ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
Πρόγραμμα Μεταπτυχιακών Σπουδών
«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»
Ακαδημαϊκό έτος 2021-2022

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
Του ΚΑΡΑΔΗΜΑ ΜΙΧΑΗΛ (Α.Μ.: ΜΔΙ2017)

"ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ,ΕΝΑ ΠΡΑΚΤΙΚΟ ΕΡΓΑΛΕΙΟ ΤΟΥ ΓΚΠΔ"

Επιβλέπων:
Καθηγητής Στέφανος Γκρίτζαλης

Πειραιάς, Ιούνιος 2022

Περιεχόμενα

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον επιβλέπων καθηγητή της παρούσας εργασίας κ.Στέφανο Γκρίτζαλη του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου 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.

ΠΕΡΙΓΡΑΦΗ

Η παρούσα εργασία έχει ως θέμα την Εκτίμηση Αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) την οποία σύστησε το άρθρο 35 του Γενικού Κανονισμού Προστασίας Δεδομένων και η διενέργεια της κρίνεται υποχρεωτική για τις δραστηριότητες επεξεργασίας που ενδέχεται να παρουσιάσουν υψηλό κίνδυνο στα δικαιώματα και την ελευθερία των υποκειμένων των δεδομένων.

Σε αυτήν την εργασία θα παρουσιαστεί η εκτίμηση αντικτύπου όπως αναφέρεται στον κανονισμό καθώς και οι προϋποθέσεις που καθιστούν υποχρεωτική την εκτέλεση της.

Στην συνέχεια θα παρουσιαστούν τα θετικά αποτελέσματα που έχει η διενέργεια της εκτίμησης αντικτύπου για τον οργανισμό. Έπειτα, θα γίνει αναφορά στο πεδίο εφαρμογής της εκτίμησης αντικτύπου.

Θα αναλυθεί μετά ο τρόπος με τον οποίο πραγματοποιείται η εκτίμηση αντικτύπου με όλα τα επιμέρους στάδια της και με όλους τους εμπλεκόμενους σύμφωνα με τα διεθνή πρότυπα και τις κυριότερες μεθοδολογίες όπως αυτών του Διεθνή Οργανισμού Τυποποίησης (ISO) και της Γαλλικής Αρχής Προστασίας Δεδομένων Προσωπικού χαρακτήρα(CNIL) .

Τέλος θα αναφερθεί ο τρόπος με τον οποίο δημιουργείται η αναφορά και επικυρώνεται η εκτίμηση αντικτύπου.

1. ΕΙΣΑΓΩΓΗ

Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ - Data Protection Impact Assessment - DPIA) είναι ένα εργαλείο ή αλλιώς μια διαδικασία για να εκτιμηθούν τα πιθανά αποτελέσματα που μπορεί να έχει πάνω στα δεδομένα προσωπικού χαρακτήρα[1] ένα πρόγραμμα, ένα πληροφοριακό σύστημα, ένα είδος λογισμικού ή κάποια άλλη συσκευή που μπορεί να επεξεργάζεται τα δεδομένα αυτά.Μέσω αυτής της διαδικασίας, γίνεται περιγραφή της επεξεργασίας των δεδομένων, εκτιμάται η αναγκαιότητα και η αναλογικότητα της επεξεργασίας αυτής ώστε να διαχειριστεί την επικινδυνότητα στα δικαιώματα των προσώπων όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων. Τελικός σκοπός της εκτίμησης αντικτύπου ,είναι να ληφθούν τα κατάλληλα μέτρα, έπειτα από διαβούλευση των ενδιαφερομένων μερών, για την μείωση του κινδύνου των προσωπικών δεδομένων.

Η DPIA είναι μια διαδικασία η οποία ξεκινάει όσο τον δυνατό νωρίτερα στην ανάπτυξη ενός προγράμματος, συστήματος ή λογισμικού καθώς υπάρχει η δυνατότητα να διαμορφώσει το αποτέλεσμα και να εξασφαλίσει έτσι την προστασία δεδομένων από τον σχεδιασμό(Privacy by Design[2]).Μια σωστή εκτίμηση αντικτύπου επιδιώκει την εμπλοκή των ενδιαφερομένων μερών από την αρχή προκειμένου να συλλέξει απόψεις και ιδέες για το πως να αποφευχθεί ή να μειωθεί το αντίκτυπο στην ιδιωτικότητα των ατόμων.

Επιπλέον η DPIA αποτελεί ένα εργαλείο λογοδοσίας, διότι βοηθάει τους υπευθύνους επεξεργασίας όχι μόνο να συμμορφώνονται με τους κανονισμούς του Γενικού Κανονισμού Προστασίας Δεδομένων, αλλά και να αποδεικνύουν ότι έχουν λάβει απαραίτητα και επαρκή μέτρα για την διασφάλιση της συμμόρφωσης με τον κανονισμό. Αλλιώς η DPIA είναι μια μέθοδος διαπίστωσης και απόδειξης συμμόρφωσης.

---

[1] Στην παρούσα εργασία τα δεδομένα προσωπικού χαρακτήρα αναφέρονται και ως ''προσωπικά δεδομένα''.

[2] Η ιδέα του privacy by design αναπτύχθηκε και τεκμηριώθηκε από την Δρ. Ann Cavoukian στα μέσα της δεκαετίας του 1990 < Office of the Victorian Information Commissioner. Privacy by Design: Effective Privacy Management in the Victorian public sector , Cavoukian, A> . Η προστασία των δεδομένων από τον σχεδιασμό υπάρχει και στον Γενικό Κανονισμό Προστασίας Δεδομένων 'Αρθρο 25

2.Η ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΓΚΠΔ ΚΑΙ ΠΟΤΕ ΕΙΝΑΙ ΥΠΟΧΡΕΩΤΙΚΗ Η ΕΚΤΕΛΕΣΗ ΤΗΣ

Ο κανονισμός 2016/679 [3](ΓΚΠΔ/GDPR) ισχύει από τις 25 Μαΐου του 2018.Στο άρθρο 35 του ΓΚΠΔ όπως και στο άρθρο 27 της οδηγίας 2016/680[4] συστήνεται η έννοια της DPIA δηλαδή της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων.

Όπως είπαμε, η DPIA είναι μια διαδικασία με την οποία μπορεί να αποδείξει ένας οργανισμός ότι συμμορφώνεται με τον νόμο. Το γεγονός ότι δεν πληρούνται τα κριτήρια που καθιστούν υποχρεωτική την εκτέλεση DPIA ,δεν αναιρεί τη γενική υποχρέωση των υπευθύνων επεξεργασίας να εφαρμόζουν μέτρα για την αποτελεσματική διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Στην πραγματικότητα, αυτό σημαίνει ότι οι υπεύθυνοι επεξεργασίας πρέπει να εξετάζουν διαρκώς τους κινδύνους που ενέχουν οι πράξεις επεξεργασίας τους, προκειμένου να προσδιορίζουν πότε μια συγκεκριμένη μορφή επεξεργασίας "ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων".

Η μη συμμόρφωση με τους κανονισμούς DPIA μπορεί να έχει ως αποτέλεσμα την επιβολή προστίμων από την αρμόδια εποπτική αρχή σύμφωνα με τον ΓΚΠΔ. Η μη εκτέλεση DPIA, όταν η επεξεργασία θεωρείται ότι είναι υψηλού κινδύνου και πρέπει να υπόκειται σε DPIA, (άρθρο 35 παράγραφοι 1 και 3 έως 4), η εσφαλμένη διενέργεια DPIA(άρθρο 35 παράγραφοι 2 και 7 έως 9) ή η μη διενέργεια DPIA (άρθρο 35 παράγραφοι 2 και 7 έως 9 ή η παράλειψη διαβούλευσης με την αρμόδια εποπτική αρχή όταν είναι απαραίτητο (άρθρο 36 παράγραφος 3 στοιχείο ε)) μπορεί να έχει ως αποτέλεσμα την επιβολή κυρώσεων όπως διοικητικές κυρώσεις ύψους έως και 10 εκατομμυρίων ευρώ ή, στην περίπτωση εταιρείας, έως και 2% των συνολικών εσόδων όποιο από τα δύο είναι υψηλότερο, του συνολικού ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους.

Η εκτέλεση της DPIA δεν είναι απαραίτητη για κάθε είδος επεξεργασίας. Όπως είπαμε, η εκτίμηση αντικτύπου είναι υποχρεωτική όταν η επεξεργασία ‘’ενδέχεται να επιφέρει

---

[3] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (γνωστός και ως ΓΚΠΔ) Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679&from=EL

[4] Οδηγία (ΕΕ) 2016/680 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EN

υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων''(Άρθρο 35 Παρ.1 ΓΚΠΔ). Πρέπει να δοθεί μεγάλη προσοχή στην έννοια του κινδύνου και στο τι σημαίνει αυτή στο πλαίσιο της ασφάλειας των δεδομένων, διότι ο κίνδυνος είναι ένας σημαντικός παράγοντας που χρησιμοποιούν οι υπεύθυνοι επεξεργασίας δεδομένων για την κλιμάκωση και την προσαρμογή των μέτρων στις εκάστοτε συνθήκες επεξεργασίας δεδομένων.[5]

Ο κίνδυνος στην προστασία των δεδομένων θα πρέπει να εξετάζεται στο πλαίσιο των "δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων", καθώς και να "ενσωματώνεται μεθοδολογικά στα μέσα διαχείρισης κινδύνου". [6]Ως εκ τούτου, είναι κρίσιμο να έχει κανείς σαφή αντίληψη του τι συνιστά κίνδυνο σύμφωνα με το βασικό νομοθετικό πλαίσιο της Ευρωπαϊκής Ένωσης για την προστασία των δεδομένων. Σύμφωνα με την Ομάδα 29 "Ο κίνδυνος είναι ένα σενάριο που περιγράφει ένα γεγονός και τις συνέπειές του, που εκτιμάται σε όρους σοβαρότητας(severity) και πιθανότητας(likelihood)".[7] Το γεγονός ότι θα πρέπει να λαμβάνονται υπόψη τόσο η πιθανότητα όσο και η σοβαρότητα επίσης αναφέρεται στις αιτιολογικές σκέψεις 75 και 76 του ΓΚΠΔ.[8] Για να καταλήξει ο υπεύθυνος επεξεργασίας δεδομένων στο συμπέρασμα ότι κάτι μπορεί να αποτελεί κίνδυνο (υψηλό ή χαμηλό), πρέπει πρώτα να προσδιορίσει αν και πόσο σοβαρός θα είναι ο κίνδυνος, καθώς και αν και πόσο πιθανό είναι να συμβεί αυτό το γεγονός. Εάν ο υπεύθυνος επεξεργασίας δεδομένων διαπιστώσει ότι είναι πιθανό να προκύψει υψηλός κίνδυνος ως αποτέλεσμα αυτής της αξιολόγησης, ο υπεύθυνος επεξεργασίας δεδομένων υποχρεούται να διενεργήσει DPIA με στόχο τη μείωση του υψηλού κινδύνου που εντοπίστηκε. Άρα μεγάλη σημασία πρέπει να δοθεί και στο πως γίνεται μέτρηση της σοβαρότητας και της πιθανότητας να συμβεί ο κίνδυνος.[9]

---

[5] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ- Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248(2017)

[6] van Dijk, N., Gellert, R. and Rommetveit, K. 'A Risk to a Right: Beyond Data Protection Risk Assessments' (2016) Volume 32, Issue 2

[7] Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' Διαθέσιμο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Πρόσβαση 30-11-2021]

[8] Αιτιολογική σκέψη 75: '' Οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ποικίλης πιθανότητας και σοβαρότητας, είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα […] Αιτιολογική σκέψη 76 Η πιθανότητα και η σοβαρότητα του κινδύνου για τα δικαιώματα και τις ελευθερίες του υποκειμένου των δεδομένων θα πρέπει να καθορίζονται σε συνάρτηση με τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας. Ο κίνδυνος θα πρέπει να αξιολογείται βάσει αντικειμενικής εκτίμησης, με την οποία διαπιστώνεται κατά πόσον οι πράξεις επεξεργασίας δεδομένων συνεπάγονται κίνδυνο ή υψηλό κίνδυνο''

[9] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ- Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248(2017)

Η αξιολόγηση πρέπει να είναι αντικειμενική, σύμφωνα με τον νομοθέτη. Όταν οι υπεύθυνοι επεξεργασίας δεδομένων αξιολογούν υποθετικούς κινδύνους, την πιθανότητα και τη σοβαρότητά τους, είναι κρίσιμο να κατανοήσουν τι είναι η "αντικειμενική αξιολόγηση" και πώς μπορεί να επιτευχθεί η αντικειμενικότητα. Οι εκτιμήσεις κινδύνου πρέπει να διενεργούνται από τους υπεύθυνους επεξεργασίας δεδομένων με τέτοιο τρόπο ώστε τα συμπεράσματα στα οποία καταλήγουν να είναι αξιόπιστα, επαληθεύσιμα, και αμφισβητήσιμα.[10] Για αυτό χρειάζονται άτομα που είναι ειδικοί στον χώρο για να τις εκτελέσουν αυτές τις εκτιμήσεις.

Παρακάτω θα παρουσιάσουμε κάποιες οδηγίες για το πότε η επεξεργασία θεωρείται υψηλού κινδύνου.

Το άρθρο 35 παράγραφος 3 του ΓΚΠΔ δίνει κάποια παραδείγματα για το ποιο είδος επεξεργασίας ''ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων''. Αυτά είναι

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

Υπάρχουν βέβαια και είδη επεξεργασίας τα οποία δεν περιλαμβάνονται στα παραπάνω αλλά μπορεί να επιφέρουν μεγάλο κίνδυνο, και θα πρέπει να εκτελούνται εκτιμήσεις αντικτύπου και για αυτά τα είδη. Η ομάδα 29 προσθέτει στα παραπάνω που αναφέρει ο ΓΚΠΔ τα εξής κριτήρια[11]:

1. Αξιολόγηση ή βαθμολόγηση, περιλαμβανομένης της κατάρτισης προφίλ και της πρόβλεψης, με βάση "πτυχές που σχετίζονται με την εργασιακή απόδοση του υποκειμένου των δεδομένων, την οικονομική κατάσταση,

[10] Katerina Demetzou – Data Protection Impact Assessment:A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation – Elsevier (2019)

[11] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ- Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248(2017)

την υγεία, τις προσωπικές προτιμήσεις ή τα ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, την τοποθεσία ή τις μετακινήσεις" (αιτιολογικές σκέψεις 71 και 91).[12]΄Ένα παράδειγμα θα ήταν ένας κρατικός φορέας να χρησιμοποιεί συστήματα τεχνητής νοημόσυνης για να κρίνει εγκληματίες.[13]

2. Λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο: επεξεργασία που αποσκοπεί στη λήψη αποφάσεων που αφορούν υποκείμενα δεδομένων και παράγουν «έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο» ή που «ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο» [άρθρο 35 παράγραφος 3 στοιχείο α)].[14]
3. Συστηματική παρακολούθηση: επεξεργασία για την παρατήρηση, την παρακολούθηση ή τον έλεγχο των υποκειμένων των δεδομένων, περιλαμβανομένων των δεδομένων που συλλέγονται μέσω δικτύων ή «συστηματική παρακολούθηση δημοσίως προσβάσιμου χώρου» [άρθρο 35 παράγραφος 3 στοιχείο γ)].
4. Ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα: σε αυτά περιλαμβάνονται ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως ορίζονται στο άρθρο 9 (για παράδειγμα, πληροφορίες για τα πολιτικά φρονήματα φυσικών προσώπων), καθώς και δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες ή αδικήματα, όπως ορίζονται στο άρθρο 10.
5. Δεδομένα μεγάλης κλίμακας επεξεργασίας: ο ΓΚΠΔ δεν ορίζει τι συνιστά μεγάλης κλίμακας επεξεργασία, ωστόσο η αιτιολογική σκέψη 91 παρέχει ορισμένες κατευθύνσεις. Σε κάθε περίπτωση, η ομάδα εργασίας του άρθρου 29 συνιστά να λαμβάνονται συγκεκριμένα υπόψη οι ακόλουθες παράμετροι κατά τον προσδιορισμό του κατά πόσον η επεξεργασία τελείται σε μεγάλη κλίμακα:

---

[12] Αιτιολογική Σκέψη 71 ΓΚΠΔ ‘’Το υποκείμενο των δεδομένων θα πρέπει… ειδικές προϋποθέσεις ‘’ και Αιτιολογική Σκέψη 91 ΓΚΠΔ ‘’Αυτό θα πρέπει…να έιναι υποχρεωτική’’

[13] ‘’Χρήση του προγράμματος COMPAS στην Αμερική που είναι ένα εργαλείο διαχείρισης υποθέσεων και υποστήριξης αποφάσεων και χρησιμοποιείται από τα δικαστήρια των ΗΠΑ για την αξιολόγηση της πιθανότητας ένας κατηγορούμενος να υποτροπιάσει.’’ – Βικιπαίδεια Διαθέσιμο: https://en.wikipedia.org/wiki/COMPAS_(software) [Πρόσβαση 22-10-21]/ Sam Corbett-Davies, Emma Pierson, Avi Feller and Sharad Goel (2016)- A computer program used for bail and sentencing decisions was labeled biased against blacks. It’s actually not that clear. – The Washington post Διαθέσιμο:
https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/ [Πρόσβαση 22-10-21]

[14] ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ- Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248(2017)

α. ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων, είτε ως συγκεκριμένος αριθμός είτε ως ποσοστό επί του συναφούς πληθυσμού.
β. ο όγκος των δεδομένων και/ή το εύρος των διαφόρων στοιχείων δεδομένων που υποβάλλονται σε επεξεργασία.
γ. η διάρκεια ή ο μόνιμος χαρακτήρας της δραστηριότητας επεξεργασίας δεδομένων
δ. δ. το γεωγραφικό εύρος της δραστηριότητας επεξεργασίας.

6. Η αντιστοίχιση ή ο συνδυασμός συνόλων δεδομένων που απορρέουν, για παράδειγμα, από δύο ή περισσότερες πράξεις επεξεργασίας δεδομένων που υλοποιούνται για διαφορετικούς σκοπούς και/ή από διαφορετικούς υπεύθυνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων
7. Δεδομένα που αφορούν ευάλωτα υποκείμενα δεδομένων (αιτιολογική σκέψη 75): η επεξεργασία του εν λόγω τύπου δεδομένων αποτελεί κριτήριο λόγω της αυξημένα άνισης σχέσης ισχύος μεταξύ των υποκειμένων των δεδομένων και του υπεύθυνου επεξεργασίας, με την έννοια ότι τα φυσικά πρόσωπα ενδέχεται να μην είναι σε θέση να συναινέσουν ή να εναντιωθούν με ευκολία στην επεξεργασία των δεδομένων τους ή να ασκήσουν τα δικαιώματά τους. Στα ευάλωτα υποκείμενα δεδομένων ενδέχεται να περιλαμβάνονται παιδιά (τα οποία μπορεί να θεωρηθεί ότι δεν είναι σε θέση να εναντιωθούν ή να συναινέσουν μετά λόγου γνώσης ή συνειδητά στην επεξεργασία των δεδομένων τους), εργαζόμενοι, πιο ευάλωτα τμήματα του πληθυσμού που χρήζουν ειδικής προστασίας (ψυχικά νοσούντες, αιτούντες άσυλο ή ηλικιωμένοι, ασθενείς κ.ο.κ.), και σε κάθε περίπτωση που εξακριβώνεται άνιση σχέση μεταξύ της θέσης του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας.
8. Καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων, όπως η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης κ.ο.κ. Ο ΓΚΠΔ καθιστά σαφές (άρθρο 35 παράγραφος 1 και αιτιολογικές σκέψεις 89 και 91) ότι η χρήση νέων τεχνολογιών, που ορίζονται «σύμφωνα με τα υφιστάμενα επίπεδα τεχνολογικής γνώσης» (αιτιολογική σκέψη 91), μπορεί να καταστήσει αναγκαία τη διενέργεια ΕΑΠΔ. Και τούτο διότι η χρήση μιας τέτοιας τεχνολογίας μπορεί να περιλαμβάνει νέες μορφές συλλογής και χρήσης δεδομένων, πιθανώς με υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Πράγματι, οι προσωπικές και κοινωνικές επιπτώσεις από τη χρήση μιας νέας τεχνολογίας ενδέχεται να είναι άγνωστες. Η διενέργεια ΕΑΠΔ θα βοηθήσει τον υπεύθυνο επεξεργασίας να κατανοήσει και να αντιμετωπίσει τους εν λόγω κινδύνους. Για παράδειγμα, συγκεκριμένες εφαρμογές του «διαδικτύου των πραγμάτων» θα μπορούσαν να έχουν

σημαντικό αντίκτυπο στην καθημερινή ζωή και την ιδιωτική ζωή των φυσικών προσώπων· και, ως εκ τούτου, απαιτείται η διενέργεια σχετικής ΕΑΠΔ.

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

Η ομάδα 29 συνιστά στους υπεύθυνους επεξεργασίας να θεωρούν ότι αν μια επεξεργασία πληροί δύο η παραπάνω κριτήρια, αυτή η επεξεργασία απαιτεί και μία εκτίμηση αντικτύπου. Όσα περισσότερα κριτήρια πληρούνται από την εν λόγω επεξεργασία, τόσο πιο μεγάλος κίνδυνος υπάρχει για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.Ακόμα και αν πληρείται μόνο ένα κριτήριο ,ενδέχεται να κριθεί από τον υπεύθυνο επεξεργασίας ότι είναι απαραίτητη η διενέργεια μιας DPIA.

Στις 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.Κάθε εποπτική αρχή , σύμφωνα με το άρθρο 35 παράγραφος 4, καταρτίζει και δημοσιοποιεί έναν κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία απαιτούνται εκτιμήσεις αντικτύπου.Αυτός ο κατάλογος ανακοινώνεται έπειτα στο Ευρωπαικό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ).

Η Ελληνική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) δημιούργησε τον παρακάτω κατάλογο με τις πράξεις επεξεργασίας που υπόκεινται σε απαίτηση DPIA.[15]

Μέσα στον κατάλογο της ΑΠΔΠΧ τα κριτήρια ταξινομούνται σε τρεις κατηγορίες.

- Στην 1η κατηγορία τοποθετούνται οι επεξεργασίες ανάλογα με τα είδη και τους σκοπούς επεξεργασίας τους.
- Στην 2η κατηγορία τοποθετούνται οι επεξεργασίες ανάλογα με το είδος των δεδομένων που επεξεργάζονται και/ή τις κατηγορίες των υποκειμένων των δεδομένων

[15] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - 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 Διαθέσιμο: https://www.dpa.gr/sites/default/files/2019-10/article_35_dpia_list_gr_2.pdf [Πρόσβαση 05-04-2022]

- Στην 3η κατηγορία τοποθετούνται οι επεξεργασίες ανάλογα με κάποια επιπλέον χαρακτηριστικά και/ή τα χρησιμοποιούμενα μέσα/συστήματα της επεξεργασίας.

Σύμφωνα με την ΑΠΔΠΧ , ο υπεύθυνος επεξεργασίας πρέπει να προχωρήσει υποχρεωτικά στην εκτέλεση της DPIA η επεξεργασία πληρεί τουλάχιστον ένα από τα κριτήρια της 1η ή της 2ης κατηγορίας.Ταυτόχρονα υποχρεωτική θεωρείται η εκτέλεση της DPIA αν πληροί η επεξεργασία ένα από τα κριτήρια της 3ης κατηγορίας και ταυτόχρονα αυτή η επεξεργασία συνδέεται με είδη και σκοπούς επεξεργασίας της 1ης κατηγορίας, ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας.

Στην 1η κατηγορία ανήκουν τα εξής κριτήρια:

- Η διενέργεια συστηματικής αξιολόγησης, βαθμολόγησης, πρόβλεψης, πρόγνωσης καθώς και η δημιουργία προφίλ , πτυχών που σχετίζονται με την υγεία, την οικονομική κατάσταση, τα ενδιαφέροντα και τις προσωπικές προτιμήσεις, την γενικότερη συμπεριφορά ή αξιοπιστία, τη θέση ή τις κινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων.
  Παράδειγμα είναι η πρόβλεψη των τοποθεσιών που θα επισκεφτεί ένα υποκείμενο των δεδομένων αφού έχει προηγηθεί η κατάρτιση προφίλ του, σύμφωνα με τις προηγούμενες θέσεις και κινήσεις του.
- Η λήψη αυτοματοποιημένων αποφάσεων που έχει προκύψει από την συστηματική επεξεργασία δεδομένων.Οι αποφάσεις αυτές έπειτα παράγουν έννομα αποτελέσματα που έχουν σχέση με τα υποκείμενα των δεδομένων ή τα επηρεάζουν σημαντικά κατά τρόπο τέτοιο που ενδέχεται να τα οδηγήσουν σε αποκλεισμό η διακρίσεις σε βάρος του φυσικού προσώπου.
  Παράδειγμα είναι ηλεκτρονικές προσλήψεις που έχουν πραγματοποιηθεί χωρίς την παρέμβαση ανθρώπου.[16]
- Η συστηματική επεξεργασία δεδομένων που ενδέχεται να μην επιτρέπει στο υποκείμενο να ασκήσει τα δικαιώματα του ή να έχει πρόσβαση σε μία υπηρεσία ή να μην μπορεί χρησιμοποιήσει μία σύμβαση , ειδικά αν δεδομένα που προέρχονται από τρίτους εμπλέκονται στην παρεμπόδιση αυτή.
  Παράδειγμα είναι όταν μία τράπεζα ελέγχει τους πελάτες και αποφασίζει αν θα τους χορηγήσει δάνειο σύμφωνα με μια βάση δεδομένων που αναλύει την οικονομική κατάσταση των πελατών, ειδικά αν αυτή η βάση έχει ληφθεί από κάποιον τρίτο.
- Μια συστηματική επεξεργασία δεδομένων που έχει σκοπό την προώθηση προϊόντων και υπηρεσιών στα υποκείμενα αφού έχει προηγηθεί η κατάρτιση προφίλ των υποκειμένων και εφόσον έχουν ληφθεί υπόψη δεδομένα που έχουν συλλεχθεί από τρίτους.
- Κριτήριο αποτελεί η συστηματική και σε μεγάλη κλίμακα επεξεργασία όταν τα υποκείμενα παρακολουθούνται, παρατηρούνται ή ελέγχονται σύμφωνα

[16] Αιτιολογική Σκέψη 71 «Σε κάθε περίπτωση, η επεξεργασία αυτή θα πρέπει να υπόκειται σε κατάλληλες εγγυήσεις, οι οποίες θα πρέπει να περιλαμβάνουν ειδική ενημέρωση του υποκειμένου των δεδομένων και το δικαίωμα εξασφάλισης ανθρώπινης παρέμβασης»

με τα δεδομένα που έχουν συλλεχθεί από συστήματα CCTV ή άλλα συστήματα σε κάποιο δημόσιο χώρο , ή κάποιο ιδιωτικό χώρο στον οποίο έχουν πρόσβαση απεριόριστος αριθμός προσώπων(π.χ. εμπορικό κατάστημα).Στην επεξεργασία αυτή περιλαμβάνεται η παρακολούθηση των πιθανών κινήσεων και θέσεων των υποκειμένων που έχουν ταυτοποιηθεί ή όχι σε πραγματικό ή μη χρόνο.

- ‘Άλλο ένα κριτήριο είναι η περίπτωση πράξης συστηματικής επεξεργασίας δεδομένων προσωπικού χαρακτήρα μεγάλης κλίμακας που αφορούν την υγεία και την δημόσια υγεία για σκοπούς δημοσίου συμφέροντος.Παράδειγμα θα μπορούσε να είναι τα συστήματα που αφορούν τα πιστοποιητικά εμβολιασμού και νόσησης από Covid.
- Τελευταίο κριτήριο της 1ης κατηγορίας αποτελεί η συστηματική επεξεργασία δεδομένων σε μεγάλη κλίμακα που έχουν σκοπό την εισαγωγή, οργάνωση, παροχή και έλεγχο της χρήσης υπηρεσιών ηλεκτρονικής διακυβέρνησης, όπως ορίζονται στο άρθρο 3 του ν.3979/2011[17].

Στην 2η κατηγορία ανήκουν τα εξής κριτήρια:

- Επεξεργασία που πραγματοποιείται σε μεγάλη κλίμακα, ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα[18] που αναφέρονται στο άρθρο 9 παράγραφο 1[19] και στο άρθρο 10 του ΓΚΠΔ[20].
- Επεξεργασία που πραγματοποιείται σε μεγάλη κλίμακα,δεδομένων ιδιαίτερης σημασίας ή εξαιρετικού χαρακτήρα όπως:
    1. Δεδομένα κοινωνικής πρόνοιας
    2. Δεδομένα ηλεκτρονικών επικοινωνιών , όπως e-mail, μεταδεδομένα,δεδομένα που αποκαλύπτουν

[17] Άρθρο 3 ν.3979/2011 « Υπηρεσίες ηλεκτρονικής διακυβέρνησης: υπηρεσίες που συνίστανται στην παραγωγή, διακίνηση και διαχείριση πληροφοριών, δεδομένων κα ηλεκτρονικών εγγράφων και στην παροχή υπηρεσιών από φορείς του δημόσιου τομέα ή στην πραγματοποίηση συναλλαγών με αυτούς τους φορείς με χρήση ΤΠΕ.»

