπου στην Ιδιωτικότητα περιλαμβάνει τεκμηρίωση για τα μέτρα που λήφθηκαν για την αντιμετώπιση της επικινδυνότητας, ενώ αξίζει να σημειωθεί ότι η δεν είναι απλώς ένα εργαλείο, αλλά μια διαδικασία που εκκινεί ήδη από τα αρχικά στάδια μιας πρωτοβουλίας όταν υπάρχει η δυνατότητα διαμόρφωσης των αποτελεσμάτων της, ώστε να επιτευχθεί ιδιωτικότητα από τον σχεδιασμό (Privacy by Design).

Τέλος, η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (DPIA) είναι ένας τρόπος για να αναλυθεί συστηματικά και διεξοδικά η επεξεργασία δεδομένων προσωπικού χαρακτήρα με σκοπό τον εντοπισμό και τη ελαχιστοποίηση των κινδύνων για την προστασία των δεδομένων. Οι υπεύθυνοι επεξεργασίας (Controllers), όσοι εμπλέκονται στον καθορισμό του τρόπου και του λόγου επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, πρέπει να διενεργούν DPIA για κάθε επεξεργασία που «ενδέχεται να προκαλέσει υψηλό κίνδυνο για τα άτομα», συμπεριλαμβανομένων ορισμένων συγκεκριμένων τύπων επεξεργασίας.

2. Τι είναι η εκτίμηση αντικτύπου για την προστασία δεδομένων;

Όταν ένας υπεύθυνος επεξεργασίας συλλέγει, αποθηκεύει ή χρησιμοποιεί (δηλαδή «επεξεργάζεται») δεδομένα προσωπικού χαρακτήρα, τα άτομα των οποίων τα δεδομένα υποβάλλονται σε επεξεργασία εκτίθενται σε κινδύνους. Οι κίνδυνοι αυτοί μπορεί να κυμαίνονται από την κλοπή ή την ακούσια δημοσιοποίηση προσωπικών δεδομένων και τη χρήση τους από εγκληματίες για να υποδυθούν το άτομο, έως την ανησυχία των ατόμων ότι τα δεδομένα τους θα χρησιμοποιηθούν για άγνωστους σκοπούς [2]. Επομένως, η DPIA, περιγράφει μια διαδικασία που αποσκοπεί στον εντοπισμό των κινδύνων που απορρέουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και στην ελαχιστοποίηση των κινδύνων αυτών όσο το δυνατόν περισσότερο και νωρίτερα. Οι DPIA είναι σημαντικά εργαλεία για την εξάλειψη των κινδύνων και για την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ. Η παρούσα καθοδήγηση προϋποθέτει ότι η DPIA θα διεξαχθεί για ένα καθορισμένο έργο και όχι για το σύνολο των δραστηριοτήτων ενός οργανισμού. Ως έργο μπορεί να θεωρηθεί μια συγκεκριμένη λειτουργία του οργανισμού ή ένα πρόγραμμα αλλαγών στις λειτουργίες του οργανισμού συνολικά.

2.1 Ποια είναι τα οφέλη από τη διενέργεια DPIA;

Η διενέργεια DPIA δύναται να βελτιώσει την ευαισθητοποίηση σχετικά με τους κινδύνους προστασίας δεδομένων που συνδέονται με ένα έργο. Αδιαμφισβήτητα, αυτό θα συμβάλει στη βελτίωση του σχεδιασμού του έργου και θα ενισχύσει την επικοινωνία σχετικά με τους κινδύνους προστασίας δεδομένων με τα ενδιαφερόμενα μέρη. Παρακάτω παρατίθενται ορισμένα από τα οφέλη της διενέργειας μιας DPIA, τα οποία περιλαμβάνουν [3]:

- Διασφάλιση και απόδειξη της συμμόρφωσης του οργανισμού με τον ΓΚΠΔ με απόρροια την αποφυγή κυρώσεων.
- Έμπνευση εμπιστοσύνης στο κοινό με τη βελτιστοποίηση της επικοινωνίας για θέματα προστασίας δεδομένων.
- Διασφάλιση ότι οι χρήστες/πελάτες δεν κινδυνεύουν από πιθανή παραβίαση των προσωπικών τους δεδομένων.
- Παρέχεται η δυνατότητα στον οργανισμό να ενσωματώσει την «προστασία των δεδομένων μέσω του σχεδιασμού» σε νέα έργα.

- Μείωση των κινδύνων που σχετίζονται με την προστασία των δεδομένων για τον οργανισμό.
- Μείωση του κόστους λειτουργίας με τη βελτιστοποίηση των ροών πληροφοριών στο πλαίσιο ενός έργου και την εξάλειψη της περιττής συλλογής και επεξεργασίας δεδομένων.
- Μείωση του κόστους και της διακοπής των προστατευτικών μέτρων για την προστασία των δεδομένων με την ενσωμάτωση τους στο σχεδιασμό του έργου σε πρώιμο στάδιο.

Αξίζει να σημειωθεί πως ο όρος «προστασία των δεδομένων μέσω του σχεδιασμού» που χρησιμοποιήθηκε παραπάνω ή αλλιώς «privacy by design [3]», περιλαμβάνει την ενσωμάτωση χαρακτηριστικών προστασίας της ιδιωτικής ζωής και τεχνολογιών ενίσχυσης της ιδιωτικής ζωής των δεδομένων κατά την διαδικασία του σχεδιασμού, σε πρώιμο στάδιο. Αυτό θα συμβάλει στη διασφάλιση καλύτερης και αποδοτικής προστασίας της ιδιωτικής ζωής των υποκειμένων των δεδομένων.

2.2 Πότε χρειάζεται να διενεργηθεί DPIA [1];

Σύμφωνα με τον ΓΚΠΔ, η διενέργεια DPIA είναι υποχρεωτική όταν η επεξεργασία δεδομένων «ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων». Αυτό είναι ιδιαίτερα σημαντικό όταν εισάγεται μια νέα τεχνολογία επεξεργασίας δεδομένων. Σε περιπτώσεις όπου δεν είναι σαφές εάν η DPIA είναι αυστηρά υποχρεωτική, η διενέργεια DPIA εξακολουθεί να αποτελεί ορθή πρακτική και χρήσιμο εργαλείο που βοηθά τους υπευθύνους επεξεργασίας δεδομένων να συμμορφώνονται με τη νομοθεσία περί προστασίας δεδομένων.

Εκτός από τους Γενικούς Κανόνες που περιγράφουν πότε απαιτείται η διενέργεια μιας DPIA, το Άρθρο 35 παράγραφος 4 του ΓΚΠΔ προσδιορίζει ορισμένους τύπους επεξεργασίας για τους οποίους η διενέργεια DPIA θεωρείται υποχρεωτική και αυτοί είναι οι εξής:

1. Χρήση δεδομένων προσωπικού χαρακτήρα σε μεγάλη κλίμακα για σκοπό(-ους) διαφορετικό(-ους) από αυτόν(-ους) για τον οποίο συλλέχθηκαν αρχικά σύμφωνα με το άρθρο 6 παράγραφος 4 του ΓΚΠΔ.
2. Δημιουργία προφίλ ευάλωτων ατόμων, συμπεριλαμβανομένων των παιδιών, για τη στόχευση του μάρκετινγκ ή των διαδικτυακών υπηρεσιών στα άτομα αυτά.

3. Profiling, χρήση αλγοριθμικών μέσων ή δεδομένων ειδικής κατηγορίας ως στοιχείο για τον καθορισμό της πρόσβασης σε υπηρεσίες ή ότι έχει ως αποτέλεσμα νομικά ή παρόμοια σημαντικά αποτελέσματα.
4. Συστηματική παρακολούθηση, εντοπισμός, καταγραφή της θέσης ακόμα και της συμπεριφοράς ατόμων.
5. Σκιαγράφηση προφίλ ατόμων σε μεγάλη κλίμακα.
6. Επεξεργασία βιομετρικών δεδομένων για τη μοναδική ταυτοποίηση ενός ατόμου για να καταστεί δυνατή ή να επιτραπεί η ταυτοποίηση/ αυθεντικοποίηση ενός ατόμου σε συνδυασμό με άλλα κριτήρια που ορίζονται στις κατευθυντήριες γραμμές DPIA της WP29, τα οποία θα αναλυθούν σε επόμενη ενότητα.
7. Επεξεργασία γενετικών δεδομένων σε συνδυασμό με οποιοδήποτε από τα κριτήρια που ορίζονται στις κατευθυντήριες γραμμές DPIA της WP29.
8. Έμμεση άντληση δεδομένων προσωπικού χαρακτήρα όταν δεν πληρούνται οι απαιτήσεις διαφάνειας του ΓΚΠΔ, συμπεριλαμβανομένης της επίκλησης απαλλαγής λόγω αδυναμίας ή δυσανάλογης προσπάθειας.
9. Συνδυασμός, συσχέτιση ή αντιπαραβολή ξεχωριστών συνόλων δεδομένων, όπου η διασύνδεση αυτή συμβάλλει σημαντικά στην κατάρτιση προφίλ (profiling), χρησιμοποιείται για την κατάρτιση προφίλ, στην συμπεριφοριστική ανάλυση των ατόμων ιδιαίτερα όταν τα σύνολα δεδομένων συνδυάζονται από διαφορετικές πηγές όπου η επεξεργασία πραγματοποιήθηκε/επιτελείται για διαφορετικούς σκοπούς ή από διαφορετικούς υπευθύνους επεξεργασίας.
10. Επεξεργασία δεδομένων προσωπικού χαρακτήρα μεγάλης κλίμακας όπου ο νόμος περί προστασίας δεδομένων του 2018 απαιτεί τη λήψη «κατάλληλων και ειδικών μέτρων» για τη διασφάλιση των θεμελιωδών δικαιωμάτων και ελευθεριών των ατόμων.

Στο πλαίσιο αυτό, ο ΓΚΠΔ παρέχει διεξοδικά παραδείγματα για το πότε η επεξεργασία δεδομένων «ενδέχεται να οδηγήσει σε υψηλούς κινδύνους», δείγμα των οποίων παρατίθεται παρακάτω προκειμένου να γίνει αντιληπτή σε μεγαλύτερο βαθμό η κρισιμότητα της επεξεργασίας δεδομένων των υποκειμένων. Συγκεκριμένα [2]:

- «Συστηματική και εκτεταμένη αξιολόγηση προσωπικών δεδομένων που αφορούν 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 επηρεάζουν ομοίως σημαντικά το φυσικό πρόσωπο»

- «Επεξεργασία σε μεγάλη κλίμακα 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»
- «Η συστηματική παρακολούθηση μιας δημόσιας προσβάσιμης περιοχής σε μεγάλη κλίμακα»

Η ομάδα εργασίας του άρθρου 29, αποτελούμενη από τους εκπροσώπους κάθε Αρχής Προστασίας Δεδομένων στην ΕΕ, ενέκρινε τις κατευθυντήριες γραμμές σχετικά με τις DPIA και το κατά πόσον η επεξεργασία ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τους σκοπούς του ΓΚΠΔ. Οι εν λόγω κατευθυντήριες γραμμές εγκρίθηκαν στη συνέχεια από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB), το οποίο αντικατέστησε την ομάδα εργασίας του άρθρου 29. Κατά την αξιολόγηση του κατά πόσον η επεξεργασία ενδέχεται να οδηγήσει σε υψηλό κίνδυνο, οι κατευθυντήριες γραμμές καθορίζουν τα ακόλουθα κριτήρια που πρέπει να ληφθούν υπόψη:

1. Αξιολόγηση ή βαθμολόγηση

Αξιολόγηση ή βαθμολόγηση, συμπεριλαμβανομένης της κατάρτισης προφίλ και της πρόβλεψης, ιδιαίτερα «από πτυχές που αφορούν την απόδοση του υποκειμένου των δεδομένων στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή τα ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, την τοποθεσία ή τις μετακινήσεις» (αιτιολογικές σκέψεις 71 και 91 ΓΚΠΔ). Χαρακτηριστικά παραδείγματα αυτού του είδους αποτελεί μια τράπεζα που ελέγχει τους πελάτες της βάσει μια βάση δεδομένων πιστωτικών στοιχείων, μια εταιρεία βιοτεχνολογίας που προσφέρει γενετικές εξετάσεις στους καταναλωτές προκειμένου να αξιολογήσει και να προβλέψει τους κινδύνους ασθένειας/υγείας, μια εταιρεία που δημιουργεί προφίλ συμπεριφοράς ή μάρκετινγκ με βάση τη χρήση και την πλοήγηση στον ιστότοπο της.

2. Αυτοματοποιημένη λήψη αποφάσεων με σημαντικά αποτελέσματα

Αυτοματοποιημένη λήψη αποφάσεων με νομικά ή παρόμοια σημαντικά αποτελέσματα ή επεξεργασία που αποσκοπεί στη λήψη αποφάσεων σχετικά με τα υποκείμενα των δεδομένων που παράγουν «νομικά αποτελέσματα που αφορούν το φυσικό πρόσωπο» ή που «επηρεάζουν παρόμοια σημαντικά το φυσικό πρόσωπο» (άρθρο 35 παράγραφος 3 στοιχείο α) ΓΚΠΔ). Για παράδειγμα, σε περίπτωση που η επεξεργασία μπορεί να οδηγήσει σε αποκλεισμό ή διάκριση εις βάρος ατόμων. Αξίζει να σημειωθεί ότι η διαδικασία επεξεργασίας με μικρή ή μηδενική επίδραση στα άτομα δεν ανταποκρίνεται στο συγκεκριμένο κριτήριο.

3. Συστηματική παρακολούθηση

Επεξεργασία που χρησιμοποιείται για την παρατήρηση, την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, συμπεριλαμβανομένων των δεδομένων που συλλέγονται μέσω «συστηματικής παρακολούθησης ενός δημόσια προσβάσιμου χώρου» (άρθρο 35 παράγραφος 3 στοιχείο γ) ΓΚΠΔ). Αυτός ο τύπος παρακολούθησης αποτελεί κριτήριο, διότι τα δεδομένα προσωπικού χαρακτήρα ενδέχεται να συλλέγονται σε συνθήκες όπου τα υποκείμενα των δεδομένων ενδέχεται να μην γνωρίζουν ποιος συλλέγει τα δεδομένα τους και πώς θα χρησιμοποιηθούν. Επιπλέον, μπορεί να είναι αδύνατο για τα άτομα να αποφύγουν να υποβληθούν σε μια τέτοια επεξεργασία σε δημόσιο (ή δημόσια προσβάσιμο) χώρο (ή χώρους).

4. Ευαίσθητα προσωπικά δεδομένα

Ευαίσθητα δεδομένα, τα οποία περιλαμβάνουν ειδικές κατηγορίες δεδομένων όπως ορίζονται στο άρθρο 9 του ΓΚΠΔ (για παράδειγμα πληροφορίες σχετικά με τις πολιτικές απόψεις των ατόμων), καθώς και δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες ή αδικήματα. Ως παράδειγμα μπορεί να θεωρηθεί ένα γενικό νοσοκομείο που τηρεί τα ιατρικά αρχεία των ασθενών ακόμα και ένας ιδιωτικός ερευνητής που διατηρεί τα στοιχεία των παραβατών. Το κριτήριο αυτό περιλαμβάνει επίσης δεδομένα τα οποία μπορούν να θεωρηθούν γενικότερα ότι αυξάνουν τον πιθανό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων, όπως δεδομένα ηλεκτρονικών επικοινωνιών, δεδομένα θέσης, οικονομικά δεδομένα, τα οποία δυνητικά θα μπορούσαν να χρησιμοποιηθούν για απάτη πληρωμών. Από την άποψη αυτή, το κατά πόσον τα δεδομένα έχουν ήδη δημοσιοποιηθεί μπορεί να θεωρηθεί παράγοντας στην αξιολόγηση, εάν τα δεδομένα αναμένεται να χρησιμοποιηθούν περαιτέρω για ορισμένους σκοπούς. Επιπλέον, το κριτήριο αυτό μπορεί να περιλαμβάνει πληροφορίες που επεξεργάζεται ένα φυσικό πρόσωπο κατά τη διάρκεια μιας καθαρά προσωπικής ή οικιακής δραστηριότητας, όπως υπηρεσίες υπολογιστικού νέφους για τη διαχείριση προσωπικών εγγράφων, υπηρεσίες ηλεκτρονικού ταχυδρομείου, ημερολόγια, ηλεκτρονικοί αναγνώστες εξοπλισμένοι με λειτουργίες καταγραφής σημειώσεων και διάφορες εφαρμογές καταγραφής ζωής που μπορεί να περιέχουν πολύ προσωπικές πληροφορίες, των οποίων η αποκάλυψη ή η επεξεργασία για οποιονδήποτε άλλο σκοπό εκτός των οικιακών δραστηριοτήτων μπορεί να θεωρηθεί πολύ παρεμβατική.

5. Επεξεργασία δεδομένων σε μεγάλη κλίμακα

Ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλης κλίμακας αν και η αιτιολογική σκέψη 91 του ΓΚΠΔ παρέχει ορισμένες οδηγίες. Σε κάθε περίπτωση, οι κατευθυντήριες γραμμές του

WP29/EDPB συνιστούν να λαμβάνονται υπόψη ιδίως οι ακόλουθοι παράγοντες κατά τον προσδιορισμό του κατά πόσον η επεξεργασία πραγματοποιείται σε μεγάλη κλίμακα:

- Ο αριθμός των ενδιαφερόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού.
- Ο όγκος των δεδομένων ή και το εύρος των διαφορετικών δεδομένων που υποβάλλονται σε επεξεργασία.
- Η διάρκεια ή η μονιμότητα της δραστηριότητας επεξεργασίας δεδομένων.
- Η γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

Σύνολα δεδομένων που έχουν αντιστοιχιστεί ή συνδυαστεί, για παράδειγμα προερχόμενα από δύο ή περισσότερες πράξεις επεξεργασίας δεδομένων που εκτελούνται για διαφορετικούς σκοπούς ή από διαφορετικούς υπευθύνους επεξεργασίας δεδομένων κατά τρόπο που υπερβαίνει τις προβλεπόμενες προσδοκίες του υποκειμένου των δεδομένων.

6. Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων

Η επεξεργασία αυτού του τύπου δεδομένων μπορεί να απαιτεί DPIA λόγω της αυξημένης ανισορροπίας ισχύος μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, πράγμα που σημαίνει ότι το άτομο μπορεί να μην είναι σε θέση να συναινέσει ή να αντιταχθεί στην επεξεργασία των δεδομένων του (αιτιολογική σκέψη 75 ΓΚΠΔ). Για παράδειγμα, οι εργαζόμενοι συχνά αντιμετωπίζουν σοβαρές δυσκολίες και υπόκεινται σε ανισορροπία ισχύος όταν προσπαθούν να αντιταχθούν στην επεξεργασία που διενεργεί ο εργοδότης τους στις περιπτώσεις που συνδέεται με τη διαχείριση των ανθρώπινων πόρων. Παρομοίως, τα παιδιά δεν μπορεί να θεωρηθεί ότι είναι σε θέση να αντιταχθούν με επίγνωση ή να συναινέσουν στην επεξεργασία των δεδομένων τους. Αυτό επηρεάζει επίσης τις πιο ευάλωτες ομάδες του πληθυσμού που χρήζουν ειδικής προστασίας, όπως για παράδειγμα οι ψυχικά ασθενείς, οι αιτούντες άσυλο, οι ηλικιωμένοι ή σε κάθε περίπτωση όπου μπορεί να εντοπιστεί ανισορροπία ισχύος στη σχέση μεταξύ της κατάστασης του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας.

7. Καινοτομία και τεχνολογία

Καινοτόμος χρήση ή εφαρμογή τεχνολογικών και οργανωτικών λύσεων, όπως ο συνδυασμός της χρήσης δεδομένων αναγνώρισης δακτυλικών αποτυπωμάτων και του προσώπου για βελτιωμένους ελέγχους φυσικής πρόσβασης. Ο ΓΚΠΔ καθιστά σαφές (άρθρο 35 παράγραφος 1 και αιτιολογικές σκέψεις 89 και 91 ΓΚΠΔ) ότι η χρήση μιας νέας τεχνολογίας μπορεί να προκαλέσει την ανάγκη διενέργειας DPIA. Αυτό οφείλεται στο

γεγονός ότι η χρήση μιας νέας τεχνολογίας μπορεί να συνεπάγεται νέες μορφές συλλογής και χρήσης δεδομένων με ενδεχομένως υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Πράγματι, οι προσωπικές και κοινωνικές συνέπειες της ανάπτυξης μιας νέας τεχνολογίας μπορεί να είναι άγνωστες, ενώ αξίζει να τονιστεί πως μια DPIA θα βοηθήσει τον υπεύθυνο επεξεργασίας δεδομένων να κατανοήσει και να αντιμετωπίσει αυτούς τους κινδύνους. Για παράδειγμα, ορισμένες εφαρμογές του «Διαδικτύου των πραγμάτων» θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην καθημερινή και την ιδιωτική ζωή των ατόμων και, ως εκ τούτου, απαιτούν DPIA.

8. Διεθνείς μεταφορές

Αφορά την διαβίβαση δεδομένων εκτός συνόρων της Ευρωπαϊκής Ένωσης (αιτιολογική σκέψη 116), λαμβάνοντας υπόψη την προβλεπόμενη χώρα ή τις προβλεπόμενες χώρες προορισμού, τη δυνατότητα περαιτέρω διαβιβάσεων ή την πιθανότητα διαβιβάσεων βάσει παρεκκλίσεων για ειδικές καταστάσεις που προβλέπονται από τον ΓΚΠΔ.

9. Δικαιώματα και συμβατικές υποχρεώσεις

Όταν η επεξεργασία αυτή καθαυτή «εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν ένα δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή μια σύμβαση» (άρθρο 22 και αιτιολογική σκέψη 91 ΓΚΠΔ). Αυτό περιλαμβάνει την επεξεργασία που πραγματοποιείται σε δημόσιο χώρο, τον οποίο οι περαστικοί δεν μπορούν να αποφύγουν, την επεξεργασία που αποσκοπεί στο να επιτρέψει, να τροποποιήσει ή να επαναχρησιμοποιήσει την πρόσβαση των υποκειμένων των δεδομένων σε μια υπηρεσία ή τη σύναψη μιας σύμβασης. Ένα παράδειγμα είναι όταν μια τράπεζα ελέγχει τους πελάτες της με βάσει μια βάση δεδομένων πιστωτικών στοιχείων προκειμένου να αποφασίσει αν θα τους προσφέρει δάνειο.

Οι κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29/EDPB [4] θεωρούν ότι όσο περισσότερα κριτήρια πληρούνται από την επεξεργασία, τόσο πιθανότερο είναι να παρουσιάζει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων με αποτέλεσμα να απαιτείται DPIA. Κατά γενικό κανόνα, η πράξη επεξεργασίας που πληροί λιγότερα από δύο κριτήρια δύναται να μην απαιτεί DPIA λόγω του χαμηλού επιπέδου κινδύνου, ενώ οι πράξεις επεξεργασίας που πληρούν τουλάχιστον δύο από αυτά τα κριτήρια απαιτούν DPIA. Στην περίπτωση λοιπόν που ο υπεύθυνος επεξεργασίας πιστεύει ότι μια πράξη επεξεργασίας που πληροί τουλάχιστον δύο από αυτά τα κριτήρια δεν είναι πιθανό να ενέχει υψηλό κίνδυνο, τότε ο ίδιος οφείλει να τεκμηριώνει διεξοδικά τους λόγους για τη μη διενέργεια DPIA.

2.3 Πότε δεν απαιτείται DPIA;

Κατά κύριο λόγο, η εκτίμηση αντικτύπου προστασίας δεδομένων δεν απαιτείται στις ακόλουθες περιπτώσεις [3]:

1. Όταν η επεξεργασία δεν είναι «πιθανό να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 35 παράγραφος 1 ΓΚΠΔ).
2. Όταν η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας είναι πολύ παρόμοιοι με την επεξεργασία για την οποία έχουν διενεργηθεί DPIA. Στις περιπτώσεις αυτές, μπορούν να χρησιμοποιηθούν τα αποτελέσματα μιας DPIA για παρόμοια επεξεργασία (άρθρο 35 παράγραφος 1 ΓΚΠΔ).
3. Στις περιπτώσεις όπου μια πράξη επεξεργασίας έχει νομική βάση στο δίκαιο της ΕΕ ή του κράτους μέλους, όταν ο νόμος ρυθμίζει τη συγκεκριμένη πράξη επεξεργασίας αλλά και όταν έχει ήδη διενεργηθεί γενική εκτίμηση επιπτώσεων σύμφωνα με τα πρότυπα του ΓΚΠΔ, στο πλαίσιο της υιοθέτησης της εν λόγω νομικής βάσης (άρθρο 35 παράγραφος 10 ΓΚΠΔ).
4. Όταν η επεξεργασία περιλαμβάνεται στον προαιρετικό κατάλογο, που καταρτίζεται από την εποπτική αρχή, των πράξεων επεξεργασίας για τις οποίες δεν απαιτείται DPIA (άρθρο 35 παράγραφος 5 ΓΚΠΔ). Ειδικότερα, ο εν λόγω κατάλογος μπορεί να περιλαμβάνει δραστηριότητες επεξεργασίας που συμμορφώνονται με τους όρους που καθορίζει η εν λόγω αρχή, ιδίως μέσω κατευθυντήριων γραμμών, ειδικών αποφάσεων ή αδειών, κανόνων συμμόρφωσης κ.λπ. Στις περιπτώσεις αυτές, και με την επιφύλαξη της επανεκτίμησης από την αρμόδια εποπτική αρχή, δεν απαιτείται DPIA, αλλά μόνο εάν η επεξεργασία εμπίπτει αυστηρά στο πεδίο εφαρμογής της σχετικής διαδικασίας που αναφέρεται στον κατάλογο και εξακολουθεί να συμμορφώνεται πλήρως με τις σχετικές απαιτήσεις.

2.4 Πρέπει να ανανεώνονται οι DPIA για τις υφιστάμενες πράξεις επεξεργασίας;

Ο ΓΚΠΔ τέθηκε σε ισχύ από τις 25 Μαΐου 2018 και οι κατευθυντήριες γραμμές της ομάδας εργασίας του άρθρου 29 σημείωσαν συγκεκριμένα ότι η απαίτηση διενέργειας DPIA εφαρμόζεται σε υφιστάμενες πράξεις επεξεργασίας που ενδέχεται να προκαλέσουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και για τις οποίες έχει

επέλθει μεταβολή των κινδύνων, λαμβάνοντας υπόψη την φύση, το πεδίο εφαρμογής πεδίο, το πλαίσιο και του σκοπού της επεξεργασίας [5]. Παρόλα αυτά, αξίζει να σημειωθεί ότι δεν απαιτείται DPIA για πράξεις επεξεργασίας που έχουν ήδη, πριν από τον ΓΚΠΔ, ελεγχθεί από Εποπτική Αρχή ή τον υπεύθυνο προστασίας δεδομένων (σύμφωνα με το άρθρο 20 της οδηγίας 95/46/ΕΚ) και οι οποίες εκτελούνται με τρόπο που δεν έχει αλλάξει από τον προηγούμενο έλεγχο. Κατά συνέπεια, κάθε επεξεργασία δεδομένων της οποίας οι όροι υλοποίησης (πεδίο εφαρμογής, σκοπός, συλλεγόμενα δεδομένα προσωπικού χαρακτήρα, ταυτότητα των υπευθύνων επεξεργασίας ή των αποδεκτών των δεδομένων, περίοδος διατήρησης δεδομένων, τεχνικά και οργανωτικά μέτρα κ.λπ.) έχουν αλλάξει από την προηγούμενη αξιολόγηση και η οποία ενδέχεται να οδηγήσει σε υψηλό κίνδυνο θα πρέπει να υπόκειται σε DPIA. Αναλυτικότερα, οι νέες DPIA ή αναθεωρήσεις των υφιστάμενων DPIA που ξεκίνησε πριν από τις 25 Μαΐου 2018, μπορεί να απαιτηθούν μετά την ημερομηνία αυτή στις ακόλουθες περιπτώσεις [5]:

1. Όταν έχει επέλθει σημαντική αλλαγή στην πράξη επεξεργασίας μετά την έναρξη ισχύος του ΓΚΠΔ, για παράδειγμα όταν τίθεται σε χρήση μια νέα τεχνολογία ή όταν τα δεδομένα χρησιμοποιούνται για διαφορετικό σκοπό. Σε αυτές τις περιπτώσεις η επεξεργασία αποτελεί ουσιαστικά μια νέα πράξη και θα μπορούσε να απαιτηθεί DPIA.
2. Όταν μεταβάλλεται ο κίνδυνος που ενέχει η πράξη επεξεργασίας. Ειδικότερα, οι κίνδυνοι και το επίπεδο κινδύνου μπορεί να αλλάξουν ως αποτέλεσμα της αλλαγής ενός εκ των στοιχείων της πράξης επεξεργασίας (δεδομένα, υποστηρικτικά στοιχεία, πηγές κινδύνου) ή επειδή το πλαίσιο της επεξεργασίας εξελίσσεται (σκοπός, λειτουργίες κ.λπ.). Επομένως, τα συστήματα επεξεργασίας δεδομένων μπορεί να εξελίσσονται με την πάροδο του χρόνου και να προκύπτουν νέες απειλές και τρωτά σημεία.
3. Τέλος, εάν το οργανωτικό ή κοινωνικό πλαίσιο της δραστηριότητας επεξεργασίας έχει αλλάξει, στην περίπτωση που τα αποτελέσματα ορισμένων αυτοματοποιημένων αποφάσεων έχουν γίνει πιο σημαντικά, νέες κατηγορίες φυσικών προσώπων καθίστανται ευάλωτες σε διακρίσεις ή τα δεδομένα πρόκειται να διαβιβαστούν σε αποδέκτες δεδομένων που βρίσκονται σε χώρα που έχει εγκαταλείψει την ΕΕ.

Στο πλαίσιο της ορθής πρακτικής, η DPIA πρέπει να επανεξετάζεται συνεχώς και να επαναξιολογείται τακτικά. Επομένως, ακόμη και όταν δεν απαιτείται αυστηρά η διενέργεια νέας DPIA για μια υφιστάμενη πράξη κατά την έναρξη ισχύος του ΓΚΠΔ, αυτομάτως

καθίσταται απαραίτητο ο υπεύθυνος επεξεργασίας να διενεργήσει DPIA στο πλαίσιο των γενικών υποχρεώσεων λογοδοσίας του.

2.5 Σε ποιο στάδιο του κύκλου ζωής ενός έργου πρέπει να διενεργείται DPIA;

Η DPIA συνίσταται να διενεργείται «πριν από την επεξεργασία» (άρθρα 35 παράγραφος 1 και 35 παράγραφος 10 και αιτιολογικές σκέψεις 90 και 93 ΓΚΠΔ), ενώ παράλληλα αποτελεί ορθή πρακτική η διενέργεια DPIA όσο το δυνατόν νωρίτερα κατά τον σχεδιασμό της πράξης επεξεργασίας [6]. Παρόλα αυτά, ενδέχεται να μην είναι δυνατή η διενέργεια DPIA από την αρχή του έργου καθώς πρέπει να προσδιοριστούν οι στόχοι του έργου και να γίνει κάποια κατανόηση του τρόπου λειτουργίας του προτού καταστεί δυνατή η αξιολόγηση των σχετικών κινδύνων για την προστασία των δεδομένων. Αδιαμφισβήτητα, για ορισμένα έργα η DPIA μπορεί να χρειαστεί να είναι μια συνεχής διαδικασία η οποία επικαιροποιείται παράλληλα με την εξέλιξη της. Βέβαια, το γεγονός ότι η DPIA μπορεί να χρειαστεί να επικαιροποιηθεί όταν η επεξεργασία έχει ήδη αρχίσει, δεν αποτελεί βάσιμο λόγο για την αναβολή ή τη μη διενέργεια της.

2.6 Ποιος πρέπει να συμμετέχει στη διενέργεια της DPIA;

Σε μια αποτελεσματική DPIA θα πρέπει να συμμετέχουν οι αρμόδιοι ενδιαφερόμενοι από διάφορες λειτουργίες του οργανισμού (π.χ. ο διαχειριστής του έργου, ο υπεύθυνος προστασίας δεδομένων του οργανισμού, το τμήμα πληροφορικής) και, όπου χρειάζεται, τα σχετικά εξωτερικά μέρη (π.χ. εμπειρογνώμονες του αντικειμένου), προκειμένου να εντοπιστούν, να αξιολογηθούν και να αντιμετωπιστούν οι κίνδυνοι για την προστασία των δεδομένων. Το πρόσωπο που ηγείται της DPIA, ο επικεφαλής της DPIA, θα πρέπει να είναι ο διαχειριστής του έργου ή ο υπεύθυνος προστασίας δεδομένων του οργανισμού.

Σύμφωνα με το άρθρο 35 παράγραφος 2 του ΓΚΠΔ [5], κάθε υπεύθυνος επεξεργασίας (controller) που διαθέτει ορισμένο υπεύθυνο προστασίας δεδομένων (ΥΠΔ) είναι απαραίτητο να ζητά τη συμβουλή του ΥΠΔ κατά τη διενέργεια DPIA. Η συμβουλή αυτή και οι αποφάσεις που λαμβάνονται θα πρέπει να τεκμηριώνονται ως μέρος της διαδικασίας DPIA, ενώ στην περίπτωση που στην επεξεργασία εμπλέκεται ο εκτελών την επεξεργασία δεδομένων (data processor), ο εκτελών την επεξεργασία δεδομένων θα πρέπει να

συνδράμει στη διενέργεια της DPIA και να παρέχει κάθε αναγκαία πληροφορία. Επιπροσθέτως, ο ΥΠΔ είναι ένα ορισμένο πρόσωπο που διορίζεται από έναν οργανισμό για να συμβουλεύει σχετικά με τις πρακτικές προστασίας δεδομένων εντός του οργανισμού, ο οποίος δύναται να είναι μέλος του προσωπικού ή εξωτερικός πάροχος υπηρεσιών. Ειδικότερα και σύμφωνα με τον ΓΚΠΔ, ο διορισμός ΥΠΔ είναι υποχρεωτικός στις ακόλουθες περιπτώσεις [5]:

- Για τους δημόσιους φορείς που διενεργούν επεξεργασία δεδομένων, εκτός από τα δικαστήρια που ενεργούν υπό τη δικαστική τους ιδιότητα
- Αν οι βασικές δραστηριότητες του οργανισμού συνίστανται σε επεξεργασία δεδομένων η οποία, λόγω του πεδίου εφαρμογής ή/και των σκοπών της, απαιτεί τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα και
- Όταν οι βασικές δραστηριότητες του οργανισμού συνίστανται σε επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων, όπως περιγράφονται στο άρθρο 9, ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες, όπως περιγράφονται στο άρθρο 10 του ΓΚΠΔ και αναλύθηκαν παραπάνω.