[18] Δεδομένα που οδηγούν στην σίγουρη ταυτοποίηση προσώπου όπως γενετικά και βιομετρικά περιλαμβάνονται στις κατηγορίες αυτές.

[19] Το άρθρο 9 παρ.1 ΓΚΠΔ αναφέρει: ‘’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’’

[20] Το άρθρο 10 ΓΚΠΔ αναφέρει: ‘’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.’’

θέση/τοποθεσία.Εξαίρεση αποτελεί η καταγραφή τηλεφωνικών κλήσεων σύμφωνα με το άρθρο 4 παρ.3 του ν.3471/2006

3. Δεδομένα όπως εθνικό αριθμό ταυτότητας ή άλλο αναγνωριστικό στοιχείο ταυτότητας γενικής εφαρμογής ή αλλαγή των προϋποθέσεων και όρων επεξεργασίας και χρήσης αυτών και των συναφών με αυτά δεδομένων προσωπικού χαρακτήρα
4. Δεδομένα που υπάρχουν σε προσωπικά έγγραφα, όπως ημερολόγια, προσωπικές σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) και σε εφαρμογές καταγραφής βίου (life logging), που προσφέρουν δυνατότητες τήρησης σημειώσεων και πολύ προσωπικών πληροφοριών
5. Δεδομένα που συλλέγονται ή παράγονται από συσκευές (όπως αυτές με αισθητήρες) ιδίως μέσω των εφαρμογών του 'διαδικτύου των πραγμάτων - IoT' (όπως έξυπνες τηλεοράσεις, έξυπνες οικιακές συσκευές, συνδεδεμένα παιχνίδια, έξυπνες πόλεις, έξυπνοι μετρητές ενέργειας κλπ) και/ή με τη χρήση άλλων μέσων

- Επεξεργασία που πραγματοποιείται μέσω της συστηματικής παρακολούθησης θέσης/τοποθεσίας καθώς και των στοιχείων των μεταδεδομένων των επικοινωνιών των εργαζομένων.Σε περίπτωση που η επεξεργασία αυτή γίνεται για λόγους ασφαλείας με την τήρηση αρχείων καταγραφής που περιέχουν τα απόλυτως απαραίτητα δεδομένα και υπάρχει τεκμηρίωση, αυτή εξαιρείται από το κριτήριο.

Στην 3η κατηγορία ανήκουν τα εξής κριτήρια:

- Επεξεργασίες στις οποίες πραγματοποιείται καινοτόμος χρήση ή εφαρμογή νέων τεχνολογιών ή οργανωτικών λύσεων, οι οποίες ενδέχεται να εμπλέκουν νέες μορφές συλλογής και χρήσης δεδομένων, που μπορεί να οδηγήσουν σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων όπως ο συνδυασμός των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης, ή άλλες «έξυπνες» εφαρμογές, από τις οποίες δημιουργείται προφίλ των χρηστών (π.χ. καθημερινές συνήθειες), ή εφαρμογές τεχνητής νοημοσύνης ή τεχνολογίες δημόσια προσπελάσιμων blockchain που περιλαμβάνουν προσωπικά δεδομένα
- Επεξεργασίες στις οποίες πραγματοποιείται συνδυασμός και/ή συσχέτιση προσωπικών δεδομένων από πολλαπλές πηγές ή τρίτους, από δύο ή περισσότερες πράξεις επεξεργασίας που υλοποιούνται για διαφορετικούς σκοπούς ή/και από διαφορετικούς υπευθύνους επεξεργασίας με τρόπο που θα μπορούσε να υπερβαίνει τις εύλογες προσδοκίες του υποκειμένου των δεδομένων.
- Επεξεργασίες που εμπλέκονται δεδομένα , τα οποία δεν έχουν συλλεγεί τα οποία δεν έχουν συλλεγεί από το υποκείμενο και η ενημέρωση των υποκειμένων σύμφωνα με το άρθρο 14 ΓΚΠΔ αποδεικνύεται αδύνατη ή θα προϋπέθετε

δυσανάλογη προσπάθεια ή είναι πιθανό να καταστήσει αδύνατη ή να βλάψει σε μεγάλο βαθμό την επίτευξη των σκοπών της επεξεργασίας.

3. Ο ΛΟΓΟΣ ΕΚΤΕΛΕΣΗΣ ΜΙΑΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Οι οργανισμοί, κυβερνητικοί και ιδιωτικοί, διενεργούν DPIAs για διάφορους σκοπούς. Σε ορισμένες περιπτώσεις, όπως στον Καναδά και στις Ηνωμένες Πολιτείες , απαιτούνται για κυβερνητικές υπηρεσίες και οργανισμούς. Στην Ευρωπαϊκή Ένωση πλέον απαιτούνται από τον νόμο για τους μεγάλους οργανισμούς,όταν πρόκειται για επεξεργασίες υψηλού κινδύνου. Σε άλλες περιπτώσεις, οι οργανισμοί πραγματοποιούν DPIA για να ελαχιστοποιήσουν ή να διαχειριστούν τους κινδύνους που σχετίζονται με την επεξεργασία προσωπικών δεδομένων , αποκομίζοντας παράλληλα συγκεκριμένα οφέλη[21].

Μια εκτίμηση αντικτύπου προστασίας δεδομένων πρέπει να βασίζεται σε μια διαδικασία εκτίμησης και διαχείρισης κινδύνου.[22] Εάν μια κυβερνητική υπηρεσία, μια επιχείρηση ή οποιοσδήποτε άλλος φορέας που ασχολείται με προσωπικά δεδομένα μπορεί να αποφύγει την ανάπτυξη μιας μεθόδου που ενδέχεται να παραβιάσει προσωπικά δεδομένων ατόμων , οι κίνδυνοι θα μειωθούν. Ένας οργανισμός που συλλέγει ή επεξεργάζεται προσωπικά αναγνωρίσιμες πληροφορίες, αντιμετωπίζει μια σειρά από κινδύνους.Ωστόσο, υπάρχει και μια σειρά από πλεονεκτήματα που μπορούν να αποκτηθούν μέσω της διενέργειας DPIA για τον εντοπισμό, την πρόληψη ή τη μείωση αυτών των κινδύνων. Η DPIA θεωρείται πλέον σημαντικό μέρος της συνολικής προσέγγισης διαχείρισης κινδύνων της εταιρείας. Ο οδηγός της Αυστραλίας αναφέρει ότι οι πληροφορίες της εκτίμησης αντικτύπου τροφοδοτούν τις ευρύτερες διαδικασίες διαχείρισης κινδύνων του έργου.[23]Οι απειλές για τα προσωπικά δεδομένα πηγάζουν από διάφορα μέρη.Οι ευπάθειες ενός οργανισμού καθώς και η διαδικασία σχεδιασμού και υλοποίησης ενός προγράμματος μπορούν να αποτελέσουν κινδύνους. Επιπρόσθετα, κίνδυνοι μπορούν να προκύψουν από εξωτερικές απειλές, όπως κακόβουλα τρίτα μέρη που χρησιμοποιούν κοινωνική μηχανική[24] για να εξαπατήσουν υπάλληλους οργανισμών ώστε να παραδώσουν ευαίσθητα δεδομένα ή εκμεταλλεύονται ευπάθειες

[21] Wright D., & de Hert P. eds. Privacy Impact Assessment. Springer, Dordrecht, 2012
[22] Wright D., & de Hert P. eds. Privacy Impact Assessment. Springer, Dordrecht, 2012
[23] Guide to undertaking privacy impact assessments (PIA Guide) – Office of the Australian Information Commissioner Διαθέσιμο: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments [Πρόσβαση 28-12-2021]
[24] Κοινωνική μηχανική - Βικιπαίδεια (wikipedia.org) < https://el.wikipedia.org/wiki/Κοινωνική_μηχανική > Accessed 31-12-2021

στους μηχανισμούς ελέγχου πρόσβασης του οργανισμού. Όλοι οι οδηγοί DPIA αναγνωρίζουν κινδύνους σε οργανισμούς που αφορούν την συλλογή και επεξεργασία προσωπικών δεδομένων.

Στις εκτιμήσεις επικινδυνότητας (risk assessments) που πραγματοποιούνται στα πληροφοριακά συστήματα και στις τεχνολογίες επικοινωνιών, ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων(ENISA) κάνει διάκριση μεταξύ ευπαθειών, απειλών και κινδύνων. Ο ENISA όπως και ο Διεθνής Οργανισμός Τυποποίησης(ISO) ορίζουν το ρίσκο ή κίνδυνο ως την πιθανότητα που έχει μια απειλή να εκμεταλλευτεί ευπάθειες ενός αγαθού και να προκαλέσει ζημιά στον οργανισμό.[25]

Συμπερασματικά πολλούς από τους κινδύνους που υπάρχουν σε μια DPIA αποτελούν απειλές και ευπάθειες για τα συστήματα που επεξεργάζονται προσωπικά δεδομένα.

3.1 Η εκτίμηση αντικτύπου

Μια εκτίμηση αντικτύπου προσωπικών δεδομένων θα πρέπει να αξιολογεί όχι μόνο τις επιπτώσεις στα προσωπικά δεδομένα, αλλά και τις επιπτώσεις σε έναν οργανισμό ως αποτέλεσμα της παραβίασης των προσωπικών αυτών δεδομένων. Πολλές επιχειρήσεις/οργανισμοί σέβονται ελάχιστα την ιδιωτική ζωή και τα προσωπικά δεδομένα των ατόμων, επομένως, για να πειστούν για τα οφέλη της DPIA μπορεί να επικεντρωθούν στις συνέπειες που θα έχει η παραβίαση δεδομένων για την εταιρεία. Είναι δυνατόν να υπάρξουν άμεσες ή έμμεσες επιπτώσεις. Όταν μια εταιρεία δεν λαμβάνει τη δέουσα μέριμνα για τα προσωπικά δεδομένα που έχει υπό τον έλεγχό της, αντιμετωπίζει ποικίλες κυρώσεις, συμπεριλαμβανομένων των ακόλουθων άμεσων και έμμεσων επιπτώσεων.

- Απώλεια αξιοπιστίας, βλάβη της εμπιστοσύνης και της φήμης.[26]
- Παραβίαση νόμων ή/και κανονισμών, η οποία μπορεί να οδηγήσει σε δικαστικές διαδικασίες και κυρώσεις, ή εισαγωγή νέων ρυθμιστικών ελέγχων ως αντίδραση στις ανησυχίες του κοινού σχετικά με το έργο, η οποία μπορεί να οδηγήσει σε απρόβλεπτες ή απροσδόκητες δαπάνες για τον οργανισμό.
- Οικονομική ζημία από πρόστιμα ή κυρώσεις.[27]

---

[25] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary . Ο ορισμός του ENISA για τον κίνδυνο είναι σχεδόν πανομοιότυπος με εκείνον του προτύπου ISO 27005, το οποίο ορίζει ως "κίνδυνο ασφάλειας πληροφοριών την πιθανότητα ότι μια δεδομένη απειλή θα εκμεταλλευτεί τις ευπάθειες σημεία ενός αγαθού ή μιας ομάδας αγαθών και θα προκαλέσει έτσι ζημία στον οργανισμό. Μετριέται με βάση το συνδυασμό της πιθανότητας ενός συμβάντος και των συνεπειών του.." International Organization for Standardization (ISO), Information Technology – Security Techniques – Information Security Risk Management, International Standard, ISO/IEC 27005:2008(E), First edition, 15 Ιουνιίου 2008

[26] Privacy, Data Breach and Reputation Management – Data Privacy Manager 2020 https://dataprivacymanager.net/data-breach-and-reputation-management/ [Πρόσβαση 03-01-2022]

[27] ''Μέχρι τον Αύγουστο του 2020, το μεγαλύτερο πρόστιμο που προέκυψε από παραβίαση δεδομένων ήταν 575 εκατομμύρια δολάρια ΗΠΑ που επιβλήθηκε στον οργανισμό αναφοράς

- Απολύσεις ή παραιτήσεις ανώτερου προσωπικού.[28]
- Ανασχεδιασμός έργων ή ακύρωση έργων.
- Απροσδόκητες ή ανεπιθύμητες συνέπειες ως αποτέλεσμα εσφαλμένων προσωπικών δεδομένων, όπως για παράδειγμα, ορισμένα άτομα μπορεί να διωχθούν ποινικά ή να κατηγορηθούν ψευδώς ή να τεθούν υπό υποψία ή μπορεί να υποστούν αδικαιολόγητη ζημία (π.χ. να βρίσκονται σε "λίστα απαγόρευσης πτήσεων" ή να μην μπορούν να εισέλθουν σε μια χώρα ή απορρίπτονται για μια θέση εργασίας) επειδή τα προσωπικά δεδομένα που κατέχει ο οργανισμός είναι εσφαλμένα.
- Απώλεια ανταγωνιστικού πλεονεκτήματος.

Εκτός από τις συνέπειες για τον οργανισμό, υποφέρουν και άλλοι. Τα άτομα των οποίων τα δεδομένα έχουν κλαπεί μπορεί να ξοδέψουν σημαντικό χρόνο, χρήμα και ανησυχία προσπαθώντας να ανακτήσουν την ταυτότητά τους ή να διορθώσουν ανακριβή δεδομένα - αν υποθέσουμε ότι μπορούν να μάθουν ποιοι οργανισμοί αποθηκεύουν προσωπικά δεδομένα για αυτούς. Εάν παραβιαστούν τα προσωπικά δεδομένα ορισμένων προσώπων (π.χ. μυστικοί πράκτορες, διασημότητες, ευάλωτες ομάδες πληθυσμού όπως τα παιδιά και τα θύματα ενδοοικογενειακής βίας), μπορεί να υποστούν υψηλότερα ασφάλιστρα ή να δυσκολευτούν να βρουν ή να διατηρήσουν μια θέση εργασίας.

3.2 Τα οφέλη της Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων

Γενικά , κύριοι στόχοι μιας εκτίμησης αντικτύπου στην προστασία δεδομένων είναι[29]:

- Καθορισμός των επιπτώσεων που έχει η επεξεργασία προσωπικών δεδομένων στην ιδιωτικότητα των ατόμων, καθορισμός των κινδύνων και των ευθυνών.

καταναλωτικών πιστώσεων Equifax για την παραβίαση δεδομένων της εταιρείας το 2017, η οποία είχε ως αποτέλεσμα να παραβιαστούν σχεδόν 148 εκατομμύρια αρχεία δεδομένων. Η δεύτερη στην κατάταξη British Airways υπέστη παραβίαση δεδομένων το 2018, η οποία είχε ως αποτέλεσμα πρόστιμα ύψους 230 εκατομμυρίων δολαρίων βάσει του τότε νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR)''. – Joseph Johnson (2021) – Statista Διαθέσιμο:<https://www.statista.com/statistics/1170520/worldwide-data-breach-fines-settlements/#:~:text=Biggest%20data%20breach%20fines%20and%20settlements%20worldwide%20as,%20%20124%20%209%20more%20rows%20 > [Πρόσβαση 03-01-2022]

[28] 6 Potential Long-Term Impacts of a Data Breach (Νοέμβριος 2021) – Security Intelligence Διαθέσιμο στο : < https://securityintelligence.com/articles/long-term-impacts-security-breach/ > [Πρόσβαση 05-01-2022]

[29] Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Version 2.0, 2009 Διαθέσιμο: https://www.academia.edu/1321883/ICO_Privacy_Impact_Assessment_Handbook

- Παροχή δεδομένων για τον σχεδιασμό συστημάτων που προστατεύουν τα προσωπικά δεδομένα (Privacy By Design)
- Να διασφαλιστεί η προστασία των προσωπικών δεδομένων σε περίπτωση αναβάθμισης/αλλαγής στα συστήματα που διαχειρίζεται αυτά τα δεδομένα.
- Την γνωστοποίηση των κινδύνων που αφορούν τους κινδύνους των προσωπικών δεδομένων με τα εμπλεκόμενα μέρη ,καθώς και την παροχή απόδειξης ότι συμμορφώνεται η επιχείρηση ή οργανισμός με τα κανονιστικά πλαίσια.

Με την εκτέλεση μιας DPIA εκτός από τα οφέλη που έχουν τα υποκείμενα των οποίων τα δεδομένα επεξεργάζονται, μπορούν ταυτόχρονα οι οργανισμοί,επιχειρήσεις που την εκτελέσουν να αποκομίσουν πολυάριθμα οφέλη.

Μια εταιρεία ή ένας κυβερνητικός φορέας που διεξάγει μια DPIA με καλές προθέσεις και πραγματικό ενδιαφέρον για τη συμμετοχή των ενδιαφερόμενων μερών, συμπεριλαμβανομένου του κοινού, έχει την ευκαιρία να αποκτήσει την εμπιστοσύνη και την καλή θέληση των πολιτών και των καταναλωτών. Ο βαθμός στον οποίο ο οργανισμός θα αποκτήσει εμπιστοσύνη και καλή θέληση θα καθοριστεί από το πόσο ανοικτή και διαφανής είναι η διαδικασία εκτέλεσης της εκτίμησης αντικτύπου. Κατά την ανάπτυξη μιας νέας υπηρεσίας, προϊόντος, πολιτικής, προγράμματος ή έργου, όσο πιο ανοικτή και διαφανής είναι η διαδικασία, τόσο πιο πιθανό είναι ο οργανισμός να ξεπεράσει τις ανησυχίες, τις υποψίες και τη δυσπιστία.[30] Μια κατάλληλη DPIA δείχνει επίσης στους καταναλωτές ή/και τους πολίτες ότι μια εταιρεία ή/και κρατικός φορέας εκτιμά την ιδιωτική τους ζωή και ότι είναι δεκτική στις ανησυχίες τους. Οι πελάτες και οι άνθρωποι τείνουν περισσότερο να εμπιστεύονται μια εταιρεία/φορέα που διεξάγει αξιολόγηση κινδύνου από ό,τι μια εταιρεία που δεν διεξάγει. Οι επιχειρήσεις που μπορούν να διατηρήσουν υψηλό βαθμό εμπιστοσύνης και σιγουριάς με τους καταναλωτές μπορούν να ξεχωρίσουν από τους ανταγωνιστές τους και να αποκτήσουν ανταγωνιστικό πλεονέκτημα.[31]

Όπως ήδη έχουμε αναφέρει μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων πρέπει να εκτελείται από τα πιο αρχικά στάδια ανάπτυξης ενός πληροφοριακού συστήματος,μιας συσκευής κλπ. Επιτρέπει σε μια επιχείρηση να εντοπίζει πιθανά ζητήματα προστασίας των προσωπικών δεδομένων που σχετίζονται

[30] Μία DPIA "επιτρέπει σε έναν οργανισμό να κατανοήσει τις προοπτικές των άλλων ενδιαφερόμενων μερών και να καταστήσει τους στόχους του έργου καλύτερα κατανοητούς." ICO - PIA Handbook

[31] What Is Data Protection And Why Is It Important? - The Freeman Online [n.d] Διαθέσιμο στο : https://www.thefreemanonline.org/what-is-data-protection-and-why-is-it-important [Πρόσβαση 05-01-2022]
4 Ways Data Protection can increase your Competitive Advantage - Debb Gannaway(2019) Διαθέσιμο: https://dgtechllc.com/4-ways-data-protection-can-increase-your-competitive-advantage/ [Πρόσβαση 05-01-2022]

με την επεξεργασία των ευαίσθητων αυτών δεδομένων .[32] Με αυτόν τον τρόπο της δίνεται η δυνατότητα να λαμβάνει τα απαραίτητα μέτρα ελέγχου και τις πρέπουσες δικλείδες ασφαλείας πριν, και όχι μετά στα αργότερα στάδια ανάπτυξης του εν λόγω συστήματος αφού έχουν δαπανηθεί πολλοί πόροι. Το κόστος της αλλαγής ενός έργου στο στάδιο του σχεδιασμού είναι συνήθως πολύ χαμηλότερο από εκείνο που προκύπτει αργότερα στην ανάπτυξη και ταυτόχρονα μετριάζονται οι διακοπές στις επιχειρηματικές δραστηριότητες.[33]Ενδέχεται το έργο να μην μπορεί να πραγματοποιηθεί καθόλου αν ο αντίκτυπος στην προστασία των δεδομένων είναι μεγάλος. Παράλληλα, λαμβάνοντας υπόψη τις πιθανές ανησυχίες των μέσων ενημέρωσης ή του κοινού, η DPIA μπορεί να βοηθήσει στην έγκαιρη ανακάλυψη ζητημάτων προστασίας της ιδιωτικότητας ή/και να μειώσει το κόστος όσον αφορά το χρόνο διαχείρισης, τις νομικές δαπάνες και τις πιθανές ανησυχίες των μέσων ενημέρωσης ή του κοινού.

Κατά την εκτέλεση της εκτίμησης αντικτύπου, επιθυμητή είναι η συνεργασία και η βοήθεια από όλα τα εμπλεκόμενα και ενδιαφερόμενα μέρη.Η συμμετοχή τους θα συμβάλλει στο να μην παραλειφθεί τίποτα που αφορά την προστασία των προσωπικών δεδομένων. Ταυτόχρονα πρέπει και να κλιμακώνονται οποιαδήποτε θέματα βρεθούν κατά την εκτέλεση της DPIA στα υψηλόβαθμα στελέχη του οργανισμού η κρατικού φορέα. Ακόμη και αν τα εμπλεκόμενα/ενδιαφερόμενα μέρη δεν είναι σε θέση να προσφέρουν κάποια ιδέα, ο οργανισμός έχει την ευκαιρία να κερδίσει την κατανόηση και τον σεβασμό των ενδιαφερομένων/εμπλεκόμενων μερών.

Εφόσον εμπλέκονται διαφορετικά μέρη ενός οργανισμού στην διαδικασία της DPIA, αυτή μπορεί να θεωρηθεί και ως άσκηση για την βελτίωση της επεξεργασίας που θα κάνει ο οργανισμός και αποτελεί και μια ευκαιρία για εκμάθηση του προσωπικού όσον αφορά τα προβλήματα που αφορούν την προστασία των προσωπικών δεδομένων.Όπως χρησιμοποιούνται δοκιμές διείσδυσης[34] και ασκήσεις ανίχνευσης ευπαθειών[35] για να

---

[32] Stewart, Blair, Privacy Impact Assessment Handbook, Office of the Privacy Commissioner, Auckland, Ιούνιος 2015 Διαθέσιμο: https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-handbook/ [Πρόσβαση 05-01-2022]

[33] Yoichi Seto – Application of Privacy Impact Assessment in the Smart City - Electronics and Communications in Japan, Vol. 98, No. 2, 2015 (Translated from Denki Gakkai Ronbunshi, Vol. 133-C, No. 7, July 2013, pp. 1427–1435)

[34] Οι δοκιμές διείσδυσης είναι προσομοιώσεις κυβερνοεπίθεσης που εξαπολύεται στο σύστημα του υπολογιστικών συστημάτων. Η προσομοίωση αυτή βοηθά στην ανακάλυψη σημείων εκμετάλλευσης και στον έλεγχο της ασφάλειας της πληροφοριακής υποδομής. Κάνοντας συνεχείς δοκιμές διείσδυσης, οι επιχειρήσεις μπορούν να αποκτήσουν ανατροφοδότηση από ειδικούς, αμερόληπτους τρίτους σχετικά με τις διαδικασίες ασφαλείας τους. Αν και δυνητικά χρονοβόρες και δαπανηρές, οι δοκιμές αυτές μπορούν να βοηθήσουν στην πρόληψη εξαιρετικά δαπανηρών και επιζήμιων παραβιάσεων. Cisco – What is penetration Testing Διαθέσιμο https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html [Πρόσβαση 06-01-2022]

[35] ''Οι ασκήσεις ανίχνευσης ευπαθειών είναι η διαδικασία εντοπισμού και αναφοράς ευπαθειών. Παρέχουν έναν τρόπο για να εντοπίζονται και να επιλύονται προβλήματα ασφάλειας , πριν κάποιος ή κάτι τα εκμεταλλευτεί. Μία από τις πιο συνηθισμένες χρήσεις για τις ασκήσεις αυτές είναι η ικανότητά τους να επικυρώνουν τα μέτρα ασφαλείας. ''. John J. Fay, David Patterson, in

βρεθούν τα τρωτά σημεία ενός πληροφοριακού συστήματος, έτσι και η DPIA πρέπει να χρησιμοποιείται για να διασφαλιστεί η προστασία των προσωπικών δεδομένων όταν γίνεται επεξεργασία τους. Μια εκτίμηση αντικτύπου που εκτελείται με διαφανή τρόπο καθιστά σαφές στο κοινό ποιες πληροφορίες συλλέγει ο οργανισμός, γιατί συλλέγονται, πώς θα χρησιμοποιηθούν και θα διαμοιραστούν, πώς θα έχουν πρόσβαση σε αυτές και πώς θα αποθηκευτούν με ασφάλεια.[36]Παράλληλα η DPIA αποτελεί έναν τρόπο για τον οργανισμό να δείξει ότι έχει εξετάσει διεξοδικά τον τρόπο με τον οποίο το έργο/πρόγραμμα/σύστημα θα χειριστεί τα προσωπικά δεδομένα. Ακόμη και αν ορισμένοι κίνδυνοι προστασίας της ιδιωτικότητας των υποκείμενων που έχουν εντοπιστεί δεν μπορούν να μετριαστούν ή/και πρέπει να γίνουν αποδεκτοί ,η αναφορά που παράγεται από την εκτέλεση της εκτίμησης αντικτύπου, ως αποτέλεσμα μιας σαφούς και συστηματικής διαδικασίας, είναι κάτι στο οποίο μπορούν να ανατρέξουν τα ενδιαφερόμενα μέρη και να ενημερωθούν για τους λόγους για τους οποίους έγιναν ορισμένες αποφάσεις.[37]Κατά συνέπεια, η DPIA ενθαρρύνει τη λήψη αποφάσεων με πληρέστερη πληροφόρηση.

Επιπλέον όφελος,αποτελεί η διαφάνεια[38] με την οποία γίνεται η DPIA καθώς συνεισφέρει στο να αποφευχθούν παραβιάσεις αργότερα.Ο οργανισμός που εκτελεί την εκτίμηση αντικτύπου με διαφανή τρόπο αποδεικνύει ότι δεν υπήρχε αμέλεια εκ μέρους του όταν ανέλαβε την επεξεργασία προσωπικών δεδομένων καθώς αποδεικνύεται και η δαπάνη πόρων αλλά και η συμμετοχή διαφορετικών εμπλεκόμενων προκειμένου να επιτευχθεί η προστασία των δεδομένων.[39] Ο οργανισμός μπορεί να μειώσει την

Contemporary Security Management (Fourth Edition), 2018 Διαθέσιμο: https://www.sciencedirect.com/topics/computer-science/vulnerability-assessment [Πρόσβαση 06-01-2022]

[36] DHS, PIAs: The Privacy Office Official Guidance Περισσότερα : https://www.dhs.gov/privacy-impact-assessments [Πρόσβαση 06-01-2022]

[37] Wright D., & de Hert P. eds. Privacy Impact Assessment. Springer, Dordrecht, 2012

[38] Η διαφάνεια αποτελεί βασική αρχή της προστασίας των δεδομένων. Ο καθένας έχει το δικαίωμα να γνωρίζει ποια από τα προσωπικά του δεδομένα συλλέγονται, χρησιμοποιούνται, ερωτώνται ή υποβάλλονται σε άλλη επεξεργασία και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή πρόκειται να υποβληθούν σε επεξεργασία. ''Transparency - European Data Protection Supervisor Διαθέσιμο :https://edps.europa.eu/data-protection/our-work/subjects/transparency_en [Πρόσβαση 06-01-2022] και'' Η διαφάνεια αποτελεί βασική αρχή της προστασίας των δεδομένων, η οποία είναι θεμελιώδης για μια προσέγγιση "προστασίας των δεδομένων από σχεδιασμού και εξ ορισμού". Διευκολύνει την άσκηση των δικαιωμάτων των ατόμων και τους δίνει μεγαλύτερο έλεγχο. Αυτό είναι ιδιαίτερα σημαντικό εάν η επεξεργασία είναι πολύπλοκη ή εάν αφορά ένα παιδί.'' ICO – Transparency https://ico.org.uk/for-organisations/accountability-framework/transparency/#:~:text=Transparency%20is%20a%20key%20data%20protection%20principle%20which,complex%20or%20if%20it%20relates%20to%20a%20child. [Πρόσβαση 07-01-2022]

[39] "A PIA provides an organisation with an opportunity to obtain a commitment from stakeholder representatives and advocates to support the project from an early stage, in order to avoid the emergence of opposition at a late and expensive stage in the design process." ICO, PIA Handbook

πιθανότητα να δεχθεί αρνητική δημοσιότητα με το να είναι από την αρχή ανοιχτός και διαφανής.[40]

Τέλος, η λογοδοσία μπορεί να επιβληθεί η τουλάχιστον να ενθαρρυνθεί μέσω της DPIA.Μια DPIA διευκρινίζει ποιος θα κάνει τι και ποιος θα είναι υπεύθυνος για τι. Θα πρέπει να καθιστά προφανές ότι η επεξεργασία προσωπικών δεδομένων που πραγματοποιεί ο εκάστοτε οργανισμός συμμορφώνεται με όλους τους ισχύοντες νόμους, κανονισμούς και κώδικες δεοντολογίας για την προστασία των προσωπικών δεδομένων. Εάν ένα στέλεχος του οργανισμού κατανοήσει ότι θα λογοδοτήσει για μια ενέργεια που παραβιάζει την ιδιωτικότητα, μπορεί να είναι λιγότερο πιθανό να την εκτελέσει εάν φαίνεται ότι είναι πιθανό να εξοργίσει τους καταναλωτές αλλά και το ευρύτερο κοινό ή θα χρειαστεί να αντιμετωπίσει τις αρχές.

4. ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Ο τρόπος πραγματοποίησης μιας DPIA εξαρτάται σε μεγάλο βαθμό από το πεδίο εφαρμογής ,την κλίμακα και τον σκοπό της. Μια εφαρμογή μικρής κλίμακας που επεξεργάζεται ευαίσθητα δεδομένα έχει διαφορετικές απαιτήσεις από μια εφαρμογή μεγάλης κλίμακας με μεγάλο αριθμό ευαίσθητων δεδομένων και (π.χ. στον τομέα της υγείας).Ωστόσο, το μέγεθος ή το χρηματικό κόστος ενός έργου επεξεργασίας δεν σημαίνει πάντα ότι θα έχει μεγάλο αντίκτυπο,καθώς ακόμα και μικρότερα έργα μπορούν να έχουν σημαντικές επιπτώσεις στην ιδιωτικότητα των υποκειμένων.[41]

Το πεδίο εφαρμογής της DPIA θα καθοριστεί από το μέγεθος των αναμενόμενων επιπτώσεων. Εάν οι επιπτώσεις αναμένεται να επηρεάσουν μόνο τους υπαλλήλους του οργανισμού (για παράδειγμα, η επιχείρηση μπορεί να επιθυμεί να βελτιώσει τον έλεγχο πρόσβασης με τη χρήση βιομετρικών στοιχείων), η DPIA θα μπορούσε να περιλαμβάνει μόνο εκπροσώπους των εργαζομένων και να είναι σχετικά ελάχιστη σε έκταση. Εάν κάποιος κυβερνητικός φορέας επιθυμεί να εφαρμόσει ένα νέο σύστημα διαχείρισης ταυτότητας για όλους τους πολίτες, θα πρέπει να προβεί σε μια σημαντικά ευρύτερη DPIA με διάφορα εξωτερικά μέρη.

Σύμφωνα με τους νόμους και τους κανονισμούς, οι οργανισμοί θα πρέπει να κάνουν αξιολόγηση για να καθοριστεί το απαιτούμενο πεδίο εφαρμογής καθώς και η κλίμακα

---

[40] Stewart, Blair, Privacy Impact Assessment Handbook, Office of the Privacy Commissioner, Auckland, Ιούνιος 2015 Διαθέσιμο: https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-handbook/ [Πρόσβαση 05-01-2022]

[41] Office of the Australian Information Commissioner (OAIC) - Guide To undertaking privacy impact assessments Διαθέσιμο: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments [Πρόσβαση 05-01-2022]

της DPIA . Η ποσότητα και η λεπτομέρεια των προσωπικά αναγνωρίσιμων πληροφοριών ανά άτομο, ο βαθμός ευαισθησίας των πληροφορίων αυτών και ο αριθμός των ατόμων που έχουν πρόσβαση στις πληροφορίες αυτές που θα υποβληθούν σε επεξεργασία αποτελούν σημαντικοί παράγοντες που επηρεάζουν αυτήν την κλίμακα.[42]

Σε κάθε περίπτωση, η δημιουργία σεναρίων και παραδειγμάτων επεξεργασίας δεδομένων είναι ζωτικής σημασίας για την αξιολόγηση της κλίμακας της DPIA από τους οργανισμούς. Σε αυτή την περίπτωση, η συμμετοχή των νομικών και των ειδικών της πληροφορικής είναι κρίσιμη. Επιπλέον, πρέπει να συμπεριληφθούν στην διαδικασία εκτέλεσης της εκτίμησης αντικτύπου οι τυπικοί χρήστες των συστημάτων που θα επεξεργάζονται τα δεδομένα για να αποφευχθεί τυχόν παράλειψη σεναρίων από τους οργανισμούς και να ληφθεί η προοπτική ενός ατόμου που ανησυχεί για την παραβίαση της ιδιωτικής του ζωής. [43]

5.ΑΡΧΙΚΑ ΣΤΑΔΙΑ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΣΧΕΤΙΚΑ ΜΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Εφόσον γίνει ανάλυση της πράξης επεξεργασίας και κριθεί απαραίτητη η εκτέλεση της εκτίμησης αντικτύπου με βάση τα κριτήρια που αναφέραμε παραπάνω , ακολουθεί η αρχή της διαδικασίας εκτίμησης αντικτύπου.

5.1 Προετοιμασία της Εκτίμησης Αντικτύπου σχετικά με την Προστασία Δεδομένων

Ο υπεύθυνος επεξεργασίας είναι υπεύθυνος για τη διασφάλιση της ολοκλήρωσης της DPIA (άρθρο 35 παράγραφος 2 του ΓΚΠΔ[44]). Η DPIA μπορεί να διενεργηθεί από κάποιον άλλον, είτε εντός είτε εκτός του οργανισμού, αλλά ο υπεύθυνος επεξεργασίας είναι τελικά υπεύθυνος γι' αυτήν.

Όταν έχει οριστεί υπεύθυνος προστασίας δεδομένων (DPO) (άρθρο 35 παράγραφος 2), ο υπεύθυνος επεξεργασίας πρέπει επίσης να ζητήσει τη συμβουλή του DPO, και η

[42] CNIL – Privacy Impact Assessment (PIA) Methodology Φεβρουάριος 2018, ISO/IEC 29134 (2017) BSI Standards Publication

[43] Stefan Strauß - Privacy and Identity in a Networked Society Refining Privacy Impact Assessment-Routledge (2019)

[44] "Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων". - Γενικός Κανονισμός Προστασίας Δεδομένων

συμβουλή αυτή, καθώς και οι επιλογές του υπευθύνου επεξεργασίας, πρέπει να τεκμηριώνονται στην DPIA. Ο DPO πρέπει επίσης να παρακολουθεί την εκτέλεση της DPIA (άρθρο 39 παράγραφος 1 στοιχείο γ) ΓΚΠΔ).

Στη φάση της προετοιμασίας λοιπόν συγκροτείται μια ομάδα για τη διενέργεια της εκτίμησης και συλλέγονται σχετικές πληροφορίες σχετικά με την προβλεπόμενη επεξεργασία δεδομένων.

Το πρόσωπο που είναι υπεύθυνο για τη διενέργεια μιας DPIA θα πρέπει να προσδιορίζεται και να διορίζεται από τον οργανισμό. Επίσης, αυτό το πρόσωπο είναι πιθανό να είναι υπεύθυνο για να κρίνει το αν είναι υποχρεωτική ή όχι η εκτέλεση της DPIA με βάση τα κριτήρια που είχαν αναφερθεί. Το πρόσωπο που είναι υπεύθυνο για την παραγωγή της έκθεσης της DPIA θα πρέπει επίσης να ορίζεται από τον οργανισμό. Υπάρχουν οδηγοί που προτείνουν ένα ανώτερο μέλος της ομάδας που διαχειρίζεται το έργο επεξεργασίας να ηγείται την ομάδα που εκτελεί την DPIA.[45] Η ομάδα θα πρέπει να διαθέτει εμπειρία και γνώσεις στην ανάπτυξη πολιτικών, στο σχεδιασμό επιχειρησιακών προγραμμάτων και επιχειρήσεων, στην τεχνολογία και τα συστήματα, στην ανάλυση κινδύνων και συμμόρφωσης, στη διαδικαστική και νομική ανάλυση που αφορά την προστασία των προσωπικών δεδομένων.

Το άτομο που ευθύνεται για την εκτέλεση της DPIA θα πρέπει να καθορίσει τα κριτήρια κινδύνου και να διασφαλίσει ότι η διοίκηση συμφωνεί με τα κριτήρια κινδύνου που θα χρησιμοποιηθούν για τον προσδιορισμό της σημασίας του κινδύνου. Τα κριτήρια αυτά μπορεί να αναπτυχθούν από τον ίδιο τον οργανισμό ή με την βοήθεια εξωτερικών συνεργατών .Ταυτόχρονα πρέπει να καθοριστούν τα κριτήρια για την εκτίμηση των επιπτώσεων και της επικινδυνότητας που σχετίζονται με την επεξεργασία δεδομένων που θα πραγματοποιήσει ο οργανισμός. Ο υπεύθυνος εκτέλεσης της DPIA θα πρέπει επίσης να καθορίσει κριτήρια αποδοχής του κινδύνου και να διασφαλίσει ότι η διοίκηση του οργανισμού συμφωνεί με αυτά.

Αυτά τα κριτήρια που θα καθοριστούν από τον υπεύθυνο εκτέλεσης της DPIA πρέπει να συμβαδίζουν με τον στόχο,τις αξίες και τους πόρους του οργανισμού. Πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό των κριτήριων αυτών παράγοντες όπως:

-Νομικοί και κανονιστικοί που αφορούν τη διασφάλιση της προστασίας των προσωπικών δεδομένων των ατόμων

- Κατευθυντήριες γραμμές του κλάδου στον οποίο δραστηριοποιείται ο οργανισμός που επεξεργάζεται τα δεδομένα, τα επαγγελματικά πρότυπα, τους κανονισμούς της εταιρείας και τις συμφωνίες με τους καταναλωτές.

[45] Information and Privacy Office, Management Board Secretariat, Ontario, Privacy Impact Assessment: A User's Guide, June 2001
Information Comissioner's Office (ICO) Conducting privacy impact assessments code of Practice

- Παράγοντες που αφορούν την χρήση κάποιας συγκεκριμένης τεχνολογίας.[46]

- Παράγοντες που αφορούν την προστασία των πληροφοριακών συστημάτων γενικότερα που είναι σημαντικοί και για την προστασία των προσωπικών δεδομένων.

5.2 Δημιουργία σχεδίου εκτέλεσης της Εκτίμησης Αντικτύπου και καθορισμός πόρων

Προκειμένου να ολοκληρωθεί επιτυχημένα μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων πρέπει να γίνει ο απαραίτητος καθώς και να καθοριστούν οι απαραίτητοι ανθρώπινοι,οικονομικοί πόροι καθώς και το χρονικό διάστημα.

Το σχέδιο πρέπει να δημιουργείται με βάση την κλίμακα της DPIA,καθώς και να υπάρχει η δυνατότητα για αλλαγές. Το σχέδιο θα πρέπει επίσης να λαμβάνει υπόψη την πιθανότητα ακύρωσης της εκτίμησης αντικτύπου αν κριθεί αυτό απαραίτητο. Παράλληλα το σχέδιο θα πρέπει να περιγράφει λεπτομερώς τι πρέπει να γίνει για την ολοκλήρωση της DPIA, ποιος από την ομάδα εκτέλεσης DPIA θα είναι υπεύθυνος για τι, το χρονοδιάγραμμα της DPIA καθώς και το πώς θα διεξαχθούν τυχόν διαβουλεύσεις. Θα πρέπει να εξηγεί γιατί η διαβούλευση με τα ενδιαφερόμενα μέρη είναι απαραίτητη σε αυτή την περίπτωση, ποιοι θα ερωτηθούν και πώς θα ερωτηθούν.

Μετά την δημιουργία σχεδίου, πρέπει να γίνει εκτίμηση των πόρων που χρειάζεται η εκτέλεση της DPIA και αυτό σημαίνει και κόστη που πρέπει να εγκριθούν από την διοίκηση.Ο υπεύθυνος εκτέλεσης της DPIA μαζί με την ομάδα πρέπει να φροντίσει να δημιουργήσει το σχέδιο σύμφωνα με τους πόρους που διαθέτει ο οργανισμός.

5.3 Περιγραφή του συστήματος επεξεργασίας του οποίου εκτιμάται το αντίκτυπο σχετικά με την προστασία δεδομένων

Προκειμένου να αποκτηθεί μια σωστή εικόνα για το τι κάνει το πληροφορικό σύστημα,πρόγραμμα ή οποιαδήποτε άλλη διαδικασία που θα διαχειριστεί προσωπικά δεδομένα πρέπει να γίνει μια εκτενής περιγραφή του.

Πιο συγκεκριμένα θα πρέπει να γίνει αναφορά στο ποια είναι τα προσωπικά δεδομένα τα οποία θα επεξεργαστούν και αν είναι δυνατή η αναγνώριση συγκεκριμένων προσώπων από αυτά.Έπειτα πρέπει να γίνει αναφορά στον σκοπό της επεξεργασίας και τι κέρδη αποσκοπεί το άτομο που παραχωρεί τα προσωπικά του δεδομένα.Θα πρέπει να γίνει επίσης περιγραφή στο πως θα διατηρηθούν αυτά τα προσωπικά δεδομένα δηλαδή από ποιον και με ποιον τρόπο. Αναφορά πρέπει να γίνει και στο πως

[46] PIA Framework for RFID Applications(2011), Διαθέσιμο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf [Πρόσβαση 15-01-2022]

θα επηρεάσει η επεξεργασία προσωπικών δεδομένων τα υποκείμενα καθώς και πως θα υλοποιηθούν οι διαδικασίες που αφορούν την συλλογή των δεδομένων (ειδοποίηση, συγκατάθεση, διαγραφή κλπ).

Επιπροσθέτως, ο οργανισμός που κάνει την επεξεργασία δεδομένων πρέπει να αναγνωρίσει τα αγαθά τα οποία θα χρησιμοποιούνται για την επεξεργασία όπως εφαρμογές,λογισμικό(λειτουργικά συστήματα,βάσεις δεδομένων κλπ) ,υλισμικό(ηλεκτρονικοί υπολογιστές, routers,switches,servers κλπ).

Ταυτόχρονα στην περιγραφή του συστήματος πρέπει να περιλαμβάνεται το πως διαχειρίζονται αυτά τα αγαθά δηλαδή ποιος έχει πρόσβαση σε αυτά και πως γίνεται η διαχείριση των χρηστών,καθώς και αν έχουν πρόσβαση σε αυτά τρίτοι.

Θα πρέπει επίσης να περιγράφεται η χρήση των μεταδεδομένων , πως γίνεται η καταγραφή, η δημιουργία αντιγράφων ασφαλείας καθώς και η ανάκτηση των δεδομένων όπως και οι τρόποι διατήρησης και διαγραφής δεδομένων.

Το στάδιο αυτό θα πρέπει επίσης να περιλαμβάνει περιγραφή τυχόν υφιστάμενων μέτρων ασφάλειας/προστασίας των προσωπικών δεδομένων, όπως αυτά που περιλαμβάνονται στην υποδομή ή τις πολιτικές του οργανισμού. Επιπλέον, επειδή οι χρήστες διαδραματίζουν σημαντικό ρόλο στο σύστημα, θα πρέπει να περιγράφονται οι προσδοκίες που έχουν για την προστασία των προσωπικών τους δεδομένων.[47]

Η περιγραφή του έργου δεν θα πρέπει να περιλαμβάνει ανάλυση των επιπτώσεων στα προσωπικά δεδομένα, καθώς αυτό θα εξεταστεί σε μεταγενέστερα στάδια της DPIA. Οι πληροφορίες που θα υπάρχουν στην περιγραφή είναι σημαντικές καθώς παρέχουν το γενικό πλαίσιο για το υπόλοιπο της DPIA. Εάν το έργο που περιλαμβάνει την επεξεργασία δεδομένων βρίσκεται ακόμη σε πρώιμο στάδιο, μπορεί να μην είναι δυνατόν να προετοιμαστεί μια λεπτομερής περιγραφή, αλλά αυτή μπορεί να επικαιροποιηθεί καθώς αναδεικνύονται περισσότερες πληροφορίες για το έργο. Η περιγραφή του έργου θα πρέπει να είναι επαρκώς λεπτομερής ώστε να επιτρέπει στα ενδιαφερόμενα μέρη να κατανοήσουν το έργο και τι θα προκύψει από αυτό.

Τέλος στην περιγραφή πρέπει να συμπεριλαμβάνονται και τα πιθανά σημεία τα οποία ενδέχεται να αλλάξουν τον σχεδιασμό του έργου που θα περιέχει επεξεργασία δεδομένων.

---

[47] Vemou, K. and Karyda, M. (2020), "Evaluating privacy impact assessment methods: guidelines and best practice", Information and Computer Security, Vol. 28 No. 1, pp. 35-53.Διαθέσιμο: https://doi.org/10.1108/ICS-04-2019-0047

5.4 Εμπλοκή των ενδιαφερομένων μερών

5.4.1 Προσδιορισμός των ενδιαφερομένων μερών

Η απλή συμμόρφωση με τους νόμους και τους κανονισμούς προστασίας δεδομένων δεν εγγυάται ότι η στρατηγική μιας εταιρείας θα είναι αποδεκτή από τους πολίτες και τους καταναλωτές. Η διαβούλευση με όλα τα ενδιαφερόμενα μέρη αποτελεί σημαντικό μέρος της διαδικασίας της DPIA. Είναι αδύνατο να επιτευχθούν οι στόχοι μιας DPIA εάν η διαδικασία διεξάγεται χωρίς την γνώση όλων των μερών. Πολλά τμήματα του πληθυσμού επηρεάζονται από ένα εξελιγμένο έργο που περιλαμβάνει ισχυρές τεχνολογίες. Είναι απαίτηση της διαδικασίας να συμμετέχουν στην αξιολόγηση μέλη του κοινού και τα αποτελέσματα να αντικατοπτρίζουν τις ανησυχίες τους.[48]

Ο οργανισμός πρέπει να προσδιορίσει λοιπόν όλα τα ενδιαφερόμενα μέρη τα οποία είναι τα άτομα που ενδέχεται να λάβουν μέρος στην διαδικασία της επεξεργασίας των προσωπικών δεδομένων ή να επηρεαστούν από την επεξεργασία τους.Οι ρυθμιστικές αρχές, οι πελάτες, οι καταναλωτές, οι πάροχοι υπηρεσιών, οι υπάλληλοι του οργανισμού που απασχολούνται στα νομικά,οικονομικά,επιχειρηματικά τμήματα καθώς και οι υπάλληλοι που διαχειρίζονται τα πληροφοριακά συστήματα και φροντίζουν για την ασφάλεια των πληροφοριών αλλά και άλλοι είναι παραδείγματα εσωτερικών και εξωτερικών ενδιαφερόμενων μερών. Και τα δύο είδη ενδιαφερομένων, καθώς και τα πρόσωπα και οι οργανισμοί εντός καθεμιάς από αυτές τις ομάδες, θα πρέπει να προσδιορίζονται στον κατάλογο ενδιαφερομένων.Αυτόν τον προσδιορισμό πρέπει να τον εκτελέσει ο υπεύθυνος της DPIA μαζί με την ομάδα του και με αυτόν τον τρόπο η διαδικασία της DPIA γίνεται διαφανής και μπορεί να πετύχει τον στόχο της για την αντιμετώπιση του κινδύνου που αφορά τα προσωπικά δεδομένα.

Κατά την επιλογή των σχετικών ενδιαφερομένων μερών, το εύρος και η πολυπλοκότητα των προσωπικών δεδομένων θα είναι κρίσιμα. Σε ένα μεγάλο κυβερνητικό έργο μπορεί να εμπλέκεται σημαντικός αριθμός ενδιαφερομένων. Σε αυτή την περίπτωση, μπορεί να χρειαστεί να αναγνωριστούν κοινωνικές ομάδες συμφερόντων, όπως οι συνήγοροι των καταναλωτών, καθώς και ενδιαφερόμενοι που χειρίζονται προσωπικά δεδομένα και είναι εντολείς . Μικρότερες εμπορικές επιχειρήσεις επεξεργασίας, από την άλλη πλευρά, μπορεί να μην απαιτούν τόσο εκτεταμένο κατάλογο ενδιαφερομένων μερών.[49]

---

[48] Clarke, Roger, "Privacy Impact Assessment Guidelines", Xamax Consultancy Pty Ltd, February 1998. < http://www.xamax.com.au/DV/PIA.html> Accessed 30 December 2021

[49] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

5.4.2 Διαβούλευση με τα ενδιαφερόμενα μέρη

Παρόλο που η διαβούλευση αποτελεί κρίσιμο στοιχείο της DPIA, δεν χρειάζεται να αντιμετωπίζεται ως ξεχωριστό στάδιο. Η συμπερίληψη της διαβούλευσης σε όλα τα στάδια της διαδικασίας DPIA μπορεί να είναι επωφελής. Αυτό επιτρέπει στους οργανισμούς να ζητούν τη γνώμη των κατάλληλων ατόμων την κατάλληλη στιγμή, αποφεύγοντας την ανάγκη να αφιερώσουν πρόσθετο χρόνο και πόρους σε μια ξεχωριστή δραστηριότητα. Μπορεί να χρησιμοποιηθεί η διαβούλευση για να αναδειχθούν προβλήματα προστασίας των προσωπικών δεδομένων στους ιδιαίτερους τομείς ενδιαφέροντος και αρμοδιότητάς τους. Τους παρέχει επίσης την ευκαιρία να προτείνουν δράσεις για τη μείωση των κινδύνων.[50]

Δεν υπάρχει τυποποιημένη διαδικασία για τη διεξαγωγή μιας διαβούλευσης. Αυτή θα ποικίλλει ανάλογα με διάφορες περιστάσεις, συμπεριλαμβανομένου του μεγέθους του οργανισμού και του πεδίου εφαρμογής του έργου.

Όλες οι DPIA πρέπει να περιλαμβάνουν αποτελεσματική διαβούλευση με άτομα που ανήκουν στον ίδιο οργανισμό. Σε έργα που δεν έχουν συμπεριλάβει συζητήσεις με όσους κατασκευάζουν ένα σύστημα ή εκτελούν διαδικασίες, οι κίνδυνοι για την προστασία των δεδομένων είναι πιθανότερο να παραμείνουν αμείωτοι. Πέρα από την ομάδα που έχει αναλάβει το έργο και κατασκευάζει το σύστημα,σημαντική είναι και η επικοινωνία με τον Υπεύθυνο Προστασίας Δεδομένων(DPO),καθώς αυτός μπορεί να προσφέρει εξειδικευμένες γνώσεις για προβλήματα ιδιωτικότητας.[51]Άλλα παραδείγματα ατόμων του οργανισμού που μπορούν να βοηθήσουν είναι η ομάδα πληροφορικής που θα δώσει συμβουλές για την ασφάλεια πληροφοριών, η ομάδα που γνωρίζει τους καταναλωτές όπως και η ομάδα που φροντίζει για τον περιορισμό του κινδύνου προς τον οργανισμό. Η εσωτερική διαβούλευση μπορεί να είναι κάποιες απλές συζητήσεις μεταξύ υπαλλήλων του οργανισμού ή η ανταλλαγή κάποιων e-mail.Όμως σε κάποιες περιστάσεις εσωτερική διαβούλευση μπορεί να γίνει με επίσημες συνεδριάσεις με την συμμετοχή υψηλόβαθμων στελεχών του οργανισμού. Οι περισσότεροι εσωτερικοί ενδιαφερόμενοι θα συμμετέχουν ήδη σε κάποιο βαθμό στο έργο. Στόχος της DPIA είναι να τους επιστήσει την προσοχή στις ανησυχίες για την προστασία των προσωπικών δεδομένων.

Θα είναι ευκολότερο να προσδιοριστεί ένα σύνολο εσωτερικών ενδιαφερόμενων μερών εάν ένας οργανισμός έχει ήδη χαρακτηρίσει λεπτομερώς τις ροές πληροφοριών, αλλά

[50] Reuben Binns - Data protection impact assessments: a meta-regulatory approach International Data Privacy Law (2017) 7 (1): 22-35. DOI: https://doi.org/10.1093/idpl/ipw027 Published: 28 April 2017

[51] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

μπορεί να χρειαστεί να διεξάγει κάποιες προκαταρκτικές εσωτερικές διαβουλεύσεις προκειμένου να περιγράψει αρχικά τις ροές πληροφοριών.[52]

Εκτός από την διαβούλευση με άτομα του ίδιου οργανισμού, σημαντική είναι και η διαβούλευση με άτομα εκτός οργανισμού, που θα επηρεαστούν από το έργο που θα πραγματοποιήσει επεξεργασία δεδομένων . Αυτό μπορεί να περιλαμβάνει μέλη του κοινού καθώς και υπαλλήλους μιας άλλης εταιρείας. Υπάρχουν δύο πρωταρχικοί στόχοι. Κατ' αρχάς, δίνει τη δυνατότητα σε έναν οργανισμό να κατανοήσει τα ζητήματα αυτών των ατόμων. Ταυτόχρονα η διαβούλευση αυτή θα αυξήσει επίσης τη διαφάνεια, ενημερώνοντας τους ανθρώπους για τον τρόπο με τον οποίο χρησιμοποιούνται οι προσωπικές τους πληροφορίες. [53]Η επίσημη διαβούλευση χρησιμοποιείται συχνότερα στον δημόσιο τομέα και σε ορισμένες περιπτώσεις επιβάλλεται από τον νόμο.

Τα είδη των κινδύνων και ο αριθμός των ατόμων που επηρεάζονται θα καθορίσουν το εύρος της διαβούλευσης. Οι ομάδες χρηστών, οι δημόσιες συνεδριάσεις και οι επιτροπές καταναλωτών ή πολιτών αποτελούν παραδείγματα διαδικασιών διαβούλευσης που θα μπορούσαν να χρησιμοποιηθούν. Οι υπάρχουσες τεχνικές διαβούλευσης θα πρέπει να χρησιμοποιούνται όποτε είναι δυνατόν για την καλύτερη κατανόηση των προσδοκιών που έχουν αυτά τα άτομα για τα προσωπικά τους δεδομένα και τον απαραίτητο σεβασμό που απαιτείται για αυτά.

Τα άτομα θα πρέπει να έχουν τη δυνατότητα να επηρεάσουν πραγματικά το έργο μέσω της διαβούλευσης. Ένας οργανισμός θα πρέπει να κατανοήσει ποια στοιχεία του έργου επιδέχονται αλλαγές και ποια όχι. Κάθε δημόσια διαβούλευση που είναι ανοικτή στο ευρύ κοινό πρέπει να είναι γραμμένη με απλά λόγια που μπορούν να γίνουν κατανοητά. Ακόμη και αν δεν είναι δυνατή η ευρεία δημόσια διαβούλευση (για παράδειγμα, αν ένας ιδιωτικός οργανισμός ανησυχεί για την ευρεία κοινοποίηση εμπορικά ευαίσθητων πληροφοριών), είναι ζωτικής σημασίας η διεξαγωγή κάποιας μορφής στοχευμένης διαβούλευσης, όπως με ομάδες που εκπροσωπούν σχετικά τμήματα του πληθυσμού ή ομάδες που έχουν γνώσεις σε θέματα προστασίας των προσωπικών δεδομένων[54].

6.ΕΚΤΕΛΕΣΗ ΤΗΣ DPIA

[52] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

[53] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

[54] Guide to undertaking privacy impact assessments (PIA Guide) – Office of the Australian Information Commissioner Διαθέσιμο: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments [Πρόσβαση 28-12-2021]

6.1 Προσδιορισμός των ροών των προσωπικών δεδομένων

Αφού έχει αναπτυχθεί μια ευρεία περιγραφή της φύσης και του πεδίου εφαρμογής του έργου που περιλαμβάνει επεξεργασία δεδομένων, πρέπει να γίνει περιγραφή και χαρτογράφηση των ροών των προσωπικών δεδομένων του έργου. Η ανάλυση θα πρέπει να είναι αρκετά εμπεριστατωμένη ώστε να δείχνει ποιες πληροφορίες και δεδομένα θα συγκεντρωθούν, θα χρησιμοποιηθούν και θα δημοσιοποιηθούν, πώς θα αποθηκευτούν και θα προστατευθούν και ποιος θα έχει πρόσβαση σε αυτές.[55]

Αυτό είναι ένα κρίσιμο στάδιο σε κάθε διαδικασία DPIA. Μόνο αν κατανοήσει σε βάθος τον τρόπο με τον οποίο χρησιμοποιούνται οι πληροφορίες σε ένα έργο, μπορεί ένας οργανισμός να διενεργήσει ενδελεχή αξιολόγηση των ζητημάτων προστασίας των προσωπικών δεδομένων.[56] Η αβεβαιότητα σχετικά με τον τρόπο χρήσης των πληροφοριών μπορεί να αποτελέσει σημαντικό κίνδυνο για την προστασία της ιδιωτικότητας.[57] Για παράδειγμα, τα δεδομένα θα μπορούσαν να χρησιμοποιηθούν για ακατάλληλους σκοπούς ή να αποκαλυφθούν με ακατάλληλο τρόπο.