Συνεπώς, ο υπεύθυνος επεξεργασίας υποχρεούται να «ζητήσει τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους» (σύμφωνα με το άρθρο 35 παράγραφος 9 του ΓΚΠΔ [5]), «κατά περίπτωση», κατά τη διενέργεια της DPIA. Σε ορισμένες όμως περιπτώσεις, τα υποκείμενα των δεδομένων μπορεί να είναι άτομα εντός του οργανισμού, ενώ η αναζήτηση των απόψεων των υποκειμένων των δεδομένων θα επιτρέψει στον υπεύθυνο επεξεργασίας να κατανοήσει τις ανησυχίες και να βελτιώσει τη διαφάνεια, καθιστώντας τα άτομα ενήμερα για τον τρόπο με τον οποίο θα χρησιμοποιηθούν τα δεδομένα τους. Τέλος, οι απόψεις των υποκειμένων των δεδομένων μπορούν να αναζητηθούν με διάφορα μέσα, ανάλογα με το πλαίσιο, σε αντίθεση με το προσωπικό που θα μπορούσε να ερωτηθεί μέσω μιας εργατικής οργάνωσης. Κατά την περίπτωση όπου η τελική απόφαση του υπεύθυνου επεξεργασίας διαφέρει από τις απόψεις των υποκειμένων των δεδομένων, οι λόγοι θα πρέπει να καταγράφονται ως μέρος της DPIA, ενώ εάν ο υπεύθυνος επεξεργασίας δεν θεωρεί σκόπιμο να ζητήσει τις απόψεις των υποκειμένων των δεδομένων τότε θα πρέπει να τεκμηριώνεται η αιτιολόγηση αυτού του γεγονότος. Συμπερασματικά, ο παρακάτω πίνακας παραθέτει τους τυπικούς ρόλους και τις αρμοδιότητες των βασικών μερών που εμπλέκονται στη DPIA [7]:

Ποιος εμπλέκεται;	Ποιοι είναι αυτοί;	Ρόλος στην DPIA
Διαχειριστής έργου (Project Manager)	Υπεύθυνος του έργου	- Επικεφαλής της DPIA, ο οποίος μπορεί να υποστηρίζεται από ομάδα DPIA. - Αξιολογεί την ανάγκη για DPIA, σχεδιάζει την DPIA και διεξάγει την DPIA. - Προσδιορίζει και ζητά τη συμβολή των σχετικών ενδιαφερομένων, συμπεριλαμβανομένης της ομάδας έργου, σχετικά με: 1. Πιθανούς κινδύνους και προκλήσεις για την προστασία των δεδομένων του έργου από την άποψη της υλοποίησης 2. Τον τρόπο με τον οποίο θα πρέπει να αντιμετωπιστούν οι εντοπισμένοι κίνδυνοι προστασίας προσωπικών δεδομένων μαζί με τις πιθανές λύσεις 3. Τεκμηριώνει την έκθεση DPIA (η οποία περιλαμβάνει την πρόταση λεπτομερούς σχεδίου δράσης) προς έγκριση από τη διοίκηση 4. Παρακολουθεί τα αποτελέσματα της DPIA και επανεξετάζει την DPIA όταν υπάρχει αλλαγή στους κινδύνους για την προστασία των δεδομένων προσωπικού χαρακτήρα.
Υπεύθυνος προστασίας δεδομένων (DPO)	Υπεύθυνος για τη δημιουργία και την εφαρμογή των πολιτικών προστασίας δεδομένων εντός του οργανισμού. Μπορεί να αξιοποιήσει τα δίκτυα ή τις Ενώσεις των ΥΠΔ για πόρους ή συμβουλές από άλλους ΥΠΔ για να καθοδηγήσει τον επικεφαλής της DPIA κατά τη διενέργεια της DPIA.	- Συμβουλεύει τον επικεφαλή της DPIA καθ' όλη τη διάρκεια της διαδικασίας DPIA, όπως: 1. Εντοπισμός και μετριασμός των εντοπισμένων κινδύνων προστασίας δεδομένων με την παροχή υποστήριξης βάσει βέλτιστων πρακτικών προσαρμοσμένων στις ανάγκες και τις περιστάσεις του οργανισμού. 2. Καθορισμός και εφαρμογή του πλαισίου αξιολόγησης κινδύνων 3. Διασφαλίζει ότι οι DPIA διενεργούνται σύμφωνα με τις πολιτικές του οργανισμού και συνιστά βελτίωση της μεθοδολογίας

		DPIA με βάση τις βέλτιστες πρακτικές του κλάδου. 4. Επανεξέταση της έκθεσης DPIA πριν από την υποβολή της στην διοίκηση - Αναπτύσσει τα υποδείγματα/ερωτηματολόγιο DPIA που απαιτούνται για την ολοκλήρωση της DPIA - Βοηθά στην αναθεώρηση της DPIA όταν υπάρχει αλλαγή σε κινδύνων για την προστασία των δεδομένων προσωπικού χαρακτήρα
Συντονιστική επιτροπή έργου (Project Steering Committee)	Διοίκηση του οργανισμού που ενέκρινε το έργο	- Αναθέτει την DPIA - Εγκρίνει το πλαίσιο αξιολόγησης κινδύνων - Εγκρίνει το σχέδιο DPIA, καθώς και τα προτεινόμενα σχέδια δράσης και τις λύσεις που προκύπτουν από την DPIA.
Άλλοι	Άλλες οργανωτικές λειτουργίες ή τμήματα που εμπλέκονται σε κάποιο βαθμό στο έργο, εξωτερικά μέρη, όπως εμπειρογνώμονες επί του θέματος ή ακόμη και άτομα που ενδέχεται να επηρεαστούν, όπου χρειάζεται.	- Παρέχει πληροφορίες σχετικά με πιθανούς κινδύνους και προκλήσεις για το έργο σε σχέση με τη λειτουργία τους. Για παράδειγμα: **Πληροφορική και Νομικά:** Παροχή συμβουλών στον επικεφαλή της DPIA σχετικά με πιθανές λύσεις ΤΠ και κινδύνους ασφάλειας/νομικούς κινδύνους κατά την εφαρμογή μέτρων για την προστασία των δεδομένων προσωπικού χαρακτήρα. Αυτό μπορεί επίσης να περιλαμβάνει τη παροχή συμβουλών σχετικά με πιθανές προκλήσεις στο σχεδιασμό και την ανάπτυξη του συστήματος. **Εξυπηρέτηση πελατών, επικοινωνία ή λειτουργίες:** Παροχή συμβουλών στον επικεφαλή της DPIA σχετικά με τις πιθανές επιπτώσεις στους καταναλωτές (π.χ. όσον αφορά τη χρηστικότητα), εάν τα αποτελέσματα της DPIA δικαιολογούν αλλαγές στην αλληλεπίδραση με τους καταναλωτές ή στις καθημερινές λειτουργίες. **Ανθρώπινοι πόροι ή ικανότητα προσωπικού:**

		Παροχή συμβουλών σχετικά με τα κατάλληλα προγράμματα κατάρτισης ή τους πόρους σε περίπτωση που τα αποτελέσματα της DPIA απαιτούν από το προσωπικό να είναι σε θέση να εκτελεί νέα μέτρα ή δραστηριότητες προστασίας δεδομένων.

Πίνακας 1: Ρόλοι και αρμοδιότητες των εμπλεκόμενων μερών

2.7 Ποια είναι τα βήματα που απαιτούνται για τη διενέργεια μιας DPIA;

Ο ΓΚΠΔ ορίζει τα ακόλουθα ελάχιστα χαρακτηριστικά που πρέπει να υπάρχουν σε μια DPIA (άρθρο 35 παράγραφος 7 και αιτιολογικές σκέψεις 84 [8] και 90 ΓΚΠΔ) [2, 9, 10]:

- Περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας,
- αξιολόγηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας,
- αξιολόγηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και
- τα μέτρα που προβλέπονται:
  → για την αντιμετώπιση των κινδύνων και
  → για να αποδείξουν τη συμμόρφωση με τον ΓΚΠΔ.

Ο ΓΚΠΔ παρουσιάζει ένα ευρύ, γενικό πλαίσιο για το σχεδιασμό και τη διενέργεια μιας DPIA, το οποίο επιτρέπει την επεκτασιμότητα, ώστε ακόμη και οι μικρότεροι υπεύθυνοι επεξεργασίας να μπορούν να σχεδιάσουν και να εφαρμόσουν μια DPIA, καθώς και την ευελιξία, ώστε ο υπεύθυνος επεξεργασίας να μπορεί να καθορίσει την ακριβή δομή και μορφή της DPIA, επιτρέποντάς της να ταιριάζει με τις υφιστάμενες πρακτικές εργασίας [5].

2.8 Μεθοδολογίες για DPIA

Συνοπτικά, οι στόχοι μιας DPIA είναι [11]:

1. Να προσδιοριστούν επακριβώς οι (υψηλοί) κίνδυνοι που ενέχει η προτεινόμενη πράξη επεξεργασίας, λαμβάνοντας υπόψη τη φύση των δεδομένων και της επεξεργασίας, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας

και τις πηγές του κινδύνου, όχι μόνο υπό κανονικές συνθήκες, αλλά και υπό ειδικές συνθήκες καθώς και βραχυπρόθεσμα και μακροπρόθεσμα.

2. Να αξιολογεί τους εντοπισμένους (υψηλούς) κινδύνους, ιδίως την προέλευση, τη φύση και την ιδιαιτερότητά τους, καθώς και την πιθανότητα και την πιθανή σοβαρότητα του κινδύνου.
3. Να προσδιορίσει ποια μέτρα μπορούν να ληφθούν για τον μετριασμό των (υψηλών) κινδύνων, τα οποία είναι κατάλληλα από την άποψη της διαθέσιμης τεχνολογίας και του κόστους εφαρμογής, καθώς και να προτείνει τα μέτρα αυτά.
4. Να καταγράφει τα ευρήματα, την αξιολόγηση και τα μέτρα που λαμβάνονται (ή δεν λαμβάνονται με τους αντίστοιχους λόγους), ώστε να είναι σε θέση να «αποδείξει τη συμμόρφωση» με τις απαιτήσεις του ΓΚΠΔ βάσει της αρχής της «λογοδοσίας» σε σχέση με την αξιολογούμενη επεξεργασία.

Όπως διατυπώνει η WP29:

«Η DPIA είναι μια διαδικασία για την οικοδόμηση και την απόδειξη της συμμόρφωσης».

3. Αξιολόγηση των μεθόδων PIA: το σημερινό τοπίο

Παρόλο που η βασική έννοια της μεθόδου PIA χρονολογείται από το 2009 και έκτοτε έχουν προταθεί πολλές μέθοδοι και κατευθυντήριες γραμμές, έχουν δημοσιευθεί ελάχιστες εργασίες για τη σύγκριση ή/και την αξιολόγηση αυτών των μεθόδων. Η πρώτη έρευνα για την αξιολόγηση των κατευθυντήριων γραμμών DPIA διεξήχθη το 2011 από τον Clarke [12], ο οποίος αξιολόγησε τις κατευθυντήριες γραμμές DPIA που δημοσιεύθηκαν από τα γραφεία Επιτρόπων του Καναδά, της Αυστραλίας κ.λπ. Τα κριτήρια αξιολόγησης επικεντρώθηκαν κυρίως στην ποιότητα του εγγράφου, όπως η δυνατότητα ανακάλυψης, η δυνατότητα εφαρμογής σε περιοχές ή βιομηχανικά τμήματα, η αποσαφήνιση ότι η ευθύνη για την PIA ανήκει στον οργανισμό και ο προσανατολισμός στη συμπλήρωση ενός προτύπου έκθεσης έναντι της διαδικασίας ανάλυσης κινδύνου. Άλλα κριτήρια που χρησιμοποιήθηκαν περιλάμβαναν: υποχρεωτικό καθεστώς και χρονοδιάγραμμα της PIA, διαστάσεις της προστατευόμενης ιδιωτικής ζωής, εφαρμοσμένα νομικά πλαίσια, εμπλοκή των ενδιαφερομένων μερών, ενσωμάτωση της διαδικασίας DPIA σε εταιρικούς μηχανισμούς, π.χ. χρηματοδότηση έργων και ο ρόλος της εποπτικής αρχής. Η αξιολόγηση του Clarke υπογράμμισε τις βέλτιστες πρακτικές των κατευθυντήριων γραμμών για τις PIA που δημοσιεύθηκαν εκείνη την εποχή και έδειξε ότι ορισμένες κατευθυντήριες γραμμές περιόριζαν τις PIA προτείνοντας ελέγχους νομικής συμμόρφωσης ή δεν μετέφεραν τη σημασία της εμπλοκής των ενδιαφερομένων μερών [6].

Στο πλαίσιο του χρηματοδοτούμενου από την Ευρωπαϊκή Επιτροπή (ΕΚ) έργου PIA, υποστηρίζεται η ανάγκη της ΕΕ να θεσπίσει το δικό της πλαίσιο διενέργειας PIA και πραγματοποίησαν μια συγκριτική αξιολόγηση των κατευθυντήριων γραμμών διαφόρων χωρών (συμπεριλαμβανομένων της Αυστραλίας, του Καναδά, της Ιρλανδίας, του Ηνωμένου Βασιλείου και των ΗΠΑ) [13] για να εντοπίσουν τα καλύτερα στοιχεία/πρακτικές που θα μπορούσαν να χρησιμοποιηθούν. Τα κριτήρια που χρησιμοποιήθηκαν για την αξιολόγηση αυτή επικεντρώθηκαν στο πλαίσιο της εφαρμογής της PIA, όπως το ενδεχόμενο για υποχρεωτικό καθεστώς της (νομοθετικά κατοχυρωμένο) και το κατά πόσον οι κατευθυντήριες γραμμές παρέχουν επιχειρήματα υπέρ της διενέργειας DPIA. Άλλα κριτήρια επικεντρώθηκαν στην ποιότητα της μεθόδου DPIA και στην παρεχόμενη βοήθεια, όπως η αντιμετώπιση διαφορετικών πτυχών της ιδιωτικής ζωής (πληροφοριακή, σωματική, εδαφική, τοπική και επικοινωνιακή), η εξέταση της αναγκαιότητας διενέργειας DPIA, η διαβούλευση με εξωτερικούς ενδιαφερόμενους, η πρόταση της δομής της έκθεσης DPIA [13], η ανάθεση της ευθύνης για την DPIA στην ανώτερη διοίκηση, η εξέταση της έκθεσης DPIA από

εξωτερική αρχή και η επισήμανση της ανάγκης για επικαιροποίηση της DPIA καθ' όλη τη διάρκεια του κύκλου ζωής ενός έργου. Προς την ίδια κατεύθυνση, οι Wadhwa και Rodrigues (2013) πρότειναν ένα εργαλείο αξιολόγησης που βαθμολογεί τις εκθέσεις PIA, το οποίο ονομάζεται DPIA Evaluation and Grading System (PEGS). Το εργαλείο αυτό εφάρμοσε ποσοτικά κριτήρια αξιολόγησης στα βήματα διενέργειας PIA, τα οποία προέκυψαν από το έργο PIAF [6]. Τα κριτήρια σταθμίστηκαν ανάλογα με τη συμβολή τους στην επιτυχή διεξαγωγή της PIA και περιλάμβαναν: αποσαφήνιση της έγκαιρης έναρξης, προσδιορισμό του ποιος διενήργησε την PIA και δημοσίευση της έκθεσης PIA (βάρος = 1), περιγραφή του έργου, του σκοπού και των σχετικών πληροφοριών του πλαισίου, χαρτογράφηση της ροής πληροφοριών, έλεγχο της συμμόρφωσης με τη νομοθεσία και προσδιορισμό της διαβούλευσης με τους ενδιαφερόμενους φορείς (βάρος = 2), προσδιορισμό των κινδύνων και των επιπτώσεων στην προστασία της ιδιωτικής ζωής, προσδιορισμό λύσεων/επιλογών για την αποφυγή και τον μετριασμό των κινδύνων και χειρισμό των συστάσεων μετά την PIA (βάρος = 3).

Οι Notario κ.ά. (2015) αξιολόγησαν τις μεθόδους εκτίμησης των επιπτώσεων στην προστασία της ιδιωτικής ζωής που προτείνονται στην ΕΕ (Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU) [14] και Privacy and Data Protection Impact Assessment Framework for RFID), στο πλαίσιο του χρηματοδοτούμενου από την ΕΕ έργου PRIPARE (Preparing Industry to Privacy by Design by supporting its Application in Research) [15]. Τα κριτήρια αξιολόγησης περιλάμβαναν την ύπαρξη υποστηρικτικών ερωτηματολογίων που εξάγονται από νομικά πλαίσια για να διασφαλιστεί η τήρηση των νομικών υποχρεώσεων ενός έργου, την εξέταση των επιπτώσεων στην προστασία της ιδιωτικής ζωής από την πλευρά του οργανισμού (οικονομικές απώλειες) ή από την πλευρά του ατόμου (αναγνωσιμότητά και ευαισθησία των προσωπικών δεδομένων), τις μετρικές που χρησιμοποιούνται για τη μέτρηση των κινδύνων για την προστασία της ιδιωτικής ζωής και την πρόταση στρατηγικών μετριασμού των κινδύνων.

Εστιάζοντας στην υλοποίηση έργων PIA, οι van Puijenbroek και Hoepman (2017) [3] αξιολόγησαν τις πρακτικές DPIA που ακολουθούσαν 15 οργανισμοί στις Κάτω Χώρες, προκειμένου να διερευνήσουν κατά πόσον αυτές οδήγησαν σε προϊόντα και συστήματα φιλικά προς την προστασία της ιδιωτικής ζωής. Η μελέτη τους, αν και βασίστηκε σε περιγραφικές απαντήσεις από Υπεύθυνους Προστασίας Δεδομένων (DPOs) ή στελέχη με αντίστοιχο ρόλο, έδειξε ότι οι PIA διενεργούνταν κυρίως από την οπτική γωνία του υπεύθυνου επεξεργασίας δεδομένων, αντί του υποκειμένου των δεδομένων που θα

επηρεάζονταν, ότι οι έλεγχοι επιλέγονταν κυρίως για τον μετριασμό και όχι για την αποφυγή των κινδύνων για την προστασία της ιδιωτικής ζωής και ότι οι PIA δεν επαναλαμβάνονταν, όπως θα έπρεπε, καθ' όλη τη διάρκεια της διαδικασίας ανάπτυξης προϊόντων ή συστημάτων. Επί του παρόντος, διατίθενται διάφορες μέθοδοι PIA διαφορετικής προέλευσης, πολλές από τις οποίες έχουν πρόσφατα επικαιροποιηθεί. Η παρούσα εργασία καταγράφει, αναλύει και συγκρίνει τις ενημερωμένες μεθόδους εκτίμησης αντικτύπου στην ιδιωτική ζωή των υποκειμένων των δεδομένων με σκοπό τη διευκόλυνση της εφαρμογής τους.

3.1 Μέθοδος έρευνας

Μέσω μιας συστηματικής ανάλυσης των σχετικών ερευνών και δημοσιεύσεων σχετικά με τις μεθόδους DPIA θα προκύψει στο 6ο Κεφάλαιο «Σύγκριση Μεθοδολογιών» ένα σύνολο κριτηρίων, τα οποία θα χρησιμοποιηθούν για την αξιολόγηση των διαθέσιμων μεθόδων DPIA (που περιλαμβάνονται στον Πίνακα 2), όσον αφορά τη διαδικασία που ακολουθείται, καθώς και τις κατευθυντήριες γραμμές που παρέχονται στους υπεύθυνους της DPIA. Τα κριτήρια διαμορφώθηκαν έτσι ώστε να αξιολογηθεί κατά πόσον οι μεθοδολογίες DPIA παρέχουν επαρκώς [16]:

- καθοδήγηση στους οργανισμούς κατά τα σημαντικά βήματα της
- υποστηρικτικό υλικό για τους φορείς που διενεργούν DPIA (π.χ. καθοδήγηση στον εντοπισμό κινδύνων, υποδείγματα εκθέσεων DPIA) για τη διευκόλυνση της διενέργειας DPIA,
- καθοδήγηση για την οργάνωση ενός έργου DPIA (π.χ. ανάθεση αρμοδιοτήτων, επιλογή μελών της ομάδας DPIA και συμμετοχή εξωτερικών ενδιαφερόμενων μερών), έτσι ώστε να παρέχονται αποτελεσματικές κατευθυντήριες γραμμές εφαρμογής καθ' όλη τη διάρκεια του κύκλου ζωής ενός έργου DPIA.

Μεθοδολογία	Περιγραφή
Μελέτη Εκπόνησης Εκτίμησης Αντικτύπου (DPIA) σύμφωνα με τον ΓΚΠΔ της ΕΕ	Διαδικασία για τη διενέργεια PIA, η οποία θέτει σε λειτουργία τις καθιερωμένες απαιτήσεις του ΓΚΠΔ της ΕΕ.
OAIC Αυστραλία	Προτείνεται από το Γραφείο του Αυστραλιανού Επιτρόπου Πληροφοριών. Περιλαμβάνει έλεγχο συμμόρφωσης με τις αρχές του νόμου της Αυστραλίας για την προστασία της ιδιωτικής ζωής.
ΑΠΔΠΧ	Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ.
Ηνωμένο Βασίλειο ICO	Δημοσιεύεται από το Γραφείο Επιτρόπου Πληροφοριών του Ηνωμένου Βασιλείου. Περιλαμβάνει καταλόγους κινδύνων και ερωτηματολόγια για την καθοδήγηση της ανάλυσης.
ISO 29134	Ένα πρότυπο που εκδόθηκε το 2017 για να καθοδηγήσει τους επαγγελματίες σχετικά με τη διενέργεια DPIA.
CNIL	Προτάθηκε από τη γαλλική Commission Nationale de l'Informatique et des Libertes (CNIL), με βάση τη μέθοδο διαχείρισης κινδύνων ασφαλείας EBIOS. Συνοδεύεται από μια beta έκδοση ενός εργαλείου για την καθοδήγηση των βημάτων της PIA.
WP29	Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων .

Πίνακας 2: Μεθοδολογίες που θα αναλυθούν

4. Μεθοδολογίες Εκτίμησης Αντικτύπου

4.1 Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) – GDPR

Το άρθρο 35 του ΓΚΠΔ εισάγει την έννοια της DPIA, εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Πρόκειται για μια μέθοδο που παρέχει καθοδηγούμενα βήματα για τον εντοπισμό και την ανάλυση του τρόπου με τον οποίο τα δικαιώματα και οι ελευθερίες των ατόμων ενδέχεται να επηρεαστούν από ορισμένες ενέργειες ή δραστηριότητες που σχετίζονται με την επεξεργασία δεδομένων και να βοηθήσει στην αποφυγή/διόρθωση αυτών των ζητημάτων.

Ο Γενικός Κανονισμός της ΕΕ για την Προστασία Δεδομένων (ΓΚΠΔ) απαιτεί από κάθε υπεύθυνο επεξεργασίας δεδομένων να αξιολογεί και να τεκμηριώνει κατά πόσον η επεξεργασία του «ενδέχεται να οδηγήσει σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες» των ατόμων (δηλ. υψηλού κινδύνου), και αν ναι να διενεργήσει «Εκπόνηση Μελέτης Εκτίμησης Αντικτύπου (DPIA)» [5]. Η DPIA είναι ουσιαστικά μια επαναληπτική διακυβέρνηση κινδύνου σε τρία στάδια όπου ο οργανισμός προσδιορίζει πρώτα τις δραστηριότητές του, στη συνέχεια ελέγχει εάν πληρούνται τα κριτήρια που απαιτούν DPIA, και αν ναι, διενεργεί DPIA. Είναι εύλογο να σημειωθεί πως ο ΓΚΠΔ δεν επιβάλλει μια αυστηρή διαδικασία για τον τρόπο με τον οποίο πρέπει να διεξάγουν τις εκτιμήσεις αντικτύπου και επιπτώσεων, αλλά καθορίζει γενικές απαιτήσεις. Οι Αρχές Προστασίας Δεδομένων (ΑΠΔΠΧ), αρμόδιες για την επιβολή του ΓΚΠΔ, έχουν δημοσιοποιήσει, στους αντίστοιχους δικτυακούς τόπους, οδηγίες και εργαλεία σχετικά με τη συμμόρφωση, συμπεριλαμβανομένης της DPIA και της διακυβέρνησης κινδύνων. Οι μεθοδολογίες αυτές μαζί με τα αντίστοιχα εργαλεία θα παρουσιαστούν και θα αναλυθούν στις ενότητες που ακολουθούν.

Οι κύριες προκλήσεις σχετικά με την DPIA που επικρατούν στο σημερινό τοπίο παρατίθενται [11]:

1. Οι DPIAs δύναται να εμπλέκουν πολλαπλά ενδιαφερόμενα μέρη (π.χ. εκτελούντες την επεξεργασία δεδομένων – Data Processors), γεγονός που δημιουργεί εξαρτήσεις πληροφοριών, δηλαδή μέτρα που εφαρμόζονται από τους εκτελούντες την επεξεργασία.
2. Δεδομένου ότι οι DPIA πρέπει να είναι συγκεκριμένες, οι υπεύθυνοι επεξεργασίας που διενεργούν παρόμοιες DPIA θα επαναλαμβάνουν πληροφορίες και καθήκοντα.

3. Παρά τα υφιστάμενα πρότυπα για τη διαχείριση των κινδύνων, υπάρχουν διαφορές στις μεθοδολογίες που εμποδίζουν την εξεύρεση κοινών καθολικών εφαρμογών και πρακτικών.
4. Τα ισχύοντα πρότυπα τεκμηρίωσης είναι σε μεγάλο βαθμό προσανατολισμένα στον άνθρωπο (π.χ. λογιστικά φύλλα, PDF), γεγονός που περιορίζει σημαντικά την ανάπτυξη και την εφαρμογή εργαλείων για DPIAs.
5. Οι λύσεις δεν λαμβάνουν υπόψη ότι οι αξιολογήσεις επιπτώσεων υψηλού κινδύνου είναι μια μορφή κοινής δραστηριότητας, δηλαδή μοιράζονται πληροφορίες σχετικά με τις δραστηριότητες επεξεργασίας, τους κινδύνους και τις επιπτώσεις με άλλες απαιτήσεις του ΓΚΠΔ (π.χ. μητρώο δραστηριοτήτων επεξεργασίας, διαβιβάσεις δεδομένων) και έχουν επικαλύψεις με παρόμοιες αξιολογήσεις σε ευθυγραμμισμένους κανονισμούς.

Οι υπερσύγχρονες τεχνολογίες περιλαμβάνουν πολύπλευρες λύσει για συγκεκριμένες εφαρμογές αναφορικά με την αποτίμηση των κινδύνων, τις μεθοδολογίες DPIA και τη συμμόρφωση με τον GDPR. Ειδικότερα, παρουσιάζονται τα πλεονεκτήματα των τεχνολογιών του σημασιολογικού ιστού για [5]:

- την εξειδίκευση για μια περίπτωση χρήσης (use-case),
- την διαλειτουργικότητα μεταξύ ενδιαφερομένων μερών και εργαλείων,
- την δημιουργία κοινών βάσεων γνώσης και τέλος
- την ανάπτυξη εργαλείων για τη συμμόρφωση με βάση τη μηχανή.
- Ωστόσο, υπάρχουν δύο σημαντικά κενά που δεν έχουν αντιμετωπιστεί: οι εκτιμήσεις επιπτώσεων και η τεκμηρίωση των DPIA.

Πιο συγκεκριμένα, το άρθρο 35 [5] [5] του ΓΚΠΔ προβλέπει απαιτήσεις για την αξιολόγηση της αναγκαιότητας των DPIA με βάση το ενδεχόμενο υψηλού κινδύνου και για την διενέργεια DPIA εάν πληρούνται ορισμένα κριτήρια. Για να προσδιοριστεί η αναγκαιότητα, οι υπεύθυνοι επεξεργασίας απαιτούν περιγραφές των δραστηριοτήτων επεξεργασίας βάσει συγκεκριμένων κριτηρίων, για παράδειγμα την κλίμακα και το εύρος των δεδομένων (άρθρο 35-3β) ή εάν πρόκειται για αυτοματοποιημένη λήψη αποφάσεων και κατάρτιση προφίλ (άρθρο 35-3α).Οι κατευθυντήριες γραμμές των ΑΠΔΠΧ παρέχουν πρόσθετες αποχρώσεις περιγραφές των εννοιών που είναι σχετικές με τον προσδιορισμό του κινδύνου, του αντικτύπου και της βάσης βάσει της οποίας πρέπει να διενεργείται DPIA. Παρόλο που ο ΓΚΠΔ σκοπεύει να παράσχει εναρμονισμένες απαιτήσεις για τις DPIAs, οι επιμέρους ΑΠΔΠΧ έχουν υιοθετήσει διαφορετικές προσεγγίσεις με αποκλίσεις όσον αφορά την χρήση

οργανωτικών διαδικασιών που σχετίζονται με τις πρακτικές διαχείρισης και τη διακυβέρνηση κινδύνων, οι οποίες δεν συνδέονται απαραίτητα με μια DPIA. Για παράδειγμα, στο πλαίσιο των υποδειγμάτων DPIA, τόσο η AEPD (Ισπανική ΑΠΔΠΧ) όσο και η CNIL (Γαλλική ΑΠΔΠΧ) ζητούν πληροφορίες σχετικά με τις «εσωτερικές πρακτικές και το πλαίσιο» του οργανισμού, οι οποίες περιλαμβάνουν «την δομή, τις λειτουργίες και τις αρμοδιότητες του οργανισμού, τις υιοθετημένες πολιτικές, τους κανόνες και τα πρότυπα, τους στόχους οργανωτικής ωριμότητας και γενικά την κουλτούρα του οργανισμού». Εξαιτίας αυτού, οι οργανισμοί αντιμετωπίζουν δυσκολίες στον προσδιορισμό των απαιτήσεων που πρέπει να πληροί μια DPIA, δεδομένου ότι η καθοδήγηση είναι ποικίλη, πολύπλοκη, διαφοροποιημένη και δύσκολο να κριθεί ως προς την επάρκειά της. Συμπερασματικά, μήπως απαιτείται η ανάγκη περαιτέρω ανάπτυξης καλύτερων μεθοδολογιών DPIA λόγω της περιορισμένης γνώσης των οργανισμών επί του θέματος;

Το άρθρο 35 παράγραφος 7 του ΓΚΠΔ ορίζει ότι (το αρχείο) μιας DPIA πρέπει να περιέχει «τουλάχιστον» τα εξής [5]:

1. συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,
2. αξιολόγηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς,
3. αξιολόγηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1, και
4. τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων ασφαλείας και των μηχανισμών που διασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα και αποδεικνύουν τη συμμόρφωση με τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Η WP29 τονίζει ότι [11] [4]:

«Όλες οι σχετικές απαιτήσεις που ορίζονται στον ΓΚΠΔ παρέχουν ένα ευρύ, γενικό πλαίσιο για τον σχεδιασμό και τη διενέργεια μιας DPIA. Η πρακτική εφαρμογή μιας DPIA θα εξαρτηθεί από τις απαιτήσεις που ορίζονται στον ΓΚΠΔ, οι οποίες μπορούν να συμπληρωθούν με αναλυτικότερες πρακτικές οδηγίες. Συνεπώς, η εφαρμογή μιας DPIA είναι κλιμακούμενη με αποτέλεσμα κάθε υπεύθυνος επεξεργασίας δεδομένων μπορεί να

σχεδιάσει και να εφαρμόσει μια DPIA που να ανταποκρίνεται στις διαδικασίες επεξεργασίας του».

Συνεπώς, οι ελεγκτές μπορούν να επιλέξουν τη μεθοδολογία που τους ταιριάζει για κάθε DPIA που πρέπει να διενεργήσουν, ενώ έχουν την δυνατότητα να αξιοποιήσουν την εμπειρία που μπορεί να έχουν με πιο τεχνικές αξιολογήσεις κινδύνου, π.χ. στο πλαίσιο του ISO 31000. Ωστόσο, η WP29 σημειώνει ορθά τη διαφορετική προοπτική από την οποία πρέπει να διεξάγονται οι DPIA βάσει του ΓΚΠΔ και οι αξιολογήσεις βάσει του ISO.

4.1.1 Απαιτήσεις του ΓΚΠΔ σχετικά με τις εκτιμήσεις αντικτύπου για την προστασία δεδομένων & μεθοδολογίες για DPIAs

Ο ΓΚΠΔ επιβάλλει γενική υποχρέωση στους υπευθύνους επεξεργασίας δεδομένων προσωπικού χαρακτήρα να «λαμβάνουν υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» που ενέχει κάθε πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα και να «εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζουν και να είναι σε θέση να αποδεικνύουν ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον παρόντα κανονισμό» (άρθρο 24 παράγραφος 1, βλ. επίσης άρθρο 24 παράγραφος 1). 25(1))) [17].

Η συμμόρφωση με αυτές τις απαιτήσεις απαιτεί την εξακρίβωση, την καταγραφή και την αντιμετώπιση (μετριασμό) των σχετικών κινδύνων. Αδιαμφισβήτητα, αυτό ισχύει πολύ περισσότερο για τις πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες, βάσει μιας τέτοιας γενικής εκτίμησης κινδύνου, θεωρείται ότι ενέχουν πιθανό «υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 35 παράγραφος 1). Σε μια τέτοια περίπτωση, ο υπεύθυνος επεξεργασίας υποχρεούται να διενεργήσει και να καταγράψει επίσημη εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA) πριν προχωρήσει στην πράξη (idem).

Πιο συγκεκριμένα, ο ΓΚΠΔ σημειώνει πως οι «υψηλοί κίνδυνοι» μπορεί να προέρχονται «ιδίως» από τη χρήση «νέων τεχνολογιών» (άρθρο 35 παράγραφος 1) και προσθέτει ότι πρέπει σε κάθε περίπτωση να διενεργείται DPIA σε περιπτώσεις πλήρως αυτοματοποιημένης λήψης αποφάσεων βάσει προφίλ, επεξεργασίας ευαίσθητων δεδομένων μεγάλης κλίμακας ή παρακολούθησης μεγάλης κλίμακας σε δημόσια προσβάσιμο χώρο (άρθρο 35 παράγραφος 3) [5]. Οι εθνικές αρχές προστασίας δεδομένων

(ΑΠΔΠΧ) πρέπει επίσης να θεσπίζουν καταλόγους των πράξεων που θα υπόκεινται σε DPIA στην επικράτειά τους, και μπορούν να θεσπίζουν καταλόγους των πράξεων που δεν θα απαιτούν DPIA, αλλά οι κατάλογοι αυτοί πρέπει να υποβάλλονται στο EDPB και μπορούν να αμφισβητηθούν από άλλες ΑΠΔΠΧ βάσει του «μηχανισμού συνέπειας» του ΓΚΠΔ (άρθρο 35 παράγραφοι 4 έως 6). Ο ΓΚΠΔ επιτρέπει επίσης στο EDPB να εκδώσει δικό του αρνητικό και θετικό κατάλογο, βασιζόμενο σε αυτούς που του υποβάλλουν οι εθνικές ΑΠΔΠΧ (οι οποίες υποχρεούνται να το πράξουν βάσει του άρθρου 64 παράγραφος 1 στοιχείο α του ΓΚΠΔ). [18]

Στην πράξη, η ομάδα εργασίας του άρθρου 29 εξέδωσε εκτενείς συμβουλές και κατευθυντήριες γραμμές σχετικά με τη διενέργεια μιας DPIA, τόσο στις κατευθυντήριες γραμμές της για τους Υπεύθυνους Προστασίας Δεδομένων (DPOs) του Δεκεμβρίου 2016, όπως αναθεωρήθηκαν τον Απρίλιο του 2017 (WP243 rev1), όσο και στις μεταγενέστερες, πιο λεπτομερείς κατευθυντήριες γραμμές της για τις DPIAs, οι οποίες εγκρίθηκαν στις 4 Απριλίου 2017, όπως αναθεωρήθηκαν και εγκρίθηκαν στις 4 Οκτωβρίου 2017 (χρονολογικά πριν από την εφαρμογή του ΓΚΠΔ) [3]. Και οι δύο εγκρίθηκαν από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων την ημέρα που τέθηκε σε πλήρη εφαρμογή ο ΓΚΠΔ, στις 25 Μαΐου 2018. Ο European Data Protection Supervisor (EDPS) παρείχε επίσης χρήσιμη καθοδήγηση στο έγγραφο του σχετικά με τη λογοδοσία επί τόπου, συμπεριλαμβανομένου ενός προσωρινού καταλόγου των πράξεων επεξεργασίας για τις οποίες, απαιτείται ή δεν απαιτείται DPIA. Επίσης, οι κατευθυντήριες γραμμές της WP29 σχετικά με τις DPIA, οι οποίες εγκρίθηκαν από το EDPB, καθορίζουν εννέα κριτήρια που θα πρέπει να λαμβάνονται υπόψη κατά τον προσδιορισμό του κατά πόσον μια πράξη επεξεργασίας είναι πιθανό να οδηγήσει σε «υψηλό κίνδυνο», και πιο συγκεκριμένα αναφέρουν ότι [11]:

«Στις περισσότερες περιπτώσεις, ένας υπεύθυνος επεξεργασίας δεδομένων μπορεί να θεωρήσει ότι μια επεξεργασία που πληροί δύο κριτήρια απαιτεί τη διενέργεια DPIA. Σε γενικές γραμμές, η WP29 θεωρεί ότι όσο περισσότερα κριτήρια πληρούνται από την επεξεργασία, τόσο πιθανότερο είναι να παρουσιάζει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, ως εκ τούτου, να απαιτεί DPIA, ανεξάρτητα από τα μέτρα που σκοπεύει να λάβει ο υπεύθυνος επεξεργασίας».

Αξίζει να σημειωθεί ότι, με κάποιες καθυστερήσεις, όλες οι εθνικές ΑΠΔΠΧ των κρατών μελών της ΕΕ (συμπεριλαμβανομένου του Ηνωμένου Βασιλείου), υιοθέτησαν τους δικούς τους προσωρινούς καταλόγους και τους υπέβαλαν στο EDPB για επανεξέταση. Ειδικότερα, το 2018 και το 2019, το EDPB διεξήγαγε τις εν λόγω αναθεωρήσεις υπό το πρίσμα των

κατευθυντήριων γραμμών της WP29 που είχε εγκρίνει και εξέδωσε σειρά γνωμοδοτήσεων σχετικά με τους εν λόγω καταλόγους (μία για κάθε σχέδιο καταλόγου). Το κύριο σημείο που διατύπωσε σταθερά το EDPB στις εν λόγω γνωμοδοτήσεις ήταν η σύσταση προς τις ΑΠΔΠΧ ότι δεν θα πρέπει να περιλαμβάνουν πράξεις επεξεργασίας στον κατάλογο των πράξεων για τις οποίες είναι υποχρεωτική η διενέργεια DPIA, εάν η εν λόγω πράξη πληροί μόνο ένα από τα κριτήρια για τον προσδιορισμό του κατά πόσον υπάρχει πιθανός «υψηλός κίνδυνος», τα οποία ορίζονται στις κατευθυντήριες γραμμές. Χαρακτηριστικό παράδειγμα αποτελεί η γνωμοδότηση της αναφορικά με το σχέδιο καταλόγου που υπέβαλε το Ηνωμένο Βασίλειο, το οποίο αναφέρει [19]:

«Ο κατάλογος που υπέβαλε η Εποπτική Αρχή του Ηνωμένου Βασιλείου για γνωμοδότηση του Συμβουλίου Προστασίας Δεδομένων αναφέρει ότι η επεξεργασία βιομετρικών δεδομένων εμπίπτει στην υποχρέωση διενέργειας DPIA από μόνη της. Το Συμβούλιο Προστασίας Δεδομένων είναι της γνώμης ότι η επεξεργασία βιομετρικών δεδομένων από μόνη της δεν είναι κατ' ανάγκη πιθανό να αντιπροσωπεύει υψηλό κίνδυνο. Ωστόσο, η επεξεργασία βιομετρικών δεδομένων με σκοπό τη μοναδική ταυτοποίηση ενός φυσικού προσώπου σε συνδυασμό με τουλάχιστον ένα άλλο κριτήριο απαιτεί τη διενέργεια DPIA. Ως εκ τούτου, το Συμβούλιο Προστασίας Δεδομένων ζητεί από την Εποπτική Αρχή του Ηνωμένου Βασιλείου να τροποποιήσει τον κατάλογό της αναλόγως, προσθέτοντας ότι το στοιχείο που αναφέρεται στην επεξεργασία βιομετρικών δεδομένων με σκοπό τη μοναδική ταυτοποίηση φυσικού προσώπου απαιτεί τη διενέργεια DPIA μόνο όταν γίνεται σε συνδυασμό με τουλάχιστον ένα άλλο κριτήριο, με την επιφύλαξη του άρθρου 35 παράγραφος 3 του ΓΚΠΔ».

Αδιαμφισβήτητα, ο υπεύθυνος επεξεργασίας μπορεί να διενεργήσει DPIA ακόμη και αν πληρείται μόνο ένα από τα κριτήρια, χωρίς όμως αυτό να αποτελεί υποχρέωση. Η απαίτηση για DPIA μπορεί να παρακαμφθεί σε περιπτώσεις στις οποίες ένας νόμος ρυθμίζει το είδος της εν λόγω πράξης και έχει διενεργηθεί γενική DPIA στο πλαίσιο της έκδοσης του νόμου (άρθρο 35 παράγραφος 10) [5]. Συνοπτικά και σύμφωνα με το WP29, η διεξαγωγή της εκτίμησης αντικτύπου δεν απαιτείται όταν:

- δεν είναι πιθανό να οδηγήσει σε «υψηλό κίνδυνο»,
- έχει εκπονηθεί παρόμοια DPIA,
- έχει εγκριθεί πριν από τον Μάϊο του 2018,
- έχει νομική βάση ή

- περιλαμβάνεται στον κατάλογο πράξεων επεξεργασίας για τις οποίες δεν απαιτείται DPIA.

4.2 WP29 (EDPB)

Το WP29 απαριθμεί μια σειρά παραγόντων, οι περισσότεροι αλλά όχι όλοι σχετικοί με τα τρία παραδείγματα του άρθρου 35, που υποδηλώνουν ότι μια πράξη μεταποίησης ενέχει «υψηλούς κινδύνους», και παραθέτει περαιτέρω, πιο συγκεκριμένα παραδείγματα. Ο EDPB παρέχει περαιτέρω παραδείγματα, τόσο στον προσωρινό του κατάλογο των πράξεων επεξεργασίας που θα απαιτούν πάντοτε DPIA, όσο και σε ένα υπόδειγμα που μπορεί να χρησιμοποιηθεί για να αξιολογηθεί κατά πόσον οι πράξεις επεξεργασίας που δεν περιλαμβάνονται ούτε στον «θετικό» κατάλογο (πράξεις που κατά την άποψή του απαιτούν πάντοτε DPIA) ούτε στον «αρνητικό» κατάλογο (πράξεις που δεν απαιτούν DPIA) θα πρέπει να υποβληθούν σε DPIA. Αυτά τα παραδείγματα της WP29 και του EDPS παρατίθενται κατωτέρω [11]:

4.2.1 Παράγοντες που υποδηλώνουν «υψηλούς κινδύνους»

1. Αξιολόγηση ή βαθμολόγηση, συμπεριλαμβανομένης της κατάρτισης προφίλ και της πρόβλεψης, ιδίως από «πτυχές που αφορούν την απόδοση του υποκειμένου των δεδομένων στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή τα ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τον τόπο διαμονής ή τις μετακινήσεις» (αιτιολογικές σκέψεις 71 και 91). Χαρακτηριστικό παράδειγμα αποτελεί μια εταιρεία βιοτεχνολογίας που προσφέρει γενετικά τεστ απευθείας στους καταναλωτές για την αξιολόγηση και την πρόβλεψη των ασθενειών/κινδύνων υγείας ή μια τράπεζα που ελέγχει τις συναλλαγές σύμφωνα με την ισχύουσα νομοθεσία για τον εντοπισμό πιθανών δόλιων συναλλαγών.

2. Αυτοματοποιημένη λήψη αποφάσεων με νομικά ή παρόμοια σημαντικά αποτελέσματα: Επεξεργασία που αποσκοπεί στη λήψη αποφάσεων σχετικά με τα υποκείμενα των δεδομένων που παράγουν «νομικά αποτελέσματα που αφορούν το φυσικό πρόσωπο» ή που «επηρεάζουν παρόμοια σημαντικά το φυσικό πρόσωπο» (άρθρο 35 παράγραφος 3 στοιχείο α), ιδιαίτερα σε περιπτώσεις στις οποίες η

επεξεργασία μπορεί να οδηγήσει σε αποκλεισμό ή διάκριση εις βάρος ατόμων. Για παράδειγμα, ο εντοπισμός παιδιών που «κινδυνεύουν» να γίνουν παχύσαρκα ή μέλη συμμοριών/εγκληματίες, βάσει προφίλ.

3. Συστηματική παρακολούθηση: Επεξεργασία που χρησιμοποιείται για την παρατήρηση, την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, συμπεριλαμβανομένων των δεδομένων που συλλέγονται μέσω δικτύων ή «συστηματικής παρακολούθησης ενός χώρου προσβάσιμου στο κοινό» (άρθρο 35 παράγραφος 3 στοιχείο γ)). Αυτό το είδος παρακολούθησης αποτελεί κριτήριο, διότι τα δεδομένα προσωπικού χαρακτήρα μπορεί να συλλέγονται σε συνθήκες όπου τα υποκείμενα των δεδομένων μπορεί να μην γνωρίζουν ποιος συλλέγει τα δεδομένα τους και πώς θα χρησιμοποιηθούν. Επιπλέον, μπορεί να είναι αδύνατο για τα άτομα να αποφύγουν να υποβληθούν σε μια τέτοια επεξεργασία σε δημόσιο (ή δημόσια προσβάσιμο) χώρο (ή χώρους). Πιο συγκεκριμένα, πρόκειται για παραδείγματα όπως μια κρυμμένη CCTV ή μια smart CCTV με λογισμικό αναγνώρισης προσώπου σε χώρους προσβάσιμους προς το κοινό, η ανάλυση της «κίνησης» στο Διαδίκτυο με παραβίαση της κρυπτογράφησης ακόμα και η επεξεργασία μεταδεδομένων (Metadata) δηλαδή ο χρόνος, η φύση αλλά και η διάρκεια μιας συναλλαγής σε τραπεζικό λογαριασμό για οργανωτικούς σκοπούς ή για την παροχή δημοσιονομικών εκτιμήσεων.

4. Ευαίσθητα δεδομένα ή δεδομένα προσωπικού χαρακτήρα: περιλαμβάνει ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 (δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, δεδομένα υγείας, γενετικά ή βιομετρικά δεδομένα και δεδομένα σεξουαλικού προσανατολισμού), καθώς και δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές διώξεις ή αδικήματα, όπως ορίζονται στο άρθρο 10. Εκτός από αυτές τις διατάξεις του ΓΚΠΔ, ορισμένες κατηγορίες δεδομένων μπορεί να θεωρηθεί ότι αυξάνουν τον πιθανό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Αξίζει να σημειωθεί πως ο όρος ευαίσθητα είναι κοινά αποδεκτός καθώς συνδέονται με οικιακές και ιδιωτικές δραστηριότητες (βλ. το δεύτερο παράδειγμα), ή επειδή επηρεάζουν την άσκηση ενός θεμελιώδους δικαιώματος (βλ. το τρίτο παράδειγμα) ή επειδή η παραβίαση τους συνεπάγεται με

σοβαρές επιπτώσεις στην καθημερινή ζωή του υποκειμένου των δεδομένων. Στο πλαίσιο αυτό, μπορεί να έχει σημασία αν τα δεδομένα έχουν ήδη δημοσιοποιηθεί από το υποκείμενο των δεδομένων ή από τρίτους, ενώ παρατίθενται σχετικά παραδείγματα:

- Γενικό νοσοκομείο που τηρεί ιατρικούς φακέλους ασθενών ή αιτούντων πρόνοιας.
- Ένας δημόσιος φορέας ή μια ιδιωτική οντότητα (π.χ. ένας εργοδότης) έχει πρόσβαση σε προσωπικά έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, ημερολόγια ή σημειώσεις από ηλεκτρονικούς αναγνώστες εξοπλισμένους με λειτουργίες σημειώσεων, οι οποίοι χρησιμοποιούνται από το προσωπικό τόσο για προσωπικούς όσο και για επαγγελματικούς σκοπούς, ιδιαίτερα σε περιπτώσεις «Bring Your Own Device» (BYOD).
- Ένας δημόσιος φορέας ή μια ιδιωτική οντότητα αποκτά πρόσβαση σε προσωπικές πληροφορίες που περιέχονται σε εφαρμογές καταγραφής ζωής ή χρησιμοποιεί πληροφορίες από τα μέσα κοινωνικής δικτύωσης σε πλαίσια που μπορούν να έχουν σημαντικό αντίκτυπο στα ενδιαφερόμενα άτομα, όπως η επιλογή ατόμων για θέσεις εργασίας ή και συνεντεύξεις.
- Οποιαδήποτε χρήση βιομετρικής ταυτοποίησης

5. <u>Επεξεργασία δεδομένων σε μεγάλη κλίμακα:</u> Ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλη κλίμακα, αν και η αιτιολογική σκέψη 91 παρέχει κάποια καθοδήγηση. Σε κάθε περίπτωση, η WP29 συνιστά να λαμβάνονται υπόψη ιδίως οι ακόλουθοι παράγοντες για να καθοριστεί εάν η επεξεργασία πραγματοποιείται σε μεγάλη κλίμακα:
    - ο αριθμός των ενδιαφερόμενων υποκειμένων των δεδομένων είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό του σχετικού πληθυσμού,
    - ο όγκος των δεδομένων ή και το εύρος των διαφορετικών στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία,
    - την διάρκεια ή την μονιμότητα της δραστηριότητας επεξεργασίας δεδομένων και
    - τη γεωγραφική έκταση της δραστηριότητας επεξεργασίας.

    Σχετικά παραδείγματα για να διευκρινιστεί η «επεξεργασία δεδομένων σε μεγάλη κλίμακα» αποτελούν οι ανταλλαγές δεδομένων μεγάλης κλίμακας μεταξύ ελεγκτών του δημόσιου τομέα (π.χ. υπουργεία, τοπικές και περιφερειακές αρχές) μέσω ηλεκτρονικών δικτύων, η μεγάλης κλίμακας συλλογή γενεαλογικών πληροφοριών για

οικογένειες ατόμων που ανήκουν σε μια συγκεκριμένη θρησκευτική ομάδα [20], η δημιουργία πολύ μεγάλων «βάσεων δεδομένων τρόπου ζωής» για σκοπούς μάρκετινγκ, οι οποίες μπορούν να χρησιμοποιηθούν και για άλλους σκοπούς αλλά και η καταγραφή από τα πολιτικά κόμματα των εκτιμώμενων προθέσεων ψήφου ενός πολύ μεγάλου αριθμού ψηφοφόρων σε εθνικό επίπεδο, βάσει συνεντεύξεων και η επακόλουθη ανάλυση και χρήση αυτών των δεδομένων [1].

6. Αντιστοίχιση ή συνδυασμός συνόλων δεδομένων, ιδίως εάν προέρχονται από δύο ή περισσότερες πράξεις επεξεργασίας δεδομένων που εκτελούνται για διαφορετικούς σκοπούς ή εκτελούνται από διαφορετικούς υπευθύνους επεξεργασίας δεδομένων κατά τρόπο που υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων. Για παράδειγμα, μια φορολογική υπηρεσία αντιπαραβάλλει τα αρχεία των φορολογικών της δηλώσεων με τα αρχεία των ιδιοκτητών ακριβών σκαφών προκειμένου να εντοπίσει άτομα που ενδεχομένως διαπράττουν φορολογική απάτη.

7. Δεδομένα που αφορούν ευάλωτα υποκείμενα των δεδομένων (αιτιολογική σκέψη 75): η επεξεργασία αυτού του τύπου δεδομένων αποτελεί κριτήριο λόγω της αυξημένης ανισορροπίας ισχύος μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας, πράγμα που σημαίνει ότι τα άτομα ενδέχεται να μην είναι σε θέση να συναινέσουν εύκολα στην επεξεργασία των δεδομένων τους ή να αντιταχθούν σε αυτήν ακόμα και να ασκήσουν τα δικαιώματά τους. Τα ευάλωτα υποκείμενα των δεδομένων μπορεί μεταξύ άλλων να περιλαμβάνουν παιδιά, τα οποία μπορεί να θεωρηθεί ότι δεν είναι σε θέση να αντιταχθούν εν γνώσει τους και να συναινέσουν, εργαζόμενους, πιο ευάλωτα τμήματα του πληθυσμού που χρήζουν ειδικής προστασίας (ψυχικά ασθενείς, αιτούντες άσυλο ή ηλικιωμένοι, ασθενείς) και σε κάθε περίπτωση οπουδήποτε μπορεί να εντοπιστεί ανισορροπία στη σχέση μεταξύ της θέσης του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας. Αδιαμφισβήτητα, η χρήση συστημάτων βιντεοεπιτήρησης και γεωεντοπισμού που

[1] Η πρακτική αυτή είναι κοινή και μάλιστα παραδοσιακή στο Ηνωμένο Βασίλειο, όπως αναγνωρίζεται στην αιτιολογική σκέψη 56 του ΓΚΠΔ. Η εν λόγω αιτιολογική σκέψη αναφέρει ότι «αυτό μπορεί να επιτραπεί για λόγους δημοσίου συμφέροντος, υπό την προϋπόθεση ότι θεσπίζονται οι κατάλληλες εγγυήσεις». Η ανάγκη να αξιολογηθεί κατά πόσον η επεξεργασία εξυπηρετεί πράγματι ένα νόμιμο δημόσιο συμφέρον και η απαίτηση για τη θέσπιση «κατάλληλων εγγυήσεων» υπογραμμίζουν την ανάγκη σοβαρής ανάλυσης κινδύνου και εκτίμησης των επιπτώσεων.

επιτρέπουν την εξ αποστάσεως παρακολούθηση των δραστηριοτήτων των εργαζομένων [21].

8. Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων [5]: Ο ΓΚΠΔ καθιστά σαφές (άρθρο 35 παράγραφος 1 και αιτιολογικές σκέψεις 89 και 91) ότι η χρήση μιας νέας τεχνολογίας, η οποία ορίζεται «σύμφωνα με την επιτευχθείσα κατάσταση των τεχνολογικών γνώσεων» (αιτιολογική σκέψη 91), μπορεί να προκαλέσει την ανάγκη διενέργειας DPIA. Αυτό οφείλεται στο γεγονός ότι η χρήση μιας τέτοιας τεχνολογίας μπορεί να συνεπάγεται νέες μορφές ή τύπους συλλογής και χρήσης δεδομένων, ενδεχομένως αόρατες και με υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των ατόμων. Για την ακρίβεια, οι προσωπικές και κοινωνικές συνέπειες της ανάπτυξης μιας νέας τεχνολογίας μπορεί να είναι άγνωστες. Η διεξαγωγή μιας DPIA θα διευκολύνει τον υπεύθυνο επεξεργασίας δεδομένων να κατανοήσει και να αντιμετωπίσει αυτούς τους κινδύνους, ενώ τα μέτρα μετριασμού θα πρέπει να επιτρέπουν στα υποκείμενα των δεδομένων και στο ευρύ κοινό να βλέπουν πώς, πότε και για ποιους σκοπούς πρόκειται να χρησιμοποιηθούν οι νέες τεχνολογίες, ώστε να μπορούν να προφυλαχθούν από εκείνες που μπορούν να υπονομεύσουν τα ατομικά δικαιώματα και ελευθερίες και να οδηγήσουν σε αυταρχική διακυβέρνηση ή μαζική παρακολούθηση από εταιρείες. Αξίζει να τονιστεί ότι σε πολλές περιπτώσεις νέων τεχνολογιών ή πρακτικών, η εκάστοτε ΑΠΔΠΧ μπορεί να εκδίδει ή να έχει ήδη εκδώσει γνώμες, κατευθυντήριες γραμμές ή συστάσεις, και οι υπεύθυνοι επεξεργασίας θα πρέπει να είναι σε εγρήγορση για να παρακολουθούν τέτοια νέα έγγραφα. Σε περίπτωση που δεν υπάρχει σχετική καθοδήγηση ή δεν έχει ακόμη εκδοθεί, θα πρέπει να συμβουλευτούν την ΑΠΔΠΧ τους. Ειδικότερα, οι νέες τεχνολογίες μπορεί να αποσκοπούν στην παρακολούθηση του χρόνου και της παρουσίας των εργαζομένων, συμπεριλαμβανομένων εκείνων που επεξεργάζονται βιομετρικά δεδομένα ή και παρακολουθούν κινητές συσκευές [4].

9. Όταν η επεξεργασία αυτή καθαυτή «εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν ένα δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή ένα συμβόλαιο» (άρθρο 22 και αιτιολογική σκέψη 91). Αυτό περιλαμβάνει πράξεις επεξεργασίας που αποσκοπούν στο να επιτραπεί, να τροποποιηθεί ή να απορριφθεί η πρόσβαση των υποκειμένων των δεδομένων σε μια υπηρεσία ή η σύναψη μιας σύμβασης. Χαρακτηριστικό παράδειγμα αποτελεί ένα χρηματοπιστωτικό ίδρυμα ή ένας

οργανισμός αναφοράς πιστώσεων που λαμβάνει υπόψη τη διαφορά ηλικίας μεταξύ των συζύγων σε έναν γάμο για να προσδιορίσει την πιστοληπτική ικανότητα, πράξη που μπορεί να εμποδίσει την ελεύθερη άσκηση του θεμελιώδους δικαιώματος του γάμου, και ως εκ τούτου απαγορεύτηκε στη Γαλλία από τη γαλλική ΑΠΔΠΧ, την CNIL, η οποία έπρεπε να αξιολογήσει το σύστημα επειδή, δεδομένου ότι έπαιρνε αποφάσεις βάσει προφίλ, υπόκειτο σε «προηγούμενη έγκριση» από την CNIL.

4.2.2 Πράξεις υψηλού κινδύνου πολλαπλών παραγόντων

Οι παράγοντες που απαριθμούνται ανωτέρω μπορούν να επικαλύπτονται ή να συνδυάζονται, π.χ. η «συστηματική παρακολούθηση» μπορεί να επικαλύπτεται και να συνδυάζεται με την αυτοματοποιημένη λήψη αποφάσεων βάσει προφίλ και μπορεί να περιλαμβάνει επεξεργασία «ευαίσθητων δεδομένων» σε «μεγάλη κλίμακα». Το WP29 παρέχει ορισμένα παραδείγματα πράξεων με τέτοιους συνδυασμένους παράγοντες (ή κριτήρια) για τις οποίες απαιτείται DPIA, καθώς και παραδείγματα πράξεων στις οποίες υπάρχει ένας ή περισσότεροι από τους παραπάνω παράγοντες, αλλά δεν απαιτείται DPIA, οι οποίοι παρατίθενται στον ακόλουθο πίνακα [11]:

Παραδείγματα επεξεργασίας	Συναφή κριτήρια	Πιθανή απαίτηση για DPIA;
Ένα νοσοκομείο επεξεργάζεται τα γενετικά και υγειονομικά δεδομένα των ασθενών του	- Ευαίσθητα δεδομένα ή δεδομένα άκρως προσωπικού χαρακτήρα. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων. - Δεδομένα που υποβάλλονται σε επεξεργασία σε μεγάλη κλίμακα.	Ναι
Η χρήση ενός συστήματος καμερών για την παρακολούθηση της οδηγικής συμπεριφοράς σε αυτοκινητόδρομους. Ο ελεγκτής προβλέπει τη χρήση ενός ευφυούς συστήματος ανάλυσης βίντεο για την απομόνωση των αυτοκινήτων και την αυτόματη αναγνώριση των πινακίδων κυκλοφορίας.	- Συστηματική παρακολούθηση. - Καινοτόμος χρήση ή εφαρμογή τεχνολογικών ή οργανωτικών λύσεων.	
Μια εταιρεία που παρακολουθεί συστηματικά τις δραστηριότητες των υπαλλήλων της, συμπεριλαμβανομένης της παρακολούθησης του σταθμού εργασίας των υπαλλήλων, της δραστηριότητας στο διαδίκτυο κ.λπ.	- Συστηματική παρακολούθηση. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.	
Η συλλογή δημόσιων δεδομένων από τα μέσα κοινωνικής δικτύωσης για τη δημιουργία προφίλ.	- Αξιολόγηση ή βαθμολόγηση. - Επεξεργασία δεδομένων σε μεγάλη κλίμακα. - Αντιστοίχιση ή συνδυασμός συνόλων δεδομένων. - Ευαίσθητα δεδομένα ή δεδομένα προσωπικού χαρακτήρα.	

Ένα ίδρυμα που δημιουργεί μια βάση δεδομένων αξιολόγησης πιστοληπτικής ικανότητας ή απάτης σε εθνικό επίπεδο.	- Αξιολόγηση ή βαθμολόγηση. - Αυτοματοποιημένη λήψη αποφάσεων με νομικό ή παρόμοιο σημαντικό αποτέλεσμα. - Εμποδίζει το υποκείμενο των δεδομένων να ασκήσει ένα δικαίωμα ή να χρησιμοποιήσει μια υπηρεσία ή μια σύμβαση. - Ευαίσθητα δεδομένα ή δεδομένα άκρως προσωπικού χαρακτήρα	
Αποθήκευση για σκοπούς αρχειοθέτησης ψευδωνυμοποιημένων ευαίσθητων προσωπικών δεδομένων που αφορούν ευάλωτα υποκείμενα ερευνητικών έργων ή κλινικών δοκιμών	- Ευαίσθητα δεδομένα. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων. - Εμποδίζουν τα υποκείμενα των δεδομένων να ασκήσουν ένα δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή μια σύμβαση.	
Επεξεργασία «προσωπικών δεδομένων ασθενών ή πελατών από μεμονωμένο ιατρό, άλλο επαγγελματία υγείας ή δικηγόρο» (αιτιολογική σκέψη 91)	- Ευαίσθητα δεδομένα ή δεδομένα άκρως προσωπικού χαρακτήρα. - Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων.	Όχι
Ένα διαδικτυακό περιοδικό που χρησιμοποιεί μια λίστα αλληλογραφίας για να στέλνει μια γενική ημερήσια σύνοψη στους συνδρομητές του με τη συγκατάθεσή τους, και η οποία περιλαμβάνει ένα εύκολο μέσο για να εξαιρεθούν από περαιτέρω αποστολές.	- Επεξεργασία δεδομένων σε μεγάλη κλίμακα.	
Ένας δικτυακός τόπος ηλεκτρονικού εμπορίου που προβάλλει διαφημίσεις για ανταλλακτικά παλαιών αυτοκινήτων και		

περιλαμβάνει περιορισμένο προφίλ με βάση τα αντικείμενα που έχουν προβληθεί ή αγοραστεί στον δικό του δικτυακό τόπο, και πάλι με εύκολη δυνατότητα εξαίρεσης.	- Αξιολόγηση ή βαθμολόγηση.	

Πίνακας 3: Παραδείγματα Επεξεργασίας

Πιο συγκεκριμένα, η WP29 παρέχει ορισμένα παραδείγματα μεθοδολογιών προστασίας δεδομένων και επιπτώσεων στην ιδιωτική ζωή που εκπονούνται από τις εθνικές ΑΠΔΠΧ, ενώ ταυτόχρονα «ενθαρρύνει την ανάπτυξη πλαισίων DPIA για συγκεκριμένους τομείς». Η ίδια έχει δημοσιεύσει ένα πλαίσιο DPIA για εφαρμογές RFID [6] και ένα πρότυπο DPIA για έξυπνα δίκτυα και έξυπνα συστήματα μέτρησης. Η WP29 προτείνει τα ακόλουθα κριτήρια τα οποία μπορούν να χρησιμοποιούν οι υπεύθυνοι επεξεργασίας δεδομένων για να αξιολογούν κατά πόσον μια DPIA ή μια μεθοδολογία για τη διενέργεια DPIA είναι επαρκώς περιεκτική ώστε να συμμορφώνεται με τον ΓΚΠΔ [22]:

1. Προβλέπεται συστηματική περιγραφή της επεξεργασίας (άρθρο 35 παράγραφος 7 στοιχείο α)):
    - λαμβάνονται υπόψη η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90),
    - καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος για την οποία θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα,
    - παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας,
    - προσδιορίζονται τα περιουσιακά στοιχεία στα οποία βασίζονται τα δεδομένα προσωπικού χαρακτήρα (υλικό, λογισμικό, δίκτυα, άνθρωποι),
    - λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 παράγραφος 8)[2].

[2] Το WP29 σημειώνεις ότι «Θα πρέπει επίσης να λαμβάνονται υπόψη τα πιστοποιητικά, οι σφραγίδες και τα σήματα για την απόδειξη της συμμόρφωσης με τον ΓΚΠΔ των πράξεων επεξεργασίας από τους υπευθύνους επεξεργασίας και τους εκτελούντες την επεξεργασία (άρθρο 42), καθώς και οι δεσμευτικοί εταιρικοί κανόνες (BCR).»

2. Αξιολογείται η αναγκαιότητα και η αναλογικότητα (άρθρο 35 παράγραφος 7 στοιχείο β)):
    - καθορίζονται τα μέτρα που προβλέπονται για τη συμμόρφωση με τον κανονισμό (άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90, κατά τα οποία λαμβάνονται υπόψη:
        → τα μέτρα που συμβάλλουν στην αναλογικότητα και την αναγκαιότητα της επεξεργασίας βάσει:
            i. καθορισμένου, ρητού και νόμιμου σκοπού (άρθρο 5 παράγραφος 1 στοιχείο β)),
            ii. τη νομιμότητα της επεξεργασίας (άρθρο 6),
            iii. επαρκή, συναφή και να περιορίζονται στα αναγκαία δεδομένα (άρθρο 5 παράγραφος 1 στοιχείο γ)) και
            iv. περιορισμένη διάρκεια αποθήκευσης (άρθρο 5 παράγραφος 1 στοιχείο ε)). [5]
        → μέτρα που συμβάλλουν στα δικαιώματα των υποκειμένων των δεδομένων:
            i. πληροφορίες που παρέχονται στο υποκείμενο των δεδομένων (άρθρα 12, 13 και 14),
            ii. δικαίωμα πρόσβασης και φορητότητας των δεδομένων (άρθρα 15 και 20),
            iii. δικαίωμα διόρθωσης και διαγραφής (άρθρα 16, 17 και 19),
            iv. δικαίωμα εναντίωσης και περιορισμού της επεξεργασίας (άρθρα 18, 19 και 21),
            v. σχέσεις με τους εκτελούντες την επεξεργασία (άρθρο 28),
            vi. διασφαλίσεις που περιβάλλουν τη διεθνή διαβίβαση (κεφάλαιο V),
            vii. προηγούμενη διαβούλευση (άρθρο 36).

3. Η διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (άρθρο 35 παράγραφος 7 στοιχείο γ):
    - εκτιμώνται η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (βλ. αιτιολογική σκέψη 84) ή, πιο συγκεκριμένα, για κάθε κίνδυνο (παράνομη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων) από την άποψη των υποκειμένων των δεδομένων:
        → λαμβάνονται υπόψη οι πηγές κινδύνου (αιτιολογική σκέψη 90),

→ προσδιορίζονται οι πιθανές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περίπτωση γεγονότων που περιλαμβάνουν παράνομη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων,

→ εντοπίζονται οι απειλές που θα μπορούσαν να οδηγήσουν σε παράνομη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων και

→ εκτιμάται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90).

- καθορίζονται τα μέτρα που προβλέπονται για την αντιμετώπιση των κινδύνων αυτών (άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90),

4. Εμπλέκονται τα ενδιαφερόμενα μέρη:
    - ζητείται η συμβουλή του ΥΠΔ (άρθρο 35 παράγραφος 2) και

ζητείται η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους, κατά περίπτωση (άρθρο 35 παράγραφος 9).

4.2.3 Αρχείο της DPIA

Ο πρώτος και κύριος σκοπός του αρχείου της DPIA, ο οποίος καλύπτει όλα τα παραπάνω «κριτήρια», είναι να υπάρχουν αποδείξεις ότι έχει διενεργηθεί ορθή, εμπεριστατωμένη DPIA σύμφωνα με τον ΓΚΠΔ, δηλαδή ότι πληροί τα παραπάνω κριτήρια. Επιπλέον, μπορεί να χρησιμοποιηθεί σε δύο αντίθετες περιπτώσεις [11]:

1. Όταν η DPIA προσδιορίζει ταυτόχρονα τόσο τους (υψηλούς) κινδύνους όσο και τα μέτρα που μπορούν να ληφθούν για την αντιμετώπιση των κινδύνων αυτών, τα οποία είναι «κατάλληλα», λαμβάνοντας υπόψη την πιθανότητα και τη σοβαρότητα των κινδύνων και το κόστος των μέτρων, και όταν τα μέτρα αυτά έχουν πράγματι εγκριθεί και υιοθετηθεί (και η έγκριση και υιοθέτηση αυτή έχει επίσης καταγραφεί), το αρχείο DPIA μπορεί να αποτελέσει σημαντικό «στοιχείο» σε μια συνολική απόδειξη της συμμόρφωσης και ένα «ειδικό μέσο» για να επιτευχθεί αυτό, αν και αυτό δεν ισοδυναμεί με νομικό τεκμήριο συμμόρφωσης, παρόλο που ο υπεύθυνος επεξεργασίας θα πρέπει ακόμη να ελέγχει και να παρακολουθεί σε συνεχή βάση ότι τα μέτρα μετριασμού εξακολουθούν να εφαρμόζονται και παραμένουν κατάλληλα υπό το πρίσμα των πρακτικών, οργανωτικών ή τεχνολογικών εξελίξεων.

Παράδειγμα περίπτωσης όπου η DPIA προσδιόρισε τόσο τους υψηλούς κινδύνους όσο και τα μέτρα μετριασμού, τα οποία θεωρήθηκαν (εν προκειμένω από την EuroPrise) επαρκή για να επιτραπεί η επεξεργασία. Κατά συνέπεια, η περίπτωση αυτή θα επέτρεπε στον υπεύθυνο επεξεργασίας να συμπεράνει με βεβαιότητα ότι το αποτέλεσμα της DPIA δείχνει ότι η επεξεργασία δεν θα έπρεπε να υποβληθεί στην αρμόδια ΑΠΔΠΧ για διαβούλευση [4]:

- Μια υπηρεσία πρόνοιας χρησιμοποιεί φωνητική βιομετρική πιστοποίηση ταυτότητας για την αντιμετώπιση της απάτης στην πρόνοια.

  Προσδιορισμός των κινδύνων: Όπως έχει επισημάνει η WP29, τρεις από τους κύριους κινδύνους που εγκυμονεί η χρήση βιομετρικών δεδομένων είναι οι εξής

  → το γεγονός ότι τα βιομετρικά χαρακτηριστικά ενός ατόμου είναι αναντικατάστατα (πράγμα που σημαίνει ότι ένα εργαλείο ελέγχου ταυτότητας που βασίζεται σε ακατέργαστα βιομετρικά δεδομένα, όταν χαθεί, δεν μπορεί να αντικατασταθεί),

  → η ευκολία με την οποία τα βιομετρικά δεδομένα μπορούν να χρησιμοποιηθούν για την αντιστοίχιση διαφορετικών συνόλων δεδομένων και

  → η πιθανότητα τα βιομετρικά δεδομένα να συλλεχθούν κρυφά.

  Μετριασμός των επιπτώσεων: χρησιμοποιείται ένα μοναδικό πρότυπο φωνής, το οποίο δημιουργείται από τα αρχικά («ακατέργαστα») βιομετρικά δεδομένα και όχι από τα ακατέργαστα δεδομένα, τα οποία καταστρέφονται μετά την εγγραφή των υποκειμένων των δεδομένων. Το πρότυπο φωνής είναι μοναδικό για κάθε συγκεκριμένη εφαρμογή και δεν μπορεί να χρησιμοποιηθεί για την επαναδημιουργία των αρχικών (ακατέργαστων) βιομετρικών δεδομένων. Με τον τρόπο αυτό αντιμετωπίζονται και οι τρεις προαναφερθέντες κίνδυνοι:

  → εάν το φωνητικό πρότυπο παραβιαστεί, μπορεί να δημιουργηθεί πολύ απλά ένα νέο, διαφορετικό (με τη βοήθεια του υποκειμένου των δεδομένων, το οποίο θα πρέπει να εγγραφεί εκ νέου)

  → τα διαφορετικά φωνητικά πρότυπα που χρησιμοποιούνται σε διαφορετικές εφαρμογές του ίδιου εργαλείου δεν μπορούν να συγκριθούν μεταξύ τους ή με άλλα φωνητικά δεδομένα ή φωνητικά πρότυπα και

→ το φωνητικό πρότυπο δημιουργείται κατά τη διαδικασία εγγραφής πρόσωπο με πρόσωπο.

Το αρχείο μπορεί επίσης να διατίθεται ή να αξιοποιείται σε διαβουλεύσεις με ενδιαφερόμενα μέρη ή πολίτες ακόμα και σε απαντήσεις ερωτημάτων και καταγγελίες υποκειμένων των δεδομένων και μη κυβερνητικών οργανώσεων που εκπροσωπούν υποκείμενα των δεδομένων. Εν προκειμένω, η WP29 παρατηρεί ότι [3]:

«Η δημοσίευση μιας DPIA δεν αποτελεί νομική απαίτηση του ΓΚΠΔ, αλλά είναι απόφαση του υπεύθυνου επεξεργασίας να το πράξει. Ωστόσο, οι υπεύθυνοι επεξεργασίας θα πρέπει να εξετάζουν το ενδεχόμενο δημοσίευσης τουλάχιστον τμημάτων, όπως μια περίληψη ή ένα συμπέρασμα της DPIA τους.».