Για να γίνει κατάλληλος προσδιορισμός των ροών δεδομένων απαραίτητη είναι η επικοινωνία με άλλα μέλη της ομάδας και τους ενδιαφερόμενους φορείς του έργου .Αν γίνει χαρτογράφηση των ροών δεδομένων μεμονωμένα, υπάρχει κίνδυνος να γίνει παράβλεψη κρίσιμων πληροφοριών που εξηγούν το πως λειτουργεί η επεξεργασία και πως χειρίζονται τα δεδομένα .Αυτό μπορεί να οδηγήσει σε δυσκολίες στο μέλλον που είναι δύσκολο ή δαπανηρό να επιλυθούν.

Στο πλαίσιο της καταγραφής των ροών δεδομένων, ιδιαίτερα βοηθητικό είναι το αρχείο δραστηριοτήτων το οποίο υποχρεωτικά τηρεί ο υπεύθυνος επεξεργασίας(Άρθρο 30 ΓΚΠΔ[58]).Μέσα στο αρχείο δραστηριότητων υπάρχουν πληροφορίες όπως:

- Προσωπικά αναγνωριστικά και στοιχεία επικοινωνίας του υπευθύνου επεξεργασίας.
- Οι σκοποί της επεξεργασίας
- Κατηγορρίες των υποκειμένων των δεδομένων και κατηγοριών δεδομένων προσωπικού χαρακτήρα
- Κατηγορίες αποδεκτών οι οποίοι θα λάβουν τα δεδομένα προσωπικού χαρακτήρα.Περιλαμβάνονται οι αποδέκτες σε τρίτες χώρες η διεθνείς οργανισμούς.

---

[55] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[56] Stefan Strauß - Privacy and Identity in a Networked Society Refining Privacy Impact Assessment-Routledge (2019)

[57] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

[58] ''Κάθε υπεύθυνος επεξεργασίας και, κατά περίπτωση, ο εκπρόσωπός του, τηρεί αρχείο των δραστηριοτήτων επεξεργασίας για τις οποίες είναι υπεύθυνος.'' – Άρθρο 30 ΓΚΠΔ

- Διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα η διεθνή οργανισμό και τεκμηρίωση των κατάλληλων εγγυήσεων
- Τον χρόνο διατήρησης των δεδομένων προσωπικού χαρακτήρα
- Μια γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφαλείας που υπάρχουν στο άρθρο 32 παράγραφο 1 του ΓΚΠΔ.

Αυτό το βήμα της διαδικασίας DPIA μπορεί να συνδυαστεί με άλλες παρόμοιες ασκήσεις που έχουν ήδη ολοκληρωθεί. Πολλές εταιρείες πραγματοποιούν σήμερα ελέγχους πληροφοριών(IT Audits), δημιουργούν διαγράμματα ροών δεδομένων(data-flow diagrams) και χαρτογραφούν συμπεριφορές χρηστών ,καθώς και παρακολουθούν τα πληροφοριακά αγαθά τους.[59]Εάν μια εταιρεία έχει ήδη δημιουργήσει μια πρόταση έργου ή άλλο συγκρίσιμο έγγραφο, μπορεί να είναι χρήσιμο για τον καθορισμό του τρόπου με τον οποίο θα χρησιμοποιηθούν τα προσωπικά δεδομένα. Οι ροές πληροφοριών μπορούν να καταγραφούν με οποιοδήποτε τρόπο προτιμά ο οργανισμός (διάγραμμα ροής, μητρώο πληροφοριακών αγαθών(asset register), σύντομη περιγραφή του σχεδιασμού του έργου), και αυτό μπορεί στη συνέχεια να χρησιμοποιηθεί ως βασικό συστατικό της τελικής αναφοράς της DPIA.

Πιο συγκεκριμένα για την αναλυτική καταγραφή των ροών προσωπικών πληροφοριών σύμφωνα με την Αυστραλιανή Αρχή Προστασίας Προσωπικών Δεδομένων θα πρέπει να αναφερθούμε στα εξής[60]:

Αυθεντικοποίηση

Πρέπει να προσδιοριστούν:

- Ο βαθμός στον οποίο το έργο που περιλαμβάνει επεξεργασία δεδομένων μπορεί να υλοποιηθεί με τη χρήση ανώνυμων δεδομένων.
- Εάν είναι απαραίτητη η επαλήθευση της ταυτότητας και πως θα αυτή θα γίνει.
- Πως θα γίνει η επαλήθευση/αυθεντικοποίηση της ταυτότητας του υποκειμένου.
- Εάν θα παραχθεί κάποιο αναγνωριστικό ταυτοποίησης για το άτομο , τον λόγο για τον οποίο θα παραχθεί καθώς και αν θα χρησιμοποιηθεί αυτό το αναγνωριστικό για άλλους λόγους ή από άλλους οργανισμούς.

Συλλογή

Θα πρέπει να προσδιοριστούν και να καταγραφούν:

[59] Ο κώδικας πρακτικής PIA του ICO συνιστά να δημιουργηθούν αρχεία τις ροές πληροφοριών σε οποιαδήποτε μορφή,περιγραφές κειμένου, ή μοντέλα όπως διαγράμματα ροής .Ωστόσο, τα σχέδια αυτά δεν αναλύονται τεχνικά. Οι μεθοδολογίες CNIL και BSI(ISO 29134(περιγράφουν τις διαδικασίες (ροές πληροφοριών) μόνο γενικά.

[60] Guide to undertaking privacy impact assessments (PIA Guide) – Office of the Australian Information Commissioner(OAIC) Διαθέσιμο: <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments> [[Πρόσβαση 28-12-2021]

- Τα προσωπικά δεδομένα που πρόκειται να συλλεχθούν, συμπεριλαμβανομένων τυχόν ευαίσθητων προσωπικών δεδομένων.
- Πώς η συλλογή σχετίζεται με τις λειτουργίες ή τις δραστηριότητες του οργανισμού ή της οργάνωσης.
- Γιατί τα προσωπικά δεδομένα που συλλέγονται είναι απαραίτητα για το έργο που εκτελεί ο οργανισμός ή η εταιρεία,καθώς και αν επιτρέπεται από τον νόμο αυτή η συλλογή.
- Αν τα προσωπικά δεδομένα που συλλέγονται μπορούν να ανωνυμοποιηθούν ή να αποθηκευτούν χωρίς να είναι δυνατή η αναγνώριση συγκεκριμένων προσώπων.
- Εάν τα άτομα έχουν τη δυνατότητα να μην παρέχουν κάποια ή όλα τα προσωπικά τους δεδομένα.

Θα πρέπει να αναλυθεί:

- Πως θα συλλεχθούν τα προσωπικά δεδομένα(φόρμες,συναλλαγές, κλειστά κυκλώματα καμερών κλπ).
- Εάν προσωπικά δεδομένα που δεν ζητήθηκαν μπορούν να χρησιμοποιηθούν στο έργο
- Από πού θα συλλεχθούν οι πληροφορίες (για παράδειγμα, απευθείας από το άτομο, από άλλα άτομα ή οντότητες ή από δημόσια διαθέσιμες πηγές).
- Πόσο συχνά πρέπει να συλλέγονται οι προσωπικές πληροφορίες (μία μόνο φορά ή συνέχεια).
- Αν χρησιμοποιούνται μέθοδοι συλλογής που θα μπορούσαν να θεωρηθούν ευαίσθητες ή παρεμβατικές (για παράδειγμα, φωτογραφίες, δακτυλικά αποτυπώματα, δοκιμές ναρκωτικών ή συλλογή γενετικών δεδομένων).
- Οποιαδήποτε νομοθεσία ή άλλη αρχή στην οποία βασίζεται ο οργανισμός για τη συλλογή των πληροφοριών.

Χρήση

Θα πρέπει να προσδιοριστούν και να καταγραφούν:

- Όλες οι προβλεπόμενες χρήσεις των προσωπικών πληροφοριών, ακόμη και αν δεν πρόκειται να είναι συχνές.
- Πώς όλες αυτές οι χρήσεις σχετίζονται με το σκοπό της συλλογής.
- Αν υπάρχουν μέτρα για την αποτροπή χρήσεων για δευτερεύοντες σκοπούς ή για να διασφαλιστεί ότι τυχόν δευτερεύουσες χρήσεις επιτρέπονται σύμφωνα με το κανονιστικό πλαίσιο.

Σε περίπτωση που γίνεται χρήση προσωπικών δεδομένων για δευτερεύουσα χρήση πρέπει να περιγραφτεί :

- Εάν απαιτείται συναίνεση για τη δευτερεύουσα χρήση.
- Εάν η χρήση σχετίζεται ή συνδέεται άμεσα με το σκοπό της συλλογής.

- Εάν ένα άτομο μπορεί να αρνηθεί τη συγκατάθεση για δευτερεύουσες χρήσεις και να εξακολουθήσει να συμμετέχει στο έργο του οργανισμού(πρόγραμμα,λογισμικό κλπ).
- Τυχόν συνέπειες για τα άτομα που αρνούνται τη συγκατάθεση.

Σε περίπτωση που τα προσωπικά δεδομένα που συλλέγονται από τα υποκείμενα συνδυαστούν με άλλες λίστες προσωπικών δεδομένων[61], αυξάνεται ο κίνδυνος που υπάρχει όσον αφορά την ιδιωτικότητα.Πρέπει να προσδιοριστούν τα εξής:

- Οποιαδήποτε πρόθεση ή δυνατότητα αντιστοίχισης, συσχέτισης ή διασταύρωσης προσωπικών δεδομένων με δεδομένα που τηρούνται σε διαφορετικές βάσεις δεδομένων (από τον ίδιο οργανισμό ή από άλλους).
- Πως γίνεται η αντιστοίχιση, η σύνδεση ή η διασταύρωση δεδομένων.
- Ποιες διασφαλίσεις έχουν εφαρμοστεί για τον περιορισμό της ακατάλληλης πρόσβασης, χρήσης και αποκάλυψης των πληροφοριών.
- Ποιες διασφαλίσεις έχουν εφαρμοστεί για την ακεραιότητα των δεδομένων των υποκειμένων.

Δημοσιοποίηση

Θα πρέπει να προσδιοριστεί και περιγραφτεί:

- Σε ποιον, πώς και γιατί θα αποκαλυφθούν τα προσωπικά δεδομένα.
- Αν οι πληροφορίες που αποκαλύπτονται θα έχουν την ίδια προστασία σχετικά με τα προσωπικά δεδομένα αφού γίνει δημοσιοποίηση και κοινοποίηση τους.
- Εάν το άτομο θα ενημερωθεί για την δημοσιοποίηση και ποιες επιλογές έχει (όπως η απόκρυψη των προσωπικών δεδομένων του).
- Εάν η δημοσιοποίηση επιτρέπεται ή απαιτείται από το νόμο, και εάν ναι, ποιος νόμος.
- Εάν τα προσωπικά δεδομένα ενδέχεται να κοινοποιηθούν διασυνοριακά.

[61] ''Το Data Matching (Αντιστοίχιση δεδομένων) είναι το έργο του εντοπισμού, της αντιστοίχισης και της συγχώνευσης εγγραφών που αντιστοιχούν στις ίδιες οντότητες από διάφορες βάσεις δεδομένων ή ακόμη και εντός μιας βάσης δεδομένων. Με βάση την έρευνα σε διάφορους τομείς, όπως η εφαρμοσμένη στατιστική, η πληροφορική της υγείας, η εξόρυξη δεδομένων, η μηχανική μάθηση, η τεχνητή νοημοσύνη, η διαχείριση βάσεων δεδομένων και οι ψηφιακές βιβλιοθήκες, την τελευταία δεκαετία έχουν επιτευχθεί σημαντικές πρόοδοι σε όλες τις πτυχές της διαδικασίας αντιστοίχισης δεδομένων, ιδίως όσον αφορά τον τρόπο βελτίωσης της ακρίβειας της αντιστοίχισης δεδομένων και την επεκτασιμότητά της σε μεγάλες βάσεις δεδομένων. ''Data matching: concepts and techniques for record linkage, entity resolution, and duplicate detection''- Peter Christen - Springer-Verlag Berlin Heidelberg(2012)

Ακρίβεια των προσωπικών δεδομένων και πληροφοριών

Σημαντική είναι η καταγραφή των εξής:

- Ποιες θα είναι οι πιθανές επιπτώσεις για τα υποκείμενα των δεδομένων σε περίπτωση που τα δεδομένα είναι λανθασμένα ή δεν έχουν ενημερωθεί πρόσφατα, καθώς και τις τυχόν αποφάσεις που θα ληφθούν με αυτά τα λάθος δεδομένα.
- Ποιες είναι οι μέθοδοι ,πολιτικές και διαδικασίες που έχει ο οργανισμός σε εφαρμογή για να διασφαλίσει την χρήση μόνο επικαιροποιημένων και σωστών δεδομένων.

Ασφάλεια

Απαραίτητο είναι ο προσδιορισμός και η περιγραφή ολόκληρης της πληροφοριακής υποδομής του οργανισμού , το σύνολο των τηλεπικοινωνιών καθώς και τα μέτρα που αφορούν την φυσική ασφάλεια της πληροφοριακής υποδομής.[62] Πιο συγκεκριμένα:

- Ποιος θα έχει πρόσβαση στις βάσεις δεδομένων και έτσι και στα προσωπικά δεδομένα
- Ποιος θα δίνει τα δικαιώματα πρόσβασης των προσωπικών δεδομένων
- Ποιες υφιστάμενες δικλείδες ασφαλείας υπάρχουν ώστε να προστατευθούν τα προσωπικά δεδομένα από απώλεια,μη εξουσιοδοτημένη πρόσβαση, ,τροποποίηση, δημοσιοποίηση ή κακόβουλη χρήση γενικότερα.
- Τον τρόπο με τον οποίο θα μεταφέρονται τα προσωπικά δεδομένα αν χρειαστεί.
- Ποια μέτρα έχουν παρθεί για τον έγκυρο εντοπισμό συμβάντων σχετικά με παραβιάσεις προσωπικών δεδομένων.
- Ποια μέτρα θα ληφθούν για την αντιμετώπιση μιας παραβίασης προσωπικών δεδομένων.

Διατήρηση και Καταστροφή

Επίσης πρέπει να γίνει καταγραφή των εξής:

- Πως τα προσωπικά δεδομένα δεν θα μπορούν να χρησιμοποιηθούν για την ταυτοποίηση συγκεκριμένων ατόμων
- Τον τρόπο με τον οποίο θα γίνει η διαγραφή των προσωπικών δεδομένων και πως θα γίνει αυτό με ασφάλεια
- Αν υφίστανται πολιτικές και διαδικασίες για την διατήρηση και την διαγραφή των δεδομένων αυτών
- Αν συμμορφώνονται αυτές οι πολιτικές και διαδικασίες με την σχετική νομοθεσία

[62] Stefan Strauß - Privacy and Identity in a Networked Society Refining Privacy Impact Assessment-Routledge (2019)

Πρόσβαση και Διόρθωση

Τέλος πρέπει να γίνει περιγραφή των εξής σημείων:

- Πως μπορούν τα υποκείμενα των δεδομένων να αποκτήσουν πρόσβαση στα δεδομένα τους και με τι κόστος
- Τον τρόπο με τον οποίο μπορούν τα υποκείμενα να διορθώσουν τυχόν λανθασμένα προσωπικά δεδομένα
- Πως θα διαχειρίζονται τα αιτήματα των υποκειμένων περί πρόσβασης και διόρθωσης δεδομένων

6.2 Εκτίμηση του κινδύνου στην προστασία των προσωπικών δεδομένων

Μετά τον προσδιορισμό των ροών των προσωπικών δεδομένων , πρέπει να πραγματοποιηθεί μια εκτίμηση για τον κίνδυνο που θα έχει η επεξεργασία που εκτελεί το έργο του οργανισμού ή της εταιρείας.

Σύμφωνα με την CNIL[63] ο κίνδυνος είναι ''ένα υποθετικό σενάριο που περιγράφει πώς οι πηγές κινδύνου μπορούν να εκμεταλλευτούν ευπάθειες στα υποστηρικτικά αγαθά , στο πλαίσιο των απειλών και επιτρέπουν την εκδήλωση φοβούμενων γεγονότων στα προσωπικά δεδομένα , δημιουργώντας έτσι ένα αντίκτυπο στην ιδιωτικότητα των υποκειμένων των δεδομένων.''

Ο σκοπός της διαδικασίας εκτίμησης κινδύνου στην προστασία των προσωπικών δεδομένων είναι να προσδιοριστούν τα σενάρια που αποτελούν πηγές κινδύνου στην προστασία δεδομένων, να πραγματοποιηθεί μια εκτενής ανάλυση των κινδύνων αυτών, να εκτιμηθούν οι κίνδυνοι καθώς και το αντίκτυπο αυτών.

Μετά το τέλος της διαδικασίας αυτής, πρέπει να καθοριστεί αν το έργο που εκτελεί επεξεργασία προσωπικών δεδομένων έχει αποδεκτές ή μη αποδεκτές επιπτώσεις για την ιδιωτικότητα των υποκειμένων.Μέσα σε αυτήν την διαδικασία πρέπει να περιλαμβάνονται τυχόν αποτελέσματα διαβουλεύσεων με ενδιαφερόμενα μέρη ή του κοινού που μπορεί να βοηθήσει τον οργανισμό στην βελτίωση των αποτελεσμάτων του έργου όσον αφορά τα προσωπικά δεδομένα και την προστασία τους.Η διαδικασία θα πρέπει να λαμβάνει υπόψη το περιεχόμενο των πληροφοριών καθώς και το πλαίσιο στο οποίο συγκεντρώθηκαν. Παρόλο που μια αρνητική επίπτωση στην προστασία των προσωπικών δεδομένων μπορεί να μην φαίνεται σημαντική, είναι κρίσιμο να θεωρείται ότι ακόμη και μικρότερης σημασίας προσωπικά δεδομένα που διαχειρίζονται εσφαλμένα μπορούν να έχουν αρνητικές επιπτώσεις στην ιδιωτικότητα κάποιου με τρόπους που ο οργανισμός δεν είχε σκοπό. Αξίζει επίσης να σημειωθεί ότι ορισμένες

[63] Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) methodology" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf [Πρόσβαση 29-11-2021]

μορφές προσωπικών δεδομένων, όπως τα γενετικά δεδομένα, τα δεδομένα υγείας ή τα δεδομένα ποινικού μητρώου, είναι πιο ευαίσθητες από άλλες.

Προτεινόμενα βήματα για την εκτίμηση του κινδύνου στην προστασία των προσωπικών δεδομένων αναλύονται παρακάτω.

6.2.1 Προσδιορισμός των κινδύνων στα προσωπικά δεδομένα

Σε αυτό το βήμα πρέπει να αναγνωριστούν όλοι οι κίνδυνοι που αφορούν τα εμπλεκόμενα μέρη που πηγάζουν από την επεξεργασία που εκτελεί το έργο είτε αυτό είναι πρόγραμμα είτε πληροφοριακό σύστημα.

Ο οργανισμός πρέπει να κάνει χρήση εργαλείων και τεχνικών για τον εντοπισμό ζητημάτων προστασίας προσωπικών δεδομένων που είναι κατάλληλα για τους στόχους, τις δυνατότητες και τους κινδύνους που αντιμετωπίζει. Για να καταστεί δυνατός ο εντοπισμός των κινδύνων παραβίασης προσωπικών δεδομένων, θα πρέπει να χρησιμοποιούνται τα συγκεκριμένα νομοθετικά πρότυπα προστασίας προσωπικών δεδομένων της χώρας στην οποία δραστηριοποιείται ο οργανισμός. Αξίζει επίσης να σημειωθεί ότι, ακόμη και αν το έργο φαίνεται να συμμορφώνεται με τη νομοθεσία της εν λόγω χώρας για την προστασία των προσωπικών δεδομένων, μπορεί να χρειαστεί να αντιμετωπιστούν άλλοι κίνδυνοι για την προστασία των προσωπικών δεδομένων, όπως οι προσδοκίες που έχει η κοινότητα για τον οργανισμό[64].

Εσωτερικοί ανθρώπινοι παράγοντες (π.χ. εργαζόμενοι, χρήστες και τρίτοι που εμπλέκονται στην επεξεργασία), εξωτερικοί ανθρώπινοι παράγοντες (π.χ. πρώην εργαζόμενοι, επισκέπτες, τρίτοι που λαμβάνουν προσωπικές πληροφορίες, προσωπικό συντήρησης και εγκληματίες στον κυβερνοχώρο) και μη ανθρώπινες πηγές (π.χ. κακόβουλος κώδικας και φυσικές καταστροφές) αποτελούν όλες πιθανές πηγές κινδύνου.[65]

‘Άλλοι κίνδυνοι για τα προσωπικά δεδομένα αποτελούν:

- Μη εξουσιοδοτημένη/παράνομη πρόσβαση στα προσωπικά δεδομένα (απώλεια εμπιστευτικότητας).
- Μη εξουσιοδοτημένη/παράνομη τροποποίηση ή μορφοποίηση των προσωπικών δεδομένων (απώλεια ακεραιότητας).
- Απώλεια,κλοπή ή μη εξουσιοδοτημένη διαγραφή των προσωπικών δεδομένων (απώλεια διαθεσιμότητας).
- Εκτεταμένη συλλογή προσωπικών δεδομένων είτε γίνει σκόπιμα η όχι.

[64] Majed Alshammari and Andrew Simpson - Towards an Effective Privacy Impact and Risk Assessment Methodology: Risk Analysis – Springer (2018)

[65] Commission Nationale de l’Informatique et des Libertes (CNIL) (2018), “Privacy impact assessment (PIA) Knowledge Bases” Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases [Πρόσβαση 30-11-2021]

- Να μην είναι ξεκάθαροι οι λόγοι που σχετίζονται με τον σκοπό της επεξεργασίας δεδομένων (δηλώνει έλλειψη διαφάνειας όσον αφορά την επεξεργασία)
- Να γίνεται σύνδεση των προσωπικών δεδομένων με άλλες βάσεις προσωπικών δεδομένων χωρίς την συγκατάθεση των υποκειμένων ή χωρίς εξουσιοδότηση.
- Να πραγματοποιηθεί επεξεργασία προσωπικών δεδομένων χωρίς την γνώση του υποκειμένου(απώλεια δικαιώματος πρόσβασης).
- Να εκτελείται επεξεργασία προσωπικών δεδομένων χωρίς την συγκατάθεση των υποκειμένων (απώλεια δικαιώματος πρόσβασης).
- Διαμοιρασμός των προσωπικών δεδομένων σε τρίτα μέρη(και εκτός της χώρας που συλλέχθηκαν αρχικά τα δεδομένα) χωρίς την συγκατάθεση ή χωρίς να το γνωρίζουν τα υποκείμενα.
- Διατήρηση των προσωπικών δεδομένων για μεγάλο χρονικό διάστημα και αφού έχει ολοκληρωθεί ο σκοπός για τον οποίο συλλέχθηκαν τα δεδομένα αυτά.

Ο προσδιορισμός όλων των κινδύνων είναι μια προκλητική διαδικασία για κάθε οργανισμό.Καθοριστικό παράγοντα στην αποτελεσματική αναγνώριση των κινδύνων είναι ο οργανισμός να λαμβάνει πληροφορίες που αφορούν αυτούς τους κινδύνους από έγκυρες και ενημερωμένες πηγές.Μεγάλο ρόλο σε αυτό παίζει η συμμετοχή ατόμων που έχουν τις απαραίτητες γνώσεις στον προσδιορισμό και την καταγραφή κινδύνων.[66]Αφού γίνει αυτός ο προσδιορισμός , είναι ύψιστης σημασίας να εξεταστούν διάφορα σενάρια που καταδεικνύουν πιθανές επιπτώσεις για τα προσωπικά δεδομένα. Για παράδειγμα σενάρια στα οποία γίνεται κακή χρήση ή κατάχρηση του συστήματος επεξεργασίας καθώς και τεχνικά προβλήματα που μπορούν να προκύψουν κατά την επεξεργασία θα πρέπει να ληφθούν υπόψη όλα αυτά τα σενάρια.

Κατά τον εντοπισμό των κινδύνων που αφορούν την προστασία προσωπικών δεδομένων, ο υπεύθυνος για τη εκτέλεση της DPIA θα πρέπει να προσπαθεί να επιτύχει τη συνεργασία των ενδιαφερόμενων μερών, όποτε αυτό είναι δυνατόν.

6.2.2 Ανάλυση Κινδύνων Προσωπικών δεδομένων

Αφού γίνει η αναγνώριση των κινδύνων στα προσωπικά δεδομένα το επόμενο βήμα είναι να γίνει ανάλυση αυτών και συγκεκριμένα να αναλυθούν οι επιπτώσεις και οι

[66]Vemou, K. and Karyda, M. (2020), "Evaluating privacy impact assessment methods: guidelines and best practice", Information and Computer Security, Vol. 28 No. 1, pp. 35-53.Διαθέσιμο: https://doi.org/10.1108/ICS-04-2019-0047 και ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

απειλές[67] των κινδύνων που εντοπίστηκαν καθώς και να εκτιμηθούν τα επίπεδα της πιθανότητας να υπάρξουν αυτοί οι κίνδυνοι και το αντίκτυπο τους.

Η πλήρης επισκόπηση ενός προγράμματος, ενός συστήματος πληροφοριών ή διαδικασίας που εκτελεί επεξεργασία δεδομένων , καθώς και των αλλαγών στα παραπάνω, αποτελεί τη βάση για την ανάλυση κινδύνου. Η ανάλυση κινδύνου περιλαμβάνει τον προσδιορισμό όλων των προσωπικών δεδομένων και των αγαθών που ενδέχεται να διατρέχουν κίνδυνο, τις ευπάθειες που σχετίζονται με αυτά τα αγαθά, τις απειλές που ενδέχεται να εκμεταλλευτούν αυτές τις ευπάθειες, την πιθανότητα και τον αντίκτυπο που θα έχει αυτό το γεγονός, καθώς και τυχόν υφιστάμενους ελέγχους που ενδέχεται να επηρεάσουν τον κίνδυνο. Κατά τη διάρκεια της ανάλυσης κινδύνου, όλες οι παραδοχές θα πρέπει να τεκμηριώνονται προσεκτικά. Εάν έχουν αντίκτυπο στο υποκείμενο του οποίου ανήκουν τα προσωπικά δεδομένα, θα πρέπει να αναφέρονται οι πηγές τόσο εντός όσο και εκτός του ελέγχου του οργανισμού.

Οι αιτίες και οι πηγές του κινδύνου στα προσωπικά δεδομένα, καθώς και οι θετικές και αρνητικές επιπτώσεις των κινδύνων και η πιθανότητα να συμβούν αυτά τα αποτελέσματα, είναι παράγοντες που πρέπει να εξεταστούν κατά την ανάλυση του κινδύνου. Η ομάδα που εκτελεί την DPIA θα πρέπει να αναζητήσει παράγοντες που επηρεάζουν την πιθανότητα και τις συνέπειες του να γίνει μια παραβίαση προσωπικών δεδομένων. Ένα τέτοιο γεγονός μπορεί να έχει ποικίλα αποτελέσματα. Επιπρόσθετα, η υπεύθυνη για την DPIA ομάδα θα πρέπει να εξετάσει τους υφιστάμενους ελέγχους και την αποτελεσματικότητά τους προκειμένου να γινεί σωστά η ανάλυση των κινδύνων.

Σε περίπτωση που ένας κίνδυνος έχει μεγάλο αντίκτυπο ή υπάρχει μεγάλη πιθανότητα να συμβεί ,σημαντική είναι η περαιτέρω διερεύνηση του κινδύνου αυτού προκειμένου να ληφθούν τα απαραίτητα μέτρα προστασίας.