Ο σκοπός μιας τέτοιας διαδικασίας θα ήταν να συμβάλει στην ενίσχυση της εμπιστοσύνης στις διαδικασίες επεξεργασίας του υπευθύνου επεξεργασίας και να επιδείξει υπευθυνότητα και διαφάνεια. Αποτελεί ιδιαίτερα καλή πρακτική η δημοσίευση μιας DPIA όταν μέλη του κοινού επηρεάζονται από την πράξη επεξεργασίας. Αυτό θα μπορούσε να συμβεί ιδίως όταν μια δημόσια αρχή διενεργεί DPIA. Ουσιαστικά, η δημοσιευμένη DPIA δεν χρειάζεται να περιέχει ολόκληρη την αξιολόγηση, ιδίως όταν θα μπορούσε να παρουσιάσει συγκεκριμένες πληροφορίες σχετικά με κινδύνους ασφαλείας για τον υπεύθυνο επεξεργασίας δεδομένων ή να αποκαλύψει εμπορικά μυστικά ή εμπορικά ευαίσθητες πληροφορίες. Σε αυτές τις περιπτώσεις, η δημοσιευμένη έκδοση θα μπορούσε να αποτελείται μόνο από μια περίληψη των κύριων συμπερασμάτων της DPIA ή ακόμη και από μια απλή δήλωση ότι έχει διενεργηθεί DPIA.

2. Στην αντίθετη περίπτωση από την παραπάνω, όταν η DPIA εντοπίζει ταυτόχρονα και τους δύο (υψηλούς) κινδύνους και διαπιστώνει ότι δεν υπάρχουν μέτρα που μπορούν να ληφθούν για την επαρκή αντιμετώπιση όλων αυτών των κινδύνων (ή τουλάχιστον δεν υπάρχουν μέτρα που να είναι «κατάλληλα» λαμβάνοντας υπόψη την πιθανότητα και τη σοβαρότητα των κινδύνων και το κόστος των μέτρων), ο υπεύθυνος επεξεργασίας υποχρεούται να ζητήσει τη γνώμη της ΑΠΔΠΧ (άρθρο 36) και το αρχείο της σχετικής DPIA πρέπει να παρασχεθεί στην ΑΠΔΠΧ:
«όταν η DPIA αποκαλύπτει υψηλούς υπολειπόμενους κινδύνους, ο υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να ζητήσει προηγούμενη διαβούλευση για την επεξεργασία από την εποπτική αρχή (άρθρο 36 παράγραφος 1). Στο πλαίσιο αυτό,

η DPIA πρέπει να παρέχεται πλήρως (άρθρο 36 παράγραφος 3 στοιχείο ε)). Η εποπτική αρχή μπορεί να παράσχει τις συμβουλές της και δεν θα θέσει σε κίνδυνο εμπορικά μυστικά ούτε θα αποκαλύψει τρωτά σημεία ασφαλείας, με την επιφύλαξη των αρχών που ισχύουν σε κάθε κράτος μέλος σχετικά με την πρόσβαση του κοινού στα επίσημα έγγραφα.

Τα κράτη μέλη μπορούν επίσης, σύμφωνα με το εθνικό τους δίκαιο [5], να απαιτούν από τους υπευθύνους επεξεργασίας να ζητούν τη γνώμη της ΑΠΔΠΧ «σε σχέση με την επεξεργασία από υπεύθυνο επεξεργασίας για την εκτέλεση καθήκοντος που εκτελεί ο υπεύθυνος επεξεργασίας προς το δημόσιο συμφέρον, συμπεριλαμβανομένης της επεξεργασίας σε σχέση με την κοινωνική προστασία και τη δημόσια υγεία» (άρθρο 36 παράγραφος 5), και αυτό έχει γίνει για τις τελευταίες αυτές περιπτώσεις π.χ. στη Γαλλία και την Ιταλία. Εάν η ΑΠΔΠΧ δεν είναι ικανοποιημένη με τις πληροφορίες που περιέχονται στο αρχείο DPIA (ή/και παρέχονται με άλλο τρόπο), η ΑΠΔΠΧ μπορεί να διατάξει τον υπεύθυνο επεξεργασίας να παράσχει κάθε περαιτέρω πληροφορία που θεωρεί ότι χρειάζεται για την αξιολόγηση του θέματος (άρθρ. 58(1)(α)).

Συνήθως, η ΑΠΔΠΧ θα προσπαθήσει να βοηθήσει τον υπεύθυνο επεξεργασίας να βρει μια λύση - δηλαδή, να προσδιορίσει μέτρα που θα μετριάσουν επαρκώς τους εντοπισμένους (υψηλούς) κινδύνους (κατά τη γνώμη της ΑΠΔΠΧ), και εφόσον ο υπεύθυνος επεξεργασίας συμφωνεί να υιοθετήσει τα μέτρα αυτά (και ότι η υιοθέτηση και η συνεχής χρήση τους ελέγχεται και παρακολουθείται από τον υπεύθυνο επεξεργασίας), αυτό θα επιλύσει το ζήτημα (όπως θα πρέπει να καταγραφεί από τον υπεύθυνο επεξεργασίας και φυσικά θα καταγραφεί και από την ΑΠΔΠΧ). Ενναλακτικά, η ΑΠΔΠΧ μπορεί είτε να εκδώσει εντολή προς τον υπεύθυνο επεξεργασίας, με την οποία να απαιτεί από τον υπεύθυνο επεξεργασίας να υιοθετήσει συγκεκριμένα μέτρα για την προτεινόμενη πράξη επεξεργασίας (βλ. άρθρ. 58(2)(δ)), είτε να απαγορεύσει την προτεινόμενη επεξεργασία (άρθρο 58(2)(στ)).

Συνοπτικά: Οι απαιτήσεις σχετικά με τη διενέργεια DPIA είναι απαιτητικές και η συμμόρφωση με αυτές είναι απαραίτητη για τις πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα «υψηλού κινδύνου». Όλες οι οντότητες που εμπλέκονται σε τέτοιου είδους πράξεις θα πρέπει να εξοικειωθούν διεξοδικά με τις απαιτήσεις αυτές και τις λεπτομερείς οδηγίες που εξέδωσε η WP29 και ενέκρινε το EDPB (καθώς και με τις εξίσου χρήσιμες οδηγίες που εξέδωσε το EDPB), όπως συνοψίζονται στο παρόν έγγραφο [11].

4.3 CNIL

CNIL είναι τα αρχικά των λέξεων Commission Nationale de l'informatique et des Libertés (Εθνική Επιτροπή για την Πληροφορική και τις Ελευθερίες), η οποία είναι η γαλλική εθνική αρχή προστασίας δεδομένων. Η CNIL Γαλλίας δημιουργήθηκε με τον γαλλικό νόμο περί προστασίας δεδομένων της 6ης Ιανουαρίου 1978 ως ανεξάρτητη διοικητική αρχή υπεύθυνη για τη διασφάλιση της προστασίας των δεδομένων προσωπικού χαρακτήρα σε αρχεία ηλεκτρονικών υπολογιστών και σε διαδικασίες επεξεργασίας, τόσο δημόσιες όσο και ιδιωτικές. Πιο συγκεκριμένα, η CNIL μπορεί να επιβάλλει τους νόμους περί προστασίας των δεδομένων στην Γαλλία, γεγονός που σημαίνει ότι έχει εφαρμόσει το French Data Protection Act, GDPR και ePrivacy Directive. Πιο συγκεκριμένα, η CNIL έχει αναπτύξει το εργαλείο PIA (εκτίμηση αντικτύπου στην ιδιωτική ζωή) που βοηθά τους οργανισμούς στην τεκμηρίωση, την αναθεώρηση και την ανταλλαγή πληροφοριών σχετικά με τις PIA. Το εργαλείο είναι ανοικτού κώδικα, ελεύθερο προς χρήση και μπορεί να χρησιμοποιηθεί ως αυτόνομο λογισμικό ή σε διακομιστή για κοινή χρήση [23]. Η DPIA διενεργείται με τη συμπλήρωση κειμένου ελεύθερης μορφής ή με την επιλογή μιας από τις καθορισμένες επιλογές εντός των διαφόρων εντύπων που αφορούν την περιγραφή των δραστηριοτήτων επεξεργασίας και τον προσδιορισμό των κινδύνων και των μετριασμών. Έτσι ο χρήστης έχει τη δυνατότητα να δημιουργήσει και να επιλέξει «πρότυπα» που περιέχουν προσυμπληρωμένες ερωτήσεις και οδηγίες, καθώς και «βάσεις γνώσεων» που επιτρέπουν τη δημιουργία εννοιών για ορισμούς, αρχές, κινδύνους και μετριασμούς. Στο τέλος της εισαγωγής, το εργαλείο παρέχει μια επισκόπηση των βαθμολογιών κινδύνου με βάση τις εισαχθείσες πληροφορίες και παρέχει τη δυνατότητα αναθεώρησης και έγκρισης από έναν ΥΠΔ.

Η μεθοδολογία της Γαλλικής Αρχής Προστασίας Δεδομένων (CNIL) περιλαμβάνει τρεις οδηγούς [23]:

1. έναν που καθορίζει την προσέγγιση,
2. Έναν που περιέχει στοιχεία που μπορούν να χρησιμοποιηθούν για την τυποποίηση της ανάλυσης και
3. έναν που παρέχει βάσεις γνώσεων (κατάλογο ελέγχων που αποσκοπούν στη συμμόρφωση με τις νομικές απαιτήσεις και την αντιμετώπιση των κινδύνων, καθώς και παραδείγματα)

Συγκεκριμένα, αυτοί οι 3 οδηγοί, χρησιμοποιούν την λέξη ιδιωτική ζωή ως συντομογραφία που περιλαμβάνει όλα τα θεμελιώδη δικαιώματα και τις ελευθερίες των υποκειμένων, όπως

αυτά αναφέρονται και στον ΓΚΠΔ, στα άρθρα 7 και 8 του EU Charter και στο άρθρο 1 «Πράξεις για την προστασία των προσωπικών δεδομένων, ιδιωτική ζωή, ανθρώπινη ταυτότητα, ανθρώπινα δικαιώματα και ατομικές ή δημόσιες ελευθερίες». Με αντίστοιχο τρόπο χρησιμοποιείται το ακρωνύμιο «PIA» που αναφέρεται στην εκτίμηση επιπτώσεων στην ιδιωτική ζωή αλλά και στην εκτίμηση επιπτώσεων στην προστασία των δεδομένων (DPIA).

Κατά κύριο λόγο, η διενέργεια της εκπόνησης εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων περιγράφεται μέσα από τον τρόπο χρήσης της μεθόδους EBIOS [24] στο ειδικό πλαίσιο της «Προστασίας δεδομένων προσωπικού χαρακτήρα». Η προσέγγιση είναι σύμφωνη με τα κριτήρια των W29, τα οποία αναλύθηκαν στην παραπάνω ενότητα και συμβατή με τα διεθνή πρότυπα για την διαχείριση κινδύνων όπως το «ISO 31000:2018 Risk management — Guidelines».

Η παρούσα μεθοδολογία δεν πραγματεύεται ούτε τις αρχικές προϋποθέσεις που καθορίζουν εάν απαιτείται ή όχι η εκπόνηση εκτίμησης αντικτύπου (άρθρο 35 παράγραφος 1 του ΓΚΠΔ), ούτε τις μεταγενέστερες απαιτήσεις που καθορίζουν αν είναι αναγκαία ή όχι η διαβούλευση με την εποπτική αρχή (άρθρο 36 παράγραφος 1 του ΓΚΠΔ). Πιο συγκεκριμένα, μια DPIA εκτελείται αρχικά από έναν υπεύθυνο επεξεργασίας δεδομένων με στόχο την οικοδόμηση και την απόδειξη της εφαρμογής των αρχών προστασίας της ιδιωτικής ζωής, ώστε τα υποκείμενα των δεδομένων να διατηρούν τον έλεγχο των προσωπικών τους δεδομένων. Πρωτίστως, απευθύνεται στους υπευθύνους επεξεργασίας δεδομένων που επιθυμούν να αποδείξουν την προσέγγιση συμμόρφωσής τους και τους ελέγχους που έχουν επιλέξει (αρχή της λογοδοσίας, άρθρο 25 του ΓΚΠΔ), καθώς και στους παρόχους προϊόντων που επιθυμούν να αποδείξουν ότι οι λύσεις τους δεν παραβιάζουν την ιδιωτική ζωή λόγω του σχεδιασμού που σέβεται την ιδιωτική ζωή (έννοια «Privacy by Design» άρθρο 25 του ΓΚΠΔ). Αποτελεί χρήσιμο εργαλείο για όλους τους εμπλεκόμενους φορείς που εμπλέκονται στη δημιουργία ή τη βελτίωση της επεξεργασίας δεδομένων ή προϊόντων προσωπικού χαρακτήρα [23]:

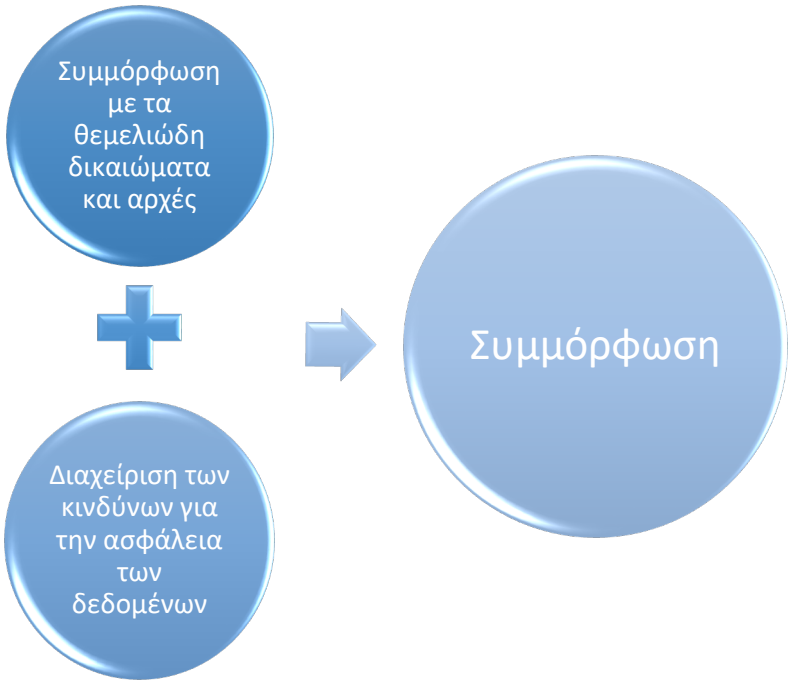
- οι αρχές που είναι αρμόδιες για τη λήψη αποφάσεων, οι οποίες αναθέτουν και επικυρώνουν τη δημιουργία νέων διαδικασιών για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ή για τα προϊόντα,
- ιδιοκτήτες έργων, οι οποίοι πρέπει να προβούν στην εκτίμηση των κινδύνων για το σύστημα και να καθορίσουν τους στόχους ασφαλείας,

- κύριοι ανάδοχοι (contractors), οι οποίοι πρέπει να προτείνουν λύσεις για την αντιμετώπιση των κινδύνων σύμφωνα με τους στόχους που έχουν καθοριστεί από τους ιδιοκτήτες του έργου,
- υπεύθυνοι προστασίας δεδομένων (ΥΠΔ), οι οποίοι πρέπει να υποστηρίζουν τους ιδιοκτήτες του έργου και τις αρχές που είναι αρμόδιες για τη λήψη αποφάσεων στον τομέα της προστασίας των δεδομένων προσωπικού χαρακτήρα και υπεύθυνοι ασφάλειας πληροφοριών (CISO), οι οποίοι πρέπει να υποστηρίζουν τους ιδιοκτήτες του έργου στον τομέα της ασφάλειας πληροφοριών (IS).

4.3.1 Ανάλυση Μεθοδολογίας

Η προσέγγιση συμμόρφωσης που εφαρμόζεται με την εκπόνηση PIA βασίζεται σε δύο άξονες [25]:

1. τα θεμελιώδη δικαιώματα και αρχές, τα οποία είναι «αμετάβλητα», καθορίζονται από το νόμο και πρέπει να γίνονται σεβαστά, ανεξάρτητα από τη φύση, τη σοβαρότητα και την πιθανότητα των κινδύνων,
2. στη διαχείριση των κινδύνων για την προστασία της ιδιωτικής ζωής των υποκειμένων των δεδομένων, η οποία καθορίζει τους κατάλληλους τεχνικούς και οργανωτικούς ελέγχους για την προστασία των δεδομένων προσωπικού χαρακτήρα.



Σχήμα 1: Προσέγγιση της συμμόρφωσης με χρήση PIA

Συμπερασματικά, για τη διενέργεια PIA τα ακόλουθα κρίνονται αναγκαία [25]:

1. ο καθορισμός και η περιγραφή ενός πλαισίου για την επεξεργασία των υπό εξέταση δεδομένων προσωπικού χαρακτήρα,
2. η ανάλυση των ελέγχων που διασφαλίζουν τη συμμόρφωση με τις θεμελιώδεις αρχές, την αναλογικότητα και αναγκαιότητα της επεξεργασίας καθώς και την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων,
3. η αξιολόγηση των κινδύνων για την προστασία της ιδιωτικής ζωής που συνεπάγεται με την ασφάλεια των δεδομένων και διασφάλιση της κατάλληλης αντιμετώπισης τους και
4. επίσημη τεκμηρίωση της επικύρωσης της PIA λαμβάνοντας υπόψη τα προγενέστερα δεδομένα που έχουν συγκεντρωθεί ή η απόφαση αναθεώρησης των προηγούμενων ενεργειών.

Αξίζει να τονιστεί πως πρόκειται για μια διαδικασία συνεχούς βελτίωσης, όπου μερικές φορές απαιτούνται αρκετές επαναλήψεις για την επίτευξη ενός αποδεκτού συστήματος προστασίας της ιδιωτικής ζωής. Επίσης, απαιτεί παρακολούθηση των αλλαγών σταδιακά (στο πλαίσιο, τους ελέγχους, τους κινδύνους κ.λπ.), για παράδειγμα κάθε χρόνο, μαζί με την διαδικασία της επικαιροποίησης κάθε φορά που επέρχεται σημαντική αλλαγή. Η προσέγγιση θα πρέπει να εφαρμόζεται αμέσως μόλις σχεδιαστεί μια νέα επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η εφαρμογή αυτής της προσέγγισης από την αρχή καθιστά δυνατό τον προσδιορισμό των αναγκαίων και επαρκών ελέγχων και, ως εκ τούτου, τη βελτιστοποίηση του κόστους. Αντίθετα, η εφαρμογή της μετά τη δημιουργία του συστήματος και την εφαρμογή των ελέγχων μπορεί να θέσει υπό αμφισβήτηση τις επιλογές που πραγματοποιήθηκαν.

4.3.2 Εκτίμηση του πλαισίου

Ως απαιτούμενη διαδικασία θεωρούνται τα ακόλουθα βήματα [23]:

1. Η συνοπτική παρουσίαση της υπό εξέτασης επεξεργασίας συμπεριλαμβανομένου του πεδίου εφαρμογής, της φύσης, του σκοπού, των συμφερόντων αλλά και του ευρύτερου πλαισίου.
2. Ο προσδιορισμός του υπευθύνου επεξεργασίας δεδομένων (data controller) αλλά και τους εκτελούντος την επεξεργασία (processor)

3. Καταγραφή της ισχύουσας για την επεξεργασία παραπομπής/αναφοράς, η οποία είναι απαραίτητη ή πρέπει να τηρείται, καθώς και τους εγκεκριμένους κώδικες δεοντολογίας (άρθρο 40 του ΓΚΠΔ) και τις πιστοποιήσεις σχετικά με την προστασία των δεδομένων (άρθρο 42 του ΓΚΠΔ).
4. Τέλος, ο καθορισμός και η λεπτομερής περιγραφή του πεδίου εφαρμογής που περιλαμβάνει την περιγραφή των διαδικασιών και των μέσων υποστήριξης των δεδομένων προσωπικού χαρακτήρα για όλον τον κύκλο ζωής των δεδομένων, από την συλλογή έως την οριστική διαγραφή τους) αλλά και ευρύτερα τα εν λόγω προσωπικά δεδομένα, τους αποδέκτες και την διάρκεια αποθήκευσης τους.

4.3.3 Θεμελιώδεις Αρχές

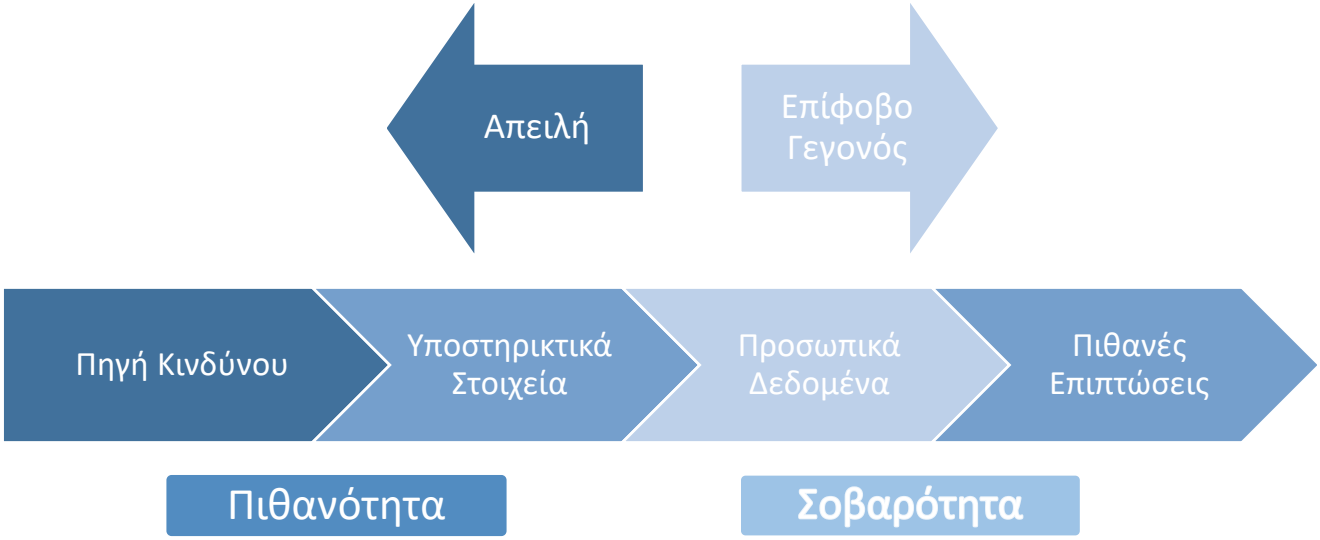
1. **Αξιολόγηση των μέτρων που διασφαλίζουν την αναλογικότητα και την αναγκαιότητα της επεξεργασίας**
   - Επεξήγηση και αιτιολόγηση των αποφάσεων που ελήφθησαν για τη συμμόρφωση με τις ακόλουθες απαιτήσεις [16]:
     - → **σκοπός(-οί):** καθορισμένος, ρητός και νόμιμος με βάσει το άρθρο 1 του Συντάγματος και το κεφάλαιο. 5.1 στοιχείο β) του ΓΚΠΔ,
     - → **βάση/θεμελίωση:** νομιμότητα της επεξεργασίας, απαγόρευση κατάχρησης με βάσει το άρθρο 6 του ΓΚΠΔ,
     - → **ελαχιστοποίηση των δεδομένων:** επαρκής, συναφής και περιορισμένη με βάσει το άρθρο 5 στοιχείο γ) του ΓΚΠΔ,
     - → **ποιότητα των δεδομένων:** ακριβή και επικαιροποιημένα δεδομένα με βάσει το άρθρο 5 (δ) του ΓΚΠΔ και
     - → **περίοδος αποθήκευσης:** περιορισμένη με βάσει το άρθρο 5 (ε) του ΓΚΠΔ.
   - Έλεγχος και επισκόπηση ότι η βελτίωση του τρόπου με τον οποίο σχεδιάζεται, αποσαφηνίζεται και αιτιολογείται κάθε σημείο, σύμφωνα με τον ΓΚΠΔ, είτε δεν είναι αναγκαία είτε δεν είναι δυνατή
   - Κατά περίπτωση, αναθεώρηση της περιγραφής τους και πρόταση πρόσθετων ελέγχων.

2. **Αξιολόγηση των ελέγχων για την προστασία των δικαιωμάτων των υποκειμένων των δεδομένων**
   - Εντοπισμός, προσδιορισμός και περιγραφή των ελέγχων (υφιστάμενων ή σχεδιαζόμενων) που έχουν επιλεχθεί για τη συμμόρφωση με τις ακόλουθες νομικές απαιτήσεις, ωστόσο κρίνεται απαραίτητο να εξηγηθεί ο τρόπος με τον οποίο θα εφαρμοσθεί:
     → ενημέρωση των υποκειμένων των δεδομένων (δίκαιη και διαφανής επεξεργασία (άρθρα 12, 13 και 14 του ΓΚΠΔ),
     → λήψη συγκατάθεσης, όπου εφαρμόζεται: ρητή, η οποία μπορεί να αποδειχθεί και να ανακληθεί (άρθρα 7 και 8 του ΓΚΠΔ),
     → άσκηση του δικαιώματος πρόσβασης και του δικαιώματος φορητότητας των δεδομένων (άρθρα 15 και 20 του ΓΚΠΔ),
     → άσκηση των δικαιωμάτων διόρθωσης και διαγραφής (άρθρα 16 και 17 του ΓΚΠΔ),
     → άσκηση του δικαιώματος περιορισμού της επεξεργασίας και του δικαιώματος εναντίωσης (άρθρα 18 και 21 του ΓΚΠΔ),
     → εκτελούντες την επεξεργασία: προσδιορίζονται και διέπονται από σύμβαση (άρθρο 28 του ΓΚΠΔ),
     → διαβιβάσεις: συμμόρφωση με τις υποχρεώσεις που αφορούν τη διαβίβαση δεδομένων εκτός της Ευρωπαϊκής Ένωσης (άρθρα 44 έως 49 του ΓΚΠΔ).
   - Έλεγχος ότι η βελτίωση κάθε ελέγχου και της περιγραφής του, σύμφωνα με τον [ΓΚΠΔ], είτε δεν είναι απαραίτητη είτε δεν είναι δυνατή.
   - Αναθεώρηση της περιγραφής τους και πρόταση πρόσθετων ελέγχων, όπου εφαρμόζεται.

4.3.4 Μελέτης Περίπτωσης

Η έννοια του κινδύνου ουσιαστικά αποτελεί ένα υποθετικό σενάριο που περιγράφει ένα επίφοβο γεγονός σε συνδυασμό με όλες τις απειλές που θα το επέτρεπαν να συμβεί. Πιο συγκεκριμένα, περιγράψει πως πηγάζει/προέρχεται ο κίνδυνος, ο οποίος θα μπορούσε να εκμεταλλευτεί τα τρωτά σημεία των υποστηρικτικών στοιχείων όπως το σύστημα διαχείρισης αρχείων που επιτρέπει τη χειραγώγηση δεδομένων, σε ένα ευρύτερο πλαίσιο απειλών και να επιτρέψει την εκδήλωση επίφοβων γεγονότων (π.χ. παράνομη πρόσβαση σε προσωπικά δεδομένα) σε προσωπικά δεδομένα, όπως στο αρχείο καταγραφής των

πελατών. Κατά συνέπεια, δημιουργούν επιπτώσεις στην ιδιωτική ζωή των υποκειμένων των δεδομένων με χαρακτηριστικά παραδείγματα τις ανεπιθύμητες προσκλήσεις, το αίσθημα παραβίασης της ιδιωτικής ζωής ή τα επαγγελματικά προβλήματα, ενώ το παρακάτω διάγραμμα αποσαφηνίζει όσα λέχθηκαν παραπάνω [25]:



Σχήμα 2: Συνιστώσες Κινδύνου

Συμπεριληπτικά, το επίπεδο κινδύνου εκτιμάται ως προς την σοβαρότητα, η οποία αντιπροσωπεύει το μέγεθος ενός κινδύνου ενώ κατά κύριο λόγο εξαρτάται από τον επιζήμιο χαρακτήρα των πιθανών επιπτώσεων και την πιθανότητα εκδήλωσης του κινδύνου αυτού. Ουσιαστικά, εξαρτάται αφενός από το επίπεδο των τρωτών σημείων των υποστηρικτικών στοιχείων στην περίπτωση απειλής, αφετέρου από το επίπεδο των ικανοτήτων των πηγών κινδύνου για την εκμετάλλευσή τους.

4.3.4.1 Αξιολόγηση των υφιστάμενων ή σχεδιαζόμενων ελέγχων

- Εντοπισμός ή προσδιορισμός των υφιστάμενων ή προγραμματισμένων ελέγχων, που έχουν ήδη πραγματοποιηθεί, οι οποίοι μπορούν να λάβουν τρεις διαφορετικές μορφές:
    1. έλεγχοι που αφορούν ειδικά τα υπό επεξεργασία δεδομένα: κρυπτογράφηση, ανωνυμοποίηση, έλεγχος πρόσβασης, ανιχνευσιμότητα
    2. γενικοί έλεγχοι ασφάλειας όσον αφορά το σύστημα στο οποίο πραγματοποιείται η επεξεργασία: ασφάλεια λειτουργίας, εφεδρικά αντίγραφα ασφαλείας, ασφάλεια του hardware

3. οργανωτικοί έλεγχοι (διακυβέρνηση): πολιτική, διαχείριση έργων, διαχείριση προσωπικού, διαχείριση περιστατικών και παραβιάσεων και σχέσεις με τρίτους

- Έλεγχος ότι η βελτιστοποίηση κάθε ελέγχου και της περιγραφής του γίνεται σύμφωνα με τις βέλτιστες πρακτικές ασφάλειας, είτε δεν είναι απαραίτητη είτε δεν είναι δυνατή.
- Κατά περίπτωση, αναθεώρηση της περιγραφής τους και πρόταση πρόσθετων ελέγχων.

4.3.4.2 Αξιολόγηση κινδύνου: Πιθανές παραβιάσεις της ιδιωτικής ζωής

Δυνητικές παραβιάσεις των προσωπικών δεδομένων των υποκειμένων [25]:

- Για κάθε επίφοβο συμβάν, όπως για παράδειγμα η παράνομη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ή η ανεπιθύμητη αλλαγή ή και εξαφάνιση των δεδομένων προσωπικού χαρακτήρα ισχύει:
    1. καθορισμός των δυνητικών επιπτώσεων στην ιδιωτική ζωή των υποκειμένων των δεδομένων, εάν συμβεί
    2. εκτίμηση τη σοβαρότητας ανάλογα με τον επιζήμιο χαρακτήρα των δυνητικών επιπτώσεων και, κατά περίπτωση, τους ελέγχους που ενδέχεται να τις τροποποιήσουν
    3. αναγνώριση των απειλών για τα υποστηρικτικά στοιχεία προσωπικών δεδομένων που θα μπορούσαν να οδηγήσουν σε αυτό το επίφοβο γεγονός και τις πηγές κινδύνου που θα μπορούσαν να το προκαλέσουν
    4. εκτίμηση της πιθανότητας ανάλογα με το επίπεδο ευπάθειας των τρωτών σημείων των στοιχείων που υποστηρίζουν τα προσωπικά δεδομένα, το επίπεδο των δυνατοτήτων των πηγών κινδύνου να τα εκμεταλλευτούν και τους ελέγχους που ενδεχομένως να τα τροποποιήσουν.
- Καθορισμός του κατά πόσον οι κίνδυνοι που εντοπίστηκαν με αυτόν τον τρόπο μπορούν να θεωρηθούν αποδεκτοί ενόψει των υφιστάμενων ή προγραμματισμένων ελέγχων.
- Σε αντίθετη περίπτωση, κρίνεται αναγκαία η πρόταση συμπληρωματικών ελέγχων και επαναξιολογήσεων του επίπεδου του εκάστοτε κινδύνου με βάσει τους τελευταίους, ώστε να προσδιοριστούν οι εναπομείναντες κίνδυνοι.

4.3.5 Επικύρωση της PIA

Η διαδικασία αυτή κατανέμεται σε δύο κατηγορίες [26]:

1. Προετοιμασία του υλικού που απαιτείται για την επικύρωση

- Συγκέντρωση και παρουσίαση των ευρημάτων της μελέτης:
    - → παρουσίαση των ελέγχων που επιλέχθηκαν για τη διασφάλιση της συμμόρφωσης με τις θεμελιώδεις αρχές, ανάλογα με τη συμμόρφωσή τους με τον ΓΚΠΔ, υπό όρους βελτίωσης ή αν θεωρούνται ότι έχουν συμμορφωθεί,
    - → παρουσίαση των ελέγχων που επιλέχθηκαν να συμβάλουν στην ασφάλεια των δεδομένων, ανάλογα με τη συμμόρφωσή τους με τις βέλτιστες πρακτικές ασφάλειας,
    - → χαρτογράφηση των κινδύνων, αρχικοί και εναπομείναντες, ανάλογα με τη σοβαρότητα και την πιθανότητά τους,
    - → κατάρτιση ενός σχεδίου δράσης με βάσει τους συμπληρωματικούς ελέγχους που επισημάνθηκαν κατά τα προηγούμενα στάδια, όπου για κάθε έλεγχο απαιτείται το πρόσωπο που είναι υπεύθυνο για την εφαρμογή του, το κόστος και το εκτιμώμενο χρονοδιάγραμμα
- Επίσημη καταγραφή της εξέτασης των ενδιαφερομένων μερών:
    - → συμβουλή του υπευθύνου για τις πτυχές της «προστασίας δεδομένων» με βάσει το άρθρο 35 (2) του ΓΚΠΔ,
    - → την άποψη των υποκειμένων των δεδομένων ή των εκπροσώπων τους σύμφωνα με το άρθρ. 35 παράγραφος 9

2. Επίσημη επικύρωση

Είναι καθοριστικό να προσδιοριστεί κατά πόσον οι επιλεγμένοι έλεγχοι, οι εναπομείναντες κίνδυνοι και το σχέδιο δράσης είναι αποδεκτά, με αιτιολόγηση υπό το πρίσμα των προηγούμενων αναγνωρισμένων κινδύνων και των απόψεων των ενδιαφερομένων μερών. Με αυτόν τον τρόπο, η PIA μπορεί να [26]:

- επικυρωθεί
- βρίσκεται υπό τη προϋπόθεση της βελτίωσης
- απορριφθεί μαζί με την υπό εξέταση επεξεργασία

Στην περίπτωση που θεωρείται απαραίτητο, τα προηγούμενα βήματα θα χρειαστεί να επαναληφθούν προκειμένου να επικυρωθεί η PIA.

4.3.6 Λογισμικό PIA

Εκτενής καθοδήγηση σχετικά με τις DPIA (συμπεριλαμβανομένης της μεθοδολογικής καθοδήγησης) έχει επίσης εκδοθεί από τις εθνικές ΑΠΔΠΧ, συμπεριλαμβανομένων εκείνων της Γαλλίας, της Ισπανίας και του Ηνωμένου Βασιλείου, καθώς και από το γερμανικό Datenschutzzentrum (το οποίο έχει εγκριθεί από τις γερμανικές ΑΠΔΠΧ) [27]. Συγκεκριμένα, η γαλλική αρχή προστασίας δεδομένων, η CNIL, σε συνεργασία με άλλες ΑΠΔΠΧ, έχει αναπτύξει ένα εργαλείο λογισμικού ανοικτού κώδικα DPIA, το οποίο «έχει ως στόχο να βοηθήσει τους υπευθύνους επεξεργασίας δεδομένων να δημιουργήσουν και να αποδείξουν τη συμμόρφωση με τον ΓΚΠΔ». Αναφορικά με το λογισμικό PIA, το οποίο κατά κύριο λόγο απευθύνεται κυρίως σε υπεύθυνους επεξεργασίας δεδομένων, οι οποίοι είναι εξοικειωμένοι με την διαδικασία εκπόνησης μελέτης εκτίμησης αντικτύπου και έχει σχεδιαστεί με βάση τρεις αρχές [28]:

1. **Μια διδακτική διεπαφή για τη διενέργεια PIA:** το εργαλείο βασίζεται σε μια φιλική προς το χρήστη διεπαφή που επιτρέπει την απλή διαχείριση των PIA σας, αναπτύσσει με σαφήνεια τη μεθοδολογία εκτίμησης επιπτώσεων στην ιδιωτική ζωή, ενώ μέσω διαφόρων εργαλείων οπτικοποίησης προσφέρει τρόπους για τη γρήγορη κατανόηση των κινδύνων.
2. **Βάση νομικών και τεχνικών γνώσεων:** το εργαλείο περιλαμβάνει τα νομικά σημεία που διασφαλίζουν τη νομιμότητα της επεξεργασίας και τα δικαιώματα των υποκειμένων των δεδομένων. Διαθέτει επίσης μια βάση γνώσεων με βάσει το πλαίσιο, προσαρμόζοντας το περιεχόμενο που εμφανίζεται. Τα δεδομένα εξάγονται από τον ΓΚΠΔ, τους οδηγούς PIA και τον οδηγό ασφάλειας της CNIL, στην υπό μελέτη πτυχή της επεξεργασίας.
3. **Ένα μορφολογικό εργαλείο:** σχεδιασμένο να βοηθήσει στην ανάπτυξη της συμμόρφωσης, καθώς δίνεται η δυνατότητα προσαρμογής του εργαλείου στις εκάστοτε ανάγκες, όπως για παράδειγμα δημιουργώντας ένα μοντέλο PIA που μπορεί να αντιγράψει και να χρησιμοποιήσει ένα σύνολο παρόμοιων πράξεων επεξεργασίας.

4.4 ICO

Το Information Commissioner's Office (ICO) είναι ένας ανεξάρτητος μη κυβερνητικός δημόσιος οργανισμός του Ηνωμένου Βασιλείου που έχει συσταθεί για να προασπίζει τα δικαιώματα πληροφόρησης προς το δημόσιο συμφέρον, προωθώντας την διαφάνεια των δημόσιων οργανισμών και την προστασία της ιδιωτικής ζωής των δεδομένων των υποκειμένων. Ο ICO έχει δημοσιεύσει έναν επικαιροποιημένο κώδικα πρακτικής για τις εκτιμήσεις αντικτύπου στην ιδιωτική ζωή, ο οποίος περιλαμβάνει χρήσιμες οδηγίες σχετικά με το πότε θα πρέπει να διενεργείται εκτίμηση αντικτύπου στην ιδιωτική ζωή και τις ενέργειες που πρέπει να εξετάζονται σε κάθε στάδιο της διαδικασίας. Αξίζει να σημειωθεί πως ο επικαιροποιημένος κώδικας έχει σχεδιαστεί για να διασφαλίσει ότι οι DPIA εντάσσονται στη διαδικασία ανάπτυξης έργων, επιτρέποντας στους οργανισμούς να ακολουθούν μια προσέγγιση «Privacy-by-Design» για την ανάπτυξη νέων τρόπων χρήσης προσωπικών δεδομένων, επιτρέποντας στους οργανισμούς να αποδεικνύουν τη συμμόρφωσή τους με τον νόμο περί προστασίας δεδομένων του Ηνωμένου Βασιλείου [29].

Η διενέργεια της DPIA αποτελεί επίσης μέρος της εκπλήρωσης άλλων υποχρεώσεων του ΓΚΠΔ, κυρίως της αρχής της «λογοδοσίας», την δυνατότητα απόδειξης της συμμόρφωσης. Οι υπεύθυνοι επεξεργασίας που δεν τηρούν την υποχρέωση αυτή μπορούν να αντιμετωπίσουν ρυθμιστικό πρόστιμο στην υψηλότερη βαθμίδα, είτε το μεγαλύτερο ποσό των 20 εκατομμυρίων ευρώ (περίπου 18 εκατομμύρια λίρες) ή το 4% του ετήσιου παγκόσμιου κύκλου εργασιών του προηγούμενου οικονομικού έτους. Ωστόσο, υπάρχουν περισσότερα πλεονεκτήματα στη διεξαγωγή DPIAs από την απλή αποφυγή προστίμων [9]:

- Εξοικονόμηση χρόνου και χρήματος στον οργανισμό με τον έγκαιρο εντοπισμό των προβλημάτων
- Μείωση του κόστους του έργου ελαχιστοποιώντας τον όγκο των δεδομένων που πρόκειται να συλλεχθούν ή απλοποιώντας τις διαδικασίες.
- Να καταστεί ο οργανισμός πιο ελκυστικός σε δυνητικούς πελάτες και συνεργάτες ή να βελτιωθούν οι υφιστάμενες σχέσεις. Σε αυτό, η ICO προτείνει τη δημοσίευση των DPIA για να προκύψει και η διαφάνεια του οργανισμού.

4.4.1 Πότε πρέπει να διεξάγεται DPIA;

Όπως έχει ήδη αναφερθεί, ο ΓΚΠΔ αναφέρει ότι η διενέργεια DPIA είναι απαραίτητη εάν η επεξεργασία ενδέχεται να ενέχει «υψηλό κίνδυνο» για τα υποκείμενα των δεδομένων. Έτσι, οι αξιολογήσεις πρέπει να διενεργούνται τόσο πριν από την έναρξη μιας δραστηριότητας επεξεργασίας όσο και όταν μια υφιστάμενη δραστηριότητα τροποποιείται, όμως το σημαντικότερο είναι ότι πρέπει να διενεργούνται όταν μπορούν να επιφέρουν θετική διαφορά στο έργο. Ωστόσο, η DPIA χαρακτηρίζεται ως «ζωντανή» διαδικασία που πρέπει να επανεξετάζεται τακτικά, ιδιαίτερα όταν γίνονται αλλαγές στη δραστηριότητα, με σκοπό την διεξοδική διαχείριση των κινδύνων που μπορεί να θέσει η επεξεργασία στα υποκείμενα. Στην περίπτωση όμως που η επεξεργασία έχει ήδη αρχίσει χωρίς να έχει προηγηθεί η διενέργεια DPIA χρήζει επίσης επανεξέτασης για να διασφαλιστεί ότι ο κίνδυνος δεν είναι υψηλός και ότι, ως εκ τούτου, δεν απαιτείται η αξιολόγηση. Ακόμα και η υιοθέτηση μιας ήπιας προσέγγισης, όπως η υποβολή μιας σειράς βασικών ερωτήσεων, θα αντιμετωπιστεί ευνοϊκά από την ICO σε περίπτωση έρευνας. Επιπροσθέτως, η ευθύνη του υπεύθυνου επεξεργασίας είναι να αξιολογεί κάθε προτεινόμενη δραστηριότητα επεξεργασίας και να καθορίζει εάν απαιτείται DPIA, αν και ο ICO έχει δημοσιεύσει έναν κατάλογο με παραδείγματα δραστηριοτήτων επεξεργασίας που θεωρεί υψηλού κινδύνου.

Οι πράξεις επεξεργασίας για τις οποίες ο ICO απαιτεί να εκπονηθεί DPIA, καθώς είναι «πιθανό να προκαλέσουν υψηλό κίνδυνο», βασίζονται στις κατευθυντήριες γραμμές που εγκρίθηκαν από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (EDPB) σχετικά με τις DPIA (WP248rev01). Ειδικότερα, ο ΓΚΠΔ του Ηνωμένου Βασιλείου αναφέρει ότι πρέπει να εκπονείται μελέτη εκτίμησης αντικτύπου, εάν πρόκειται ένας οργανισμός να προβεί στις παρακάτω ενέργειες [30]:

- χρησιμοποιούν συστηματικό και εκτεταμένο profiling με σημαντικά αποτελέσματα,
- επεξεργάζονται δεδομένα ειδικών κατηγοριών ή ποινικών αδικημάτων σε μεγάλη κλίμακα ή
- παρακολουθούν συστηματικά και σε μεγάλη κλίμακα χώρους προσβάσιμους στο κοινό.

Όταν εξετάζεται αν η επεξεργασία είναι πιθανό να οδηγήσει σε υψηλό κίνδυνο, θα πρέπει να ληφθούν υπόψη οι σχετικές ευρωπαϊκές κατευθυντήριες γραμμές. Αυτές ορίζουν εννέα κριτήρια για τις εργασίες επεξεργασίας που ενδέχεται να προκαλέσουν υψηλό κίνδυνο και σύμφωνα με τις κατευθυντήριες γραμμές υποδεικνύουν ότι κάθε πράξη επεξεργασίας που

περιλαμβάνει δύο ή περισσότερα από αυτά τα κριτήρια απαιτεί DPIA. Σύμφωνα όμως με τον ICO, η ικανοποίηση ενός μόνο κριτηρίου μπορεί να απαιτεί DPIA. Πιο συγκεκριμένα, με βάσει τον ICO, απαιτείται επίσης η διενέργεια εκτίμησης αντικτύπου στις παρακάτω περιπτώσεις [31]:

- χρήση καινοτόμου τεχνολογίας (σε συνδυασμό με οποιοδήποτε από τα κριτήρια των ευρωπαϊκών κατευθυντήριων γραμμών),
- profilling ή δεδομένα ειδικής κατηγορίας για να αποφασίζεται η πρόσβαση στις υπηρεσίες,
- δημιουργία προφίλ ατόμων σε μεγάλη κλίμακα,
- επεξεργασία βιομετρικών δεδομένων (σε συνδυασμό με οποιοδήποτε από τα κριτήρια των ευρωπαϊκών κατευθυντήριων γραμμών),
- επεξεργασία γενετικών δεδομένων (σε συνδυασμό με οποιοδήποτε από τα κριτήρια των ευρωπαϊκών κατευθυντήριων γραμμών),
- αντιστοίχιση δεδομένων ή συνδυασμός συνόλων δεδομένων από διαφορετικές πηγές,
- συλλογή δεδομένα προσωπικού χαρακτήρα από πηγή που δεν προέρχεται από το ίδιο το άτομο χωρίς να του παρέχουν ειδοποίηση προστασίας προσωπικών δεδομένων, «αόρατη επεξεργασία», (σε συνδυασμό με οποιοδήποτε από τα κριτήρια των ευρωπαϊκών κατευθυντήριων γραμμών),
- παρακολούθηση της θέσης ή της συμπεριφοράς των ατόμων (σε συνδυασμό με οποιοδήποτε από τα κριτήρια των ευρωπαϊκών κατευθυντήριων γραμμών),
- σκιαγράφηση του προφίλ παιδιών ή στοχευμμένο marketing και
- επεξεργασία δεδομένων που ενδέχεται να θέσουν σε κίνδυνο τη σωματική υγεία ή την ασφάλεια του ατόμου σε περίπτωση παραβίασης της ασφάλειας.

Αξίζει να σημειωθεί πως ακόμα και αν δεν υπάρχει συγκεκριμένη ένδειξη για πιθανό υψηλό κίνδυνο, αποτελεί καλή πρακτική η διενέργεια DPIA για κάθε σημαντικό νέο έργο που περιλαμβάνει τη χρήση δεδομένων προσωπικού χαρακτήρα. Επιπλέον, διατίθενται και μπορούν να προσαρμοστούν οι κατάλογοι ελέγχου (checklists) για την πραγματοποίηση αυτής της άσκηση διαλογής.

4.4.2 Πώς διεξάγετε μια DPIA;

Η διαδικασία DPIA ευέλικτη και ενσωματώνεται στην υφιστάμενη προσέγγιση ενός οργανισμού για τη διαχείριση έργων, ενώ ο χρόνος και οι πόροι που αφιερώνονται σε πρέπει να προσαρμόζονται στη φύση του έργου. Όπως περιγράφεται παραπάνω, η DPIA πρέπει να πραγματοποιείται σε πρώιμο στάδιο κατά τη διάρκεια του έργου, πριν από την έναρξη της επεξεργασίας και να διεξάγεται παράλληλα με τη διαδικασία του σχεδιασμού και της ανάπτυξης και περιλαμβάνει τα ακόλουθα βήματα μαζί με παραδείγματα που αποτελούν υπόδειγμα του τρόπου με τον οποίο δύναται να καταγραφή η διαδικασία και τα αποτελέσματα της DPIA [10]:

1. **Αναγνώριση της ανάγκης για DPIA:**

Η ανάγκη αυτή δύναται να εντοπιστεί στο πλαίσιο της καθιερωμένης διαδικασίας διαχείρισης έργων ενός οργανισμού ή με τη χρήση των ερωτήσεων διαλογής προκειμένου να προσδιοριστεί ο πιθανός αντίκτυπος που να ενδέχεται να έχει στη ιδιωτική ζωή. Πρωταρχικό μέλημα είναι η γνωστοποίηση των ζητημάτων προστασίας με τους ενδιαφερόμενους (stakeholders), καθώς επίσης και πως η διαδικασία διαχείρισης έργου μπορεί να αντιμετωπίσει ζητήματα προστασίας της ιδιωτικής ζωής. Ο ICO έχει καταρτίσει ορισμένες απλές ερωτήσεις διαλογής για να βοηθήσει τους οργανισμούς να εντοπίσουν πότε απαιτείται η διενέργεια DPIA και να ενθαρρύνει επίσης τους οργανισμούς να ενσωματώσουν τις ερωτήσεις αυτές στις δικές τους μεθοδολογίες ή διαδικασίες διαχείρισης έργων. Παρόλα αυτά οι ερωτήσεις διαλογής (screening questions) έχουν σχεδιαστεί για να χρησιμοποιούνται από διαχειριστές έργων ή άλλο προσωπικό που δεν είναι ειδικοί σε θέματα προστασίας της ιδιωτικής ζωής ή προστασίας δεδομένων. Σύμφωνα με τον ICO καταγράφονται οι παρακάτω ερωτήσεις:

- «Εξηγήστε τι στοχεύει να επιτύχει το έργο, ποια θα είναι τα οφέλη για τον οργανισμό, τα άτομα και τα άλλα μέρη.»
- «Μπορεί να σας φανεί χρήσιμο να συσχετίσετε άλλα σχετικά έγγραφα που σχετίζονται με το έργο, για παράδειγμα μια πρόταση έργου.»
- «Συνοψίστε επίσης γιατί διαπιστώθηκε η ανάγκη για DPIA.»

2. Περιγραφή των ροών πληροφοριών

Η κατανόηση των ροών πληροφοριών που εμπλέκονται σε ένα έργο είναι απαραίτητη για την ορθή αξιολόγηση των κινδύνων προστασίας της ιδιωτικής ζωής. Οι υφιστάμενες διαδικασίες και πόροι, όπως οι έλεγχοι πληροφοριών και τα μητρώα περιουσιακών στοιχείων πληροφοριών, μπορούν να αποτελέσουν χρήσιμα εργαλεία για την ολοκλήρωση αυτού του σταδίου. Επιπλέον, η διαδικασία αυτή μπορεί να βοηθήσει στον εντοπισμό πιθανών «λειτουργικών παρεκκλίσεων», απρόβλεπτες ή ακούσιες χρήσεις των δεδομένων, π.χ. κοινή χρήση δεδομένων. Σε αυτό το στάδιο η πληροφορία που χρήζει καταγραφής απαρτίζεται από [32]:

- Περιγράψτε τη φύση της επεξεργασίας: «Πώς θα συλλέγετε, χρησιμοποιείτε, αποθηκεύετε και διαγράφετε δεδομένα; Ποια είναι η πηγή των δεδομένων; Θα μοιραστείτε τα δεδομένα με οποιονδήποτε; Μπορεί να σας φανεί χρήσιμο να ανατρέξετε σε ένα διάγραμμα ροής ή σε έναν άλλο τρόπο περιγραφής της ροής δεδομένων. Επίσης ποιοι τύποι επεξεργασίας που έχουν προσδιοριστεί ως πιθανώς υψηλού κινδύνου εμπλέκονται;»
- Περιγράψτε το πεδίο εφαρμογής της επεξεργασίας: «Ποια είναι η φύση των δεδομένων και περιλαμβάνουν δεδομένα ειδικής κατηγορίας ή ποινικού αδικήματος; Πόσα δεδομένα θα συλλέξετε και θα χρησιμοποιήσετε; Πόσο συχνά; Πόσο καιρό θα τα διατηρείτε; Πόσα άτομα επηρεάζονται; Ποια γεωγραφική περιοχή καλύπτει;»
- Περιγράψτε το πλαίσιο της επεξεργασίας: «Ποια είναι η φύση της σχέσης σας με τα άτομα; Πόσο έλεγχο θα έχουν; Θα περίμεναν ότι θα χρησιμοποιούσατε τα δεδομένα τους με αυτόν τον τρόπο; Περιλαμβάνουν παιδιά ή άλλες ευάλωτες ομάδες; Υπάρχουν προηγούμενες ανησυχίες σχετικά με αυτό το είδος επεξεργασίας ή αδυναμίες ασφαλείας; Υπάρχουν τρέχοντα ζητήματα δημόσιας ανησυχίας που θα πρέπει να λάβετε υπόψη σας; Έχετε προσχωρήσει σε εγκεκριμένο κώδικα δεοντολογίας ή σύστημα πιστοποίησης (εφόσον έχει εγκριθεί);»
- Περιγράψτε τους σκοπούς της επεξεργασίας: «Τι θέλετε να επιτύχετε; Ποιο είναι το επιδιωκόμενο αποτέλεσμα στα άτομα; Ποια είναι τα οφέλη της επεξεργασίας για εσάς αλλά και ευρύτερα;»

3. Διαδικασία διαβούλευσης

Στο στάδιο αυτό θα χρειαστεί να διευκρινισθούν ποια πρακτικά μέτρα θα λάβει ένας οργανισμός για να διασφαλίσει ότι εντοπίζει και αντιμετωπίζει τους κινδύνους για την προστασία της ιδιωτικής ζωής. Βέβαια, πρόκειται για ένα στάδιο το οποίο μπορεί να χρησιμοποιηθεί σε οποιοδήποτε άλλο σημείο της διαδικασίας αυτής. Ουσιαστικά [32]:

- «Πότε και πώς θα ζητήσετε τις απόψεις των ατόμων ή πώς θα δικαιολογήσετε γιατί δεν είναι σκόπιμο να το κάνετε; Ποιους άλλους πρέπει να εμπλέξετε στον οργανισμό σας; Πρέπει να ζητήσετε τη συνδρομή των επεξεργαστών σας; Σκοπεύετε να συμβουλευτείτε εμπειρογνώμονες σε θέματα ασφάλειας πληροφοριών ή άλλους εμπειρογνώμονες;»

4. Αξιολόγηση της αναγκαιότητας και της αναλογικότητας

Σε αυτό το στάδιο, ο οργανισμός πρέπει να εξηγήσει γιατί η επεξεργασία των δεδομένων των υποκειμένων είναι απαραίτητη και ανάλογη με την υπηρεσία που προσφέρει. Με βάση των ΓΚΠΔ, οι πληροφορίες που θα συμπεριληφθούν και σχετίζονται με τον τρόπο συμμόρφωσης [10]:

→ τη νόμιμη βάση σας για την επεξεργασία,
→ την προϋπόθεση για την επεξεργασία δεδομένων ειδικής κατηγορίας,
→ μέτρα για τη διασφάλιση της ακρίβειας, την αποφυγή μεροληψίας και την επεξήγηση της χρήσης της AI
→ συγκεκριμένες λεπτομέρειες σχετικά με τα τεχνολογικά μέτρα ασφαλείας (π.χ. πρότυπα κατακερματισμού ή κρυπτογράφησης).

Ειδικότερα:

- Περιγράψτε τα μέτρα συμμόρφωσης και αναλογικότητας: «Ποια είναι η νόμιμη βάση της επεξεργασίας σας; Επιτυγχάνει πράγματι η επεξεργασία τον σκοπό σας; Υπάρχει άλλος τρόπος να επιτευχθεί το ίδιο αποτέλεσμα; Πώς θα διασφαλίσετε την ποιότητα των δεδομένων και την ελαχιστοποίηση των δεδομένων; Τι πληροφορίες θα δώσετε στα άτομα; Πώς θα βοηθήσετε στην υποστήριξη των δικαιωμάτων τους; Ποια μέτρα λαμβάνετε για να διασφαλίσετε τη συμμόρφωση των εκτελούντων την επεξεργασία; Πώς διασφαλίζετε τυχόν διεθνείς διαβιβάσεις;»

5. Προσδιορισμός και αξιολόγηση των κινδύνων

Κατά τη διενέργεια DPIA ένας οργανισμός πρέπει να εντοπίζει τυχόν κινδύνους για την προστασία της ιδιωτικής ζωής των ατόμων, κινδύνους συμμόρφωσης και πιθανούς συσχετιζόμενους κινδύνους για τον οργανισμό, όπως πρόστιμα για μη συμμόρφωση με τη νομοθεσία ή βλάβη της φήμης που οδηγεί σε απώλεια επιχειρηματικής δραστηριότητας. Συγκεκριμένα [10]:

- «Περιγράψτε την πηγή του κινδύνου και τη φύση των πιθανών επιπτώσεων στα άτομα. Συμπεριλάβετε τους συναφείς κινδύνους συμμόρφωσης και εταιρικούς κινδύνους, εφόσον απαιτείται.». Για να επιτευχθεί ο προσδιορισμός τους καταγράφεται η πιθανότητα της βλάβης, δηλαδή κατά πόσο είναι πιθανή να πραγματοποιηθεί, η σοβαρότητα της βλάβης, προσπαθώντας να την προσδιορίσουν ως προς την σοβαρότητα και την σπουδαιότητας της κα τέλος ο συνολικός κίνδυνος που μπορεί να χαρακτηριστεί χαμηλός, μέτριος ή υψηλός.

6. Προσδιορισμός μέτρων για τη μείωση του κινδύνου

Ουσιαστικά στο βήμα αυτό, βασικός σκοπός είναι ο προσδιορισμός και η αξιολόγηση των προτεινόμενων λύσεων για την προστασία της ιδιωτικής ζωής [10]:

→ ανάπτυξη τρόπου(-ων) για τη μείωση ή την εξάλειψη του κινδύνου που απορρέει στην προστασία των δεδομένων των υποκειμένων

→ αξιολόγηση του κόστους και τα οφέλη κάθε προσέγγισης εξετάζοντας τον αντίκτυπο στην προστασία της ιδιωτικής ζωής και τη επίδραση στα αποτελέσματα του έργου

→ Παραπομπή στο μητρώο κινδύνων για την προστασία της ιδιωτικής ζωής μέχρι να διαπιστωθεί ο συνολικός αντίκτυπος στην προστασία των δεδομένων

Οι οργανισμοί πρέπει να προσδιορίσουν πιθανές λύσεις για την προστασία της ιδιωτικής ζωής για την αντιμετώπιση των κινδύνων που έχουν εντοπιστεί. Ουσιαστικά, η DPIA θα πρέπει να εκθέτει τις επιλογές του οργανισμού για την αντιμετώπιση κάθε κινδύνου που έχει εντοπιστεί και να δηλώνει αν κάθε επιλογή θα είχε ως αποτέλεσμα ο κίνδυνος:

→ να εξαλειφθεί

→ να μειωθεί ή

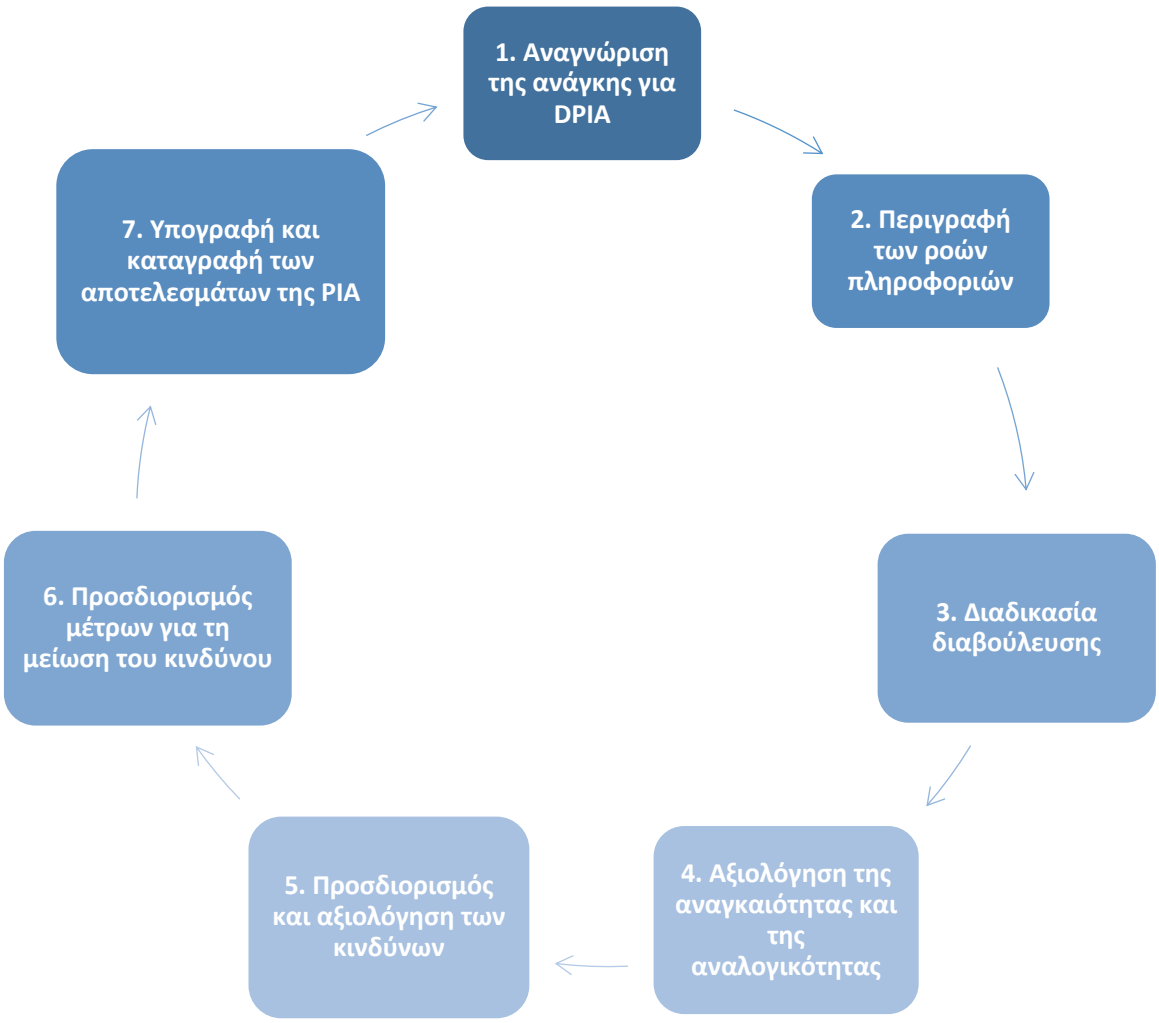
→ να γίνει αποδεκτός

Σε καθεμία εκ των τριών περιπτώσεων είναι σκόπιμο να αξιολογηθεί το πιθανό κόστος και τα οφέλη κάθε δυνητικής επιλογής ή λύσης.

7. Υπογραφή και καταγραφή των αποτελεσμάτων της PIA

Ως τελευταίο στάδιο, απαιτείται η λήψη κατάλληλης υπογραφής εντός του οργανισμού, η παραγωγής μιας έκθεσης αναφοράς (report) με βάση το υλικό που παρήχθη κατά τη διάρκεια της διενέργειας και τέλος το ενδεχόμενο δημοσίευσης της εν λόγω αναφοράς/έκθεσης ή άλλων σχετικών πληροφοριών χερικά με την διαδικασία. Βασικό μέρος της διαδικασίας DPIA είναι η απόφαση για το ποιες λύσεις προστασίας της ιδιωτικής ζωής θα προωθηθούν και η καταγραφή του κατά πόσον οι κίνδυνοι που έχουν εντοπιστεί πρέπει να εξαλειφθούν, να μειωθούν ή να γίνουν αποδεκτοί. Μερικές φορές οι οργανισμοί αποφασίζουν ότι ένας εντοπισμένος κίνδυνος είναι αποδεκτός [32]. Ωστόσο στην περίπτωση όπου υπάρχουν προσβλητικοί («unacceptable») κίνδυνοι προστασίας της ιδιωτικής ζωής που δεν μπορούν να εξαλειφθούν ή να μειωθούν, τότε ο οργανισμός θα πρέπει να επανεκτιμήσει τη βιωσιμότητα του έργου του. Τέλος, στο στάδιο αυτό αποτελεί καλή πρακτική να καταγράφονται τα στοιχεία του υπεύθυνου λήψης αποφάσεων που έχει υπογράψει κάθε κίνδυνο μαζί με του λόγους της απόφασης του. Αδιαμφισβήτητα, η δημοσίευση μιας έκθεσης DPIA θα βελτιώσει την διαφάνεια και την λογοδοσία ενώ ταυτόχρονα θα βοηθήσει τα άτομα να κατανοήσουν τον τρόπο και την ποσότητα που ένα έργο δύναται να τους επηρεάσει.

Ουσιαστικά, η παρακάτω εικόνα σκιαγραφεί την εν λόγω διαδικασία υπογραμμίζοντας όπως αναφέρθηκε παραπάνω, πως η διενέργεια μιας DPIA αποτελεί μια «ζωντανή» διαδικασία με συνεχή ανατροφοδότηση από την «ίδια»:



Σχήμα 3: Επισκόπηση της διαδικασίας DPIA

4.4.3 Ισχύουσα νομοθεσία

Η μεταβατική περίοδος για το Brexit έληξε στις 31 Δεκεμβρίου 2020. Ο ΓΚΠΔ έχει διατηρηθεί στο δίκαιο του Ηνωμένου Βασιλείου ως GDPR του Ηνωμένου Βασιλείου και θα συνεχίσει να διαβάζεται παράλληλα με τον Νόμο περί Προστασίας Δεδομένων του 2018, με τεχνικές τροποποιήσεις για να διασφαλιστεί ότι μπορεί να λειτουργήσει στο δίκαιο του Ηνωμένου Βασιλείου. Παρόλα αυτά από την 1η Ιανουαρίου, δεν θα υπάρξει καμία σημαντική αλλαγή στο καθεστώς προστασίας δεδομένων του Ηνωμένου Βασιλείου ή στα κριτήρια που υποχρεώνουν τις DPIAs. Τέλος, ο παραπάνω οδηγός έχει αναθεωρηθεί για να υιοθετήσει τη γνωμοδότηση 22/2018 του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων σχετικά με τον κατάλογο του ICO αναφορικά με τις πράξεις επεξεργασίας που υπόκεινται στην απαίτηση διενέργειας DPIA [33].

4.5 ISO/IEC 29134:2017

Το πρότυπο ISO/IEC 29134 παρέχει κατευθυντήριες γραμμές για μια διαδικασία αξιολόγησης των επιπτώσεων στην ιδιωτική ζωή, καθώς και για τη δομή και το περιεχόμενο μιας έκθεσης PIA. Πιο συγκεκριμένα, εφαρμόζεται σε όλους τους τύπους και τα μεγέθη οργανισμών, συμπεριλαμβανομένων δημόσιων και ιδιωτικών εταιρειών, κυβερνητικών φορέων και μη κερδοσκοπικών οργανισμών. Συγκεκριμένα, η διενέργεια εκτίμησης αντικτύπου μπορεί να περιγραφεί ως σύστημα έγκαιρης προειδοποίησης, όπου παρέχει έναν τρόπο εντοπισμού πιθανών κινδύνων για την προστασία της ιδιωτικής ζωής των υποκειμένων που απορρέουν από την επεξεργασία των PII και ως εκ' τούτου ενημερώνει τον οργανισμό για που θα πρέπει να λάβει προφυλάξεις και να δημιουργήσει προσαρμοσμένες εγγυήσεις προτού ο εκάστοτε οργανισμός προβεί σε μεγάλες επενδύσεις [1]. Αν και η PIA θα πρέπει να είναι κάτι περισσότερο από έναν απλό έλεγχο συμμόρφωσης, συμβάλλει ωστόσο στην απόδειξη της συμμόρφωσης του οργανισμού με τις σχετικές απαιτήσεις προστασίας της ιδιωτικής ζωής και των δεδομένων σε περίπτωση μεταγενέστερης καταγγελίας, ελέγχου της ιδιωτικής ζωής ή έρευνας συμμόρφωσης. Σε περίπτωση που προκύψει κίνδυνος ή παραβίαση της ιδιωτικής ζωής, η έκθεση PIA μπορεί να παράσχει αποδείξεις ότι ο οργανισμός ενήργησε κατάλληλα στην προσπάθεια του να αποτρέψει το περιστατικό. Αναμφίβολα αυτό μπορεί να συμβάλει στη μείωση ή ακόμη και στην εξάλειψη οποιασδήποτε ευθύνης, αρνητικής δημοσιότητας και απώλειας φήμη, ενώ μια κατάλληλη PIA αποδεικνύει επίσης στους πελάτες ή/και τους πολίτες ενός οργανισμού ότι σέβεται την ιδιωτική τους ζωή και ότι ανταποκρίνεται στις ανησυχίες τους. Συνεπώς, η PIA αποτελεί ένα εργαλείο για τη συστηματική ανάλυση των ζητημάτων προστασίας της ιδιωτικής ζωής που προκύπτουν από ένα έργο με σκοπό την ενημέρωση των υπευθύνων λήψης αποφάσεων, ταυτόχρονα δε δύναται να αποτελέσει αξιόπιστη πηγή πληροφοριών [34, 35].

4.5.1 Στόχοι της υποβολής εκθέσεων PIA

Ο στόχος της υποβολής εκθέσεων PIA είναι η γνωστοποίηση των αποτελεσμάτων της αξιολόγησης στα ενδιαφερόμενα μέρη. Οι προσδοκίες από μια PIA προέρχονται από πολλούς εμπλεκόμενους φορείς (stakeholders), ενώ τα ακόλουθα αποτελούν τυπικά παραδείγματα εμπλεκόμενων φορέων μαζί με τις προσδοκίες τους [1]:

1. Η PIA είναι ένα μέσο που επιτρέπει στα υποκείμενα των PII να έχουν την βεβαιότητα ότι η ιδιωτική τους ζωή προστατεύεται.
2. Η ενσωμάτωση της PIA στα πρώτα στάδια του έργου διασφαλίζει ότι οι απαιτήσεις προστασίας της ιδιωτικής ζωής περιλαμβάνονται στις λειτουργικές και μη λειτουργικές προδιαγραφές, είναι εφικτές, βιώσιμες και παρακολουθούνται μέσω της διαχείρισης αλλαγών και των κινδύνων ενώ μπορεί να οδηγήσουν στη μη πραγματοποίηση ή την ακύρωση του έργου. Η προσπάθεια ταξινόμησης και διαχείρισης των προσωπικών δεδομένων του έργου θα πρέπει να αντιμετωπιστεί ως ξεχωριστό επενδυτικό στοιχείο, ένα ανεξάρτητο ποσό στον προϋπολογισμό του έργου ή του προγράμματος, αποδεκτό από όλα τα ενδιαφερόμενα μέρη.
3. Ρυθμιστική αρχή: Η PIA είναι ένα μέσο που συμβάλλει στην απόδειξη της συμμόρφωσης με τις ισχύουσες νομικές απαιτήσεις. Δύναται να παράσχει αποδεικτικά στοιχεία για τη δέουσα επιμέλεια που έλαβε ο οργανισμός σε περίπτωση παραβίασης, μη συμμόρφωσης, καταγγελίας κ.λπ.
4. Τέλος, η PIA είναι ένα μέσο για την αξιολόγηση του τρόπου με τον οποίο ο εκτελών την επεξεργασία των PII ή ο υπεύθυνος επεξεργασίας των PII διαχειρίζεται τα PII και παρέχει στοιχεία που αποδεικνύουν ότι ακολουθεί τις συμβατικές υποχρεώσεις.

Συνολικά, η υποβολή εκθέσεων PIA θα πρέπει να εκπληρώνει δυο βασικές λειτουργίες. Η πρώτη, αποκαλούμενη «Κατάλογος», ενημερώνει τα συγκεκριμένα ενδιαφερόμενα μέρη για τις εντοπισμένες επηρεαζόμενες οντότητες, το επηρεαζόμενο περιβάλλον και τους κινδύνους για την προστασία της ιδιωτικής ζωής σχετικά με τον κύκλο ζωής των εμπλεκόμενων οντοτήτων, είτε πρόκειται για εγγενείς είτε για μετριασμένους κινδύνους [1]. Από την άλλη, η δεύτερη, «Στοιχεία Δράσης» είναι ένας μηχανισμός παρακολούθησης των ενεργειών που βελτιώνουν ή επιλύουν τους εντοπισμένους κινδύνους προστασίας της ιδιωτικής ζωής. Η ευαισθησία όσον αφορά τη διανομή και τη δημοσιοποίηση των πληροφοριών αναφοράς πρέπει να αξιολογηθεί ρητώς και να ταξινομηθεί σε ιδιωτική, εμπιστευτική, δημόσια κ.λπ.