Μέσα στην ανάλυση των κινδύνων των προσωπικών δεδομένων πρέπει να γίνεται και η καταγραφή πιθανών απειλών. Επειδή ο κίνδυνος ορίζεται ως ένα ακούσιο συμβάν (όπως η μη εξουσιοδοτημένη απόκτηση, χρήση, αλλοίωση ή διάδοση προσωπικών δεδομένων) που οδηγεί σε παραβίαση της ιδιωτικότητας των υποκειμένων, πρέπει να λαμβάνονται υπόψη παραδείγματα τέτοιων πράξεων και να αποτελούν τη βάση της ανάλυσης. Για τη σύνταξη μια λίστας , οι υπεύθυνοι για την εκτέλεση της DPIA θα πρέπει να εξετάζουν απειλές που αφορούν τα προσωπικά δεδομένα από ποικίλες πηγές.[68]

Ταυτόχρονα πρέπει να προσδιορίζονται και τα σενάρια των απειλών.Εφόσον έχει επιτευχθεί ο προσδιορισμός των ροών δεδομένων , αρχίζουν και φανερώνονται σενάρια

---

[67] Απειλή σύμφωνα με τον ENISA είναι ''κάθε περίσταση ή γεγονός που μπορεί να επηρεάσει αρνητικά ένα αγαθό μέσω μη εξουσιοδοτημένης πρόσβασης, καταστροφής, αποκάλυψης, τροποποίησης δεδομένων ή/και άρνησης παροχής υπηρεσιών''.

[68] Πηγές : Daniel J.Solove – A Taxonomy of Privacy - University of Pennsylvania Law Review, Vol. 154, No. 3 (2006), pp. 477-564 και εκθέσεις του Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια [ENISA]) και τους αναγνωρισμένους στόχους προστασίας της ιδιωτικής ζωής του συστήματος, οι οποίοι, εάν αντιστραφούν, θα μπορούσαν να θεωρηθούν απειλές.

απειλών που μπορούν να προκαλέσουν ένα συμβάν το οποίο θα έχει αρνητική επίπτωση στην ιδιωτικότητα των υποκειμένων. Είναι κρίσιμο η ομάδα υπεύθυνη για την DPIA να διενεργεί εκτιμήσεις κινδύνου με βάση τις ροές δεδομένων και όχι το αντίστροφο.[69]Αφού αναγνωριστούν οι απειλές και τα σενάρια απειλών πρέπει έπειτα να συνδεθούν και με τα αγαθά που διαθέτει ο οργανισμός(λογισμικό,προγράμματα,πληροφοριακά συστήματα) τα οποία μπορούν να εκμεταλλευτούν λόγω τυχόν ευπαθειών που αυτά έχουν.Από την μελέτη των εξωτερικών συνεργατών του οργανισμού που ενδέχεται να έχουν κάποια δεδομένα ,μπορούν επίσης να προκύψουν σενάρια απειλών.[70]

Παρακάτω θα αναφέρουμε κάποιους από τους κινδύνους καθώς και τις απειλές που είναι πιθανό να αντιμετωπίσει ένας οργανισμός σύμφωνα με τον ISO[71] και την CNIL[72] :

1ος Κίνδυνος)Μη εξουσιοδοτημένη/παράνομη πρόσβαση στα προσωπικά δεδομένα

Εξαιτίας του όγκου και της ευαισθησίας των δεδομένων, η μη εξουσιοδοτημένη πρόσβαση μπορεί να προκαλέσει σημαντική ζημία στα υποκείμενα των δεδομένων, συμπεριλαμβανομένων διακρίσεων, ζημίας στη φήμη, οικονομικής απώλειας κ.ο.κ. Κάποιες απειλές είναι:

Αγαθά που επηρεάζονται	Απειλές και σενάρια απειλών
Υλικό(Ηλεκτρονικοί υπολογιστές,μέσα αποθήκευσης όπως USB,σκληροί δίσκοι κλπ)	Χρήση μέσων αποθήκευσης USB ή δίσκων που είναι ακατάλληλοι για την ευαισθησία των δεδομένων. Ένας επιτιθέμενος αποκτά παράνομα τα μέσα αποθήκευσης που περιέχουν τα ευαίσθητα προσωπικά δεδομένα.
Υλικό	Κλοπή ενός φορητού ηλεκτρονικού υπολογιστή ή ενός επαγγελματικού τηλεφώνου τα οποία μπορεί να έχουν πρόσβαση σε προσωπικά δεδομένα
Υλικό	Λανθασμένη διαδικασία διαγραφής ή των προσωπικών δεδομένων που μπορεί

[69] Vemou, K. and Karyda, M. (2020), "Evaluating privacy impact assessment methods: guidelines and best practice", Information and Computer Security, Vol. 28 No. 1, pp. 35-53.Διαθέσιμο: https://doi.org/10.1108/ICS-04-2019-0047

[70] Sourya Joyee De and Daniel Le M´etayer "A Refinement Approach for the Reuse of Privacy Risk Analysis Results "

[71] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[72] CN Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) Knowledge Bases" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases [Πρόσβαση 30-11-2021]

	να σημαίνει ότι κάποιος μπορεί να αποκτήσει πρόσβαση σε αυτά.
Λογισμικό	Κακή διαχείριση δικαιωμάτων στα πληροφοριακά συστήματα που σημαίνει ότι ένας κακόβουλος χρήστης μπορεί να έχει πρόσβαση σε προσωπικά δεδομένα.
Λογισμικό	Κυβερνοεπίθεση χρησιμοποιώντας κάποια ευπάθεια των πληροφοριακών συστημάτων ή του λογισμικού που χρησιμοποιεί ο οργανισμός
Δίκτυα Υπολογιστών	Επιθέσεις που δίνουν την δυνατότητα στον επιτιθέμενο να κρυφακούει κάποια επικοινωνία (man-in-the middle attacks)
'Άτομα	Επιθέσεις κοινωνικής μηχανικής(social engineering attacks). 'Ενας επιτιθέμενος στέλνει κάποιο phishing e-mail και το θύμα μοιράζεται προσωπικά δεδομένα
'Άτομα	Συγχώνευση εταιρειών με αποτέλεσμα να πάρουν ευαίσθητα προσωπικά δεδομένα οργανισμοί που μπορούν να τα χρησιμοποιήσουν με μη επιθυμητό τρόπο
Φυσικά 'Έγγραφα	Αν υπάρχουν φυσικά έγγραφα που περιέχουν προσωπικά δεδομένα μπορεί να γίνει αντιγραφή αυτών ή να φωτογραφηθούν.

Πίνακας 1:Απειλές και αγαθά που σχετίζονται με μη εξουσιοδοτημένη/παράνομη πρόσβαση

2ος Κίνδυνος) Ανεπιθύμητη αλλαγή δεδομένων

Η ανεπιθύμητη αλλαγή των δεδομένων προσωπικού χαρακτήρα αποτελεί και αυτή βασικό κίνδυνο για τα υποκείμενα των δεδομένων καθώς σε κάποιες περιπτώσεις (π.χ. αλλαγές σε δεδομένα υγείας) μπορούν να έχουν σημαντικό αντίκτυπο στην ζωή των ατόμων.Απειλές είναι:

Αγαθά που επηρεάζονται	Απειλές και σενάρια απειλών
Υλικό	Βλάβη υλικού μπορεί να προκαλέσει την ανεπιθύμητη τροποποίηση δεδομένων.
Λογισμικό	Ανεπιθύμητη τροποποίηση των δεδομένων στις βάσεις δεδομένων λόγω λαθών κατά την διαμόρφωση,ενημέρωση ή συντήρηση των λειτουργικών συστημάτων
Λογισμικό	Τυχόν σφάλματα λογισμικού κατά την ενημέρωση,διαμόρφωση ή συντήρηση λογισμικού και μόλυνση από κακόβουλο λογισμικό μπορεί να προκαλέσει αλλαγή

	στα αποθηκευμένα δεδομένα
Λογισμικό	Επιθέσεις υπερχείλισης στοίβας (Injection) [73]
Φυσικά Έγγραφα	Αντικατάσταση πρωτότυπου εγγράφου (χαρτί) με ένα πλαστό

Πίνακας 2:Απειλές και αγαθά που σχετίζονται με ανεπιθύμητη αλλαγή δεδομένων

3ος Κίνδυνος) Απώλεια δεδομένων προσωπικού χαρακτήρα

Η απώλεια των προσωπικών δεδομένων επηρεάζει την διαθεσιμότητα των δεδομένων αυτών. Σε πολλές περιπτώσεις αυτό έχει πολύ σημαντικές επιπτώσεις στο υποκείμενο των δεδομένων.Για παράδειγμα σε ψηφιακές έρευνες, η διαθεσιμότητα των δεδομένων πρέπει να είναι υψηλή, κατά προτίμηση 24 ώρες το 24ωρο, διαφορετικά η ποσότητα των αποδεικτικών στοιχείων που βρίσκονται στο ψηφιακό υλικό θα μειωθεί και ο χρόνος που απαιτείται για την εξιχνίαση μιας υπόθεσης θα αυξηθεί.[74]Κάποιες απειλές που οδηγούν στην απώλεια δεδομένων είναι:

Αγαθά που επηρεάζονται	Απειλές και σενάρια απειλών
Υλικό	Κλοπή ενός φορητού ηλεκτρονικού υπολογιστή ή ενός επαγγελματικού τηλεφώνου τα οποία μπορεί να έχουν πρόσβαση σε προσωπικά δεδομένα οδηγούν σε απώλεια δεδομένων
Υλικό	Πλημμύρες,πυρκαγίες,ζημιές από φυσική φθορά,δυσλειτουργία συσκευών μπορούν όλα να προκαλέσουν απώλεια δεδομένων
Υλικό	Αν είναι γεμάτη η μονάδα αποθηκεύσης ,αν γίνει κάποια διακοπή ρεύματος, αν υπερφορτωθεί ο επεξεργαστής των συστημάτων μπορεί να προκληθεί απώλεια δεδομένων.
Λογισμικό	Κατανεμημένες επιθέσεις άρνησης εξυπηρέτησης (DDoS Attacks)[75]

[73] Injection – Owasp (2021) https://owasp.org/Top10/A03_2021-Injection/

[74] H.M.A. van Beek, E.J. van Eijk, R.B. van Baar, M. Ugen, J.N.C. Bodde, A.J. Siemelink, Digital forensics as a service: Game on, Digital Investigation, Volume 15, 2015, Pages 20-38, https://doi.org/10.1016/j.diin.2015.07.004. Διαθέσιμο : (https://www.sciencedirect.com/science/article/pii/S1742287615000857) [Πρόσβαση 06-02-2022]

[75] CNIL 2017, '' Μια κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDoS) είναι μια κακόβουλη προσπάθεια να διακοπεί η κανονική κυκλοφορία ενός στοχευμένου διακομιστή, υπηρεσίας ή δικτύου, κατακλύζοντας τον στόχο ή την περιβάλλουσα υποδομή του με πλημμύρα

Λογισμικό	Τυχόν σφάλματα λογισμικού κατά την ενημέρωση,διαμόρφωση ή συντήρηση λογισμικού και μόλυνση από κακόβουλο λογισμικό μπορεί να προκαλέσει αλλαγή στα αποθηκευμένα δεδομένα
Λογισμικό	Επιθέσεις υπερχείλισης στοίβας (Injection)
Φυσικά Έγγραφα	Τα φυσικά έγγραφα μπορούν να χαθούν από άτομα ή να καταστραφούν είτε τυχαία είτε από παρέμβαση ενός κακόβουλου ατόμου

Πίνακας 3:Απειλές και αγαθά που σχετίζονται με απώλεια δεδομένων

Στην συνέχεια και αφού γίνει μελέτη των απειλών πρέπει να εκτιμηθεί η πιθανότητα των εν λόγω απειλών , έχοντας υπόψη τις ευπάθειες των αγαθών του οργανισμού,τις δυνατότητες που έχουν οι πηγές κινδύνου(δεξιότητες επιτιθέμενων, διαθέσιμος χρόνος, οικονομικοί πόροι, εγγύτητα στο σύστημα πληροφοριών, κίνητρα κλπ.) καθώς και τις υφιστάμενες δικλείδες ασφάλειας και ελέγχου προσωπικών δεδομένων που έχει ο οργανισμός.

Σύμφωνα με την CNIL[76],ISO[77],ENISA[78] συνιστάται μια κλίμακα τεσσάρων βαθμών.

1)Ασήμαντη/Μικρή πιθανότητα	Σε αυτό το επίπεδο η πραγματοποίηση μίας απειλής με την εκμέταλλευση ευπαθειών των αγαθών είναι σχεδόν ή εντελώς αδύνατη για τις επιλεγμένες πηγές κινδύνου.
2)Περιορισμένη πιθανότητα	Σε αυτό το επίπεδο η πραγματοποίηση μίας απειλής με την εκμετάλλευση ευπαθειών των αγαθών έιναι δύσκολη για τις επιλεγμένες πηγές κινδύνου.
3)Σημαντική πιθανότητα	Σε αυτό το επίπεδο η πραγματοποίηση μίας απειλής με την εκμετάλλευση ευπαθειών των αγαθών είναι δυνατή για τις επιλεγμένες πηγές κινδύνου.
4)Μέγιστη πιθανότητα	Σε αυτό το επίπεδο η πραγματοποίηση μίας απειλής με την εκμετάλλευση ευπαθειών των αγαθών είναι πολύ εύκολη για τις επιλεγμένες πηγές κινδύνου.

Πίνακας 4:Κλίμακα πιθανότητας απειλής

κυκλοφορίας στο Διαδίκτυο.''- Cloudflare – What is a DDoS attack Διαθέσιμο: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ [Πρόσβαση 06-02-2022]

[76] Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) template" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf [Πρόσβαση 29-11-2021]

[77] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[78] ENISA - Handbook on Security of Personal Data Processing (2017) Διαθέσιμο: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing [Πρόσβαση 20-04-2022]

Η τιμή του επιπέδου που ταιριάζει καλύτερα στις απειλές πρέπει να επιλεχθεί. Η πρόσβαση στο Διαδίκτυο, η ανταλλαγή δεδομένων με ξένες τοποθεσίες, οι διασυνδέσεις με άλλα πληροφοριακά συστήματα και ο υψηλός βαθμός μεταβλητότητας του συστήματος μπορεί να αυξήσουν την πιθανότητα. Αντίθετα, ένα ομοιογενές, σταθερό σύστημα χωρίς διασυνδέσεις και χωρίς πρόσβαση στο Διαδίκτυο μπορεί να μειώσει την πιθανότητα.

‘Έπειτα, αφού ολοκληρωθεί η εκτίμηση της πιθανότητας ενός κινδύνου πρέπει να πραγματοποιηθεί και η εκτίμηση του αντικτύπου του.Η ομάδα που είναι υπεύθυνη για την εκτέλεση της DPIA πρέπει να λάβει υπόψη της πολλούς παράγοντες που μπορούν να έχουν αντίκτυπο στην ιδιωτικότητα των υποκειμένων των προσωπικών δεδομένων.Για παράδειγμα ο εκνευρισμός ατόμων επειδή χρησιμοποιούνται λανθασμένα τα προσωπικά του δεδομένα είναι ένα πιθανό αντίκτυπο. Άλλο πιθανό αντίκτυπο θα μπορούσε να ήταν επιπλέον οικονομικά χρέη για ένα άτομο λόγω λανθασμένων προσωπικών δεδομένων.Η CNIL παρέχει μια λίστα από φυσικά,υλικά και ηθικά είδη αντίκτυπου.[79]

Είναι επίσης απαραίτητο να αναλυθούν οι επιπτώσεις στα άτομα και την κοινωνία στο σύνολό της. Παραδείγματα περιλαμβάνουν τη δυσπιστία των υποκειμένων των δεδομένων έναντι των κυβερνητικών υπηρεσιών και το αίσθημα ανασφάλειας μετά από μια παραβίαση δεδομένων, καθώς και την αλλαγή των εκλογικών αποτελεσμάτων.[80] Σε αυτό το στάδιο θα πρέπει να απευθυνθείτε σε επαγγελματίες σε θέματα κινδύνου, όπως ο DPO του οργανισμού, αλλά και οι ενδιαφερόμενοι φορείς μπορεί επίσης να είναι σε θέση να βοηθήσουν με τη γνώση πολλών παραγόντων επιπτώσεων.

Αν και το πιο σημαντικό είναι η προστασία της ιδιωτικότητας των ατόμων, πρέπει επίσης να προσδιοριστεί και να καταγραφεί το αντίκτυπο που θα έχει ο κίνδυνος της επεξεργασίας ή της παραβίασης των προσωπικών δεδομένων στον ίδιο το οργανισμό δηλαδή τον υπεύθυνο επεξεργασίας(π.χ. οικονομικά πρόστιμα, απώλεια φήμης κλπ.). Λαμβάνοντας υπόψη και αυτό τον παράγοντα ίσως επηρεάζεται η συνολική σοβαρότητα του κινδύνου καθώς και τα μέτρα προστασίας που θα ληφθούν.

Αυτή η εκτίμηση αντικτύπου είναι ιδιαίτερα χρήσιμη στις απαιτήσεις του ΓΚΠΔ και συγκεκριμένα στο άρθρο 33 [81]κατά το οποίο ο οργανισμός πρέπει να περιγράψει τις

---

[79] Commission Nationale de l’Informatique et des Libertes (CNIL) (2018), “Privacy impact assessment (PIA) Application to Connected Objects” Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf [Πρόσβαση 30-11-2021]

[80] Βικιπαίδεια(Wikipedia) - Σκάνδαλο δεδομένων Facebook-Cambridge Analytica Διαθέσιμο: https://el.wikipedia.org/wiki/Σκάνδαλο_δεδομένων_Facebook-Cambridge_Analytica [Πρόσβαση 05-03-2022]

[81] Άρθρο 33 παράγραφος 3 στοιχείο γ – ΓΚΠΔ: ‘’ περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα’’

πιθανές επιπτώσεις μια παραβίασης προσωπικών δεδομένων και στο άρθρο 34 κατά το οποίο ο οργανισμός πρέπει να περιγράψει ποια άτομα επηρεάζει η παραβίαση αυτή[82].

Επιπρόσθετα , μια κλίμακα ή τεχνική για την αξιολόγηση ενός περιστατικού παραβίασης προσωπικών δεδομένων θα πρέπει να λαμβάνει υπόψη τις κατηγορίες και το πλήθος των εκτεθειμένων δεδομένων, καθώς και το κατά πόσον η ζημία μπορεί να μετριαστεί ή όχι μέσω διορθωτικών ενεργειών. Για παράδειγμα, η σοβαρότητα μιας παραβίασης οικονομικών δεδομένων θα ήταν μεγαλύτερη εάν μπορεί να επιτρέψει την απάτη ή τη δημιουργία ενός οικονομικού προφίλ, σε αντίθεση με τη σοβαρότητα ενός περιστατικού κατά το οποίο αποκαλύπτονται γενικές οικονομικές πληροφορίες για ένα άτομο, όπως ότι είναι πελάτης μιας συγκεκριμένης τράπεζας. Επιπλέον, εάν ο αντίκτυπος μπορεί να μειωθεί με μικρή προσπάθεια, η σοβαρότητα θα μειωνόταν (π.χ. η ακύρωση και η έκδοση νέας πιστωτικής κάρτας απαιτεί λιγότερη προσπάθεια σε σύγκριση με ενέργειες για την αντιστροφή ενός οικονομικού προφίλ).

Όπως και με την εκτίμηση της πιθανότητας λοιπόν συνιστάται πάλι σύμφωνα με τις ίδιες μεθοδολογίες μια κλίμακα τεσσάρων βαθμών.

1)Ασήμαντο αντίκτυπο	Σε αυτό το επίπεδο το αντίκτυπο στα υποκείμενα των δεδομένων είναι πολύ μικρό και δεν θα αντιμετωπίσουν κάποια σημαντική δυσκολία.
2)Περιορισμένο αντίκτυπο	Σε αυτό το επίπεδο το αντίκτυπο στα υποκείμενα των δεδομένων θα αντιμετωπίσουν ένα μέτριο αντίκτυπο το οποίο θα μπορέσουν να ξεπεράσουν αντιμετωπίζοντας ορισμένες δυσκολίες (π.χ. παραπάνω χρηματικές επιβαρύνσεις,δυσκολίες πρόσβασης σε υπηρεσίες κλπ.)
3)Σημαντικό αντίκτυπο	Σε αυτό το επίπεδο τα υποκείμενα των δεδομένων θα αντιμετωπίσουν σοβαρές επιπτώσεις, τις οποίες θα μπορούν να ξεπεράσουν αντιμετωπίζοντας σημαντικές δυσκολίες (π.χ. απώλεια εργασίας λόγω λανθασμένης χρήσης δεδομένων/αξιολόγησης κλπ.)
4)Μέγιστο αντίκτυπο	Σε αυτό το επίπεδο τα υποκείμενα των δεδομένων βρίσκονται αντιμέτωπα με πολύ σημαντικές ή/και αξεπέραστες επιπτώσεις (π.χ. αδυναμία εύρεσης εργασίας κλπ.)

Πίνακας 4:Κλίμακα αντικτύπου απειλής

[82] Άρθρο 34 παράγραφος 1 – ΓΚΠΔ : '' [13].ταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων.''

Ο τρόπος με τον οποίο εκφράζονται και συνδυάζονται οι επιπτώσεις/αντίκτυπο και η πιθανότητα για τον προσδιορισμό ενός επιπέδου κινδύνου ποικίλλει ανάλογα με τον τύπο του κινδύνου προστασίας των προσωπικών δεδομένων, το επίπεδο που επηρεάζει τα υποκείμενα των δεδομένων καθώς και τον οργανισμό. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, η επιχείρηση/οργανισμός θα πρέπει να χρησιμοποιήσει τις διαθέσιμες πληροφορίες καθώς και τα αποτελέσματα της ανάλυσης κινδύνου προστασίας δεδομένων.

Επίσης ,ο υπεύθυνος για την εκτέλεση της DPIA είναι σημαντικό να έχει μια ολοκληρωμένη εικόνα για το επίπεδο των κινδύνων μετά την ανάλυση ώστε να μπορεί να μεταδώσει τις σχετικές πληροφορίες στα εμπλεκόμενα στην επεξεργασία δεδομένων μέρη αν χρειαστεί.Όπως σε όλα τα στάδια είναι απαραίτητο να γίνεται διαβούλευση με τα εμπλεκόμενα μέρη προκειμένου να εκτιμηθεί ο κίνδυνος.

Στις περισσότερες περιπτώσεις είναι πολύ πιο απλό να γίνει μια ποιοτική ανάλυση του κινδύνου ώστε να εξαχθεί ένα γενικό συμπέρασμα για το επίπεδο του κινδύνου που αντιμετωπίζει ο οργανισμός καθώς και τα σημεία στα οποία υστερεί περισσότερο όσον αφορά την προστασία των προσωπικών δεδομένων. Οι οργανισμοί πρέπει να σταθμίσουν το κόστος και τα οφέλη των διαφόρων επιλογών προστασίας της ιδιωτικότητας. Ορισμένα από αυτά τα κόστη ενδέχεται να είναι χρηματικά (π.χ. ένας οργανισμός είναι πιθανό να προμηθευτεί ένα καινούργιο λογισμικό προκειμένου να αποκτήσει μεγαλύτερο έλεγχο της πρόσβασης και της διατήρησης δεδομένων). Το κόστος μπορεί να σταθμιστεί σε σχέση με τα οφέλη, όπως η ενισχυμένη προστασία από παραβιάσεις δεδομένων και η μικρότερη πιθανότητα κανονιστικών μέτρων και ζημίας της φήμης.Αν ο οργανισμός διαθέτει τους απαραίτητους πόρους, συνιστάται μια λεπτομερή και ποσοτική αξιολόγηση των κινδύνων.

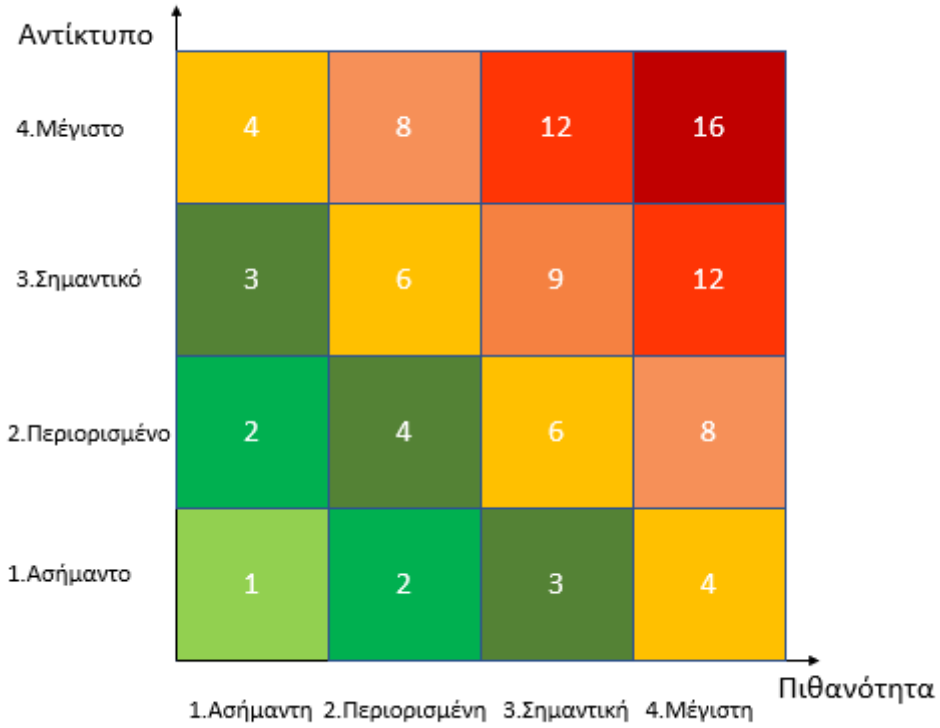
Η διαδικασία εκτίμησης του κινδύνου συνεπάγεται την απόδοση τιμών στις πιθανές επιπτώσεις (αντίκτυπο) και απειλές (πιθανότητα) ενός κινδύνου.

Κάθε οργανισμός θα πρέπει να χρησιμοποιήσει τα κατάλληλα εργαλεία και τις σωστές τεχνικές για την αξιολόγηση των κινδύνων προστασίας της ιδιωτικότητας ανάλογα με τους στόχους, τις δυνατότητες και τους κινδύνους του.Σε ορισμένες περιπτώσεις ίσως είναι πιο ευνοϊκό για τον οργανισμό να προχωρήσει ο ίδιος στην δημιουργία των εργαλείων και των τεχνικών αυτών. Για να επιτευχθεί αυτό,θα πρέπει να επεκταθούν ανάλογα οι προηγούμενες περιγραφές του έργου και οι ροές πληροφοριών. Αυτό θα επιτρέψει στους οργανισμούς να ακολουθήσουν μια μεθοδική και συνεπή στρατηγική.

6.2.3 Αξιολόγηση των κινδύνων

Προκειμένου να ολοκληρωθεί η εκτίμηση του κινδύνου για τα προσωπικά δεδομένα πρέπει να αξιολογηθούν οι κίνδυνοι που αναγνωρίστηκαν και αναλύθηκαν στα προηγούμενα βήματα.Όπως είπαμε θα αποδοθούν τιμές στο αντίκτυπο και στην πιθανότητα του κινδύνου.Σύμφωνα με τις περισσότερες μεθοδολογίες το επίπεδο

επικινδυνότητας που θα είναι και αυτό μια τιμή, προκύπτει από το γινόμενο των τιμών του αντίκτυπου και της πιθανότητας.[83]



Πίνακας 5:Παράδειγμα χάρτη επικινδυνότητας

Αφού εκτιμηθούν οι τιμές επικινδυνότητας, η σχετική προτεραιότητα του κινδύνου που αφορά την προστασία των προσωπικών δεδομένων πρέπει να καθοριστεί με βάση την σοβαρότητα του αντικτύπου στην ιδιωτικότητα των υποκειμένων των δεδομένων καθώς και του συνολικού αντικτύπου που έχει η επεξεργασία δεδομένων στον οργανισμό.Το βήμα του καθορισμού της προτεραιότητας στους αναγνωρισμένους κινδύνους είναι ιδιαίτερης σημασίας.Τα μέτρα προστασίας που μπορούν να χρειαστούν για να υπάρχει αποτελεσματική προστασία των προσωπικών δεδομένων ενδέχεται να απαιτούν περισσότερους πόρους από αυτούς που διατίθεται ο οργανισμός να διαθέσει.[84]Αν έχει καθοριστεί η προτεραιότητα μπορούν να καθοριστούν και οι ελάχιστες απαιτούμενες δικλείδες προστασίας.

---

[83] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication και Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) methodology" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf [Πρόσβαση 29-11-2021]

[84] Sourya Joyee De and Daniel Le M´etayer "A Refinement Approach for the Reuse of Privacy Risk Analysis Results "

Όπου είναι πρακτικό και σκόπιμο, οι αποφάσεις σχετικά με τον κίνδυνο θα πρέπει να λαμβάνουν υπόψη όλες τους σχετικούς παράγοντες, όπως της ανοχής των ενδιαφερομένων μερών στον κίνδυνο, συμπεριλαμβανομένου, μεταξύ άλλων, τα άτομα των οποίων τα προσωπικά δεδομένα επεξεργάζονται. Κατά τη λήψη αποφάσεων πρέπει να λαμβάνονται υπόψη νομικά, κανονιστικά και άλλα κριτήρια.