4.5.2 Εκτέλεση της PIA [34]

1. Προσδιορισμός των ροών πληροφοριών PII

- **Στόχος (Objective):** Προσδιορισμός των ροών πληροφοριών των υπό αξιολόγηση PII

- **Είσοδος (Input):** Περιγραφή της διαδικασίας και του πληροφοριακού συστήματος προς αξιολόγηση
- **Προσδοκώμενο αποτέλεσμα (Expected output):** Σύνοψη των ευρημάτων σχετικά με τη ροή πληροφοριών των PII στο πλαίσιο της διαδικασίας.
- **Ενέργειες (Actions):** Ο υπεύθυνος για τη διενέργεια PIA θα πρέπει να συμβουλευτεί άλλους εντός του οργανισμού και ίσως και εξωτερικούς προς τον οργανισμό για να περιγράψει τις ροές PII και συγκεκριμένα:
  - → τον τρόπο συλλογής των PII και τη σχετική πηγή
  - → ποιος είναι υπόλογος και ποιος είναι υπεύθυνος εντός του οργανισμού για την επεξεργασία των PII
  - → για ποιο σκοπό γίνεται επεξεργασία των PII
  - → πώς θα υποβληθούν σε επεξεργασία τα PII
  - → πολιτική διατήρησης και διάθεσης PII
  - → πώς θα γίνεται η διαχείριση και η τροποποίηση των PII
  - → προσδιορισμός τυχόν μεταβιβάσεων PII σε δικαιοδοσίες όπου ισχύουν χαμηλότερα επίπεδα προστασίας των PII
  - → εάν συντρέχει λόγος, να ενημερώνουν τις αρμόδιες αρχές για κάθε νέα επεξεργασία PII και να ζητούν τις απαραίτητες εγκρίσεις.

Όσον αφορά τη ροή πληροφοριών σχετικά με τα PII θα πρέπει να τεκμηριώνονται στην έκθεση PIA.

Ως στοιχείο εισόδου στη PIA, ο οργανισμός θα πρέπει να περιγράψει τη ροή πληροφοριών με όσο το δυνατόν πιο λεπτομερή τρόπο, ώστε να βοηθήσει στον εντοπισμό πιθανών κινδύνων για την προστασία της ιδιωτικής ζωής. Ο εμπειρογνώμονας θα πρέπει να εξετάζει τις επιπτώσεις όχι μόνο στο απόρρητο των πληροφοριών, αλλά και τη συμμόρφωση με τους κανονισμούς που σχετίζονται με το απόρρητο, ενώ θα πρέπει να εξετάζεται ολόκληρος ο κύκλος ζωής των PII.

2. Ανάλυση των επιπτώσεων της περίπτωσης χρήσης

- **Στόχος (Objective):** Εντοπισμός πιθανής συμπεριφοράς των χρηστών
- **Είσοδος (Input):** Το είδος των δυνητικών εντολέων και των περιπτώσεων χρήσης τους, ιδιαίτερα τη χρήση ψηφιακών συσκευών για τον εντοπισμό των κινδύνων για την προστασία της ιδιωτικής ζωής.

- **Προσδοκώμενο αποτέλεσμα (Expected output):** Σύνοψη των ευρημάτων σχετικά με τις περιπτώσεις χρήσης των χρηστών στο πλαίσιο της επιχειρησιακής διαδικασίας.
- **Ενέργειες (Actions):** Προσδιορισμός και περιγραφή των επιπτώσεων στην προστασία της ιδιωτικής ζωής στην έκθεση PIA. Η μείωση των κινδύνων για την προστασία της ιδιωτικής ζωής δύναται να επιτευχθεί μέσω της συμπεριφοράς των χρηστών με γνώμονα τις συνοπτικές πληροφορίες της PIA όσον αφορά τους κινδύνους και τις ενέργειες μετριασμού των χρηστών.

3. Καθορισμός των σχετικών απαιτήσεων διασφάλισης της ιδιωτικής ζωής

- **Στόχος (Objective):** Καθορισμός των σχετικών απαιτήσεων διασφάλισης της ιδιωτικής ζωής για τον σκοπό του προγράμματος, του συστήματος πληροφοριών ή της διαδικασίας υπό αξιολόγηση.
- **Είσοδος (Input):** Περιγραφή της επιχειρησιακής διαδικασίας και του πληροφοριακού συστήματος προς αξιολόγηση, περίληψη των ευρημάτων σχετικά με τη ροή πληροφοριών των PII και τις επιπτώσεις της περίπτωσης χρήσης στο πλαίσιο της επιχειρησιακής διαδικασίας.
- **Προσδοκώμενο αποτέλεσμα (Expected output):** Κατάλογος απαιτήσεων διασφάλισης της ιδιωτικής ζωής
- **Ενέργειες (Actions):** Ο υπεύθυνος για τη διενέργεια PIA ή οι νομικοί του εμπειρογνώμονες θα πρέπει να διασφαλίζουν ότι η επιχειρησιακή διαδικασία που εμπίπτει στο πεδίο εφαρμογής συμμορφώνεται με τυχόν νομοθετικές, κανονιστικές, επιχειρηματικές απαιτήσεις και συμβατικές απαιτήσεις σχετικά με την προστασία της ιδιωτικής ζωής ή/και την προστασία των δεδομένων**.**

4. Εκτίμηση του κινδύνου προστασίας της ιδιωτικής ζωής

1. <u>Προσδιορισμός των κινδύνων απορρήτου:</u>

→ **Στόχος (Objective):** Εντοπισμός των κινδύνων για τα ενδιαφερόμενα μέρη που απορρέουν από το πρόγραμμα, το πληροφοριακό σύστημα ή τη διαδικασία που αξιολογείται.

→ **Είσοδος (Input):** Περιγραφή του προγράμματος, του πληροφοριακού συστήματος ή της διαδικασίας που πρόκειται να αξιολογηθεί.

→ **Προσδοκώμενο αποτέλεσμα (Expected output):** Αναγνωρισμένοι κίνδυνοι για την προστασία της ιδιωτικής ζωής.

→ **Ενέργειες (Actions):** Οι οργανισμοί πρέπει να προσδιορίζουν τους κινδύνους που πρέπει να αξιολογηθούν, ενώ τα αποτελέσματα των εντοπισμένων κινδύνων θα πρέπει να τεκμηριώνονται στην έκθεση PIA.

Ο εκτιμητής θα πρέπει να εμπλέκει άτομα με τις κατάλληλες γνώσεις στον εντοπισμό των κινδύνων για την προστασία της ιδιωτικής ζωής, διότι αφού προσδιοριστεί τι μπορεί να συμβεί, είναι απαραίτητο να εξεταστούν πιθανά σενάρια που να καταγράφουν ποιες συνέπειες μπορεί να προκύψουν.

2. <u>Ανάλυση κινδύνου απορρήτου:</u>

→ **Στόχος (Objective):** Ανάλυση των πιθανών συνεπειών και απειλών των εντοπισμένων κινδύνων για την προστασία της ιδιωτικής ζωής και εκτίμηση των αντίστοιχων επιπέδων επιπτώσεων και πιθανότητας.

→ **Είσοδος (Input):** Αναγνωρισμένοι κίνδυνοι για την προστασία της ιδιωτικής ζωής.

→ **Προσδοκώμενο αποτέλεσμα (Expected output):** Αποτέλεσμα από την ανάλυση κινδύνων για την προστασία της ιδιωτικής ζωής, που περιλαμβάνει την περιγραφή τους, την εκτίμηση του επιπέδου των επιπτώσεων και την πιθανότητα.

→ **Ενέργειες (Actions):** Οι οργανισμοί θα πρέπει να προσδιορίζουν τον αντίκτυπο ενός κινδύνου προστασίας της ιδιωτικής ζωής και αυτό αντιστοίχως να καταγράφεται στην αναφορά PIA.

Ουσιαστικά το στάδιο της ανάλυσης κινδύνου περιλαμβάνει τον προσδιορισμό των PII, των υποστηρικτικών στοιχείων που ενδέχεται να διατρέχουν κίνδυνο, τα τρωτά σημεία που σχετίζονται με τα στοιχεία αυτά, τις απειλές που ενδέχεται να εκμεταλλευτούν αυτά τα τρωτά σημεία, την πιθανότητα και τον αντίκτυπο αυτού του γεγονότος, καθώς και τυχόν υφιστάμενους ελέγχους που ενδέχεται να επηρεάσουν τον κίνδυνο. Το σύνολο των παραδοχών που γίνονται κατά την ανάλυση κινδύνου θα πρέπει να τεκμηριώνεται κατάλληλα.

3. <u>Αξιολόγηση του κινδύνου απορρήτου:</u>

→ **Στόχος (Objective):** Ιεράρχηση των εντοπισμένων κινδύνων για την προστασία της ιδιωτικής ζωής.

→ **Είσοδος (Input):** Αναγνωρισμένοι κίνδυνοι για την προστασία της ιδιωτικής ζωής και ανάλυση κινδύνων για την προστασία της ιδιωτικής ζωής.

→ **Προσδοκώμενο αποτέλεσμα (Expected output):** Χάρτης κινδύνου απορρήτου

→ **Ενέργειες (Actions):** Εκπόνηση αξιολόγησης κινδύνου και καταγραφή της στην αναφορά όπως σημειώθηκε και στις παραπάνω περιπτώσεις.

Η εκπόνηση αξιολόγησης του κινδύνου προστασίας της ιδιωτικής ζωής θα πρέπει να περιλαμβάνει τη σχετική ιεράρχηση του κινδύνου προστασίας της ιδιωτικής ζωής, με βάση τη σοβαρότητα των επιπτώσεων στην ιδιωτική ζωή των εντολέων PII, καθώς και τις συνολικές επιπτώσεις στον οργανισμό.

5. Προετοιμασία για την αντιμετώπιση κινδύνων απορρήτου

1. Επιλογή των θεραπευτικών επιλογών κινδύνου απορρήτου:

→ **Στόχος (Objective):** Απόφαση σχετικά με την επιλογή θεραπείας για κάθε κίνδυνο προστασίας της ιδιωτικής ζωής που εκτιμάται

→ **Είσοδος (Input):** Χάρτης κινδύνου απορρήτου

→ **Προσδοκώμενο αποτέλεσμα (Expected output):** Κατάλογος με τις καταλληλότερες θεραπευτικές επιλογές για κάθε εκτιμώμενο κίνδυνο προστασίας της ιδιωτικής ζωής.

→ **Ενέργειες (Actions):** Επιλογή των πιο κατάλληλων θεραπευτικών μέτρων.

Η αντιμετώπιση του κινδύνου μπορεί να περιλαμβάνει τη διενέργεια ανασχεδιασμού εφαρμογών ή διαδικασιών ανάλογα με το πεδίο εφαρμογής της αξιολόγησης, το πλαίσιο της διαχείρισης του κινδύνου και τον κλάδο. Από την άλλη η επιλογή της καταλληλότερης επιλογής αντιμετώπισης του κινδύνου προστασίας της ιδιωτικής ζωής περιλαμβάνει την εξισορρόπηση του κόστους και της προσπάθειας υλοποίησης με την υποχρέωση του οργανισμού να προστατεύει την ιδιωτική ζωή κάθε ενδιαφερόμενου μέρους του οποίου η ιδιωτική ζωή μπορεί να επηρεαστεί από τον οργανισμό, π.χ. τα PII τους ελέγχονται ή υποβάλλονται σε επεξεργασία από τον οργανισμό.

2. Καθορισμός ελέγχων:

→ **Στόχος (Objective):** Προσδιορισμός των κατάλληλων ελέγχων για τις επιλεγμένες θεραπευτικές επιλογές.

→ **Είσοδος (Input):** Κατάλογος με τις καταλληλότερες θεραπευτικές επιλογές για κάθε εκτιμώμενο κίνδυνο προστασίας της ιδιωτικής ζωής.

→ **Προσδοκώμενο αποτέλεσμα (Expected output):** Κατάλογος επιλεγμένων ελέγχων

→ **Ενέργειες (Actions):** Πρέπει να επισημανθούν οι κατάλληλοι έλεγχοι για τις επιλεγμένες επιλογές αντιμετώπισης του κινδύνου, καθώς και οι νομικά απαιτούμενοι έλεγχοι.

Οι πρόσθετοι έλεγχοι μπορούν να επιλέγονται από υφιστάμενα σύνολα ελέγχων που ορίζονται σε αναγνωρισμένα διεθνή πρότυπα ή εκδίδονται από αναγνωρισμένους φορείς. Μπορούν επίσης να αναπτυχθούν από τον οργανισμό ανεξάρτητα από τυχόν υπάρχοντα σύνολα ελέγχου. Εάν είναι αναγκαίο, οι έλεγχοι πρέπει να προσαρμόζονται στο συγκεκριμένο πλαίσιο του προγράμματος, του συστήματος πληροφοριών ή της εξεταζόμενης διαδικασίας.

3. Δημιουργία σχεδίων αντιμετώπισης του κινδύνου προστασίας της ιδιωτικής ζωής
   → **Στόχος (Objective):** Σχεδιασμός και εφαρμογή των δράσεων αντιμετώπισης των κινδύνων.
   → **Είσοδος (Input):** Κατάλογος των επιλεγμένων ελέγχων.
   → **Προσδοκώμενο αποτέλεσμα (Expected output):** Σχέδιο αντιμετώπισης του κινδύνου προστασίας της ιδιωτικής ζωής, σχέδιο ελέγχου, εγκρίσεις του ιδιοκτήτη του κινδύνου και δήλωση αποδοχής του.
   → **Ενέργειες (Actions):** Απαιτείται η διατύπωση ενός ή περισσότερων σχεδίων αντιμετώπισης του κινδύνου προστασίας της ιδιωτικής ζωής.

   Ο ιδιοκτήτης του κινδύνου θα πρέπει να εγκρίνει το σχέδιο επεξεργασίας των κινδύνων προστασίας της ιδιωτικής ζωής και να αποδέχεται τους εναπομείναντες κινδύνους προστασίας της ιδιωτικής ζωής.

4.5.3 Πεδίο εφαρμογής της PIA

Το πεδίο εφαρμογής της διενεργηθείσας PIA πρέπει να καθορίζεται στην τελική έκθεση PIA. Συγκεκριμένα, ο εκάστοτε οργανισμός θα πρέπει να παρέχει την πληρέστερη δυνατή περιγραφή της διαδικασίας, του προγράμματος, του πληροφοριακού συστήματος που θα αποτελέσει και το αντικείμενο της PIA. Επιπροσθέτως, σε αυτή την έκθεση πρέπει να καταγράφεται ο τρόπος με τον οποίο τα υποκείμενα των δεδομένων ενημερώνονται ότι ο εκάστοτε οργανισμός συλλέγει πληροφορίες σχετικά με αυτά και κατά δεύτερον ποιος είναι ο ρόλος της συγκατάθεσης. Ένα ακόμη πεδίο το οποίο χρήζει αναφοράς σε μια έκθεση αποτελεί το εάν οι πληροφορίες που έχουν ή πρόκειται να συλλεχθούν συνδυάζονται ή αντιστοιχίζονται με πληροφορίες από άλλες πηγές και, εάν ναι, βάσει ποιας νομικής

εξουσιοδότησης. Επιπροσθέτως, ο οργανισμός θα πρέπει να αναφέρει τον τρόπο με τον οποίο προτίθεται να διαγράψει τα PII όταν δεν τα χρειάζεται, ενώ θα πρέπει να αναφέρει ποιες διαδικασίες θα θέσει σε εφαρμογή για να επιτρέπει στα υποκείμενα να βλέπουν τα PII τους, να τα διορθώνουν (εάν είναι απαραίτητο) ή να ζητούν τη διαγραφή τους. Τέλος, θα πρέπει να αναφέρει τις διαδικασίες προσφυγής σε περίπτωση που ο οργανισμός αρνείται να διαγράψει τις πληροφορίες ή να επιτρέψει την πρόσβαση σε αυτές καθώς επίσης πρέπει να περιλαμβάνει τα ακόλουθα [34]:

1. Πληροφορίες σχετικά με τις απαιτήσεις του συστήματος

Οι πληροφορίες για τις απαιτήσεις του συστήματος πρέπει να περιέχουν:

- το σκοπό της επεξεργασίας,
- περιγραφή της επιχειρησιακής διαδικασίας που υποστηρίζεται ή θα υποστηριχθεί από το πληροφοριακό σύστημα,
- τον κατάλογο των λειτουργικών απαιτήσεων που ορίζονται για το πληροφοριακό σύστημα και το επίπεδο υποχρέωσης ή υλοποίησής τους,
- τους στόχους ασφάλειας των πληροφοριών
- περιγραφή του τρόπου με τον οποίο θα συλλέγονται τα δεδομένα, από ποιον και για ποιους λόγους. Επίσης η περιγραφή θα πρέπει να αναφέρει ποιος θα έχει πρόσβαση στα PII, συμπεριλαμβανομένων των παραμέτρων σχετικά με την κύρια πρόσβαση στα PII.
- εάν το σύστημα πληροφοριών ή τα PII πρόκειται να κοινοποιηθούν σε τρίτους, απαιτούνται τότε λεπτομέρειες σε ποιους θα κοινοποιηθεί το σύστημα πληροφοριών ή τα PII και για ποιους σκοπούς και την
- δήλωση σχετικά με την αιτιολόγηση της επεξεργασίας των PII που εμπλέκονται στο εν λόγω σύστημα πληροφοριών.

2. Πληροφορίες για επιχειρησιακά σχέδια και τις διαδικασίες

Οι πληροφορίες για τα επιχειρησιακά σχέδια και τις διαδικασίες θα πρέπει να περιλαμβάνουν:

- την έννοια της διαχείρισης της ταυτότητας και των χρηστών για το σύστημα πληροφοριών,

- την επιχειρησιακή αντίληψη, συμπεριλαμβανομένου του εάν το σύστημα πληροφοριών ή τμήματα αυτού λειτουργούν επιτόπου ή εξωτερικά ή σε υπολογιστικό νέφος και πού
- την έννοια της καταγραφής και τα αντίστοιχα σχέδια διατήρησης των καταγεγραμμένων πληροφοριών,
- την έννοια της υποστήριξης, ιδίως την ονομαστική απαρίθμηση των τρίτων μερών που συμμετέχουν στην υποστήριξη του πληροφοριακού συστήματος, το βαθμό στον οποίο θα έχουν πρόσβαση στα PII και τις τοποθεσίες από τις οποίες είναι δυνατή η πρόσβαση στα PII,
- τα σχέδια δημιουργίας αντιγράφων ασφαλείας και ανάκτησης,
- την προστασία και τη διαχείριση των μεταδεδομένων,
- τα σχέδια διατήρησης και διαγραφής δεδομένων και διάθεσης μέσων και
- την έννοια του απόσυρσης.

3. Κριτήρια κινδύνου

Στο μέρος αυτό πρέπει να περιγράφονται τα επιλεγμένα κριτήρια κινδύνου, που είναι τα εξής:

- τα κριτήρια για την εκτίμηση του επιπέδου των επιπτώσεων,
- τα κριτήρια για την εκτίμηση της πιθανότητας,
- τις κλίμακες και για τα δύο και
- τα κριτήρια αποδοχής του κινδύνου

4. Διαβούλευση με τα ενδιαφερόμενα μέρη

Κατά τη διαδικασία της PIA, ο οργανισμός αναμένεται να έχει προσδιορίσει τα είδη των ενδιαφερομένων μερών που πρέπει να ζητηθεί η γνώμη τους αλλά και να έχει διευκρινίσει πώς ζητήθηκε η γνώμη τους (π.χ. μέσω ερευνών, συνεντεύξεων, εργαστηρίων). Ουσιαστικά, η έκθεση PIA θα πρέπει να αναφέρει το αποτέλεσμα της διαβούλευσης με τα ενδιαφερόμενα μέρη, και αν και κατά πόσο είχε η διαβούλευση συνέπειες για το σχεδιασμό του προγράμματος, της διαδικασίας, του συστήματος πληροφοριών ή άλλης πρωτοβουλίας που αποτέλεσε αντικείμενο της PIA.

5. Απαιτήσεις απορρήτου

Η έκθεση PIA θα πρέπει να απαριθμεί τις σχετικές πηγές για τις απαιτήσεις που η ομάδα PIA προσδιόρισε ότι πρέπει να πληρούνται.

6. Εκτίμηση κινδύνου (Risk assessment)

- **Πηγές κινδύνου (Risk sources):** Η έκθεση PIA θα πρέπει να απαριθμεί τις πηγές κινδύνου προστασίας της ιδιωτικής ζωής που έχει εντοπίσει ο οργανισμός.
- **Απειλές και η πιθανότητά τους:** Για κάθε επεξεργασία PII και κάθε πιθανή συνέπεια στην ιδιωτική ζωή, η έκθεση PIA θα πρέπει να απαριθμεί τις καθορισμένες απειλές που μπορούν να επιτρέψουν την εμφάνιση των εντοπισμένων κινδύνων μαζί με την αντίστοιχη πιθανότητα τους.
- **Συνέπειες και το επίπεδο των επιπτώσεων τους:** Η έκθεση PIA θα πρέπει να τεκμηριώνει το επίπεδο των επιπτώσεων για κάθε εντοπισμένο κίνδυνο.
- **Αξιολόγηση κινδύνου (Risk evaluation):** Η έκθεση PIA θα πρέπει να παρέχει έναν χάρτη κινδύνων για την προστασία της ιδιωτικής ζωής, ο οποίος θα απεικονίζει το επίπεδο των επιπτώσεων και την πιθανότητα των εκτιμώμενων κινδύνων. Αδιαμφισβήτητα, θα πρέπει να τεθούν προτεραιότητες, με βάση το πού βρίσκονται οι κίνδυνοι στο χάρτη (με σειρά προτεραιότητας) αλλά και με βάση τα κριτήρια κινδύνου.
- **Ανάλυση συμμόρφωσης:** Η έκθεση PIA θα πρέπει να καταγράφει ανά στοιχείο εάν η επεξεργασία που αξιολογήθηκε κρίνεται σύμφωνη με τις διάφορες πτυχές της αντίστοιχης υποχρέωσης, ενώ σε περίπτωση που δεν κρίνεται πλήρως σύμφωνη, σε ποιο βαθμό.

7. Σχέδιο αντιμετώπισης κινδύνου (Risk treatment plan)

Η έκθεση PIA θα πρέπει να καταγράφει το σχέδιο αντιμετώπισης των κινδύνων και το στάδιο εφαρμογής οποιουδήποτε από τους περιεχόμενους ελέγχους.

8. Συμπέρασμα και αποφάσεις

Οι αποφάσεις που λαμβάνονται κατά τη διάρκεια της διαδικασίας PIA σχετικά με την αποδοχή των εναπομεινάντων κινδύνων για την προστασία της ιδιωτικής ζωής, τη μη εφαρμογή των συστάσεων της PIA στο σχέδιο επεξεργασίας και τη μη δημοσίευση

στοιχείων της έκθεσης PIA θα πρέπει να καταγράφονται, μαζί με τα συμπεράσματα που οδήγησαν σε αυτές τις αποφάσεις.

9. Δημόσια περίληψη PIA

Προκειμένου να παρέχονται πληροφορίες για τον κίνδυνο προστασίας της ιδιωτικής ζωής στους χρήστες, ο εκτιμητής μπορεί να χρειαστεί να προετοιμάσει μια δημόσια περίληψη της κύριας έκθεσης PIA. Εάν είναι απαραίτητο, η περίληψη θα πρέπει να αφαιρεί τις εμπορικά ευαίσθητες πληροφορίες που ενδέχεται να υπάρχουν στην πλήρη έκθεση PIA και να περιλαμβάνει μόνο τις βασικές πτυχές που αφορούν τους κύριους των PII. Συνεπώς, η δημόσια συνοπτική έκθεση PIA θα πρέπει να περιέχει τα εξής:

- τα οφέλη του συστήματος πληροφοριών ή της διαδικασίας,
- τους τύπους PII που θα υποβληθούν σε επεξεργασία και θα συλλεχθούν,
- τις νομικές δικαιοδοσίες υπό τις οποίες θα πραγματοποιηθεί η επεξεργασία των PIA,
- την περίληψη της ανάλυσης συμμόρφωσης,
- την περίληψη τυχόν μέτρων για τη συμμόρφωση με τις απαιτήσεις προστασίας της ιδιωτικής ζωής ή για την αντιμετώπιση του κινδύνου προστασίας της ιδιωτικής ζωής που ο οργανισμός προτίθεται να λάβει ή έχει ήδη λάβει,
- τυχόν μέτρα που συνιστάται να λαμβάνουν οι εντολείς των PII αλλά και
- τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας PII.

Τέλος, όταν η δημόσια περίληψη της PIA απευθύνεται στους εντολείς των PII ως μέλη του κοινού, θα πρέπει να παρουσιάζει όλες τις παραπάνω πληροφορίες και όλες τις πρόσθετες πληροφορίες με διαφανή, σαφή και κατανοητό τρόπο.

4.6 EDPS

Ο Ευρωπαϊκός Επιθεωρητής Προστασίας Δεδομένων (European Data Protection Supervisor, EDPS) είναι μια ανεξάρτητη αρχή της ΕΕ, υπεύθυνη σύμφωνα με το άρθρο 52 παράγραφος 2 του κανονισμού 2018/1725 «Όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα... για να διασφαλίζει ότι τα θεσμικά όργανα και οι οργανισμοί της Ένωσης σέβονται τα θεμελιώδη δικαιώματα και τις ελευθερίες των φυσικών προσώπων, και ιδίως το δικαίωμά τους στην προστασία των δεδομένων», και σύμφωνα με το άρθρο 52 παράγραφος 3 «...για να συμβουλεύει τα θεσμικά όργανα και τους οργανισμούς της Ένωσης και τα υποκείμενα των δεδομένων για όλα τα θέματα που αφορούν την επεξεργασία δεδομένων προσωπικού χαρακτήρα». Σύμφωνα με το άρθρο 58 παράγραφος 3 στοιχείο γ) του κανονισμού 2018/1725, ο EDPS έχει την εξουσία «να εκδίδει, με δική του πρωτοβουλία ή κατόπιν αιτήματος, γνωμοδοτήσεις προς τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και προς το κοινό για οποιοδήποτε θέμα που αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα» [36].

Στις 6 Ιουλίου του 2020, ο EDPS δημοσίευσε έκθεση σχετικά με τον τρόπο με τον οποίο τα θεσμικά όργανα, οι οργανισμοί και οι υπηρεσίες της ΕΕ διενεργούν εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων όταν επεξεργάζονται πληροφορίες που ενέχουν υψηλό κίνδυνο για τα δικαιώματα και την ελευθερία των φυσικών προσώπων. Ο Wojciech Wiewiórowski, ο οποίος στις 5 Δεκεμβρίου του 2019 ορίστηκε από το συμβούλιο ως Ευρωπαίος Επόπτης Προστασίας Δεδομένων (EDPS) για τα επόμενα πέντε (5) χρόνια, αναφέρει [36]:

«Οι εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων είναι ένα από τα νέα και πολύτιμα εργαλεία λογοδοσίας που χρησιμοποιούν οι EUIs όταν επεξεργάζονται ευαίσθητα δεδομένα προσωπικού χαρακτήρα για να μετρήσουν τον αντίκτυπο και τους κινδύνους για τα άτομα. Οι DPIA βοηθούν επίσης στην καλύτερη κατανόηση του τρόπου με τον οποίο αλλάζει η επεξεργασία δεδομένων στην πράξη. Η έκθεσή μας, μαζί με τις απαντήσεις που ελήφθησαν από την έρευνά μας, επιτρέπει στον EDPS να παράσχει περαιτέρω καθοδήγηση σχετικά με τις DPIA σύμφωνα με το άρθρο 39 του κανονισμού που ισχύει για τα θεσμικά όργανα της ΕΕ».

Ο EDPS δημοσίευσε στις 30 Σεπτεμβρίου 2020, το 82ο ενημερωτικό δελτίο του, συμπεριλαμβανομένης της άτυπης διαβούλευσης σχετικά με την έννοια της «μεγάλης κλίμακας» σύμφωνα με το άρθρο 39 παράγραφος 3 στοιχείο β) του κανονισμού (ΕΕ)

2018/1725 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα, τους οργανισμούς και τις υπηρεσίες της Ένωσης και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ. Ειδικότερα, ο EDPS διαπίστωσε ότι το ποσοστό του σχετικού πληθυσμού, σε σχέση με το οποίο δεν μπορεί να παρασχεθεί καμία αυστηρή αριθμητική καθοδήγηση ως προς το τι πρέπει να θεωρείται επεξεργασία μεγάλης κλίμακας, καθώς και η φύση των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και οι πιθανοί κίνδυνοι που προκύπτουν, είναι πτυχές που συνηγορούν αθροιστικά υπέρ της διενέργειας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων για την επεξεργασία [36].

4.6.1 Η «μεγάλης κλίμακας» επεξεργασία

Ο EDPS έχει ανεπίσημα γνωμοδοτήσει σχετικά με το κατά πόσον ένας συγκεκριμένος αριθμός υποκειμένων δεδομένων που αφορά μια επεξεργασία θα πρέπει να θεωρείται «μεγάλης κλίμακας» κατά την έννοια του άρθρου 39 παράγραφος 3 στοιχείο β) του κανονισμού (ΕΕ) 2018/1725, παρόλα αυτά όπως έχει αναφερθεί και στις παραπάνω μεθοδολογίες ο ίδιος ο κανονισμός δεν ορίζει τι συνιστάται «μεγάλης κλίμακας», αφήνοντας αυτόν τον όρο ανεξέλεγκτο. Όπως έχει καταγραφεί στο κεφάλαιο 4.2, οι κατευθυντήριες γραμμές του WP29 σχετικά με την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA) και τον προσδιορισμό του κατά πόσον η επεξεργασία «ενδέχεται να οδηγήσει σε υψηλό κίνδυνο» για τους σκοπούς του κανονισμού (ΕΕ) 2016/679, όσον αφορά τα «δεδομένα που υποβάλλονται σε επεξεργασία σε μεγάλη κλίμακα», αναφέρουν ότι «...ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλη κλίμακα, αν και η αιτιολογική σκέψη 91 παρέχει κάποια καθοδήγηση» [21]. Σύμφωνα λοιπόν με την αιτιολογική σκέψη 91, «Θα πρέπει επίσης να διενεργείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για τη λήψη αποφάσεων σχετικά με συγκεκριμένα φυσικά πρόσωπα μετά από οποιαδήποτε συστηματική και εκτεταμένη αξιολόγηση προσωπικών πτυχών που αφορούν φυσικά πρόσωπα...μετά από την επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα...ή δεδομένων σχετικά με ποινικές καταδίκες και αδικήματα...». Στην προκειμένη περίπτωση της άτυπης διαβούλευσης, η ΕΕ σχεδίαζε να αξιολογήσει τις δεξιότητες των υποψηφίων, συμπεριλαμβανομένου του κατά πόσον έχει ποτέ κινηθεί εναντίον τους πειθαρχική διαδικασία. Ωστόσο, δεν προβλέπεται κανένας αριθμητικός δείκτης για το τι θα μπορούσε

να θεωρηθεί «εκτεταμένη αξιολόγηση» κατά την έννοια της αιτιολογικής σκέψης 91. Παρομοίως, στην σύσταση του 01/2019 σχετικά με το σχέδιο καταλόγου του EDPS όσον αφορά τις πράξεις επεξεργασίας που υπόκεινται στην απαίτηση εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων (άρθρο 39 παράγραφος 4 του κανονισμού (ΕΕ) 2018/1725), παράγραφος 15, το EDPB αρνήθηκε να εγκρίνει αριθμητική καθοδήγηση σχετικά με το τι θα πρέπει να θεωρείται επεξεργασία μεγάλης κλίμακας. Τέλος, υπό το πρίσμα των ανωτέρω ο EDPS ενέκρινε στην άτυπη διαβούλευση ότι οι ακόλουθες πτυχές «τάσσονται» υπέρ της διενέργειας DPIA σχετικά με την επεξεργασία [36]:

1. **Το ποσοστό του σχετικού πληθυσμού**: Όσον αφορά τον συνολικό αριθμό των ατόμων που αφορά η επεξεργασία, δεν μπορεί να δοθεί καμία αυστηρή και σταθερή αριθμητική καθοδήγηση σχετικά με το τι πρέπει να θεωρείται επεξεργασία μεγάλης κλίμακας, αλλά η έννοια της «μεγάλης κλίμακας» αναφέρεται επίσης στο ποσοστό του σχετικού πληθυσμού. Αναφορικά με αυτό, το 2019 το EDPB υπογράμμισε ότι «Το Συμβούλιο Προστασίας Δεδομένων σημειώνει ότι ο EDPS κάνει αναφορά στον εσωτερικό τηλεφωνικό κατάλογο ενός θεσμικού οργάνου της ΕΕ ως αντιπαράδειγμα επεξεργασίας μεγάλης κλίμακας. Με την επιφύλαξη του κατά πόσον όντως απαιτείται DPIA, δεν είναι σαφές γιατί ένας τηλεφωνικός κατάλογος ενός θεσμικού οργάνου της ΕΕ δεν εμπίπτει από μόνος του στην έννοια της επεξεργασίας μεγάλης κλίμακας, ιδίως εφόσον μπορεί δυνητικά να περιλαμβάνει δεδομένα προσωπικού χαρακτήρα μεγάλου αριθμού ατόμων.».
2. **Η φύση των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία και οι πιθανοί κίνδυνοι που προκύπτουν:** Η αξιολόγηση των δεξιοτήτων των υποκειμένων των δεδομένων, συμπεριλαμβανομένου του κατά πόσον έχει ποτέ κινηθεί εναντίον τους πειθαρχική διαδικασία. Ουσιαστικά, ενδέχεται να υπάρχουν πράξεις επεξεργασίας «υψηλού κινδύνου» που δεν περιλαμβάνονται στον κατάλογο αυτό, αλλά ενέχουν παρόμοιους υψηλούς κινδύνους, γεγονός που καθιστά ότι εν λόγω πράξεις επεξεργασίας θα πρέπει επίσης να υπόκεινται σε DPIA.