6.3 Διαδικασία αντιμετώπισης του κινδύνου

Αφού πραγματοποιηθεί πλήρως η εκτίμηση των κινδύνων που αντιμετωπίζει ο οργανισμός,πρέπει να καθοριστεί ο τρόπος που θα αντιμετωπιστούν αυτοί οι κίνδυνοι.

Σκοπός σε αυτό το στάδιο είναι να βρεθούν όλες οι επιλογές που έχει ο οργανισμός όσον αφορά την μείωση του κινδύνου,να γίνει αξιολόγηση της συμμόρφωσης που έχει ο οργανισμός,να προσδιοριστούν τα υφιστάμενα και μελλοντικά μέτρα προστασίας των προσωπικών δεδομένων καθώς και να δημιουργηθούν τα σχέδια που θα περιγράφουν πως θα εφαρμοστούν αυτά τα μέτρα και πως μετριάσουν τους κινδύνους. Τόσο ο DPO όσο και ο υπεύθυνος ασφάλειας πληροφοριών του οργανισμού(CISO) θα πρέπει να συμμετέχουν σε αυτό το στάδιο που εκτελεί η ομάδα της DPIA.

6.3.1 Προσδιορισμός επιλογών αντιμετώπισης κινδύνου

Η εύρεση της σωστής επιλογής αποτελεί ένα δύσκολο κομμάτι της γενικής διαδικασίας αντιμετώπισης του κινδύνου.Προκειμένου να βρεθούν οι βέλτιστες επιλογές, πρέπει να ληφθούν υπόψη όχι μόνο οι υποχρεώσεις που έχει ο οργανισμός που πραγματοποιεί την επεξεργασία δεδομένων απέναντι στα υποκείμενα των δεδομένων αυτών αλλά και το κόστος που θα έχει ο οργανισμός για να εφαρμόσει τα σωστά προστατευτικά μέτρα.[85] Οι επιλογές μείωσης κινδύνου μπορεί να είναι ποικίλες και αυτό εξαρτάται από τις δραστηριότητες επεξεργασίας του οργανισμού και τα υφιστάμενα μέτρα προστασίας.Αυτές οι επιλογές μπορούν να περιλαμβάνουν ακόμα και τον ανασχεδιασμό των εφαρμογών ή των συστημάτων που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

Μετά από την αξιολόγηση των κινδύνων ενδέχεται να αποφασίσει τελικά ο οργανισμός να μην χρειαστεί παραπάνω μέτρα προκειμένου να μειωθεί ο κίνδυνος. Ο οργανισμός θα πάρει την απόφαση αυτή αφού ορίσει το επίπεδο κινδύνου που θεωρεί αποδεκτό.[86]Ο

[85] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[86] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

ορισμός του επιπέδου κινδύνου καθώς και οι επιλογές μείωσης κινδύνου είναι προτιμότερο να γίνουν μετά από διαβουλεύσεις με τα ενδιαφερόμενα μέρη, όπου αυτό είναι εφικτό.

Ο οργανισμός θα πρέπει να λαμβάνει υπόψη του τις αξίες και τις απόψεις των ενδιαφερομένων μερών, καθώς και τους καλύτερους τρόπους επικοινωνίας μαζί τους, ενώ αποφασίζει για τις επιλογές αντιμετώπισης των κινδύνων. Όταν οι λύσεις μείωσης του κινδύνου της ιδιωτικότητας έχουν τη δυνατότητα να επηρεάσουν τον κίνδυνο αυτό σε κάποιο άλλο σημείο της εταιρείας, θα πρέπει να εξετάζονται οι τομείς αυτοί.Ορισμένες επιλογές μείωσης κινδύνου μπορεί να είναι περισσότερο αποδεκτές από τα ενδιαφερόμενα μέρη από άλλες, παρά το γεγονός ότι και οι δύο είναι εξίσου αποτελεσματικές.

Επιπλέον,στο στάδιο εύρεσης επιλογών, καθώς υπάρχει η πιθανότητα οι πόροι που έχει διαθέσιμους ο οργανισμός μπορεί να είναι περιορισμένοι , είναι σημαντικό να καθοριστεί η προτεραιότητα με την οποία θα εφαρμοστούν οι λύσεις για την προστασία της ιδιωτικότητας.

Κατά την διάρκεια της διαδικασίας αντιμετώπισης κινδύνου, η ίδια η διαδικασία μπορεί να προκαλέσει κινδύνους στην ιδιωτικότητα οι οποίοι πρέπει να εκτιμηθούν και να επιλυθούν.Ένας σημαντικός κίνδυνος που ενδέχεται να προκύψει είναι η αδυναμία των μέτρων προστασίας των δεδομένων προσωπικού χαρακτήρα που θα ληφθούν.Αυτός ο κίνδυνος πρέπει να συμπεριληφθεί στο γενικό σχέδιο απομείωσης κινδύνου.

Ο ISO [87]συνιστά 4 επιλογές τις οποίες έχει διαθέσιμες ένας οργανισμός για να αντιμετωπίσει τους κινδύνους που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα: 1) Απομείωση κινδύνου 2)αποφυγή κινδύνου 3)Διατήρηση κινδύνου 4)Μεταφορά κινδύνου

1)Απομείωση Κινδύνου

Η απομείωση κινδύνου αποτελεί μια επιλογή η οποία μπορεί να επιτευχθεί μέσω της εφαρμογής των κατάλληλων μέτρων προστασίας.Μετά από την εφαρμογή μέτρων προστασίας ,εάν κριθεί ότι υπάρχει εναπομείναντας κίνδυνος ,πρέπει να καθοριστεί αν αυτός ο κίνδυνος είναι αποδεκτός από τον οργανισμό και δεν θα προβεί στην προσθήκη επιπλέον μέτρων προστασίας ή αν θα χρειαστεί να πραγματοποιήσει αυτήν την ενέργεια.

[87] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

Οι οργανισμοί θέλουν σε κάθε περίπτωση να εξασφαλίσουν τα μέγιστα δυνατά οφέλη από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.[88]Ωστόσο,ο οργανισμός δεν μπορεί να ακολουθήσει μια προσέγγιση στην οποία δεν μειώνουν σημαντικά τον κίνδυνο ακόμα και αν πρόκειται για μικρή ομάδα ατόμων καθώς η επεξεργασία αφορά ανθρώπινα δικαίωματα.[89] Έτσι, στην προσπάθεια των οργανισμών να μειώσουν τον κίνδυνο ενδέχεται να περιοριστούν και τα οφέλη αυτά καθώς πολλά από τα μέτρα προστασίας εμποδίζουν την αποτελεσματική επεξεργασία δεδομένων.Η απόφαση να προστεθούν πολλά ή λίγα μέτρα προστασίας πρέπει να ληφθεί αφού ζυγιστούν τα οφέλη και τα μειονέκτηματα.Ταυτόχρονα μπορεί να δοθεί προτεραίοτητα σε κάποια μέτρα που προσφέρουν την μεγαλύτερη προστασία για τα υποκείμενα των δεδομένων σύμφωνα με τους κανονισμούς και αναλόγως τον κίνδυνο που προσπαθούν να μειώσουν.[90]

Υπάρχουν πολλά προστατευτικά μέτρα τα οποία μπορούν να χρησιμοποιηθούν για την μείωση του κινδύνου.Μεταξύ άλλων:

- Διαμόρφωση των συστημάτων που επεξεργάζονται τα δεδομένα είτε αποτρέποντας κάποιο είδος επεξεργασίας,είτε διορθώνοντας κάποια επεξεργασία που επεξεργάζεται λάθος τα δεδομένα προσωπικού χαρακτήρα είτε κάποια άλλη διαμόρφωση.
- Τροποποίηση των κατηγοριών των προσωπικών δεδομένων που πρόκειται να επεξεργαστούν.[91]
- Αλλαγή στις πολιτικές δεδομένων και διαδικασίες του οργανισμού.
- Εκπαίδευση και ενημέρωση του προσωπικού του οργανισμού όσον αφορά την προστασία των προσωπικών δεδομένων.[92]

2)Αποφυγή κινδύνου

Η δεύτερη επιλογή που είναι διαθέσιμη στον οργανισμό είναι αυτή της αποφυγής κινδύνου.Ο οργανισμός,μετά την διαδικασία εκτίμησης κινδύνου μπορεί τελικά να αποφασίσει να διακόψει πλήρως την επεξεργασία προσωπικών δεδομένων ή να την αλλάξει σημαντικά καθώς αναδείχθηκε υψηλός κίνδυνος ο οποίος δεν είναι αποδεκτός.

---

[88] David Wright – The state of the art in privacy impact assessment – Elsevier (2012)

[89] A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation -Felix Bieker , Michael Friedewald , Marit Hansen, Hannah Obersteller, and Martin Rost – Springer (2016)

[90] A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation -Felix Bieker , Michael Friedewald , Marit Hansen, Hannah Obersteller, and Martin Rost – Springer (2016)

[91] Office of the Australian Information Commissioner - Part 3: Responding to data breaches — four key steps Διαθέσιμο: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps [Πρόσβαση 08-04-2022]

[92] Why you need Privacy Awareness Training- Information Managers Διαθέσιμο : https://informationmanagers.ca/privacy-awareness-training/ [Πρόσβαση 10-02-2022]

3)Διατήρηση κινδύνου

Ο οργανισμός θα επιλέξει την ενέργεια της διατήρησης κινδύνου σε περίπτωση που ,μετά από την εκτίμηση κινδύνου , θεωρήσει ότι ο κίνδυνος αυτός είναι αποδεκτός για τον σκοπό της επεξεργασίας και δεν χρειάζεται να προβεί σε προσθήκη μέτρων προστασίας.

4)Μεταφορά Κινδύνου

Ο οργανισμός που θα διαλέξει την μεταφορά κινδύνου για να αντιμετωπίσει τον κίνδυνο της επεξεργασίας δεδομένων θα χρειαστεί την συμβολή ενός τρίτου,εξωτερικού συνεργάτη.Μέσω της συνεργασίας με έναν τρίτο μπορεί ο οργανισμός να αποκτήσει ασφάλεια όσον αφορά την επεξεργασία δεδομένων.Επιπλέον ,η ασφάλεια των πληροφοριακών συστημάτων που κάνουν την επεξεργασία μπορεί να ανατεθεί στον εξωτερικό συνεργάτη.

6.4 Αξιολόγηση Συμμόρφωσης και Μέτρων Προστασίας και καθορισμός νέων μέτρων

Όπως αναφέρεται και στο άρθρο 35 παράγραφος 7 στοιχείο δ) του ΓΚΠΔ[93], η DPIA πρέπει να περιλαμβάνει δικλείδες ασφαλείας και μέτρα προστασίας που θα εξασφαλίζουν την προστασία των δεδομένων προσωπικού χαρακτήρα προκειμένου να μετριαστούν οι κίνδυνοι που εντοπίστηκαν,καθώς και να αποδεικνύει την συμμόρφωση του με τον ΓΚΠΔ στο σύνολο του,όπως έχει αναφερθεί παραπάνω.

Θα πρέπει να γίνει λοιπόν αρχικά , μια εκτίμηση των μέτρων που εξασφαλίζουν την αναγκαιότητα και την αναλογικότητα της επεξεργασίας.Συγκεκριμένα θα είναι μέτρα που αφορούν τις εξής απαιτήσεις:

1)Σκοπό επεξεργασίας, ο οποίος πρέπει να είναι ξεκάθαρος και νόμιμος.[94]

2)Βάση επεξεργασίας η οποία θα αποδεικνύει την νομιμότητα.[95]

3)Ελαχιστοποίηση Δεδομένων ώστε να είναι περιορισμένα και σχετικά με την επεξεργασία.[96]

4)Ποιότητα των Δεδομένων ώστε να είναι ακριβή και ενημερωμένα.[97]

5)Χρόνοι διατήρησης δεδομένων ώστε να είναι περιορισμένοι.[98]

---

[93]" Τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων…. των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.'' – Άρθρο 35 παράγραφος 7 στοιχείο δ ΓΚΠΔ

[94] Άρθρο 5 Παράγραφος 1 Στοιχείο Β - ΓΚΠΔ

[95] Άρθρο 6 ΓΚΠΔ

[96] 'Αρθρο 5 στοιχείο γ -ΓΚΠΔ

[97] 'Αρθρο 5 στοιχείο ε -ΓΚΠΔ

Μέτρα θα πρέπει να υπάρχουν και για τις απαιτήσεις προστασίας των δικαιωμάτων των υποκειμένων των δεδομένων όπως:

1)Παροχή πληροφοριών στα υποκείμενα των δεδομένων (για την δίκαιη επεξεργασία των δεδομένων τους).[99]

2)Απόκτηση συγκατάθεσης.[100]

3)Δικαίωμα πρόσβασης και φορητότητας των δεδομένων.[101]

4)Δικαίωμα διόρθωσης και διαγραφής.[102]

5)Δικαίωμα περιορισμού επεξεργασίας και εναντίωσης.[103]

6)Όσον αφορά τους εκτελούντες την επεξεργασία να υπάρχουν σχετικές συμβάσεις.[104]

7)Όσον αφορά τις διαβιβάσεις εκτός Ευρωπαϊκής Ένωσης να υπάρχουν σχετικά μέτρα προστασίας.[105]

Υπάρχουν διάφορα μέτρα προστασίας που μπορούν να εφαρμοστούν ανάλογα πάντα με τον οργανισμό και την φύση της επεξεργασίας.Τεχνικά και οργανωτικά μέτρα αποτελούν μια λύση σε αρκετά προβλήματα προστασίας δεδομένων.[106]Παράλληλα η εφαρμογή συγκεκριμένων πολιτικών που αποσκοπούν σε αυτήν την προστασία είναι άλλη μία λύση.Επιπλέον υπάρχουν τεχνολογίες ενίσχυσης ιδιωτικότητας(Privacy-Enhancing Technologies- PETs) που μπορούν να εφαρμοστούν. Τα PETs είναι κυρίως τεχνολογίες κρυπτογράφησης,τείχη προστασίας (firewalls), διαφορετικές επικοινωνίες δρομολόγησης και άλλα εργαλεία που έχουν σκοπό την καλύτερη προστασία του συστήματος από άποψη κυβερνοασφάλειας και προσωπικών δεδομένων.[107]

Εφόσον πρέπει να εξεταστούν διαφορετικά μέτρα ελέγχου η CNIL[108] προτείνει τα εξής βήματα:Πρώτα,πρέπει να αναγνωριστούν τα ήδη υπάρχοντα μέτρα προστασίας που διαθέτει ο οργανισμός ή που πρόκειται να υλοποιήσει στο εγγύς μέλλον.Πιο συγκεκριμένα,μέτρα που αφορούν τον τρόπο επεξεργασίας πρέπει να εξεταστούν όπως κρυπτογράφηση ,ανωνυμοποίηση, έλεγχος πρόσβασης κλπ.. Έπειτα πρέπει να μελετηθεί ο τρόπος που γίνεται η διακυβέρνηση της ασφάλειας πληροφοριών(οργανωτικά μέτρα όπως πολιτικές,διαχείριση ανθρώπινων και πληροφοριακών

---

[98] 'Αρθρο 5 στοιχείο ε- ΓΚΠΔ
[99] 'Αρθρο 12,13,14 - ΓΚΠΔ
[100] 'Αρθρο 7,8 -ΓΚΠΔ
[101] 'Αρθρο 15 και 20 - ΓΚΠΔ
[102] 'Αρθρο 16 και 17 - ΓΚΠΔ
[103] 'Αρθρο 18 και 21 - ΓΚΠΔ
[104] 'Αρθρο 28 - ΓΚΠΔ
[105] 'Αρθρο 44 και 49 - ΓΚΠΔ
[106] Όπως ISO 27001
[107] Van Blarkom GW, Borking JJ, Olk JGE (eds.) (2003) The handbook of privacy and privacyenhancing technologies: the case of intelligent software agents.The Hague, Hes R, Borking J (eds) (2000) Privacy-enhancing technologies: the path to anonymity
[108] cnil-pia-1-en-methodology.pdf

πόρων,διαχείριση παραβιάσεων,διαχείριση σχέσεων με τρίτους κλπ).Στην συνέχεια πρέπει να εξεταστούν τα γενικά μέτρα προστασίας που αφορούν το σύστημα που εκτελεί την επεξεργασία όπως μέτρα που περιορίζουν το αντίκτυπο ενός κινδύνου (π.χ. αντίγραφα ασφάλειας) και μέτρα που αποτρέπουν την πραγματοποίηση των κινδύνων (ασφάλεια λογισμικού και υλικού, εργαλεία logging κλπ). Τέλος, θα πρέπει να εξεταστεί το επίπεδο των υποστηρικτικών αγαθών , τόσο όσον αφορά τους ελέγχους για τον μετριασμό των ευπαθειών όσο και την παρακολούθηση για τον εντοπισμό των απειλών(monitoring).

Προκειμένου να γίνει ευκολότερος ο προσδιορισμός των υπαρχόντων μέτρων και η αξιολόγηση της συμμόρφωσης που έχει ο οργανισμός καθώς και αργότερα να διευκολυνθεί η διαδικασία προσθήκης μέτρων, ο ISO προτείνει να γίνει η εξέταση αυτή με κριτήριο την ικανοποίηση απαιτήσεων κάποιων βασικών αρχών ιδιωτικότητας.[109]Ταυτόχρονα αυτά τα μέτρα πρέπει να συγκριθούν με άλλα μέτρα που προτείνουν διεθνή πρότυπα.[110].Αφού προσδιοριστούν τα υπάρχοντα μέτρα πρέπει να γίνει προσθήκη επιπλέον μέτρων μέχρι να γίνει αποδεκτός ο συνολικός κίνδυνος για τον οργανισμό.

Παρακάτω θα αναφερθούμε τις αρχές ιδιωτικότητας που προτείνει ο ISO[111],ο οργανισμός ιδιωτικότητας της Νέας Ζηλανδίας[112] και Αυστραλίας[113]:

1η Αρχή)Συλλογή πληροφοριών και ελαχιστοποίηση της συλλογής αυτής

Η πιο αποτελεσματική μέθοδος προστασίας δεδομένων είναι να μην συλλέγονται τα δεδομένα αν αυτά δεν χρειάζονται.[114]Οι οργανισμοί δεν πρέπει να συλλέγουν δεδομένα προσωπικού χαρακτήρα αδιακρίτως. Από την αρχή οι οργανισμοί οφείλουν να είναι ξεκάθαροι όσον αφορά τον λόγο που χρειάζονται τα δεδομένα, ποια άτομα θα έχουν πρόσβαση σε αυτά τα δεδομένα και πως θα τα χρησιμοποιήσουν κατάλληλα. Η ποσότητα και το είδος των συλλεγόμενων δεδομένων προσωπικού χαρακτήρα θα πρέπει να περιορίζονται σε αυτά που απαιτούνται για την επίτευξη του νόμιμου σκοπού που έχει τεθεί από τον υπεύθυνο επεξεργασίας. Πριν ξεκινήσουν τη συλλογή

[109] ISO/IEC 29100 (2011) – Information technology – Security Techniques – Privacy framework

[110] Για παράδειγμα ISO 29151,CNIL και ENISA - Handbook on Security of Personal Data Processing (2017) Διαθέσιμο: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing [Πρόσβαση 20-04-2022]

[111] ISO/IEC 29100 (2011) - Privacy framework

[112] Office of the Privacy Commissioner,2015 Privacy Impact Assessment Toolkit – Part 2 How to do a Privacy Impact Assessment Διαθέσιμο: https://privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Impact-Assessment-Part-2-FA.pdf [Πρόσβαση 03-03-2022]

[113] Guide to undertaking privacy impact assessments (PIA Guide) – Office of the Australian Information Commissioner(OAIC) Διαθέσιμο: <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments> [[Πρόσβαση 28-12-2021]

[114] Office of the Privacy Commissioner,2015 Privacy Impact Assessment Toolkit – Part 2 How to do a Privacy Impact Assessment Διαθέσιμο: https://privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Impact-Assessment-Part-2-FA.pdf [Πρόσβαση 03-03-2022]

προσωπικών δεδομένων, οι οργανισμοί θα πρέπει να εξετάζουν προσεκτικά ποια δεδομένα θα απαιτηθούν για την επίτευξη ενός συγκεκριμένου στόχου.[115]Για την εξασφάλιση αυτής της αρχής πρέπει να πραγματοποιούνται τα εξής:

- Ελαχιστοποίηση συλλογής προσωπικών δεδομένων στα απολύτως απαραίτητα.
- Προσδιορισμός και τεκμηρίωση με σαφήνεια των σκοπών συλλογής πληροφοριών και γνωστοποίηση των σκοπών αυτών στα εμπλεκόμενα μέρη της επεξεργασίας.
- Χρήση πληροφοριών που δεν είναι αρκετές για την ταυτοποίηση ατόμων.
- Περιορισμός συλλογής πληροφοριών που συλλέγονται μη έμμεσα από το υποκείμενο των δεδομένων (vlogs ιστοτόπου, συστήματος)

Για την ελαχιστοποίηση των πληροφοριών που συλλέγονται ο οργανισμός μπορεί να προχωρήσει στις εξής ενέργειες/μέτρα:

- Για την παρακολούθηση τον αριθμό των επισκεπτών σε μια ιστοσελίδα ,μπορεί να γίνει η καταμέτρηση αυτή χωρίς να κρατιούνται οι διευθύνσεις IP των των επισκεπτών.[116]
- Παραμετροποίηση των πληροφοριακών συστημάτων έτσι ώστε να μην αποθηκεύονται στις βάσεις δεδομένων , περιττές πληροφορίες.
- Τα ηλεκτρονικά έντυπα που συμπληρώνουν οι επισκέπτες να ζητάνε μόνο απαραίτητες πληροφορίες.
- Να γίνεται καταγραφή εικόνων ή βίντεο μόνο όταν υπάρχει πιθανό ζήτημα ασφάλειας και να διαγράφονται εγκαίρως αυτές οι εικόνες και βίντεο.
- Να ενημερώνεται σωστά ο επισκέπτης όταν του δίνεται η δυνατότητα να παρέχει προαιρετικές πληροφορίες και να υπάρχει εξήγηση των συνεπειών σε περίπτωση που δεν δοθούν αυτές οι πληροφορίες.

2η Αρχή) Συγκατάθεση και επιλογή του χρήστη

Η τήρηση της αρχής της συγκατάθεσης περιλαμβάνει την παρουσίαση στο υποκείμενο των δεδομένων της επιλογής του να επιτρέψει ή όχι την επεξεργασία των προσωπικών του δεδομένων , εκτός αν επιτρέπει ρητά η νομοθεσία την επεξεργασία των δεδομένων χωρίς την συγκατάθεση του υποκειμένου.Επίσης η επιλογή του υποκειμένου πρέπει να γίνεται ελεύθερα,αφού έχει προηγηθεί η ενημέρωση του αναφορικά με τα δικαιώματα του και για τον τρόπο με τον οποίο θα επεξεργαστούν τα δεδομένα του.Η ενημέρωση αυτή πρέπει να γίνεται με πλήρης διαφάνεια και ταυτόχρονα πρέπει να γνωστοποιηθούν στα υποκείμενα οι επιπτώσεις της συγκατάθεσης ή της άρνησης.

---

[115] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[116] Office of the Privacy Commissioner,2015 Privacy Impact Assessment Toolkit – Part 2 How to do a Privacy Impact Assessment Διαθέσιμο: https://privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Impact-Assessment-Part-2-FA.pdf [Πρόσβαση 03-03-2022]

Ο οργανισμός πρέπει να έχει τα εξής μέτρα:

- Καθορισμός των πρακτικών τρόπων με τους οποίους θα δίνει την συγκατάθεση του,το υποκείμενο των δεδομένων.Οι τρόποι αυτοί πρέπει να επανεξετάζονται και να αναθεωρούνται σε περίπτωση που δεν είναι λειτουργικοί, για να διασφαλίζεται ότι η συγκατάθεση λαμβάνεται πριν την αρχή οποιασδήποτε επεξεργασίας[117].
- Να καταγράφεται η συγκατάθεση σε περίπτωση που η συγκατάθεση δίνεται από κάποιον αντιπρόσωπο για άλλο άτομο (π.χ. για ένα παιδί κάτω των 13 χρόνων από τον γονέα του ή για ένα άτομο που είναι ανίκανο να δώσει συγκατάθεση από κάποιον άλλο).
- Να ενημερώνει τα υποκείμενα των δεδομένων σε περίπτωση που τα δεδομένα του διαβιβάζονται σε τρίτους ή σε χώρες με διαφορετική νομοθεσία αναφορικά με τα προσωπικά δεδομένα και να παρέχονται τρόποι με τους οποίους το υποκείμενο μπορεί να δώσει την συγκατάθεση του για αυτές τις διαβιβάσεις.
- Απόκτηση συγκατάθεσης από το υποκείμενο ,πριν από οποιαδήποτε καινούργια επεξεργασία δεδομένων που συλλέχθηκαν προηγουμένως , όπου αυτό είναι εφικτό και το απαιτεί ο νόμος.
- Πρέπει να διασφαλίζει ότι η συγκατάθεση δίνεται με έναν διαφανή τρόπο και αφού έχει προηγηθεί η επαρκής ενημέρωση του υποκειμένου σχετικά με τον σκοπό της επεξεργασίας.[118]
- Παροχή στο υποκείμενο , μηχανισμών που του επιτρέπουν να διαμορφώνει την συγκατάθεση του (είτε να την αφαιρεί ή να συμφωνεί σε μικρότερη επεξεργασία).Οι απαραίτητες αλλαγές στις βάσεις δεδομένων πρέπει να γίνονται σε εύλογο χρονικό διάστημα.
- Τήρηση όλων των νομικών απαιτήσεων , και όπου είναι απαραίτητο των απαιτήσεων που αφορούν ευαίσθητα προσωπικά δεδομένα όταν δίνει συγκατάθεση το υποκείμενο.
- Πρέπει να υπάρχουν ειδοποιήσεις ιδιωτικότητας για όλες τις μορφές επεξεργασίας πριν αυτές εφαρμοστούν και πρέπει να επιβεβαιώνονται όπου χρειάζεται η ταυτότητα των υποκειμένων ή του αντιπροσώπου του.Οι πληροφορίες για την ταυτοποίηση πρέπει να είναι όσο τον δυνατόν πιο λίγες και να διατηρούνται μόνο για όσο εξυπηρετούν τον σκοπό τους, καθώς πρέπει να διαγράφονται όταν δεν χρειάζονται πλέον.

Οι οργανισμοί πρέπει να παρέχουν στα υποκείμενα τα εργαλεία ώστε να μπορούν να κάνουν εύκολα, γρήγορα, κατανοητά την επιλογή τους αναφορικά με την επεξεργασία των δεδομένων τους εκτός από τις περιπτώσεις που το υποκείμενο δεν μπορεί να μην δώσει την συγκατάθεση του λόγω κάποιας νομοθεσίας.Πιο συγκεκριμένα οι οργανισμοί οφείλουν τα εξής:

---

[117] Επεξεργασία θεωρείται η συλλογή, αποθήκευση, μεταβολή, ανάκτηση, διαβούλευση, κοινοποίηση, ανωνυμοποίηση, διάδοση ή άλλη διάθεση, διαγραφή ή καταστροφή των δεδομένων προσωπικού χαρακτήρα.

[118] Άρθρο (12,13,14) ΓΚΠΔ

- Πριν την πραγματοποίηση οποιασδήποτε επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να έχει διαβεβαιωθεί ότι τα υποκείμενα επέλεξαν να γίνει αυτή η επεξεργασία.
- Πρέπει να παρέχουν στα υποκείμενα τους μηχανισμούς με τους οποίους μπορούν να αρνηθούν την επεξεργασία των δεδομένων τους.[119]
- Πρέπει να γίνεται διαβάθμιση των δεδομένων και να αποθηκεύονται με τέτοιο τρόπο που να επιτρέπει στα υποκείμενα να μπορούν να εξασκήσουν το δικαίωμα της εναντίωσης[120].
- Εφόσον έχει γίνει κοινοποίηση των δεδομένων με τρίτους,αυτοί πρέπει να ενημερώνονται σε περίπτωση που το υποκείμενο εναντιωθεί στην επεξεργασία.
- Αν και όπου είναι εφικτό, το υποκείμενο των δεδομένων πρέπει να έχει την δυνατότητα να επιλέξει ή να εναντιωθεί σε συγκεκριμένες επεξεργασίες δεδομένων και όχι στο σύνολο τους.