4.6.2 Βασικές Απαιτήσεις

Η διαδικασία DPIA αποσκοπεί στην παροχή διαβεβαίωσης ότι οι υπεύθυνοι επεξεργασίας αντιμετωπίζουν επαρκώς τους κινδύνους για την προστασία της ιδιωτικής ζωής και των δεδομένων από «επικίνδυνες» πράξεις επεξεργασίας. Παρέχοντας έναν

δομημένο τρόπο σκέψης σχετικά με τους κινδύνους για τα υποκείμενα των δεδομένων και τον τρόπο μετριασμού τους, οι DPIA βοηθούν τους οργανισμούς να συμμορφωθούν με την απαίτηση της «προστασίας των δεδομένων εκ του σχεδιασμού». Κατά κύριο λόγο ο EDPS δεν επιβάλλει μια τυποποιημένη μεθοδολογία για τη διενέργεια DPIA, ωστόσο καταγράφει και υπογραμμίζει οδηγίες και κατευθυντήριες ερωτήσεις προς τις αρχές προστασίας δεδομένων. Συγκεκριμένα, οι οδηγίες αυτές περιλαμβάνουν [21]:

1. **Αμεροληψία** της επεξεργασίας έχει διάφορες πτυχές: Είναι η επεξεργασία απροσδόκητη για τα πρόσωπα που «θίγονται»; Έχει ανασταλτικά αποτελέσματα στην άσκηση των άλλων δικαιωμάτων τους; Είναι η επεξεργασία απροσδόκητη για τα υποκείμενα των δεδομένων, π.χ. επειδή επαναχρησιμοποιούνται τα δεδομένα για διαφορετικό σκοπό από αυτόν για τον οποίο συλλέχθηκαν αρχικά ή επειδή δύο ξεχωριστές βάσεις δεδομένων συγχωνεύθηκαν με νέα νομοθεσία; Ακόμη και αν τα υποκείμενα των δεδομένων δεν διαβάζουν την ανακοίνωση προστασίας δεδομένων, θα περίμεναν ότι θα συνέβαινε κάτι τέτοιο;
2. Η **«διαφάνεια»** ομαδοποιείται με τη δικαιοσύνη. Αυτό σημαίνει ότι τα άτομα των οποίων τα δεδομένα επεξεργάζονται πρέπει αφενός να είναι ενήμεροι και να έχουν δώσει την συγκατάθεση τους γι' αυτή την διαδικασία, αφετέρου να είναι σε θέση να κατανοήσουν τι συμβαίνει με τα δεδομένα τους και γιατί. Συνεπώς, είναι οι πληροφορίες πλήρεις και κατανοητές;, είναι στοχευμένες για το κοινό; Π.χ. τα παιδιά μπορεί να χρειάζονται εξατομικευμένες πληροφορίες.
3. Ο **«περιορισμός του σκοπού»** είναι η αρχή ότι τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται για έναν σκοπό δεν πρέπει να επαναχρησιμοποιούνται για άλλους, ασύμβατους σκοπούς. Ένα σημαντικό χαρακτηριστικό σχεδιασμού που μπορεί συχνά να είναι χρήσιμο είναι η «μη συνδεσιμότητα». Η έννοια αυτή αναφέρεται στην ιδιότητα να μην είναι δυνατή η εύκολη σύνδεση προσωπικών δεδομένων με άλλες πληροφορίες για το ίδιο πρόσωπο. Συνεπώς, αυτό δύναται συμβάλλει στην επιβολή του περιορισμού του σκοπού και συντελεί στην αποτροπή της δημιουργίας ολοκληρωμένων προφίλ ατόμων για σκοπούς που δεν θα γνώριζαν.
4. **«Ελαχιστοποίηση των δεδομένων**» σημαίνει επεξεργάζονται μόνο τα δεδομένα προσωπικού χαρακτήρα που πραγματικά χρειάζεται για την εκπλήρωση του σκοπού της επεξεργασίας και διατηρούνται μόνο για όσο χρονικό διάστημα είναι απαραίτητο για τον σκοπό αυτό. Αυτό είναι επίσης βασικό στοιχείο για την αποφυγή παράνομης υπερβολικής επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Συνεπώς, γίνεται

σαφή διάκριση μεταξύ υποχρεωτικών και προαιρετικών στοιχείων στα έντυπα συμπλήρωσης;

5. «**Ακρίβεια»** σημαίνει ότι οι πληροφορίες που επεξεργάζονται για τους ανθρώπους είναι ακριβείς; Επομένως, πώς διασφαλίζεται ότι τα δεδομένα που συλλέγονται είναι ακριβή ή ακόμα περισσότερα τα δεδομένα που συλλέγονται από τρίτους; Διατίθενται εργαλεία που να επιτρέπουν ελέγχους συνέπειας;
6. **«Περιορισμός της αποθήκευσης»** αναφέρεται στη διατήρηση δεδομένων προσωπικού χαρακτήρα «για όσο χρονικό διάστημα είναι αναγκαίο και όσο το δυνατόν συντομότερο». Ουσιαστικά, μπορεί να διακριθούν οι περίοδοι αποθήκευσης για διαφορετικά τμήματα των δεδομένων ή μπορεί να περιοριστεί η πρόσβαση σε αυτά;
7. **«Ασφάλεια»**, όρος που κατά κύριο λόγο παραπέμπει στις έννοιες της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων. Η παραβίαση των εννοιών αυτών εμποδίζει την ίδια την χρήση των δεδομένων αλλά μπορεί να επηρεάσει και τα ενδιαφερόμενα πρόσωπα. Υπάρχουν οργανισμοί που στοχεύουν στις επιπτώσεις όσον αφορά τα θεμελιώδη δικαιώματα, τις ελευθερίες και τα συμφέροντα των υποκειμένων ή μόνο στους κινδύνους που μπορεί να προκαλέσουν «ζημιά» στον οργανισμό; Επιπλέον, επανεξετάζονται και επικαιροποιούνται συστηματικά τα μέτρα ασφαλείας σε σχέση με το πλαίσιο της επεξεργασίας και τους κινδύνους;

4.7 Εποπτικές Αρχές Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

4.7.1 Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Από τις παραπάνω ενότητες έχει καταστεί σαφές πως σύμφωνα με την προσέγγιση βάσει κινδύνου που υιοθετεί ο ΓΚΠΔ, δεν απαιτείται η διενέργεια DPIA σε κάθε πράξη επεξεργασίας. Αντιθέτως η διενέργεια DPIA απαιτείται μόνον όταν ένα είδος επεξεργασίας «ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 35 παράγραφος 1) [5]. Αδιαμφισβήτητα, το γεγονός της μη πλήρωσης των όρων που ενεργοποιούν την υποχρέωση διενέργειας DPIA 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. Καθίσταται σαφές, πως τις χώρες όπου βρίσκεται σε εφαρμογή ο ΓΚΠΔ, πρέπει ταυτόχρονα με τα παραπάνω κριτήρια να λαμβάνονται υπόψη και οι οδηγίες της εποπτικής αρχής της εκάστοτε χώρας. Ειδικότερα, όπως ορίζει το άρθρο 35 παράγραφος 4, καταρτίζει και δημοσιοποιεί έναν κατάλογο με τα είδη των πράξεων επεξεργασίας τα οποία απαιτούνται προκειμένου να εκπονηθεί εκτίμηση αντικτύπου. Στην συνέχεια, ο κατάλογος αυτός ανακοινώνεται στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ).

Συγκεκριμένα, η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), σύμφωνα με την αριθμό απόφασης 65/2018, έχει συντάξει τον κατάλογο που παρατίθεται παρακάτω που περιλαμβάνει τις πράξεις επεξεργασίας που υπόκεινται σε απαίτηση DPIA [37]. Η ΑΠΔΠΧ έχει ταξινομήσει τα κριτήρια σε τρεις κατηγορίες [38]:

- **1η Κατηγορία:** Περιλαμβάνει τις επεξεργασίες ανάλογα με τα είδη και τους σκοπούς της επεξεργασίας τους.
- **2η Κατηγορία:** Περιλαμβάνει τις επεξεργασίες ανάλογα με το είδος των δεδομένων που επεξεργάζονται και τις κατηγορίες των υποκειμένων των δεδομένων
- **3η Κατηγορία:** Περιλαμβάνει τις επεξεργασίες ανάλογα με τα επιπρόσθετα χαρακτηριστικά τους αλλά και τα χρησιμοποιούμενα συστήματα ή μέσα της επεξεργασίας.

Με βάση την ΑΠΔΠΧ, ο υπεύθυνος επεξεργασίας πρέπει να προχωρήσει υποχρεωτικά στην διενέργεια DPIA, στην περίπτωση όπου η επεξεργασία πληροί τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Επιπροσθέτως, κρίνεται ακόμα ως υποχρεωτική όταν

πληροί ένα από τα κριτήρια της 3ης κατηγορίας και συγχρόνως η επεξεργασία αυτή δύναται να συνδεθεί με τους σκοπούς και τα είδη της επεξεργασίας τα οποία αναφέρονται στην 1η κατηγορία ή και στα είδη των δεδομένων αλλά και τα είδη των υποκειμένων των δεδομένων, τα οποία περιλαμβάνονται στην 2η κατηγορία.

Συνεπώς, προκειμένου να καταστεί σαφής ο διαχωρισμός των κατηγοριών, παρατίθενται αναλυτικά οι εκάστοτε κατηγορίες με τα αντίστοιχα κριτήρια [38]:

- **Στην 1η κατηγορία ανήκουν:**
  - → Αυτοματοποιημένη λήψη αποφάσεων που έχει προκύψει από συστηματική επεξεργασία δεδομένων. Οι αποφάσεις αυτές παράγουν στη συνέχεια παράνομα αποτελέσματα που αφορούν τα υποκείμενα των δεδομένων ή τα επηρεάζουν σημαντικά με τρόπο εφικτό να τα οδηγήσουν σε αποκλεισμό ή σε διακρίσεις εις βάρος του φυσικού προσώπου. Χαρακτηριστικό παράδειγμα αποτελεί η ηλεκτρονική πρόσληψη προσωπικού, η οποία έχει πραγματοποιηθεί χωρίς ανθρώπινη παρέμβαση.
  - → Συστηματικής επεξεργασίας δεδομένων προσωπικού χαρακτήρα μεγάλης κλίμακας που αφορούν την υγεία και τη δημόσια υγεία για σκοπούς δημοσίου συμφέροντος. Χαρακτηριστικό παράδειγμα είναι τα συστήματα που αφορούν τον εμβολιασμό και το Covid.
  - → Συστηματική επεξεργασία δεδομένων που μπορεί να εμποδίσει το υποκείμενο των δεδομένων να ασκήσει τα δικαιώματά του, να έχει πρόσβαση σε μια υπηρεσία ή να χρησιμοποιήσει μια σύμβαση, ιδιαίτερα όταν στην παρεμπόδιση αυτή εμπλέκονται δεδομένα τρίτων. Ένα παράδειγμα αποτελεί όταν μια τράπεζα ελέγχει τους πελάτες και αποφασίζει αν θα τους χορηγήσει δάνειο σύμφωνα με μια βάση δεδομένων που αναλύει την οικονομική κατάσταση των πελατών, ιδίως αν η βάση δεδομένων αυτή προέρχεται από τρίτους.
  - → Συστηματική αξιολόγηση, βαθμολόγηση, πρόγνωση, πρόβλεψη και κατάρτιση προφίλ των πτυχών που σχετίζονται με την υγεία, την οικονομική κατάσταση, τα ενδιαφέροντα και τις προσωπικές προτιμήσεις, τη γενική συμπεριφορά ή την αξιοπιστία, τη θέση ή τις μετακινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων. Ως παράδειγμα τίθεται η πρόβλεψη του τόπου θα επισκεφθεί ένα υποκείμενο των δεδομένων μετά την κατάρτιση προφίλ σύμφωνα με τις προηγούμενες θέσεις και μετακινήσεις του.

→ Συστηματική επεξεργασία δεδομένων με σκοπό την εμπορική προώθηση προϊόντων και υπηρεσιών στα υποκείμενα των δεδομένων μετά από προηγούμενη κατάρτιση προφίλ των υποκειμένων των δεδομένων και λαμβάνοντας υπόψη τα δεδομένα που συλλέγονται από τρίτους.

→ Συστηματική επεξεργασία δεδομένων σε μεγάλη κλίμακα για την εισαγωγή, την οργάνωση, την παροχή και τον έλεγχο της χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης, όπως ορίζεται στο άρθρο 3 του νόμου 3979/201 [39].

→ Συστηματική και μεγάλης κλίμακας επεξεργασία κατά την οποία τα υποκείμενα παρακολουθούνται, παρατηρούνται ή ελέγχονται σύμφωνα με τα δεδομένα που συλλέγονται από συστήματα κλειστού κυκλώματος παρακολούθησης ή άλλα συστήματα σε δημόσιο χώρο ή σε ιδιωτικό χώρο στον οποίο έχει πρόσβαση απροσδιόριστος αριθμός ατόμων (π.χ. εμπορικό κατάστημα). Η επεξεργασία αυτή περιλαμβάνει την παρακολούθηση των πιθανών κινήσεων και θέσεων αναγνωρισμένων ή μη αναγνωρισμένων υποκειμένων σε πραγματικό ή μη χρόνο.

- **Στην 2η κατηγορία ανήκουν** [38]**:**
  → Επεξεργασία σε μεγάλη κλίμακα ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα[3] που αναφέρονται στο άρθρο 9 παράγραφος 119[4] και στο άρθρο 10[5] του ΓΚΠΔ.

  → Επεξεργασία που πραγματοποιείται μέσω της συστηματικής παρακολούθησης των δεδομένων θέσης/τοποθέτησης και των μεταδεδομένων επικοινωνίας των εργαζομένων. Παρόλα αυτά δύναται να εξαιρεθεί από το κριτήριο, όταν η εν λόγω επεξεργασία πραγματοποιείται για λόγους ασφαλείας με την τήρηση αρχείων καταγραφής που περιέχουν τα απαραίτητα δεδομένα και υπάρχει τεκμηρίωση.

[3] Στις κατηγορίες αυτές περιλαμβάνονται τα δεδομένα που οδηγούν στη σαφή ταυτοποίηση ενός προσώπου, όπως τα γενετικά και βιομετρικά δεδομένα.

[4] Παράγραφος 119, ΓΚΠΔ: «Δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.»

[5] Σύμφωνα με το άρθρο 10: «Δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας που βασίζονται στο άρθρο 6 παράγραφος 1 διενεργείται μόνο υπό τον έλεγχο επίσημης αρχής ή εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.»

→ Επεξεργασία σε μεγάλη κλίμακα δεδομένων ιδιαίτερης σημασίας ή εξαιρετικού χαρακτήρα, όπως:

- Ο αριθμός ταυτότητας, άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής ή αλλαγή των όρων και προϋποθέσεων για την επεξεργασία και τη χρήση αυτών και σχετικών προσωπικών δεδομένων.
- Δεδομένα ηλεκτρονικών επικοινωνιών, όπως ηλεκτρονικό ταχυδρομείο, μεταδεδομένα, δεδομένα που αποκαλύπτουν την τοποθεσία ενός υποκειμένου. Επίσης εξαίρεση αποτελεί η καταγραφή τηλεφωνικών κλήσεων σύμφωνα με το άρθρο 4 παράγραφος 3 του νόμου 3471/2006.
- Δεδομένα που συλλέγονται ή παράγονται από συσκευές μέσω εφαρμογών «Διαδικτύου των πραγμάτων (IoT)», όπως έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, συνδεδεμένα παιχνίδια, έξυπνες πόλεις, έξυπνοι μετρητές ενέργειας κ.λπ.
- Δεδομένα που περιέχονται σε προσωπικά έγγραφα, όπως ημερολόγια, προσωπικές σημειώσεις από ηλεκτρονικούς αναγνώστες και εφαρμογές καταγραφής ζωής, οι οποίες προσφέρουν τη δυνατότητα τήρησης σημειώσεων και πληροφοριών που αφορούν πολλούς ανθρώπους.

- **Στην 3η κατηγορία ανήκουν:**
  → Πράξεις επεξεργασίας που αφορούν δεδομένα τα οποία δεν έχουν συλλεχθεί από το υποκείμενο των δεδομένων, ενώ η ενημέρωση των υποκειμένων των δεδομένων σύμφωνα με το άρθρο 14 του ΓΚΠΔ καθίσταται αδύνατη και θα μπορούσε να βλάψει σοβαρά την επίτευξη των σκοπών της επεξεργασίας.
  → Πράξεις επεξεργασίας που περιλαμβάνουν την καινοτόμο χρήση ή εφαρμογή νέων τεχνολογιών, οι οποίες μπορεί να περιλαμβάνουν νέες μορφές συλλογής και χρήσης δεδομένων που δύναται να οδηγήσουν σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, όπως ο συνδυασμός δακτυλικών αποτυπωμάτων και αναγνώρισης προσώπου για ενισχυμένο φυσικό έλεγχο πρόσβασης, ή «έξυπνες» εφαρμογές, οι οποίες δημιουργούν προφίλ χρηστών ακόμα και εφαρμογές τεχνητής νοημοσύνης [38].
  → Επεξεργασία κατά την οποία δεδομένα προσωπικού χαρακτήρα συνδυάζονται ή συγκεντρώνονται από πολλαπλές πηγές ή τρίτους, από δύο ή περισσότερες πράξεις επεξεργασίας που πραγματοποιούνται για διαφορετικούς σκοπούς ή από

διαφορετικούς υπευθύνους επεξεργασίας κατά τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων.

Επιπλέον αξίζει να σημειωθεί πως σε κάθε περίπτωση που η μελέτη DPIA καταδεικνύει ότι οι υπολειπόμενοι κίνδυνοι παραμένουν υψηλοί, ο υπεύθυνος επεξεργασίας οφείλει να ζητήσει τη γνώμη της Αρχής, σύμφωνα με τα προβλεπόμενα στο άρθρο 36 του ΓΚΠΔ. Συνεπώς, απαιτείται προηγούμενη διαβούλευση με την Αρχή, όταν ο υπεύθυνος επεξεργασίας δεν μπορεί να βρει επαρκή μέτρα για τη μείωση των κίνδυνων σε αποδεκτό επίπεδο. Χαρακτηριστικό παράδειγμα αποτελεί ένα αίτημα διαβούλευσης, βάσει του άρθρου 36 ΓΚΠΔ, το οποίο υποβλήθηκε στην Αρχή από το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ) σχετικά με υπολειπόμενο κίνδυνο κατά την επεξεργασία δεδομένων που αφορά την ανάρτηση στον διαδικτυακό του τόπο πινάκων κατάταξης, οι οποίοι δύναται να περιλαμβάνουν ειδικές κατηγορίες δεδομένων. Ειδικότερα, το ΑΣΕΠ ζήτησε τη γνώμη της Αρχής διότι η μελέτη DPIA την οποία εκπόνησε υπέδειξε ότι ακόμα και μετά την λήψη μέτρων μετριασμού του κινδύνου, η επεξεργασία διά της ανάρτησης ειδικών κατηγοριών δεδομένων δύναται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Η σχετική γνωμοδότηση της Αρχής εκδόθηκε στις αρχές του 2020.

4.7.2 Γραφείο Επιτρόπου Πληροφοριών της Αυστραλίας (OAIC)

Κατά την ανάπτυξη ή την αναθεώρηση ενός έργου, προκύπτει η ανάγκη διενέργειας εκτίμησης αντικτύπου στην ιδιωτική ζωή (PIA). Η PIA προσδιορίζει τον τρόπο με τον οποίο ένα έργο μπορεί να έχει επιπτώσεις στην ιδιωτική ζωή των ατόμων και διατυπώνει συστάσεις για τη διαχείριση, την ελαχιστοποίηση ή την εξάλειψη των επιπτώσεων στην ιδιωτική ζωή. Συγκεκριμένα, ο Οδηγός για την πραγματοποίηση εκτιμήσεων αντικτύπου στην ιδιωτική ζωή εκπονήθηκε από το Γραφείο του Επιτρόπου Πληροφοριών της Αυστραλίας (Office of the Australian Information Commissioner, OAIC) για να περιγράψει μια διαδικασία για την πραγματοποίηση εκτίμησης αντικτύπου στην ιδιωτική ζωή (PIA). Αυτός ο οδηγός PIA προορίζεται να παράσχει καθοδήγηση σε όλες τις οντότητες της Αυστραλιανής Αρχής Προστασίας Προσωπικών Δεδομένων (APP). Σύμφωνα με OAIC [39] [39]για να θεωρηθεί μια PIA αποτελεσματική θα πρέπει να αποτελεί αναπόσπαστο μέρος της διαδικασίας σχεδιασμού του έργου, ενώ μπορεί να συμβάλλει στην διευκόλυνση της προσέγγισης της προστασίας της ιδιωτικής ζωής από τον σχεδιασμό, στον εντοπισμό

καλύτερων πρακτικών και στη διασφάλιση της συμμόρφωσης με τον νόμο περί προστασίας της ιδιωτικής ζωής.

Ειδικότερα, το APP [40] απαιτεί από τις οντότητες να λαμβάνουν εύλογα μέτρα για την εφαρμογή μεθόδων, διαδικασιών και συστημάτων που θα διασφαλίζουν τη συμμόρφωση με τα APP και θα τους επιτρέπουν να αντιμετωπίζουν ερωτήματα ή καταγγελίες σχετικά με τη συμμόρφωση με την προστασία της ιδιωτικής ζωής. Με αυτόν τον τρόπο, οι APP απαιτούν «προστασία της ιδιωτικής ζωής εκ κατασκευής», μια προσέγγιση σύμφωνα με την οποία η συμμόρφωση με την προστασία της ιδιωτικής ζωής σχεδιάζεται στα έργα που ασχολούνται με προσωπικές πληροφορίες από την αρχή, αντί να προστίθεται εκ των υστέρων. Η διενέργεια PIA διευκολύνει τις οντότητες να διασφαλίσουν τη συμμόρφωση με την προστασία της ιδιωτικής ζωής και να εντοπίσουν καλύτερες πρακτικές.

Συνεπώς, ο οδηγός PIA καθορίζει μια προτεινόμενη διαδικασία δέκα βημάτων για την πραγματοποίηση μιας PIA, ενώ τονίζει πως είναι δυνατό να χρησιμοποιηθεί παράλληλα με τις υπάρχουσες μεθοδολογίες διαχείρισης έργων και διαχείρισης κινδύνων αλλά και ως αυτόνομη διαδικασία. Κατά την εξέταση της διαδικασίας PIA, τόσο οι κυβερνητικές υπηρεσίες όσο και οι οργανισμοί του ιδιωτικού τομέα θα μπορούσαν να εξετάσουν κατά πόσον η διαδικασία που περιγράφεται στον παρόντα οδηγό θα μπορούσε να προσαρμοστεί ώστε να ανταποκρίνεται σε συγκεκριμένες επιχειρηματικές ανάγκες ή λειτουργίες της οντότητας. Προτού καταγραφούν τα δέκα αυτά βήματα αξίζει να σημειωθεί πως ο Κώδικας για την προστασία της ιδιωτικής ζωής APP του 2017 [41] απαιτεί από τις αυστραλιανές κυβερνητικές υπηρεσίες που υπόκεινται στον νόμο περί προστασίας της ιδιωτικής ζωής να διεξάγουν PIA για όλα τα «έργα υψηλού κινδύνου προστασίας της ιδιωτικής ζωής». Επίσης κρίνεται απαραίτητο για τους οργανισμούς να διεξάγουν PIA εάν τους δοθεί σχετική εντολή από τον OAIC. Σύμφωνα λοιπόν με τον νόμο περί προστασίας της ιδιωτικής ζωής, ο OAIC μπορεί να δώσει εντολή σε έναν οργανισμό να υποβάλει PIA για μια δραστηριότητα ή λειτουργία που αφορά τον χειρισμό προσωπικών δεδομένων ατόμων. Επομένως, τα δέκα βήματα για την διενέργεια εκτίμησης αντικτύπου στην ιδιωτική ζωή είναι τα ακόλουθα [35]:

1. **Αξιολόγηση κατωφλίου (Threshold assessment)**

Εάν μια οντότητα που δεσμεύεται από τον νόμο περί απορρήτου αναπτύσσει ένα έργο που περιλαμβάνει προσωπικές πληροφορίες, πρέπει να συμμορφώνεται με τον εν λόγω νόμο. Η οντότητα αυτή είναι υπεύθυνη και υπόλογη για τις προσωπικές πληροφορίες που συλλέγει, ακόμη και όταν οι πληροφορίες τηρούνται από εξωτερικούς παρόχους υπηρεσιών

ή εργολάβους που δραστηριοποιούνται στην Αυστραλία ή στο εξωτερικό. Η αξιολόγηση κατωφλίου βοηθά στον υπολογισμό, σε πρώιμο στάδιο του έργου, εάν είναι απαραίτητη η διενέργεια PIA, καθώς κάθε έργο εξετάζεται ξεχωριστά. Η αξιολόγηση αυτή επιτρέπει να εντοπιστούν σχετικά εύκολα και γρήγορα έργα με μηδενικές ή ελάχιστες επιπτώσεις στην προστασία της ιδιωτικής ζωής των πληροφοριών. Το πρώτο ερώτημα που τίθεται κατά την αξιολόγηση του κατά πόσον απαιτείται PIA είναι: «Θα συλλεχθούν, αποθηκευτούν, χρησιμοποιηθούν ή αποκαλυφθούν προσωπικές πληροφορίες στο πλαίσιο του έργου;».

2. Σχεδιασμός της PIA

Ο σχεδιασμός θα πρέπει να εξετάζει μια σειρά στοιχείων, συμπεριλαμβανομένων των εξής:

- πόσο λεπτομερής πρέπει να είναι η PIA με βάση μια ευρεία αξιολόγηση του έργου και του πεδίου προστασίας της ιδιωτικής ζωής του,
- ποιος θα διεξάγει τη PIA,
- το χρονοδιάγραμμα της PIA,
- ο προϋπολογισμός και οι άλλοι διαθέσιμοι πόροι για την PIA,
- την έκταση και το χρονοδιάγραμμα των διαβουλεύσεων με τα ενδιαφερόμενα μέρη και το κοινό καθώς και
- τα βήματα που θα πρέπει να ληφθούν μετά την PIA, συμπεριλαμβανομένης της εφαρμογής των συστάσεων και της συνεχούς παρακολούθησης.

Κατά την διαδικασία σχεδιασμού, θα πρέπει να λαμβάνεται υπόψη ότι η PIA είναι μια διαδικασία η οποία θα πρέπει να συνεχιστεί πέραν της ανάπτυξης συστάσεων και της προετοιμασίας της έκθεσης PIA και να περιλαμβάνει την εφαρμογή και την παρακολούθηση.

3. Περιγραφή του έργου

Η PIA χρειάζεται μια ευρεία, «μεγάλη εικόνα» του έργου, η οποία περιλαμβάνει:

- τους γενικούς στόχους του έργου,
- πώς οι στόχοι αυτοί ταιριάζουν με τους ευρύτερους στόχους του οργανισμού ή της υπηρεσίας,
- το πεδίο και την έκταση του έργου,
- τυχόν συνδέσεις με υφιστάμενα προγράμματα ή άλλα έργα,
- τον υπεύθυνο του έργου,

- χρονοδιάγραμμα για τη λήψη αποφάσεων που θα επηρεάσουν το σχεδιασμό του έργου και
- ορισμένα από τα βασικά στοιχεία προστασίας της ιδιωτικής ζωής όπως για παράδειγμα, η έκταση και το είδος των πληροφοριών που θα συλλεχθούν, ο τρόπος με τον οποίο θα αντιμετωπιστούν η ασφάλεια και η ποιότητα των πληροφοριών και ο τρόπος με τον οποίο θα χρησιμοποιηθούν και θα κοινοποιηθούν οι πληροφορίες.

Η περιγραφή του έργου θα πρέπει να είναι αρκετά σύντομη, λεπτομερώς γραμμένη και δεν θα πρέπει να περιλαμβάνει ανάλυση των επιπτώσεων στην προστασία της ιδιωτικής ζωής, δεδομένου ότι αυτό θα εξεταστεί σε μεταγενέστερα στάδια της PIA.

4. Προσδιορισμός και διαβούλευση με τους ενδιαφερόμενους φορείς [39]

Τα ενδιαφερόμενα μέρη είναι όσοι ενδιαφέρονται ή ενδέχεται να ενδιαφερθούν ή να επηρεαστούν από το υπό εξέταση έργο. Μια οντότητα θα έχει εσωτερικά ενδιαφερόμενα μέρη και εξωτερικά ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των ρυθμιστικών αρχών, των πελατών, των οργανώσεων υπεράσπισης, των πάροχων υπηρεσιών, των εμπειρογνωμόνων του κλάδου, των ακαδημαϊκών και άλλων. Επίσης, η διαβούλευση με τα ενδιαφερόμενα μέρη μπορεί να βοηθήσει στον εντοπισμό κινδύνων και ανησυχιών για την προστασία της ιδιωτικής ζωής που δεν έχουν εντοπιστεί από την ομάδα που αναλαμβάνει τη PIA, καθώς και πιθανών στρατηγικών για τον μετριασμό των κινδύνων αυτών. Η διαβούλευση μπορεί επίσης να προσφέρει στα ενδιαφερόμενα μέρη την ευκαιρία να συζητήσουν τους κινδύνους και τις ανησυχίες με την οντότητα και να κατανοήσουν καλύτερα και να υποβάλουν παρατηρήσεις σχετικά με τυχόν προτεινόμενες στρατηγικές μετριασμού.

5. Χαρτογράφηση των ροών προσωπικών πληροφοριών

Η ανάλυση θα πρέπει να είναι αρκετά λεπτομερής ώστε να παρέχει μια αίσθηση του ποιες πληροφορίες θα συλλέγονται, θα χρησιμοποιούνται και θα αποκαλύπτονται, πώς θα τηρούνται και θα προστατεύονται και ποιος θα έχει πρόσβαση σε αυτές. Η αποτελεσματική χαρτογράφηση των ροών πληροφοριών, θα πρέπει να καταγράφονται με το προσωπικό και τα ενδιαφερόμενα μέρη του έργου, καθώς σε περίπτωση μεμονωμένης καταγραφής, ελλοχεύει ο κίνδυνος της παράληψης πληροφοριών σχετικά με τον τρόπο λειτουργίας του έργου ή τον τρόπο χειρισμού των προσωπικών πληροφοριών. Αυτή η λεπτομερής περιγραφή περιλαμβάνει:

- αν θα είναι απαραίτητη η επαλήθευση της ταυτότητας,
- ποιες προσωπικές πληροφορίες θα συλλέγονται και πώς θα συλλέγονται,
- τη χρήση και αποκάλυψη τους,
- τις διαδικασίες διασφάλισης της ποιότητας των πληροφοριών,
- τις εγγυήσεις ασφαλείας που υπάρχουν (ή θα υπάρξουν) και
- τη δυνατότητα που έχουν τα άτομα να έχουν πρόσβαση και να διορθώνουν τις προσωπικές τους πληροφορίες.

Η χαρτογράφηση θα πρέπει επίσης να περιγράφει το τρέχον περιβάλλον προσωπικών πληροφοριών και τον τρόπο με τον οποίο το έργο θα το επηρεάσει

6. Ανάλυση των επιπτώσεων στην προστασία της ιδιωτικής ζωής και έλεγχος συμμόρφωσης

Στο στάδιο αυτό πρέπει να προσδιοριστεί και να αναλυθεί κριτικά ο τρόπος με τον οποίο το έργο επηρεάζει την ιδιωτική ζωή, τόσο θετικά όσο και αρνητικά. Η ανάλυση των επιπτώσεων στην ιδιωτική ζωή διερευνά [39]:

- τον κίνδυνο επιπτώσεων στην ιδιωτική ζωή των ατόμων ως αποτέλεσμα του τρόπου χειρισμού των προσωπικών πληροφοριών,
- κατά πόσον οι επιπτώσεις στην ιδιωτική ζωή είναι αναγκαίες ή μπορούν να αποφευχθούν
- εάν υπάρχουν υφιστάμενοι παράγοντες που έχουν τη δυνατότητα να μετριάσουν τυχόν αρνητικές επιπτώσεις στην ιδιωτική ζωή
- πώς οι επιπτώσεις στην ιδιωτική ζωή μπορεί να επηρεάσουν τους γενικούς στόχους του έργου
- την επίδραση του έργου στις επιλογές ενός ατόμου σχετικά με το ποιος έχει πρόσβαση στις προσωπικές του πληροφορίες

Τελικά, η ανάλυση των επιπτώσεων στην προστασία της ιδιωτικής ζωής θα πρέπει να προσπαθήσει να καθορίσει αν το έργο έχει αποδεκτά αποτελέσματα ή μη αποδεκτές επιπτώσεις στην προστασία της ιδιωτικής ζωής. Η ανάλυση θα πρέπει να περιλαμβάνει την εξέταση του περιεχομένου των πληροφοριών και του πλαισίου στο οποίο συλλέγονται οι πληροφορίες. Ένας αρνητικός αντίκτυπος στην ιδιωτική ζωή μπορεί να μην φαίνεται σημαντικός, αλλά είναι σημαντικό να σημειωθεί ότι ακόμη και ελάχιστες προσωπικές πληροφορίες, με ακατάλληλο χειρισμό, μπορεί να επηρεάσουν την ιδιωτική ζωή κάποιου με

τρόπο που δεν είχε πρόθεση η οντότητα. Καταγράφονται επίσης ορισμένα παραδείγματα ερωτήσεων που πρέπει να εξεταστούν [39]:

- Πρέπει τα άτομα να παραιτηθούν από τον έλεγχο των προσωπικών τους πληροφοριών;
- Θα αλλάξει το έργο τον τρόπο με τον οποίο τα άτομα αλληλεπιδρούν με την οντότητα, όπως μέσω συχνότερων ελέγχων ταυτότητας, κόστους ή επιπτώσεων σε άτομα ή ομάδες που δεν διαθέτουν έγγραφα ταυτότητας;
- Θα ληφθούν αποφάσεις που έχουν συνέπειες για τα άτομα ως αποτέλεσμα του τρόπου χειρισμού των προσωπικών πληροφοριών στο πλαίσιο του έργου (όπως αποφάσεις σχετικά με υπηρεσίες ή παροχές);
- Υπάρχει μηχανισμός διαχείρισης παραπόνων; Εάν ναι, είναι ορατός, περιεκτικός και αποτελεσματικός;
- Υπάρχουν μηχανισμοί ελέγχου και εποπτείας (συμπεριλαμβανομένων διαδικασιών έκτακτης ανάγκης) σε περίπτωση αποτυχίας του συστήματος;
- Πόσο πολύτιμες θα ήταν οι πληροφορίες για μη εξουσιοδοτημένους χρήστες;

7. Διαχείριση του απορρήτου, αντιμετώπιση κινδύνων

Μέσω της ανάλυσης επιπτώσεων στην προστασία της ιδιωτικής ζωής και του ελέγχου συμμόρφωσης, ενδέχεται να έχουν εντοπιστεί κίνδυνοι για την προστασία της ιδιωτικής ζωής στον τρέχοντα σχεδιασμό του έργου. Κίνδυνοι για την προστασία της ιδιωτικής ζωής μπορεί να προκύψουν σε πολλές περιπτώσεις, για παράδειγμα, από τη συλλογή περισσότερων πληροφοριών από ό,τι χρειάζεται, τη χρήση παρεμβατικών μέσων συλλογής ή τη γνωστοποίηση ευαίσθητων στοιχείων ευρύτερα από ό,τι δικαιολογείται ή είναι απαραίτητο. Αυτοί οι κίνδυνοι μπορεί να αφορούν την ιδιωτική ζωή του ατόμου, τη συμμόρφωση και τη φήμη μιας οντότητας ή και τα δύο. Σε αυτό το στάδιο, πρέπει να εξεταστεί ποιες επιλογές μπορεί να επιτρέψουν την άρση, την ελαχιστοποίηση ή τον μετριασμό τυχόν αρνητικών επιπτώσεων στην προστασία της ιδιωτικής ζωής που εντοπίζονται μέσω της ανάλυσης επιπτώσεων στην προστασία της ιδιωτικής ζωής. Κατά την εξέταση των στρατηγικών για την αντιμετώπιση των αρνητικών επιπτώσεων στην ιδιωτική ζωή που εντοπίζονται στο στάδιο της ανάλυσης επιπτώσεων στην ιδιωτική ζωή, πρέπει να λαμβάνονται υπόψη διάφοροι παράγοντες, μεταξύ των οποίων:

- Αναγκαιότητα/ελαχιστοποίηση της συλλογής προσωπικών πληροφοριών στο απολύτως αναγκαίο μέτρο

- Αναλογικότητα, κάθε αρνητικός αντίκτυπος στην ιδιωτική ζωή πρέπει να είναι ανάλογος ή να εξισορροπείται με τα οφέλη που πρόκειται να επιτευχθούν από το έργο
- Διαφάνεια και λογοδοσία, τα μέτρα προστασίας της ιδιωτικής ζωής θα πρέπει να είναι διαφανή για τα άτομα μέσω κατάλληλων ειδοποιήσεων για τη συλλογή και πολιτικών προστασίας της ιδιωτικής ζωής
- Εφαρμογή της προστασίας της ιδιωτικής ζωής, όπου εξετάζεται πώς οι οργανωτικές/υπηρεσιακές πολιτικές και διαδικασίες μπορούν να υποστηρίξουν την ιδιωτική ζωή αλλά και πιο πρακτικά στοιχεία όπως η εκπαίδευση του προσωπικού.
- Ευελιξία, να ληφθεί υπόψη η ποικιλομορφία των ατόμων που επηρεάζονται από το έργο και κατά πόσον μπορεί να αντιδράσουν ή να επηρεαστούν διαφορετικά από την κοινοποίηση των προσωπικών τους πληροφοριών
- Προστασία της ιδιωτικής ζωής από το σχεδιασμό, η προστασία της ιδιωτικής ζωής θα πρέπει να περιλαμβάνεται στο νόμο ή σε άλλες δεσμευτικές υποχρεώσεις και να ενσωματώνεται στις νέες τεχνολογίες
- Τεχνολογίες που ενισχύουν την προστασία της ιδιωτικής ζωής, να εξεταστεί κατά πόσον μπορούν να χρησιμοποιηθούν στο έργο τεχνολογίες που ενισχύουν την προστασία της ιδιωτικής ζωής, καθώς και ο αντίκτυπος των τεχνολογιών που παραβιάζουν την προστασία της ιδιωτικής ζωής.