3η Αρχή) Νομιμότητα και καθορισμός σκοπού

Για την τήρηση αυτής της αρχής ο οργανισμός πρέπει να διασφαλίζει ότι ο σκοπός επεξεργασίας συμμορφώνεται με την ισχύουσα νομοθεσία και βασίζεται σε μια έγκυρη νομική βάση.Παράλληλα ο οργανισμός οφείλει να ενημερώσει το υποκείμενο των δεδομένων για τον σκοπό ή τους σκοπούς επεξεργασίας πριν γίνει συλλογή ή χρήση των δεδομένων για κάποιον νέο σκοπό.Η ενημέρωση αυτή πρέπει να γίνεται με ξεκάθαρο τρόπο και να υπάρχει δικαιολόγηση για την επεξεργασία αν είναι απαραίτητη.Ειδικά για τα ευαίσθητα δεδομένα προσωπικού χαρακτήρα υπάρχουν πιο αυστηροί κανόνες και για έναν σκοπό επεξεργασίας μπορεί να χρειαστεί μια συγκεκριμένη νομική βάση ή έγκριση από την αρχή προστασίας δεδομένων προσωπικού χαρακτήρα.Αν ο σκοπός δεν συμμορφώνεται με την νομοθεσία,η επεξεργασία δεν πρέπει να πραγματοποιηθεί.

Πιο συγκεκριμένα για την νομιμότητα του σκοπού πρέπει :

- Να διαπιστωθεί εάν η προβλεπόμενη επεξεργασία μπορεί να πραγματοποιηθεί βασισμένη νομικά πέρα από την συγκατάθεση (π.χ. δημόσιο συμφέρον, νομική υποχρέωση, έννομο συμφέρον του υποκειμένου των δεδομένων[121] κλπ.)
- Να καθοριστεί έαν υπάρχει κάποιος νομικός λόγος που απαγορεύει στα υποκείμενα των δεδομένων να εναντιωθούν στην επεξεργασία των δεδομένων τους (π.χ. εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας)

[119] Οι μηχανισμοί αυτοί πρέπει να επανεξετάζονται και να αναθεωρούνται αν αυτό χρειαστεί.
[120] Άρθρο 21 ΓΚΠΔ - Δικαίωμα εναντίωσης
[121] Άρθρο 6 ΓΚΠΔ – Νομιμότητα της επεξεργασίας

- Να προσδιοριστούν οι νομικές βάσεις που επιτρέπουν την επεξεργασία των προσωπικών δεδομένων
- Να ενσωματωθούν διαδικασίες που θα διασφαλίζουν ότι οι επεξεργασίες που πραγματοποιεί ο οργανισμός πραγματοποιούνται σύμφωνα με την ισχύουσα νομοθεσία. Το γενικό πλαίσιο της επεξεργασίας θα πρέπει να λαμβάνεται υπόψη όταν προσδιορίζεται η νομιμότητα του σκοπού της. Αυτό θα περιλαμβάνει τη φύση της σχέσης μεταξύ του υπευθύνου επεξεργασίας και των υποκειμένων των δεδομένων, τις επιστημονικές και τεχνολογικές εξελίξεις και τις αλλαγές στις κοινωνικές και πολιτιστικές συμπεριφορές.

Όταν καθορίζεται ο σκοπός της επεξεργασίας πρέπει να γίνονται τα εξής:

- Να αναγνωρίζονται τα δεδομένα προσωπικού χαρακτήρα που χρησιμοποιούνται μόνο για κάθε συγκεκριμένη επιχειρηματική δραστηριότητα
- Να διαχωρίζονται τα δεδομένα που είναι χρήσιμα για κάθε επεξεργασία
- Για κάθε επιχειρηματική δραστηριότητα που περιλαμβάνει επεξεργασία πρέπει να γίνεται σωστή διαχείριση των δικαιωμάτων πρόσβασης και να υπάρχει ένα εξειδικευμένο πληροφοριακό περιβάλλον για τα ευαίσθητα προσωπικά δεδομένα.

4η Αρχή) Ελαχιστοποίηση επεξεργασίας δεδομένων

Αυτή η αρχή συνδέεται άμεσα με την ελαχιστοποίηση στην συλλογή δεδομένων αλλά επεκτείνεται περαιτέρω. Για την τήρηση της αρχής αυτής, γίνεται επεξεργασία μόνο των απολύτως απαραίτητων δεδομένων προσωπικού χαρακτήρα προκείμενου να εξασφαλιστεί το έννομο συμφέρον του υπευθύνου επεξεργασίας. Ταυτόχρονα, περιορίζεται η αποκάλυψη των δεδομένων αυτών σε ελάχιστο αριθμό ενδιαφερόμενων μερών. Οι οργανισμοί οφείλουν λοιπόν να εφαρμόζουν κατάλληλα μέτρα για να ελαχιστοποιήσουν τα δεδομένα που επεξεργάζονται. Πιο συγκεκριμένα:

- Μόνο εξουσιοδοτημένα άτομα που χρειάζονται τα δεδομένα για να εκτελέσουν τα καθήκοντα τους πρέπει να έχουν πρόσβαση στα δεδομένα αυτά.
- Πρέπει να περιορίζεται η συνδεσιμότητα των δεδομένων προσωπικού χαρακτήρα που έχουν συλλεχθεί. Η διασταύρωση με άλλες βάσεις δεδομένων πρέπει να γίνεται σε ελάχιστο βαθμό και μόνο αφού έχει διαβεβαιωθεί η νομιμότητα αυτής της πράξης.
- Είναι σημαντική η επανεξέταση των διαδικασιών επεξεργασίας ώστε να διαβεβαιωθεί ότι τα δεδομένα είναι ακόμα απαραίτητα για την επιχειρηματική δραστηριότητα που εκτελεί ο οργανισμός.
- Η διαβίβαση των προσωπικών δεδομένων πρέπει να είναι περιορισμένη.
- Πρέπει να καθοριστούν τα δεδομένα , τα οποία θα ανωνυμοποιηθούν όταν αποθηκευτούν.

- Τα δεδομένα πρέπει να διαγράφονται όταν ο σκοπός επεξεργασίας δεν ισχύει πλέον και δεν υπάρχουν νομικές απαιτήσεις που να ορίζουν την διατήρηση τους.

Γενικά, κατά τη συλλογή προαιρετικών δεδομένων προσωπικού χαρακτήρα, οι οργανισμοί θα πρέπει να συλλέγουν μόνο τα υποχρεωτικά δεδομένα που απαιτούνται για την παροχή υπηρεσιών και να λαμβάνουν την κατάλληλη συγκατάθεση από τα υποκείμενα των δεδομένων.Επίσης, όπου είναι δυνατόν, οι οργανισμοί θα πρέπει να περιορίσουν τα μητρώα δεδομένων τους για να μειώσουν τους κινδύνους που αφορούν την προστασία της ιδιωτικότητας. Οι οργανισμοί θα πρέπει να διενεργούν αξιολογήσεις των μητρώων δεδομένων τους για να διασφαλίσουν ότι οι εν λόγω συλλογές δεδομένων είναι ακριβείς, συναφείς, τρέχουσες και πλήρεις στο μέγιστο δυνατό βαθμό.

5η Αρχή) Περιορισμός χρήσης, διατήρησης και κοινοποίησης δεδομένων

Με αυτήν την αρχή ο στόχος που θέλει να πετύχει ο οργανισμός είναι να περιορίσει τη χρήση και κοινοποίηση των δεδομένων προσωπικού χαρακτήρα για συγκεκριμένους, σαφείς και νόμιμους σκοπούς και να διατηρεί τα δεδομένα για όχι περισσότερο από ότι είναι αναγκαίο προκειμένου να εκπληρωθούν οι δηλωθέντες σκοποί ή για την τήρηση των εφαρμοστέων νόμων.

Πιο συγκεκριμένα τα μέτρα για τον περιορισμό χρήσης είναι:

- Αρχειοθέτηση, ασφάλιση και απαγόρευση επεξεργασίας δεδομένων όταν ο σκοπός επεξεργασίας δεν ισχύει πλέον αλλά η διατήρηση είναι απαραίτητη λόγω αντίστοιχης νομοθεσίας.
- Εφαρμογή κατάλληλων μηχανισμών διαγραφής και συνολικής καταστροφής δεδομένων προσωπικού χαρακτήρα.
- Περιορισμός της πρόσβασης τρίτων και εξωτερικών μερών στα συστήματα που διαχειρίζονται τα δεδομένα.Η πρόσβαση πρέπει να δίνεται αφού έχει υπάρξει διαδικασία έγκρισης και εξουσιοδότησης για τα μέρη αυτά.
- Σε περίπτωση που πρέπει να συνδεθούν εξωτερικά συστήματα στα συστήματα του οργανισμού που επεξεργάζονται δεδομένα , πρέπει να υπάρχουν και οι απαραίτητες δικλείδες ασφαλείας προσωπικών δεδομένων προτού γίνει η σύνδεση αυτή.
- Ανασκόπηση των δικλείδων ασφαλείας που έχουν εφαρμοστεί από τρίτους προκειμένου να διασφαλιστούν οι απαιτήσεις ασφάλειας που έχει ο οργανισμός.
- Εφαρμογή κατάλληλων μηχανισμών ελέγχου πρόσβασης προσωπικών δεδομένων όταν πρόκειται για απομακρυσμένη σύνδεση, καθώς και διατήρηση σχετικών αρχείων logs.
- Παροχή πληροφοριών στα υποκείμενα μέσω ειδοποιήσεων ιδιωτικότητας σε περίπτωση που αλλάξει η χρήση των δεδομένων τους.

Όσον αφορά την διατήρηση δεδομένων τα μέτρα είναι:

- Διατήρηση των δεδομένων προσωπικού χαρακτήρα μόνο για το χρονικό διάστημα που εξυπηρετεί τον σκοπό της επεξεργασίας και για το οποίο έχει ενημερωθεί το υποκείμενο μέσω της ειδοποίησης ιδιωτικότητας.Όταν τελειώσει το διάστημα διατήρησης, τα δεδομένα πρέπει να διαγράφονται.
- Ανωνυμοποίηση των δεδομένων , αν χρειαστεί να διατηρηθούν για παραπάνω από ότι απαιτείται για την εκτέλεση επιχειρηματικών δραστηριοτήτων.
- Καθορισμός περιόδου διατήρησης των δεδομένων προσωπικού χαρακτήρα που είναι χρονικά περιορισμένες και αναλογικές ως προς τον σκοπό της επεξεργασίας.
- Το πληροφοριακό σύστημα πρέπει να είναι ικανό να αναγνωρίζει την λήξη του χρονικού διαστήματος διατήρησης δεδομένων.
- Ανάπτυξη μιας αυτοματοποιημένης λειτουργίας που διαγράφει τα προσωπικά δεδομένα μετά την λήξη της περιόδου διατήρησης.
- Εφαρμογή μηχανισμών που καθιστούν αδύνατη την ταυτοποίηση προσώπων από τα δεδομένα τους
- Εφαρμογή μηχανισμών (π.χ. κατακερματισμός[122]) για την προστασία των δεδομένων στα οποία δεν μπορούν να εφαρμοστούν οι από πάνω μηχανισμοί.

Επιπλέον ο οργανισμός πρέπει να παρέχει τεχνικά μέτρα τα οποία εξασφαλίζουν ότι τα προσωρινά αρχεία[123] πρέπει να διαγράφονται και να καταστρέφονται εντός ενός συγκεκριμένου και καταγεγραμμένου χρονικού διαστήματος.

Όσον αφορά τα μέτρα για τον περιορισμό της κοινοποίησης, οι οργανισμοί πρέπει:

- Να αποφεύγουν την κοινοποίηση των δεδομένων προσωπικού χαρακτήρα που έχουν συλλέξει σε εξωτερικούς αποδέκτες χωρίς την γνώση και συγκατάθεση των υποκειμένων των δεδομένων,εκτός αν αυτό επιτρέπεται από την νομοθεσία.

---

[122] Η συνάρτηση κατατεμαχισμού, γνωστή και ως συνάρτηση κατακερματισμού, είναι μια μαθηματική συνάρτηση που δέχεται ως είσοδο κάποιο δεδομένο τυχαίου μεγέθους και επιστρέφει ένα ακέραιο σταθερού μεγέθους αναπαράστασης. Οι τιμές που επιστρέφει η συνάρτηση κατατεμαχισμού ονομάζονται τιμές κατατεμαχισμού (hash values), κώδικες κατατεμαχισμού (hash codes), αθροίσματα κατατεμαχισμού (hash sums) ή απλά τιμές κατατεμαχισμού (hashes). Συνάρτηση κατατεμαχισμού – Βικιπαίδεια Διαθέσιμο: https://el.wikipedia.org/wiki/Συνάρτηση_κατατεμαχισμού [Πρόσβαση 04-04-2022]

[123] Κατά την εκτέλεση των επιχειρηματικών δραστηριοτήτων του οργανισμού, τα πληροφοριακά συστήματα ενδέχεται να δημιουργούν προσωρινά αρχεία που περιέχουν δεδομένα προσωπικού χαρακτήρα. Τα αρχεία αυτά είναι ειδικά για το σύστημα και την εφαρμογή, αλλά μπορεί να περιλαμβάνουν ένα σύστημα αρχείων επαναφοράς και προσωρινά αρχεία που συνδέονται με ενημερώσεις βάσεων δεδομένων και τη λειτουργία άλλου λογισμικού.Αυτά τα προσωρινά αρχεία δεν χρειάζονται αφού εκτελεστεί η επεξεργασία αλλά σε ορισμένες περιπτώσεις ενδέχεται να μην καταστρέφονται αυτόματα.

- Να ενσωματώσουν μέτρα που προστατεύουν τα δεδομένα κατά την μεταφορά τους, όπως κρυπτογράφηση επικοινωνιών και μηχανισμούς ελέγχου ακεραιότητας.

Επιπροσθέτως όταν υπάρχει εκτελών την επεξεργασία η σύμβαση μεταξύ αυτού και του υπευθύνου επεξεργασίας πρέπει να απαιτεί από τον εκτελών να ειδοποιεί τον υπεύθυνο, σύμφωνα με οποιαδήποτε διαδικασία και χρονικές περιόδους που συμφωνούνται στη σύμβαση, για κάθε νομικά δεσμευτικό αίτημα κοινοποίησης των δεδομένων αν το επιβάλλει ο νόμος ή άλλη αρχή, εκτός εάν η εν λόγω κοινοποίηση απαγορεύεται διαφορετικά από το νόμο.

Επίσης,κατά την διάρκεια της επιχειρηματικής δραστηριότητας, ενδέχεται τα δεδομένα προσωπικού χαρακτήρα να αποκαλυφθούν ή να κοινοποιηθούν.Σε περίπτωση που συμβεί αυτό, αυτές οι ενέργειες πρέπει να καταγράφονται.Αν γίνει κάποια πρόσθετη κοινοποίηση σε τρίτους, όπως αυτές που προκύπτουν από έρευνες των αρχών ή από εξωτερικούς ελέγχους, τότε και αυτή η κοινοποίηση πρέπει να καταγράφεται. Τα αρχεία καταγραφής θα πρέπει να περιλαμβάνουν τον λόγο κοινοποίησης καθώς και το πως έγινε η εξουσιοδότηση για αυτήν την ενέργεια.

6η Αρχή) Ακρίβεια των δεδομένων

Ο οργανισμός οφείλει τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται να είναι ακριβή, πλήρης, επικαιροποιημένα, επαρκή και σχετικά με το σκοπό της χρήσης.Τα μέτρα τα οποία χρειάζεται ο οργανισμός για την τήρηση αυτής της αρχής έχουν ως εξής:

- Ανάπτυξη και εφαρμογή πολιτικών και διαδικασιών που διασφαλίζουν την ακρίβεια των δεδομένων.
- Εφαρμογή μηχανισμών που διασφαλίζουν την ανίχνευση τροποποιήσεων στα δεδομένα μετά την συλλογή τους.
- Διαβεβαίωση , από την στιγμή της συλλογής των προσωπικών δεδομένων, της ακρίβειας και πληρότητας των δεδομένων στο μέγιστο δυνατό βαθμό.
- Επαλήθευση μέσω κατάλληλων μέτρων της εγκυρότητας και ορθότητας των αιτήσεων διόρθωσης που υποβάλλονται από τα υποκείμενα των δεδομένων πριν γίνει οποιαδήποτε αλλαγή στα δεδομένα.
- Περιοδικός έλεγχος των δεδομένων προσωπικού χαρακτήρα προκειμένου να είναι σωστά και επικαιροποιημένα.
- Οι οργανισμοί θα πρέπει να λαμβάνουν εύλογα τεχνικά μέτρα για την επιβεβαίωση της ακρίβειας των δεδομένων αυτών. Τέτοια βήματα μπορεί να περιλαμβάνουν, για παράδειγμα, την επεξεργασία και την επικύρωση των διευθύνσεων καθώς συλλέγονται ή εισάγονται σε πληροφοριακά συστήματα με τη χρήση αυτοματοποιημένων διεπαφών προγραμματισμού εφαρμογών (API).

Ιδιαίτερη προσοχή πρέπει να δοθεί στην ακρίβεια των ευαίσθητων δεδομένων προσωπικού χαρακτήρα.Οι οργανισμοί πρέπει να εφαρμόζουν τεχνικά μέτρα στα πληροφοριακά συστήματα και διαδικασίες που θα καθορίζουν τον τρόπο και την συχνότητα με τον οποίο θα ενημερώνονται τα ευαίσθητα δεδομένα. Για να ελαχιστοποιηθεί το ενδεχόμενο ανακρίβειας των δεδομένων, τα προσωπικά αυτά δεδομένα θα πρέπει να εισάγονται στα πληροφοριακά συστήματα απευθείας από τον υποκείμενο των δεδομένων.Σε πολλές περιπτώσεις θα πρέπει να παρέχουν στο υποκείμενο την δυνατότητα να ενημερώνει αυτό τα δεδομένα του για να αποφευχθούν ανακρίβειες.

7η αρχή) Διαφάνεια και ειδοποίηση ιδιωτικότητας

1)Ειδοποίηση ιδιωτικότητας

Απαραίτητο μέτρο που οφείλουν να έχουν οι οργανισμοί είναι η ειδοποίηση ιδιωτικότητας.Ειδικότερα, πρέπει να παρέχουν στα υποκείμενα των δεδομένων πληροφορίες αναφορικά με την επεξεργασία των δεδομένων και τον σκοπό επεξεργασίας. Αναλυτικά για την ειδοποίηση ιδιωτικότητας πρέπει ο οργανισμός να εφαρμόζει τα εξής :

- Να παρέχει ενημερώσεις και ειδοποιήσεις σχετικά με
  α) τις δραστηριότητες που επηρεάζουν την ιδιωτικότητα τους (π.χ. η συλλογή,χρήση,κοινοποίηση και προστασία των προσωπικών τους δεδομένων.),
  β) την νομική βάση επεξεργασίας δεδομένων
  γ) τις επιλογές που έχουν αναφορικά με την χρήση των προσωπικών δεδομένων από τον οργανισμό
  δ) την δυνατότητα υποκειμένου να εναντιωθεί στην επεξεργασία.
- Να επανεξετάζει την ειδοποίηση ιδιωτικότητας σε περίπτωση που προκύψει κάποια αλλαγή στην επεξεργασία που εκτελείται ή στις πολιτικές και διαδικασίες που ακολουθεί ο οργανισμός.
- Να διασφαλίζει ότι η ειδοποίηση είναι πλήρης και κατάλληλη για το κοινό στο οποίο απευθύνεται.Ταυτόχρονα πρέπει να είναι γραμμένη με τέτοιο τρόπο που να είναι κατανοητή.
- Η ειδοποίηση ιδιωτικότητας πρέπει να λαμβάνεται υπόψη από το υποκείμενο προτού συλλεχθούν τα δεδομένα του.

2)Διαφάνεια

Ο οργανισμός πρέπει να παρέχει στα υποκείμενα των δεδομένων πληροφορίες ,μέσω κατάλληλων μέτρων, που περιγράφουν τις διαδικασίες και πολιτικές που ακολουθεί ο οργανισμός αναφορικά με την επεξεργασία των δεδομένων.Αναλυτικά:

- Ποια είναι τα δεδομένα προσωπικού χαρακτήρα που συλλέγει ο οργανισμός και ποιος είναι ο σκοπός επεξεργασίας για τον οποίο συλλέγουν τα δεδομένα.
- Πως χρησιμοποιούνται τα δεδομένα αυτά εσωτερικά στον οργανισμό.
- Πληροφορίες που αφορούν την κοινοποίηση προσωπικών δεδομένων σε τρίτους, όπως ο λόγος κοινοποίησης. Ταυτόχρονα πρέπει να παρέχονται πληροφορίες στα υποκείμενα των δεδομένων σε περίπτωση που ο οργανισμός χρησιμοποιεί κάποιον εξωτερικό εκτελών την επεξεργασία ή προωθεί τα δεδομένα σε κάποιον άλλο τρίτο έναντι αμοιβής.
- Πληροφορίες που περιγράφουν αν το υποκείμενο έχει την δυνατότητα να δώσει την συγκατάθεση του σε συγκεκριμένες επεξεργασίες.
- Το χρονικό διάστημα για το οποίο θα διατηρηθούν τα δεδομένα προσωπικού χαρακτήρα.
- Ο τρόπος με τον οποίο μπορεί το υποκείμενο να διορθώσει τα δεδομένα του.
- Πληροφορίες που περιγράφουν τα μέτρα προστασίας των προσωπικών δεδομένων.
- Πληροφορίες που αφορούν παραβιάσεις δεδομένων.

8η Αρχή) Συμμετοχή και πρόσβαση του υποκειμένου των δεδομένων

Οι οργανισμοί πρέπει να λαμβάνουν τα κατάλληλα μέτρα για να παρέχουν στα υποκείμενα των δεδομένων πρόσβαση στα δεδομένα τους, καθώς και τη δυνατότητα να ζητήσουν διόρθωση ή διαγραφή των δεδομένων τους.[124]Πιο συγκεκριμένα:

- Πρέπει να υλοποιηθούν οι λειτουργίες που επιτρέπουν στο υποκείμενο να ασκήσει το δικαίωμα της πρόσβασης του.Είναι απαραίτητο τα άτομα να είναι ικανά να ασκήσουν το δικαίωμα αυτό γρήγορα και εύκολα.
- Σε περίπτωση που οι παραπάνω λειτουργίες είναι δύσχρηστες πρέπει να αναδιαμορφωθούν και να υπάρχουν διαθέσιμες εναλλακτικές λειτουργίες.
- Οι οδηγίες που αναφέρουν πως το υποκείμενο μπορεί να ζητήσει πρόσβαση στα δεδομένα του πρέπει να δημοσιοποιούνται.
- Μέσω των μέτρων αυτών χρειάζεται να διασφαλίζεται ότι η πρόσβαση στα δεδομένα προσωπικού χαρακτήρα την έχει μόνο το άτομο στο οποίο του ανήκουν ή είναι αντιπρόσωπος του ατόμου που του ανήκουν.Σε αυτήν την περίπτωση ενδέχεται να χρειαστεί αυθεντικοποίηση και ταυτοποίηση του ατόμου.
- Είναι απαραίτητο να διασφαλίζει ο οργανισμός ότι τα δεδομένα προσωπικού χαρακτήρα αποστέλλονται μόνο στο σωστό υποκείμενο και ότι η αποστολή αυτή γίνεται με ασφαλή τρόπο.
- Πρέπει να διασφαλίζεται ότι πρέπει να μπορούν να υλοποιηθούν τα αιτήματα ενός υποκειμένου χωρίς αυτό να επηρεάζει τα άλλα υποκείμενα.

[124] Αιτιολογική σκέψη 63 ΓΚΠΔ

- Αν ο εκτελών την επεξεργασία είναι διαφορετικός από τον υπεύθυνο , τότε πρέπει να υποστηρίζει την λειτουργία διαγραφής,διόρθωσης ή πρόσβασης του υποκειμένου.

9η αρχή) Λογοδοσία

Με την τήρηση αυτής της αρχής εξασφαλίζουμε έναν από τους βασικούς σκοπούς της εκτίμησης αντικτύπου όπως είχαμε αναφέρει, που είναι να αποδεικνύει ότι έχει λάβει τα απαραίτητα μέτρα για την προστασία των δεδομένων των υποκειμένων.Για την τήρηση της αρχής της λογοδοσίας χρειάζονται αρκετές ενέργειες.Αρχικά, είναι αναγκαίο ο οργανισμός να εφαρμόσει μέτρα για την σωστή διακυβέρνηση των δεδομένων που επεξεργάζονται. Παρακάτω θα αναφέρουμε τα μέτρα:

- Ο ορισμός ενός υπεύθυνου ατόμου ή μια ομάδας για την διακυβέρνηση της προστασίας των προσωπικών δεδομένων σε επίπεδο οργανισμού.Οι ευθύνες της ομάδας ή του ατόμου είναι η συμμόρφωση με όλους του ισχύοντες νόμους και κανονισμούς που αφορούν την επεξεργασία προσωπικών δεδομένων.Το υπεύθυνο άτομο ή ομάδα θα χρειαστεί να έχει τις απαραίτητες γνώσεις για να εκτελέσει τα καθήκοντα του.
- Κάθε θέμα προστασίας δεδομένων πρέπει να ελέγχεται από τους υπεύθυνους και αν χρειαστεί, το άτομο πρέπει να μπορεί να αναφέρει το θέμα απευθείας στην ανώτερη διοίκηση του οργανισμού.
- Ανάπτυξη και εφαρμογή διαδικασιών και πολιτικών για την προστασία των δεδομένων προσωπικού χαρακτήρα καθώς και για τον έλεγχο των δικλείδων ασφαλείας των πληροφοριακών συστημάτων.Οι εν λόγω πολιτικές και διαδικασίες πρέπει να ενημερώνονται συχνά.
- Παρακολούθηση του επιπέδου συμμόρφωσης του οργανισμού αναφορικά με την προστασία των προσωπικών δεδομένων.

Δεν είναι αρκετό για έναν οργανισμό απλά να έχει πολιτικές και διαδικασίες σχετικά με την προστασία των προσωπικών δεδομένων. Ταυτόχρονα ,είναι απαραίτητο να ελέγχει και να παρακολουθεί ότι αυτές οι πολιτικές, οι διαδικασίες και γενικότερα τα υπόλοιπα μέτρα προστασίας ιδιωτικότητας είναι αποτελεσματικά.Άρα ο οργανισμός πρέπει να:

- Ελέγχει συχνά τις δραστηριότητες επεξεργασίας, ειδικά αν επεξεργάζονται ευαίσθητα προσωπικά δεδομένα και να βεβαιώνονται ότι οι δραστηριότητες αυτές γίνονται σύμφωνα με τον νόμο.
- Ελέγχει τις πολιτικές,τις διαδικασίες και τα μέτρα ώστε να συμμορφώνονται με την νομοθεσία.
- Διενέργει ελέγχους που προέρχονται είτε εσωτερικά από τον οργανισμό είτε εξωτερικά , ώστε να είναι αξιόπιστοι.

Μέτρα χρειάζεται να ληφθούν για να διασφαλίσουν ότι οι εξωτερικοί συνεργάτες του οργανισμού και πιθανοί εκτελούντες την επεξεργασία έχουν αντίστοιχα επίπεδα ασφάλειας δεδομένων.Για την επίτευξη της προστασίας οι οργανισμοί πρέπει:

- Στην σύμβαση επεξεργασίας δεδομένων μεταξύ υπευθύνου και εκτελών την επεξεργασία να υπάρχουν , όροι , οι οποίοι απαιτούν από τον εκτελών να έχει τα απαραίτητα μέτρα προστασίας προσωπικών δεδομένων[125].
- Να διαβεβαιώσουν ότι ο εκτελών την επεξεργασία που είναι εξωτερικός συνεργάτης κατέχει τα απαραίτητα μέτρα, μέσα από ελέγχους και παρακολούθηση.Ειναι επιθυμητό να υπάρχει καταγραφή των πολιτικών και διαδικασιών που ακολουθεί ο εκτελών , ώστε ο υπεύθυνος να κάνει κατάλληλες προτάσεις αν χρειαστεί.
- Να καθοριστούν οι συνθήκες , οι οποίες καθιστούν την επεξεργασία υψηλού κινδύνου για τον υπεύθυνο επεξεργασίας εξαιτίας του εκτελών, και αποτελεί αιτία για την διακοπή της συνεργασίας.
- Στην συνεργασία του οργανισμού και του εκτελών να υπάρχει μία ρήτρα εμπιστευτικότητας η οποία θα δεσμεύει τον εκτελών και όποιους εργαζομένους απασχολεί.
- Να καθοριστούν όλες οι αρμοδιότητες και ευθύνες που έχει ο εκτελών για την προστασία των προσωπικών δεδομένων , και μεταξύ άλλων σε περίπτωση που γίνει κάποια παραβίαση δεδομένων οφείλει ο εκτελών να ενημερώσει τον υπεύθυνο επεξεργασίας άμεσα.