8. Συστάσεις

Από τα παραπάνω στάδια μπορούν να προκύψουν ορισμένες συστάσεις για το μέλλον του έργου, οι οποίες θα πρέπει να προσδιορίζουν τις επιπτώσεις ή τους κινδύνους που μπορούν να αποφευχθούν και πώς μπορούν να εξαλειφθούν ή να μειωθούν σε ένα πιο αποδεκτό επίπεδο. Για παράδειγμα, οι συστάσεις θα μπορούσαν να αφορούν [35]:

- αλλαγές που θα επιτύχουν μια πιο κατάλληλη ισορροπία μεταξύ των στόχων του έργου, των συμφερόντων των επηρεαζόμενων ατόμων και των συμφερόντων του φορέα
- στρατηγικές διαχείρισης της ιδιωτικής ζωής, που θα μειώσουν ή θα μετριάσουν τους κινδύνους για την ιδιωτική ζωή
- την ανάγκη για περαιτέρω διαβούλευση
- κατά πόσον οι επιπτώσεις στην ιδιωτική ζωή είναι τόσο σημαντικές ώστε το έργο δεν πρέπει να προχωρήσει.

Οι συστάσεις θα πρέπει να παρατίθενται στην έκθεση PIA και θα πρέπει να είναι σαφές σε ποιον απευθύνονται π.χ. σε διάφορους τομείς του οργανισμού ή της υπηρεσίας, σε

συγκεκριμένα μέλη της ομάδας έργου ή σε όσους κατέχουν θέσεις εξουσίας εντός του οργανισμού ή της υπηρεσίας. Τέλος, θα πρέπει επίσης να περιλαμβάνουν ένα χρονοδιάγραμμα για την υλοποίηση.

9. Προετοιμασία της έκθεσης

Μια έκθεση που παραθέτει όλες τις πληροφορίες της PIA αποτελεί σημαντικό αποτέλεσμα της διαδικασίας. Τα βασικά στοιχεία για τη συμπερίληψη σε μια έκθεση PIA περιλαμβάνουν [35]:

- περιγραφή του έργου,
- μεθοδολογία PIA,
- περιγραφή των ροών πληροφοριών,
- αποτέλεσμα της ανάλυσης επιπτώσεων στην ιδιωτική ζωή και των ελέγχων συμμόρφωσης, συμπεριλαμβανομένων των θετικών επιπτώσεων στην ιδιωτική ζωή και των κινδύνων για την ιδιωτική ζωή που έχουν εντοπιστεί, καθώς και των στρατηγικών που έχουν ήδη εφαρμοστεί για την προστασία της ιδιωτικής ζωής
- συστάσεις για την αποφυγή ή τον μετριασμό των κινδύνων για την προστασία της ιδιωτικής ζωής
- περιγραφή τυχόν κινδύνων για την προστασία της ιδιωτικής ζωής που δεν μπορούν να μετριαστούν, η πιθανή αντίδραση της κοινότητας σε αυτούς τους κινδύνους και κατά πόσον οι κίνδυνοι αυτοί αντισταθμίζονται από το δημόσιο όφελος που θα προκύψει από το έργο και
- εάν κρίνεται απαραίτητο, λεπτομερέστερες πληροφορίες μπορούν να παρασχεθούν σε παραρτήματα.

Ο OAIC έχει επίσης αναπτύξει ένα εργαλείο PIA [42] για την διεξαγωγή μιας PIA, την αναφορά των ευρημάτων και την ανταπόκριση στις συστάσεις. Οι φορείς ενθαρρύνονται να υιοθετήσουν μια ευέλικτη προσέγγιση και να προσαρμόσουν το εργαλείο ανάλογα με το μέγεθος, την πολυπλοκότητα και το επίπεδο κινδύνου του έργου τους.

10. Ανταπόκριση και επανεξέταση

Είναι σημαντικό να αναληφθεί δράση για την αντιμετώπιση των συστάσεων που διατυπώνονται στην έκθεση καθώς η PIA πρέπει να είναι μια συνεχής διαδικασία που δεν τελειώνει με την προετοιμασία μιας έκθεσης. Είναι εξίσου σημαντικό να λαμβάνονται μέτρα

για την ανταπόκριση στις συστάσεις της έκθεσης, καθώς και για την επανεξέταση και επικαιροποίηση της PIA.

5. Σύγκριση Μεθοδολογιών

Οι μεθοδολογίες που αναλύθηκαν περιλάμβαναν παρόμοια βήματα, όπως ένα βήμα για να αποφασιστεί αν είναι απαραίτητη μια ενδελεχής DPIA, τον εντοπισμό απειλών, την επιλογή επιλογών αντιμετώπισης κινδύνων και την τεκμηρίωση, ενώ διέφεραν ως προς την παροχή υποστηρικτικού υλικού για τη διεξαγωγή αυτών των βημάτων, την ανάθεση ρόλων και των αρμοδιοτήτων. Πιο συγκεκριμένα, παρακάτω η σύγκριση των μεθοδολογιών γίνεται με βάση τα ακόλουθα [3]:

5.1 Πλαίσιο αξιολόγησης και ανάλυση των διαθέσιμων μεθόδων PIA

5.1.1 Προσδιορισμός κινδύνων (Risk identification)

Η ανάλυση διαπίστωσε ότι σε πολλές περιπτώσεις η δομημένη καθοδήγηση για τον εντοπισμό κινδύνων (ερωτηματολόγια/μήτρες ή κατάλογοι παραδειγμάτων κινδύνων) βασίζεται σε συγκεκριμένα νομικά πλαίσια. Η πρακτική αυτή, αν και επιτρέπει στους οργανισμούς να επιτύχουν συμμόρφωση σε συγκεκριμένα νομικά πλαίσια, μπορεί να παραπλανήσει τους επαγγελματίες της PIA και να περιορίσει την άποψη τους για τους κινδύνους προστασίας της ιδιωτικής ζωής που προκύπτουν από την επεξεργασία των PIA. Επίσης, ενώ όλες οι μέθοδοι εντοπίζουν κινδύνους προστασίας της ιδιωτικής ζωής για τα άτομα, μόνο ένα υποσύνολο αυτών εντοπίζει κινδύνους για τον οργανισμό που προέκυψαν από την επεξεργασία προσωπικών δεδομένων, όπως συμβαίνει στη περίπτωση της Αυστραλίας.

5.1.2 Έλεγχοι αντιμετώπισης κινδύνων (Risk Treatment Controls)

Οι διαθέσιμες μέθοδοι PIA παρέχουν ελέγχους προστασίας της ιδιωτικής ζωής σε διαφορετικά επίπεδα λεπτομέρειας για τον μετριασμό των κινδύνων. Ενώ ορισμένες παρέχουν υψηλού επιπέδου (γενικούς), οργανωτικούς ελέγχους (UK ICO), άλλες προτείνουν συγκεκριμένους τεχνικούς ελέγχους (CNIL). Το πιο σημαντικό όμως είναι ότι δεν δίνεται ιδιαίτερη έμφαση στην ανάγκη εξάλειψης των κινδύνων για την προστασία της ιδιωτικής ζωής αντί της αντιμετώπισής τους, επανεξετάζοντας τη διαδικασία επεξεργασίας δεδομένων και αποφασίζοντας να μην επεξεργαστούν ορισμένα στοιχεία δεδομένων, εάν δεν είναι κρίσιμα για τον επιθυμητό σκοπό (UK ICO και ISO).

5.1.3 Εργαλεία αυτοματοποίησης της διαδικασίας PIA

Με εξαίρεση την beta έκδοση του λογισμικού PIA της CNIL και του αντίστοιχου της Αυστραλιανής Αρχής Προστασίας Δεδομένων, οι διαθέσιμες μέθοδοι δεν αναφέρονται σε εργαλεία που μπορούν να αυτοματοποιήσουν τη διαδικασία PIA ή να δημιουργήσουν μια έκθεση PIA.

5.1.4 Οργάνωση έργων PIA

Όσον αφορά την οργάνωση ενός έργου PIA, οι περισσότερες από τις μεθόδους που αναλύθηκαν αναφέρονται στο πρόσωπο που οργανώνει ένα έργο PIA, χωρίς ωστόσο να καθορίζουν σαφώς το ρόλο και τις αρμοδιότητές του. Για παράδειγμα, η CNIL προτείνει τη διενέργεια PIA από τον υπεύθυνο προστασίας δεδομένων, ο OAIC αναθέτει την ευθύνη στον υπεύθυνο έργου (PM) και η ISO σε έναν από τους δύο. Επίσης, η καθοδήγηση για την αντιστοίχιση των βημάτων της PIA (ή των επαναλήψεών της) σε ειδικές φάσεις του έργου παρέχεται σε λίγες μόνο από τις εξεταζόμενες μεθόδους (UK ICO), ενώ επίσης δεν παρέχονται κατευθυντήριες γραμμές για την επιλογή της ομάδας PIA, εκτός από την μέθοδο UK ICO. Ακόμα, αξίζει να σημειωθεί ότι η ευθύνη για τις περιοδικές αναθεωρήσεις της PIA, καθώς και τα σχετικά κατώτατα όρια δεν αποσαφηνίζονται, αντιθέτως υπονοούνται, ενώ παράλληλα δεν περιγράφονται ρητά στις διαθέσιμες μεθόδους.

Ως κοινό χαρακτηριστικό των μεθόδων αυτών είναι η δυνατότητα παροχής εξωτερικής υπογραφής από τις αρχές προστασίας δεδομένων ή από ανεξάρτητο τρίτο μέρος.

5.1.5 Εξωτερικοί ενδιαφερόμενοι (External stakeholders)

Όσον αφορά τη συμμετοχή εξωτερικών ενδιαφερόμενων στην αξιολόγηση κινδύνων, όπως οι συνήγοροι της ιδιωτικής ζωής και οι εκπρόσωποι των καταναλωτών, όλες οι μέθοδοι που αναλύθηκαν χαρακτηρίζουν την ανάγκη αυτή ως προαιρετική αλλά χρήσιμη και οι περισσότερες παρέχουν γενικές οδηγίες για τον εντοπισμό τους. Ωστόσο, μόνο λίγες παρέχουν καθοδήγηση σχετικά με τον τρόπο κατάρτισης σχεδίων διαβούλευσης με εξωτερικά ενδιαφερόμενα μέρη, χαρακτηριστικό παράδειγμα αποτελεί ο OAIC.

Παρακάτω, παρατίθεται συγκεντρωτικά το πλαίσιο αξιολόγησης και τα αποτελέσματα αυτής:

	1. Αξιολόγηση κατωφλίου	2. Νομικό πλαίσιο	3. Κίνδυνοι για τον Οργανισμό	4. Καθοδήγηση για την αξιολόγηση κινδύνων	5. Εργαλείο αυτοματισμού	6. Υπεύθυνος PIA
Μεθοδολογία DPIA υπό τον ΓΚΠΔ	✓	ΓΚΠΔ	✗	✗	✗	Υπεύθυνος έργου
OAIC Αυστραλία	✓	Αυστραλιανή Αρχή Δεδομένων	✗	Ερωτηματολόγιο για τον εντοπισμό κινδύνων	✓	Υπεύθυνος έργου
ΑΠΔΠΧ	✗	ΓΚΠΔ	✗	Κατευθυντήριες γραμμές	✗	Υπεύθυνος έργου
EDPS	✗	ΓΚΠΔ	✗	Κατευθυντήριες γραμμές	✗	Υπεύθυνος έργου
Ηνωμένο Βασίλειο ICO	✓	✗	✓	Παραδείγματα ερωτήσεων διαλογής, κινδύνων και στρατηγικών θεραπείας	✗	DPO
ISO 29134	✓	✗	✓	Μετρήσεις για την αξιολόγηση του αντίκτυπου και της πιθανότητας κινδύνου παραδείγματα κινδύνων για την προστασία της ιδιωτικής ζωής	✗	Υπεύθυνος έργου
CNIL	✗	ΓΚΠΔ	✗	Πρότυπο καθοδήγησης PIA, μετρήσεις για την αξιολόγηση των επιπτώσεων των κινδύνων, παραδείγματα απειλών & κατάλογος ελέγχων	✓	Ιδιοκτήτης έργου
WP29	✗	ΓΚΠΔ	✓	Κατευθυντήριες γραμμές	✗	Υπεύθυνος έργου

	7. Sign-off Ρόλος	8. Συμμετοχή εξωτερικών ενδιαφερομένων	9. Εξωτερικός έλεγχος της έκθεσης PIA	10. Δημοσίευση της έκθεσης PIA	11. Περιοδικές αναθεωρήσεις	12. Υπόδειγμα έκθεσης PIA
Μεθοδολογία DPIA υπό τον ΓΚΠΔ	✗	✓	Από ανεξάρτητο τρίτο μέρος και την DPA	✓	✓	✓
OAIC Αυστραλία	✗	✓	Έλεγχος από την DPA	✓	✓	✓
ΑΠΔΠΧ	✗	✓	Έλεγχος από την DPA	✓	✓	✓
EDPS	✗	✓	Έλεγχος από την DPA	✓	✓	✓
Ηνωμένο Βασίλειο ICO	Υπεύθυνος έργου	✓	✗	✓	Κατά την διάρκεια του έργου	✓
ISO 29134	Υπεύθυνος για το project	✓	Έλεγχος από την DPA	✓	✓	✓
CNIL	✗	✗	✗	✓	✓	✓
WP29	✗	✓	Έλεγχος από την DPA	✓	✓	✓

Πίνακας 4: Σύγκριση Μεθοδολογιών

5.2 Πώς εκιμούνται οι κίνδυνοι;

Όπως σημειώθηκε στην αρχή του παρόντος εγγράφου, ο ΓΚΠΔ επιβάλλει στους υπευθύνους επεξεργασίας τη γενική υποχρέωση να «λαμβάνουν υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» που ενέχει κάθε πράξη επεξεργασίας δεδομένων προσωπικού χαρακτήρα και να «εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζουν και να είναι σε θέση να αποδείξουν ότι η επεξεργασία πραγματοποιείται σύμφωνα με τον παρόντα κανονισμό» (άρθρο 24 παράγραφος 1, βλ. επίσης άρθρο 24 παράγραφος 1). 25(1))).

Η WP29 όρισε τις έννοιες «κίνδυνος» και «διαχείριση κινδύνου» ως εξής:

Ο «κίνδυνος» είναι ένα σενάριο που περιγράφει ένα γεγονός και τις συνέπειες του, εκτιμώμενο από άποψη σοβαρότητας και πιθανότητας. Η «διαχείριση κινδύνου», από την άλλη πλευρά, μπορεί να οριστεί ως οι συντονισμένες δραστηριότητες για την καθοδήγηση και τον έλεγχο ενός οργανισμού όσον αφορά τον κίνδυνο. Αξίζει να διευκρινιστεί ότι οι κίνδυνοι που πρέπει να εκτιμηθούν δεν είναι μόνο οι κίνδυνοι ασφάλειας, όπως η πιθανότητα και ο αντίκτυπος μιας παραβίασης δεδομένων, αλλά οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων (και άλλων ατόμων) που μπορεί να προκύψουν από την πράξη επεξεργασίας. Αυτό περιλαμβάνει όχι μόνο τα γενικά δικαιώματά τους στην ιδιωτική ζωή και την προστασία της ιδιωτικής ζωής, καθώς και τα ειδικά δικαιώματα των υποκειμένων των δεδομένων, αλλά και τα δικαιώματά τους στην ελευθερία της έκφρασης, την ελευθερία της κυκλοφορίας, την ελευθερία από την απαγόρευση των διακρίσεων, την ελευθερία από την αυταρχική εξουσία και το δικαίωμα παραμονής σε μια δημοκρατική κοινωνία χωρίς αδικαιολόγητη επιτήρηση από τη δική τους ή από άλλες χώρες, καθώς και το δικαίωμα αποτελεσματικής προσφυγής. Κατά συνέπεια, ο υπεύθυνος επεξεργασίας οφείλει να ελέγχει προσεκτικά όλες τις πτυχές κάθε ξεχωριστής πράξης και λειτουργίας επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όπως προτείνεται από την ιταλική αρχή προστασίας δεδομένων, την Garante, είναι χρήσιμο να ακολουθηθεί η προσέγγιση που υιοθετήθηκε από τον ENISA (Οργανισμός της ΕΕ για την ασφάλεια δικτύων και πληροφοριών), ο οποίος με τη σειρά του βασίζεται στο ευρέως αποδεκτό πρότυπο ISO 27005:

«Οι απειλές κάνουν κατάχρηση των τρωτών σημείων των περιουσιακών στοιχείων για να προκαλέσουν ζημιά στον οργανισμό», και ειδικότερα η έννοια του κινδύνου αποτελείται από τα ακόλουθα στοιχεία:

- περιουσιακό στοιχείο (τρωτά σημεία, έλεγχοι),
- απειλή (προφίλ παράγοντα απειλής, πιθανότητα) και
- αντίκτυπος

Όπως περιγράφεται επίσης από την Garante, η ορθή εκτίμηση κινδύνου περιλαμβάνει τέσσερα βήματα:

1. Καθορισμός της διαδικασίας μεταποίησης και του πλαισίου της.
2. Κατανόηση και αξιολόγηση των επιπτώσεων.
3. Ορισμός των πιθανών απειλών και αξιολόγηση της πιθανότητάς τους (πιθανότητα εμφάνισης απειλής).

4. Αξιολόγηση του κινδύνου (συνδυασμός πιθανότητας εμφάνισης απειλής και επιπτώσεων).

Αναλυτικότερα, το πρώτο είναι το αρχικό βήμα, το οποίο περιλαμβάνει την αποσαφήνιση και καταγραφή της λειτουργίας επεξεργασίας και του πλαισίου της, ενώ το δεύτερο βήμα περιλαμβάνει τον καθορισμό διαφόρων επιπέδων επιπτώσεων, τα οποία λογικά μπορούν να παραμείνουν σε τέσσερα επίπεδα, ως εξής:

Επίπεδο Αντικτύπου	Περιγραφή
Χαμηλό	Τα άτομα μπορεί να αντιμετωπίσουν μερικές μικρές δυσκολίες, τις οποίες θα ξεπεράσουν χωρίς κανένα πρόβλημα (χρόνος που δαπανάται για την εκ νέου εισαγωγή πληροφοριών, ενοχλήσεις, εκνευρισμοί κ.λπ.).
Μεσαίο	Τα άτομα μπορεί να αντιμετωπίσουν σημαντικές δυσχέρειες, τις οποίες θα μπορέσουν να ξεπεράσουν παρά τις ορισμένες δυσκολίες (επιπλέον κόστος, άρνηση πρόσβασης σε επιχειρηματικές υπηρεσίες, φόβος, έλλειψη κατανόησης, άγχος, μικρές σωματικές ασθένειες κ.λπ.)
Υψηλό	Τα άτομα ενδέχεται να αντιμετωπίσουν σημαντικές επιπτώσεις, τις οποίες θα πρέπει να είναι σε θέση να ξεπεράσουν, έστω και με σοβαρές δυσκολίες (υπεξαίρεση κεφαλαίων, μαύρη λίστα από χρηματοπιστωτικά ιδρύματα, υλικές ζημίες, απώλεια εργασίας, κλήτευση, επιδείνωση της υγείας κ.λπ.)
Πολύ υψηλό	Άτομα που μπορεί να αντιμετωπίσουν σημαντικές ή και μη αναστρέψιμες συνέπειες, τις οποίες δεν μπορούν να ξεπεράσουν (ανικανότητα εργασίας, μακροχρόνιες ψυχολογικές ή σωματικές παθήσεις, θάνατος κ.λπ.).

Πίνακας 5: Επίπεδο Αντικτύπου

Η Garante σημειώνει τέσσερις κύριους τομείς αξιολόγησης όσον αφορά την ασφάλεια των δεδομένων, δηλαδή:

1. Δίκτυο και τεχνικοί πόροι (εξοπλισμός υλικού και λογισμικό)
2. Διαδικασίες/διαδικασίες που σχετίζονται με τη λειτουργία επεξεργασίας δεδομένων
3. Διάφορα μέρη και άτομα που εμπλέκονται στη διαδικασία επεξεργασίας
4. Επιχειρηματικός τομέας και κλίμακα της επεξεργασίας

Για κάθε τομέα αξιολόγησης, διατυπώνονται πέντε ερωτήσεις, η θετική απάντηση στις οποίες υποδηλώνει κίνδυνο, όπως παρατίθεται στον πίνακα που ακολουθεί. Ωστόσο, θα πρέπει να επαναληφθεί ότι οι «κίνδυνοι για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» δεν απορρέουν μόνο από παραβιάσεις δεδομένων. Ο ίδιος ο ΓΚΠΔ ορίζει στο άρθρο 35 παράγραφος 1 ότι «υψηλοί κίνδυνοι» αυτού του είδους μπορούν να προέρχονται από:

- συστηματική και εκτεταμένη αξιολόγηση προσωπικών πτυχών που αφορούν φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα που αφορούν το φυσικό πρόσωπο ή επηρεάζουν ομοίως σημαντικά το φυσικό πρόσωπο,
- την επεξεργασία σε μεγάλη κλίμακα 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,
- συστηματική παρακολούθηση ενός προσβάσιμου στο κοινό χώρου σε μεγάλη κλίμακα.

Σε αυτές τις περιπτώσεις, ακριβώς επειδή οι εν λόγω πράξεις επεξεργασίας ενέχουν εγγενώς υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των ατόμων, απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων (και σε ορισμένες περιπτώσεις πρέπει να ζητείται η γνώμη της οικείας ΑΠΔΠΧ ή των οικείων ΑΠΔΠΧ, όπως σημειώνεται στη συνέχεια).

6. Συμπεράσματα

Οι εκτιμήσεις αντικτύπου σχετικά με την προστασία των δεδομένων (DPIA), οι οποίες υποχρεούνται από τον Γενικό Κανονισμό της ΕΕ για την Προστασία Δεδομένων (GDPR), αποτελούν σημαντικό μέρος της διασφάλισης της λογοδοσίας και της υπευθυνότητας της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθώς και του εντοπισμού και της ελαχιστοποίησης των επιβλαβών επιπτώσεων στα άτομα όσον αφορά τα θεμελιώδη δικαιώματά τους.

Η ανάλυση εντόπισε βήματα στα οποία παρέχεται καθοδήγηση από τις περισσότερες μεθόδους, όπως η ανάλυση των ορίων, ο προσδιορισμός των κινδύνων και η προετοιμασία της έκθεσης DPIA, ωστόσο, εντοπίστηκαν επίσης διαφορετικές προσεγγίσεις στις κατευθυντήριες γραμμές, συμπεριλαμβανομένου του προσδιορισμού των κινδύνων. Αναλύοντας λοιπόν τις διαθέσιμες μεθόδους εντοπίσαμε πρακτικές που διαδραματίζουν σημαντικό ρόλο για την επιτυχία των έργων PIA, όπως για παράδειγμα, η διερεύνηση των κινδύνων προστασίας της ιδιωτικής ζωής από την οπτική γωνία του οργανισμού όπου συμβάλλει σε μια ολιστική θεώρηση των κινδύνων που προκαλούνται και προκαλεί μια πιο επιμελή προσπάθεια για την αντιμετώπιση ή την πρόληψη των κινδύνων προστασίας της ιδιωτικής ζωής. Επίσης, θα πρέπει να υποστηριχθεί η εξάλειψη των κινδύνων προστασίας της ιδιωτικής ζωής αντί της αντιμετώπισής τους, με επανεξέταση της διαδικασίας δεδομένων και απόφαση να μην επεξεργάζονται ορισμένα στοιχεία δεδομένων, εάν δεν είναι κρίσιμα για τον επιθυμητό σκοπό προκειμένου να επιτευχθεί η προστασία της ιδιωτικής ζωής κατά το σχεδιασμό. Για το λόγο αυτό, οι μέθοδοι DPIA θα πρέπει να προτείνουν άμεσα την επανεξέταση του καταλόγου των εμπλεκόμενων προσωπικών δεδομένων σε κάθε κύκλο μετριασμού των κινδύνων. Τέλος, η εξάρτηση από συγκεκριμένα νομικά πλαίσια είναι επίσης άμεση στη φάση εντοπισμού κινδύνων πολλών μεθόδων, οι οποίες παρέχουν υποστηρικτικά ερωτηματολόγια ή παραδείγματα κινδύνων με βάση τους νόμους περί προστασίας δεδομένων. Τέτοιες οδηγίες, αν και βοηθούν τους επαγγελματίες της DPIA, θα πρέπει να χρησιμοποιούνται κριτικά, καθώς περιορίζουν την εφαρμοσιμότητα των μεθόδων DPIA σε διαφορετικές δικαιοδοσίες και ενέχουν τον κίνδυνο να περιοριστεί το πεδίο εφαρμογής της DPIA στην προστασία των δεδομένων, παραμελώντας έτσι τις επιπτώσεις μιας διαδικασίας σε άλλες πτυχές της καθημερινής ζωής του ατόμου (από απειλές για την προστασία της ιδιωτικής ζωής, όπως η επιτήρηση και η παρέμβαση σε αποφάσεις).

7. Πίνακας Ορολογιών

Ξενόγλωσσος όρος	Ελληνικός Όρος
DPIA [Data Protection Impact Assessment]	ΕΑΠΔ [Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων]
PIA [Privacy Impact Assessment]	Εκτίμηση επιπτώσεων στην ιδιωτική ζωή
GDPR [General Data Protection Regulation Data Protection Conference]	ΓΚΠΔ [Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού Χαρακτήρα]
DPO	Υπεύθυνος Προστασίας Δεδομένων [ΥΠΔ]
PII [Personal Identifiable Information]	Πληροφορίες Αναγνωσιμότητας Φυσικού προσώπου
Privacy risk	Αντιμετώπιση της επικινδυνότητας ιδιωτικότητας
Privacy by design	Ιδιωτικότητα από τον σχεδιασμό
Controllers	Υπεύθυνοι Επεξεργασίας
Profiling	Κατάρτιση προφίλ
Data Processor	Εκτελών την επεξεργασία
Project Manager	Διαχειριστής έργου
Project Steering Committee	Συντονιστική επιτροπή έργου
Information Security (IS)	Ασφάλεια Πληροφοριών
Checklists	Κατάλογοι Ελέγχου
Stakeholders	Ενδιαφερόμενα μέρη
Screening questions	Ερωτήσεις διαλογής
Objective	Στόχος

Input	Είσοδος
Expected output	Προσδοκώμενο αποτέλεσμα
Actions	Ενέργειες
Risk sources	Πηγές κινδύνου
Risk evaluation	Αξιολόγηση κινδύνου
Risk treatment plan	Σχέδιο αντιμετώπισης κινδύνου
IoT	Διαδικτύου των πραγμάτων
Threshold assessment	Αξιολόγηση κατωφλίου
Risk identification	Προσδιορισμός κινδύνων
Risk Treatment Controls	Έλεγχοι αντιμετώπισης κινδύνων
External stakeholders	Εξωτερικοί ενδιαφερόμενοι
Threat	Απειλή
Feared event	Επίφοβο γεγονός
Supporting asset	Υποστηρικτικό περιουσιακό στοιχείο
Severity	Σοβαρότητα
Likelihood	Πιθανότητα
Risk	Κίνδυνος
Control	Έλεγχος
Metadata	Μεταδεδομένα

8. Συντμήσεις – Αρκτικόλεξα – Ακρωνύμια

ΑΠΔΠΧ	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
ΥΠΔ	Υπεύθυνος Προστασίας Δεδομένων
EDPB	Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων
ΕΕ	Ευρωπαϊκή Ένωση
CNIL	Γαλλική Αρχή Προστασίας Δεδομένων
OAIC	Γραφείο του Επιτρόπου Πληροφοριών της Αυστραλίας

9. Παράρτημα Ι

Υποκείμενα των δεδομένων (Data subject)	Πρόσωπα στα οποία αναφέρονται τα δεδομένα που καλύπτονται από την επεξεργασία.
Υπεύθυνος επεξεργασίας δεδομένων (Data controller)	Το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, ο οργανισμός ή άλλος φορέας που καθορίζει, μόνος ή από κοινού με άλλους, τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, όταν οι σκοποί και τα μέσα της εν λόγω επεξεργασίας καθορίζονται από το δίκαιο της Ένωσης ή του κράτους μέλους.
Προσωπικά δεδομένα (Personal Data)	Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο, «υποκείμενο των δεδομένων», ως «ταυτοποιήσιμο φυσικό πρόσωπο» νοείται εκείνο που μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα, ιδίως με αναφορά σε αναγνωριστικό στοιχείο όπως όνομα, αριθμό ταυτότητας, δεδομένα θέσης, ηλεκτρονικό αναγνωριστικό σε έναν ή και περισσότερους παράγοντες που σχετίζονται με τη φυσική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.
Έλεγχος (Control)	Ενέργειες που πρέπει να πραγματοποιηθούν.
Επεξεργασία δεδομένων προσωπικού χαρακτήρα (Personal Data Processing)	Κάθε πράξη ή σύνολο πράξεων που εκτελείται σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, είτε με αυτοματοποιημένα μέσα είτε όχι, όπως η συλλογή, η καταχώριση, η οργάνωση, η διαμόρφωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση, η διαβούλευση, η χρήση, η κοινοποίηση με διαβίβαση, η διάδοση ή η με άλλο τρόπο διάθεση, η ευθυγράμμιση ή ο συνδυασμός, ο περιορισμός και η διαγραφή ή η καταστροφή.
Κίνδυνος (Risk)	Σενάριο που περιγράφει ένα επίφοβο συμβάν σε συνδυασμό με όλες τις απειλές που το καθιστούν πιθανό. Εκτιμάται ως προς την σοβαρότητα και την πιθανότητα.
Πιθανότητα (Likelihood)	Εκτίμηση της πιθανότητας εμφάνισης ενός κινδύνου. Εξαρτάται από το επίπεδο των εκμεταλλεύσιμων ευπαθειών και το επίπεδο των δυνατοτήτων των πηγών κινδύνου να τις εκμεταλλευτούν.

Πηγή κινδύνου (Risk source)	Φυσικό πρόσωπο ή μη ανθρώπινη πηγή που μπορεί να προκαλέσει κίνδυνο. Η πηγή αυτή δύναται να ενεργεί σκόπιμα ή τυχαία.
Σοβαρότητα (Severity)	Εκτίμηση του μεγέθους των πιθανών επιπτώσεων στην ιδιωτική ζωή των υποκειμένων των δεδομένων. Κατά κύριο λόγο εξαρτάται από τον επιζήμιο χαρακτήρα των πιθανών επιπτώσεων.
Επίφοβο γεγονός (Feared event)	Πιθανή παραβίαση δεδομένων που ενδέχεται να έχει επιπτώσεις στην ιδιωτική ζωή των υποκειμένων των δεδομένων.
Υποστηρικτικό περιουσιακό στοιχείο (Supporting asset)	Το στοιχείο στο οποίο στηρίζονται τα προσωπικά δεδομένα. Αυτό μπορεί να είναι υλικό, λογισμικό, δίκτυα, άνθρωποι κ.α.
Απειλή (Threat)	Διαδικασία που περιλαμβάνει μία ή περισσότερες μεμονωμένες ενέργειες σε στοιχεία που υποστηρίζουν δεδομένα.

10. Βιβλιογραφικές Αναφορές

[1] S. Gkritzalis, *Guidelines for Privacy Impact Assessment ISO 29134:2017.*

[2] D. P. Commission, *Guide to Data Protection Impact Assessments (DPIAs),* 2019.

[3] D. K. E. P. o. I. Law, "GDPR requirements on Data Protection Impact Assessments & methodologies for DPIAs," 2020.

[4] A. 2. D. P. W. PARTY, "Opinion 2/2017 on data processing at work," 2017.

[5] "GDPR.EU," [Online]. Available: https://gdpr.eu/article-35-impact-assessment/. [Accessed Οκτώβριος 2022].

[6] K. M. &. V. M., *An Evaluation Framework for Privacy Impact Assessment Methods,* 2018.

[7] PDPC, *Guide to Data Protection Impact Assessment,* 2021.

[8] G. D. P. R. (GDPR), "Art. 84 GDPR Penalties," 2022. [Online]. Available: https://gdpr.eu/article-84-member-state-penalties/.

[9] A. G. I. Group, "Evolvetrust," 2019. [Online]. Available: https://www.evolvetrust.org/downloads/gdpr/hub/concise_guide_dpias_sep_19__1_.pdf. [Accessed Δεκέμβριος 2022].

[10] ICO, *Sample DPIA Template.*

[11] A. 2. D. P. W. PARTY, "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," 2017.

[12] R. Clarke, "An Evaluation of Privacy Impact Assessment Guidance Documents.” International Data Privacy Law," 2011.

[13] M. &. Heisel, "Supporting privacy impact assessments using problem-based privacy analysis," in *International Conference on Software Technologies*, 2017.

[14] Anonymous, 2014. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/DPIA%20template_incl%20line%20numbers.pdf. [Accessed 2022].

[15] Métayer, "A Refinement Approach for the Reuse of Privacy Risk Analysis Results," *Annual Privacy Forum,* pp. 52-83, 2017.

[16] "Official Journal of the European Union," 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. [Accessed Δεκέμβριος 2022].

[17] "Art. 24 GDPR Responsibility of the controller," [Online]. Available: https://gdpr.eu/article-24-responsibility-of-the-data-controller/.

[18] E. Commission, "Assessment of the EU Member States' rules on health data in the light of GDPR," 2021.

[19] "iapp.org," 2018. [Online]. Available: https://iapp.org/news/a/uk-ico-publishes-updated-pia-guidance/. [Accessed Οκτώβριος].

[20] Anonymous, "L' OBS," [Online]. Available: https://www.nouvelobs.com/societe/20130613.OBS3162/les-mormons-autorises-par-la-cnil-a-numeriser-l-etat-civil-francais.html . [Accessed Νοέμβριος 2022].

[21] E. D. P. S. [EDPS], "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation," 2019.

[22] S. Spiekermann, "The RFID PIA–developed by industry, endorsed by regulators. "Privacy impact assessment, Springer Netherlands, 323-346., (2012).

[23] H. J. Pandit, "A Semantic Specification for Data Protection Impact Assessments (DPIA)," 2022.

[24] "ANSSI," [Online]. Available: https://www.ssi.gouv.fr/en/guide/ebios-risk-manager-the-method/. [Accessed Νοέμβριος 2022].

[25] CNIL, 2018. [Online]. Available: https://www.cnil.fr/en/privacy-impact-assessments-cnil-publishes-its-pia-manual. [Accessed Οκτώβριος 2022].

[26] CNIL, 2017. [Online]. Available: https://www.cnil.fr/en/guidelines-dpia.

[27] "CNIL," 30 June 2021. [Online]. Available: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment.

[28] "Observatory of Public Sector Innovation," 2020. [Online]. Available: https://oecd-opsi.org/innovations/pia-tool/.

[29] "Information Commissioner's Office," [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/. [Accessed Δεκέμβριος 2022].

[30] I. C. Office, 2018. [Ηλεκτρονικό]. Available: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.

[31] ICO, "Examples of processing 'likely to result in high risk'," 2019.

[32] «ICO,» 14 October 2022 . [Ηλεκτρονικό]. Available: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf.

[33] ICO, "Data protection impact assessments," https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/.

[34] I. O. f. S. (ISO), *Information technology — Security techniques — Guidelines for privacy impact assessment,* 2017.

[35] O. o. t. A. I. C. (OAIC), "10 steps to undertaking a privacy impact assessment (PIA)," 2021.

[36] EDPS, 2020. [Online]. Available: https://edps.europa.eu/sites/edp/files/publication/20-08-19-informal_consultation_on_dpias_en_0.pdf. [Accessed Νοέμβριος 2022].

[37] H. D. P. Authority, "DPA," [Online]. Available: https://www.dpa.gr/sites/default/files/2019-10/article_35_dpia_list_gr_2.pdf. [Accessed Δεκέμβριος 2022].

[38] "The Journal of the Government of the Hellenic Republic," 2019. [Online]. Available: https://tzellis.gr/gdpr/pia/FEK-B-1622-2019.pdf. [Accessed Οκτώβριος 2022].

[39] G. t. u. p. impact, "Australian Goverment," 2021. [Online]. Available: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments#ftn1. [Accessed Δεκέμβριος 2022].

[40] Anonymous, "Chapter B: Key concepts," 2019. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts.

[41] Anonymous, 2019. [Online]. Available: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information. [Accessed Δεκέμβριος 2022].

[42] OAIC, "Privacy impact assessment tool," 2021. [Online]. Available: https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-impact-assessment-tool. [Accessed Οκτώβριος 2022].

[43] Anonymous, "Australian Goverment," [Online]. Available: https://www.oaic.gov.au/privacy/privacy-impact-assessments. [Accessed Δεκέμβριος 2022].