Δεν πρέπει να παραλειφθεί ως μέτρο, η εκπαίδευση και η ευαισθητοποίηση του προσωπικού του οργανισμού, το οποίο πιθανότατα θα έχει πρόσβαση στα δεδομένα προσωπικού χαρακτήρα των υποκειμένων.Ο οργανισμός πρέπει να φροντίσει να παρέχει κατάλληλα προγράμματα εκπαίδευσης και ευαισθητοποίησης στο προσωπικό του ώστε να κατανοήσουν οι εργαζόμενοι τις ευθύνες τους και τις αρμοδιότητες τους.[126]Τα προγράμματα αυτά πρέπει να πραγματοποιούνται συχνά (π.χ. κάθε 6 μήνες).Ίσως είναι χρήσιμο να δημιουργηθούν μηχανισμοί οι οποίοι θα υπενθυμίζουν στο προσωπικό τις ευθύνες του και το ενημερώνει για την ισχύουσα νομοθεσία.

Τέλος, προκειμένου να επιδεικνύουν υπευθυνότητα ως προς το νομοθετικό και κανονιστικό πλαίσιο, οι οργανισμοί θα πρέπει να αναπτύσσουν, να διαδίδουν, κατά περίπτωση, και να επικαιροποιούν αναφορές (π.χ. αναφορές σχετικά με παραβιάσεις,

---

[125] Πέρα από τα μέτρα προστασίας, μέσα στην σύμβαση πρέπει να περιγράφονται και άλλες πληροφορίες που αφορούν την επεξεργασία όπως το χρονικό διάστημα για το οποίο θα γίνεται η επεξεργασία από τον εκτελών,με ποιον τρόπο καθώς και οι κατηγορίες δεδομένων που επεξεργάζονται. Data Processing Agreement (DPA) -GDPRregister [n.d] Διαθέσιμο: https://www.gdprregister.eu/gdpr/data-processing-agreement-dpa/ [Πρόσβαση 25-04-2022]

[126] Larry G. Wlosinski - The Benefits of Information Security and Privacy Awareness Training Programs – ISACA(2019) Διαθέσιμο: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs_joa_eng_0219.pdf [Πρόσβαση 07-04-2022]

έρευνες, ελέγχους) προς τα ανώτερα διοικητικά στελέχη και το λοιπό προσωπικό που είναι υπεύθυνο για την παρακολούθηση της προστασίας των προσωπικών δεδομένων.

10η Αρχή) Συμμόρφωση με την νομοθεσία και τους κανονισμούς ιδιωτικότητας

Με την τήρηση της αρχής αυτής σκοπό έχει ο οργανισμός να αποφύγει οποιαδήποτε παραβίαση νόμου ή κανονισμού ή κάποιας άλλης σύμβασης που αφορά την ιδιωτικότητα των υποκειμένων των δεδομένων.Προκειμένου να αποφευχθούν οι παραβιάσεις αυτές ο οργανισμός μπορεί να υλοποιήσει τα εξής μέτρα:

- Δημιουργία μιας έκθεσης σε ετήσια βάση που θα περιγράφει λεπτομερώς το επίπεδο συμμόρφωσης του οργανισμού, μέσα από την καταγραφή υφιστάμενων κινδύνων και εκκρεμών ενεργειών που πρέπει να λάβει ο οργανισμός.
- Ανάπτυξη κατάλληλων διαδικασιών αντιμετώπισης παραβιάσεων δεδομένων προσωπικού χαρακτήρα.[127]

Επίσης ιδιαίτερη προσοχή πρέπει να δοθεί από τον οργανισμό αναφορικά με τις διασυνοριακές ροές, δηλαδή τις περιπτώσεις που μεταφέρονται τα προσωπικά δεδομένα που επεξεργάζονται σε διαφορετικές χώρες.Οι κανονισμοί που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα στην χώρα που μεταφέρονται μπορεί να έχουν διαφορετικούς περιορισμούς από αυτούς στην χώρα που ήταν αποθηκευμένα εξαρχής.Για αυτό ο οργανισμός ίσως χρειαστεί να ειδοποιήσει την αρχή προστασίας προσωπικών δεδομένων της χώρας που λαμβάνει τα δεδομένα.Αν πρόκειται για μεταφορά ευαίσθητων προσωπικών δεδομένων ενδέχεται να χρειαστεί την έγκριση της.Επίσης εφόσον μεταφέρονται τα δεδομένα σε μια άλλη χώρα, τα δεδομένα αυτά πρέπει να έχουν τις κατάλληλες δικλείδες ασφαλείας στο επίπεδο που απαιτεί η χώρα προέλευσης των προσωπικών δεδομένων.

11η Αρχή) Ασφάλεια Δεδομένων

Με την τελευταία αρχή προσπαθούμε να εξασφαλίσουμε ότι ο οργανισμός έχει λάβει τα κατάλληλα μέτρα ασφάλειας είτε αυτά είναι οργανωτικά είτε τεχνικά προκειμένου να προστατεύσει την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα των δεδομένων προσωπικού χαρακτήρα.[128]Στα πλαίσια αυτής της προσπάθειας ο

[127] Office of the Australian Information Commissioner - Part 3: Responding to data breaches — four key steps Διαθέσιμο: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps [Πρόσβαση 08-04-2022]
[128] ICO – Security Διαθέσιμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ [Πρόσβαση 05-05-2022]

οργανισμός θα πρέπει να διενεργήσει και κάποια εκτίμηση επικινδυνότητας.Παρακάτω θα αναφέρουμε κάποια από τα οργανωτικά και τεχνικά μέτρα που προτείνει ο ENISA[129] και ο ISO[130]:

Είδος Μέτρου	Περιγραφή
Πολιτική και διαδικασίες Ασφάλειας για την προστασία δεδομένων προσωπικού χαρακτήρα	Ο οργανισμός πρέπει να αναπτύξει και να έχει καταγεγραμμένες συγκεκριμένες πολιτικές και διαδικασίες ασφάλειας για την προστασία δεδομένων πέρα από την γενικές πολιτικές και διαδικασίες που έχει για την ασφάλεια των πληροφοριακών συστημάτων του.Πρέπει να γίνεται ανασκόπηση και αναθεώρηση των πολιτικών αυτών σε ετήσια βάση.
Ρόλοι και Αρμοδιότητες	Είναι απαραίτητο ο οργανισμός να καθορίσει συγκεκριμένους ρόλους και αρμοδιότητες για τα άτομα που διαχειρίζονται τα προσωπικά δεδομένα.Αυτός ο καθορισμός πρέπει να γίνεται με βάση την πολιτική ασφάλειας.Σε περίπτωση που γίνονται αναδιοργανώσεις εντός του οργανισμού(μετακίνηση/απόλυση προσωπικού κλπ.) πρέπει να γίνονται ανάλογες αλλαγές στα δικαιώματα πρόσβασης και στις αρμοδιότητες που θα έχει το προσωπικό.
Πολιτική Πρόσβασης	Ο οργανισμός οφείλει να φροντίσει για την κατανομή δικαιωμάτων πρόσβασης στο προσωπικό που εμπλέκεται στην επεξεργασία δεδομένων σύμφωνα με τους ρόλους τους.
Διαχείριση αγαθών	Απαιτείται η διατήρηση ενός μητρώου στο οποίο να καταγράφονται όλα τα πληροφοριακά αγαθά που εμπλέκονται στην επεξεργασία των προσωπικών δεδομένων.Πρέπει να καθοριστεί ένα άτομο το οποίο θα ευθύνεται για την ενημέρωση του μητρώου αυτού.

[129] ENISA - Handbook on Security of Personal Data Processing (2017) Διαθέσιμο: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing [Πρόσβαση 20-04-2022]

[130] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

	Επίσης τα αγαθά πρέπει να επανεξετάζονται και να ανανεώνονται αν χρειαστεί.
Διαχείριση αλλαγών	Οποιαδήποτε αλλαγή που γίνεται στα πληροφοριακά συστήματα που επεξεργάζονται δεδομένα πρέπει να καταγράφονται και να παρακολουθούνται από ένα προκαθορισμένο άτομο. Αν πρόκειται να γίνει κάποια αλλαγή σε λογισμικό ή αναπτύσσει ο ίδιος ο οργανισμός λογισμικό που αφορά την επξεργασία προσωπικών δεδομένων είναι σημαντικό πρώτα να γίνουν δοκιμές.Οι δοκιμές αυτές πρέπει να διενεργούνται σε ένα ξεχωριστό δοκιμαστικό περιβάλλον με μη αληθινά δεδομένα.
Διαχείριση περιστατικών / Παραβιάσεις δεδομένων προσωπικού χαρακτήρα.	Ο οργανισμός πρέπει να έχει ένα καταγεγραμμένο σχέδιο με αναλυτικές διαδικασίες για την αποτελεσματική αντιμετωπίση περιστατικών
Σχέδιο ανάκαμψης από καταστροφή και επιχειρηματική συνέχεια	Ο οργανισμός πρέπει να υλοποιήσει τα μέτρα και τις διαδικασίες με τις οποίες θα εξασφαλίσει την διαθεσιμότητα των πληροφοριακών συστημάτων που επεξεργάζονται προσωπικά δεδομένα.
Έλεγχος πρόσβασης και αυθεντικοποίηση	Η εφαρμογή ενός συστήματος που θα επιτρέπει την δημιουργία,έγκριση, αναθεώρηση και διαγραφή λογαριασμών θα βοηθήσει στον έλεγχο πρόσβασης .Το σύστημα αυτό είναι απαραίτητο να ελέγχει όλους τους χρήστες που θα έχουν πρόσβαση στα πληροφοριακά συστήματα. Το σύστημα πρέπει να παρέχει μηχανισμούς αυθεντικοποίησης.[131] Για την σωστή υλοποίηση αυτού του μέτρου απαραίτητη είναι η εφαρμογή σωστών πολιτικών κωδικών πρόσβασης.
Ασφάλεια Server/ Βάσεων Δεδομένων	Οι βάσεις δεδομένων καθώς και οι server εφαρμογών πρέπει να διαμορφωθούν

[131] Μερικοί μηχανισμοί αυθεντικοποίησης : Κωδικοί Πρόσβασης,Αυθεντικοποίηση με Token,Βιομετρική Αυθεντικοποίηση κλπ . Types of Authentication Methods – OptimalIdm Διαθέσιμο: https://optimalidm.com/resources/blog/types-of-authentication-methods/ [Πρόσβαση 05-04-2022]

	ώστε να μπορούν να λειτουργούν με την χρήση ενός ξεχωριστού λογαριασμού, με ελάχιστα προνόμια του λειτουργικού συστήματος.
Ασφάλεια Τερματικών εργασίας	Απαιτείται ο χρήστης να μην μπορεί να απενεργοποιήσει ή να παρακάμψει τις βασικές ρυθμίσεις ασφάλειας,καθώς και να μην μπορεί να εγκαταστήσει μη εξουσιοδοτημένα προγράμματα. Πρέπει να υπάρχουν λύσεις anti-virus και IDS/IPS. Πρέπει να γίνονται όλες οι κρίσιμες ενημερώσεις ασφαλείας.
Ασφάλεια Δικτύων/Επικοινωνιών	Χρήση κρυπτογραφημένων επικοινωνιών μέσω ασφαλών πρωτοκόλλων(TLS/SSL) όταν επιχειρείται απομακρυσμένη πρόσβαση
Αντίγραφα Ασφαλείας	Ο οργανισμός πρέπει να διαθέτει πολιτικές και διαδικασίες που αφορούν την λήψη αντιγράφων ασφαλείας καθώς και την επαναφορά των συστημάτων μέσω αυτών των αντιγράφων. Τα αντίγραφα ασφαλείας είναι απαραίτητο να προστατευόνται με τα ίδια φυσικά και περιβαλλοντικά μέτρα που προστατεύονται και τα αρχικά προσωπικά δεδομένα Η λήψη αντιγράφων ασφαλείας πρέπει να παρακολουθείται από ειδικό λογισμικό και συνιστάται να γίνεται τακτικά δοκιμή επαναφοράς μέσω των αντιγράφων ασφάλειας.
Φορητές/Κινητές Συσκευές	Ο τρόπος διαχείρισης των φορητών/κινητών συσκευών πρέπει να είναι καθορισμένος και καταγεγραμμένος. Οι φορητές/κινητές συσκευές πρέπει να εξουσιοδηθούν προτού έχουν πρόσβαση στα δεδομένα προσωπικού χαρακτήρα και ταυτόχρονα πρέπει να έχουν τεχνικά μέτρα προστασίας ανάλογα με τα υπόλοιπα τερματικά.
Ασφάλεια Εφαρμογών για τον Κύκλο Ζωής τους	Κατά τον κύκλο ζωής των εφαρμογών είναι απαραίτητο να ακολουθούνται οι πιο σύγχρονες πρακτικές και πρότυπα

	για την ασφάλεια τους. Οι απαιτήσεις ασφάλειας πρέπει να καθορίζονται στα πρώτα στάδια του κύκλου ζωής. Η χρήση τεχνολογιών ενίσχυσης ιδιωτικότητας καθώς και η υιόθετηση ασφαλών πρακτικών ανάπτυξης κώδικα είναι σημαντικές.
Ασφαλής Διαγραφή/Καταστροφή Δεδομένων	Ειδικό λογισμικό που κάνει ολοκληρωτική διαγραφή κάνοντας επεγγραφή στους δίσκους αλλιώς πρέπει να γίνεται φυσική καταστροφή των δίσκων. Αν τα δεδομένα προσωπικού χαρακτήρα υπάρχουν σε φυσική μορφή (π.χ. χάρτινα έγγραφα) πρέπει να καταστραφούν χρησιμοποιώντας ειδικό μηχάνημα.
Φυσική Ασφάλεια	Η φυσική περίμετρος της πληροφοριακής υποδομής του συστήματος δεν πρέπει να είναι προσβάσιμη από μη εξουσιοδοτημένο προσωπικό.

Πίνακας 6: Τεχνικά και Οργανωτικά Μέτρα για την Ασφάλεια των Δεδομένων

Αν η ανάλυση με βάση τα παραπάνω μέτρα, δηλαδή η αναγνώριση των υπαρχόντων μέτρων προστασίας καθώς και ο καθορισμός των νέων μέτρων που πρέπει να προστεθούν παρέχει αρκετές πληροφορίες ώστε να δρομολογηθούν ενέργειες που θα κάνουν το επίπεδο κινδύνου που έχει ο οργανισμός για μια επεξεργασία αποδεκτό, τότε δεν χρειάζεται κάποια περαιτέρω ανάλυση στον κίνδυνο αυτό.[132]

Σε περίπτωση που μετά την ανάλυση, θεωρήσει ο υπεύθυνος για την εκτέλεση της DPIA ότι οι πληροφορίες δεν είναι αρκετές , τότε ο υπεύθυνος θα πρέπει να επαναλάβει την διαδικασία της εκτίμησης κινδύνου με ένα αναθεωρημένο πλαίσιο(π.χ. διαφορετικά κριτήρια αποδοχής κινδύνου η αντικτύπου) σε ένα πιθανώς περιορισμένο πεδίο εφαρμογής και όχι ολόκληρο.

Ο υπεύθυνος για την εκτίμηση αντικτύπου θα πρέπει να εκτιμήσει τα επίπεδα του αντικτύπου και της πιθανότητας των υπολειπόμενων κινδύνων (των κινδύνων που παραμένουν μετά την εφαρμογή των μέτρων προστασίας που επιλέχθηκαν).Οι κίνδυνοι έπειτα μπορούν να απεικονιστούν στο διάγραμμα κινδύνου ιδιωτικότητας.[133]

[132] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[133] Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) methodology" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf [Πρόσβαση 29-11-2021], ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

Έπειτα , είναι απαραίτητο ο υπεύθυνος να εξηγήσει πως ο υπολειπόμενος κίνδυνος είναι αποδεκτός, βασισμένος στα νέα επίπεδα αντικτύπου και πιθανότητας.

6.4.1 Σχέδιο για την αντιμετώπιση κινδύνου

Εφόσον έχουν αναγνωριστεί τα μέτρα προστασίας που θα πρέπει να προστεθούν από τις προηγούμενες διαδικασίες πρέπει να καταρτιστεί το σχέδιο με το οποίο θα εφαρμοστούν τα μέτρα αυτά.[134]Το σχέδιο αυτό πρέπει να εκτιμά το κόστος (π.χ. οικονομικό,χρονικό) εφαρμογής των μέτρων.Σημαντικό στην κατάρτιση του σχεδίου είναι η διαβούλευση με τα κατάλληλα ενδιαφερόμενα μέρη.Ο οργανισμός κατά την διάρκεια κατάρτισης του σχεδίου πρέπει να ορίσει τον υπεύθυνο που θα αναλάβει την υλοποίηση του σχεδίου, ποιοι πόροι θα απαιτηθούν για την ολοκλήρωση του σχεδίου, ποιες ενέργειες ακριβώς πρέπει να γίνουν, το χρονικό διάστημα το οποίο χρείαζεται για την ολοκλήρωση.Τέλος ,πρέπει να καθοριστεί και πως θα αξιολογηθούν τα αποτελέσματα του σχεδίου.

Ένα σχέδιο αντιμετώπισης κινδύνου θα πρέπει να περιέχει τις εξής πληροφορίες:

- Αντιστοίχιση των μέτρων προστασίας με τους κινδύνους που προσπαθούν να μειώσουν/αφαιρέσουν.
- Μια λίστα από τα δεδομένα προσωπικού χαρακτήρα που πρόκειται να προστατευθούν.
- Τα άτομα που είναι υπεύθυνα για την έγκριση/απόρριψη του σχεδίου καθώς και τα άτομα που ευθύνονται για την υλοποίηση του σχεδίου.
- Τις προτεινόμενες ενέργειες για την αντιμετώπιση του κινδύνου.
- Τους ανθρώπινους πόρους που είναι απαραίτητοι για την υλοποίηση του σχεδίου.
- Τους τρόπους με τους οποίους θα παρακολουθείται η διενέργεια του σχεδίου για να διαπιστωθεί ότι λειτουργεί σωστά.
- Το χρονικό περιθώριο που χρειάζεται το σχέδιο.

7.ΔΗΜΙΟΥΡΓΙΑ ΑΝΑΦΟΡΑΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

[134] Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) methodology" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf [Πρόσβαση 29-11-2021]

Παρά το γεγονός ότι η σύνταξη αναφοράς μιας DPIA δεν είναι υποχρεωτική, η αναφορά αποτελεί ένα σημαντικό παράγωγο της εκτίμησης αντικτύπου.[135]Μια αναλυτική καταγραφή των αποτελεσμάτων όλων των παραπάνω βημάτων θα πρέπει να υπάρχει μέσα στην αναφορά.Σε αυτήν την αναφορά είναι σημαντικό να υπάρχει καταγεγραμμένη η αιτιολόγηση των αποφάσεων που θα παρθούν.[136]Επίσης η αναφορά αυτή θα συνταχθεί από το πρόσωπο που είναι υπεύθυνο για την εκτέλεση της DPIA και θα υπογραφτεί επίσημα από την διοίκηση του οργανισμού που εκτελεί την DPIA.Επιπροσθέτως, η αναφορά αυτή θα πρέπει να αξιολογηθεί και να συζητηθεί από τα αρμόδια άτομα της διοίκησης, με την βοήθεια και του DPO.Η αναφορά πρέπει να έχει κατάλληλη δομή για τα άτομα στα οποία ενδέχεται να κοινοποιηθεί. Τα ενδιαφερόμενα μέρη θα πρέπει να έχουν πρόσβαση στα συμφωνηθέντα τμήματα της αναφοράς της DPIA.

Το περιεχόμενο της αναφοράς της DPIA εξαρτάται σε σημαντικό βαθμό από τις κατηγορίες και την ευαισθησία των προσωπικών δεδομένων που επεξεργάζονται, το πεδίο εφαρμογής και τους στόχους της DPIA.Όπως προαναφέρθηκε, ορισμένα δεδομένα και πληροφορίες στην αναφορά της DPIA ενδέχεται να χαρακτηριστούν εμπιστευτικές. Μπορεί να περιέχονται ιδιωτικά επιχειρηματικά θέματα που δεν πρέπει να δημοσιοποιηθούν. Μέσα στην αναφορά μπορεί να υπάρχουν πληροφορίες αναφορικά με τα σχέδια αντιμετώπισης κινδύνου και τους υπολειπόμενους κινδύνους. Αυτές οι πληροφορίες ενδέχεται να αυξήσουν τον κίνδυνο παραβίασης των συστημάτων. Αν η επεξεργασία περιείχε ευαίσθητα δεδομένα προσωπικού χαρακτήρα ,αυτά θα πρέπει να υπάρχουν σε ένα εμπιστευτικό ξεχωριστό παράρτημα της αναφοράς , το οποίο δεν θα είναι διαθέσιμο σε όλους. Μια αναφορά που παρέχεται εμπιστευτικά σε έναν εξωτερικό ανεξάρτητο ελεγκτή ή σε μια αρχή προστασίας δεδομένων μπορεί να περιέχει περισσότερες πληροφορίες από αυτή που παρέχεται στο κοινό.

Μέσα στην αναφορά θα πρέπει να υπάρχει η δομή της, το πεδίο εφαρμογής της DPIA , τις απαιτήσεις ιδιωτικότητας που αναγνώρισε η ομάδα που την εκτέλεσε , την εκτίμηση επικινδυνότητας, το σχέδιο αντιμετώπισης κινδύνου καθώς και τα συμπεράσματα και τις αποφάσεις που λήφθηκαν μετά το τέλος της DPIA.Τέλος θα πρέπει να υπάρχει στην αναφορά μία σύνοψη για το κοινό προκειμένου να ενημερωθούν τα υποκείμενα των δεδομένων για τον κίνδυνο που σχετίζεται με το πρόγραμμα επεξεργασίας.

7.1 Δομή της Αναφοράς Εκτίμησης Αντικτύπου

[135] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

[136] Vemou, K. and Karyda, M. (2020), "Evaluating privacy impact assessment methods: guidelines and best practice", Information and Computer Security, Vol. 28 No. 1, pp. 35-53.Διαθέσιμο: https://doi.org/10.1108/ICS-04-2019-0047

Η αναφορά πρέπει να προσαρμοστεί στις συνθήκες του έργου που περιλαμβάνει την επεξεργασία.Γενικά όμως στο εξώφυλλο της , θα πρέπει να υπάρχει τουλάχιστον το όνομα της επεξεργασίας,το πληροφοριακό σύστημα ή πρόγραμμα , το όνομα του υπευθύνου επεξεργασίας και του οργανισμού που εκτελεί την DPIA , και άλλες λεπτομέρειες όπως η έκδοση της αναφοράς,ημερομηνία κλπ.

Η εισαγωγή της αναφοράς είναι σημαντικό να περιέχει τον λόγο εκτέλεσης της DPIA , το χρονικό διάστημα κατά το οποίο πραγματοποιήθηκε και ποια ήταν τα άτομα που ευθύνονταν για την εκτέλεση της.Επιπρόσθετα θα πρέπει να παρέχονται κάποιες βασικές πληροφορίες για την επεξεργασία , καθώς και ποιες οδηγίες ακολουθήθηκαν για την εκτέλεση της DPIA.Παράλληλα η εισαγωγή μπορεί να παρέχει γενικές πληροφορίες για τον οργανισμό (π.χ. τις πολιτικές ιδιωτικότητας του,τις υποχρεώσεις του οργανισμού κλπ.).

Αν η αναφορά της DPIA είναι εκτενής,θα πρέπει να συμπεριλαμβάνεται μια διοικητική σύνοψη που θα αναφέρει τα βασικά ευρήματα της εκτίμησης, τις συστάσεις που έγιναν κατά την εκτέλεση της καθώς και ποια ενδιαφερόμενα μέρη πήραν μέρος κατά την διαδικασία της διαβούλευσης.Φυσικά, η διοικητική σύνοψη θα περιέχει μια σύντομη περιγραφή του προγράμματος επεξεργασίας, του πληροφοριακού συστήματος, ή οτιδήποτε άλλο αποτέλεσε αντικείμενο της DPIA. Θα πρέπει να προσδιορίζει τις κύριες επιπτώσεις στην ιδιωτικότητα των υποκειμένων και τις εναλλακτικές λύσεις για την ελαχιστοποίηση ή την αποφυγή των αρνητικών επιπτώσεων.

7.2 Περιεχόμενο της Αναφοράς

Η αναφορά πρέπει να περιέχει το πεδίο εφαρμογής της DPIA που εκτελέστηκε.Η διοίκηση μπορεί να κάνει κάποια δήλωση σχετικά με τα όρια της εκτίμησης και ποια σημεία ήταν εκτός πεδίου εφαρμογής.Όπως και κατά την εκτέλεση της DPIA έτσι και στην αναφορά ,είναι πολύ σημαντικό ο οργανισμός να δώσει την πιο λεπτομερή περιγραφή της επεξεργασίας.[137]

Επίσης μέσα στην αναφορά πρέπει να υπάρχει περιγραφή των ροών των προσωπικών δεδομένων όπως έιχε αναλυθεί κατά την εκτέλεση της DPIA.Ενδεικτικά,ο τρόπος με τους οποίον ειδοποιούνται τα υποκείμενα για την επεξεργασία των δεδομένων τους, και τι ρόλο παίζει η συγκατάθεση τους στην επεξεργασία.Σε περίπτωση που γίνεται κάποια αντιστοίχιση με άλλα δεδομένα από άλλες πηγές πρέπει επίσης να είναι καταγεγραμμένο στην αναφορά το γεγονός αυτό καθώς και να αναφέρεται η νομική βάση που το επιτρέπει.Ο οργανισμός θα πρέπει να αναφέρει τον τρόπο με τον οποίο θα γίνει η διαγραφή των δεδομένων προσωπικού χαρακτήρα όταν αυτά γίνουν αχρείαστα. Θα πρέπει να αναφέρει ποιες διαδικασίες θα θέσει σε εφαρμογή για να επιτρέπει στα άτομα να βλέπουν τα δεδομένα τους και να τα διορθώνουν εάν είναι απαραίτητο ή να

[137] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

ζητήσουν τη διαγραφή τους.[138] Θα πρέπει να αναφέρει ποιες διαδικασίες υπάρχουν εάν ο οργανισμός αρνηθεί να διαγράψει τις πληροφορίες ή να επιτρέψει την πρόσβαση σε αυτές. Ο οργανισμός θα πρέπει επίσης να προσδιορίζει το κόστος, εάν υπάρχει, της δυνατότητας πρόσβασης του ατόμου στα δεδομένα του και πόσο χρόνο χρειάζεται ο οργανισμός για να ανταποκριθεί στα αιτήματα των υποκειμένων.

Μια αναφορά της DPIA είναι σημαντικό να έχει βασικές πληροφορίες σχετικά με τις απαιτήσεις του συστήματος που θα κάνει την επεξεργασία(π.χ. σκοπός επεξεργασία, επιχειρηματική δραστηριότητα, δικλείδες ασφάλειας κλπ.), πληροφορίες σχετικά με τον σχεδιασμό του συστήματος (π.χ. βάσεις δεδομένων, αρχιτεκτονική συστήματος, τα καταγεγραμμένα διαγράμματα από τις ροές δεδομένων κλπ.) , πληροφορίες σχετικά με τις πολιτικές και διαδικασίες που ακολουθεί ο οργανισμός για την επεξεργασία (π.χ. διαδικασίες λήψης αντιγράφων ασφάλειας, τους μηχανισμούς αυθεντικοποίησης για τα άτομα που θα αποκτήσουν πρόσβαση κλπ.).[139]Μια αναφορά μπορεί να περιέχει τα κριτήρια με τα οποία μετρήθηκε το επίπεδο του αντικτύπου και της πιθανότητας, καθώς και τα κριτήρια που μετρήθηκε ο αποδεκτός κίνδυνος. Ο οργανισμός μπορεί να περιλάβει στην αναφορά τα αποτελέσματα των διαβουλεύσεων με τα ενδιαφερόμενα και εμπλεκόμενα μέρη.[140]Όλες οι παραπάνω πληροφορίες πηγάζουν από τα εκάστοτε στάδια της DPIA.

Επίσης, στην αναφορά θα πρέπει να υπάρχουν πληροφορίες για την εκτίμηση επικινδυνότητας που πραγματοποιήθηκε από την ομάδα εκτέλεσης της DPIA και τι πηγές κινδύνου εντοπίστηκαν.Σημαντικό είναι να υπάρχει μια λίστα στην αναφορά που θα περιέχει τις απειλές ,την πιθανότητα ,τις επιπτώσεις και το αντίκτυπο τους όπως αυτά βρέθηκαν κατά την εκτέλεση της DPIA.Θα πρέπει ταυτόχρονα να αναφέρεται πως έγινε η αξιολόγηση των κινδύνων.

Μέσα στην αναφορά φυσικά πρέπει να υπάρχει και η ανάλυση που έγινε σχετικά με το επίπεδο συμμόρφωσης που έχει ο οργανισμός, τις απαιτήσεις ασφάλειας που εντοπίστηκαν καθώς και ποιο είναι το σχέδιο για να αντιμετωπιστούν οι κίνδυνοι που αναδείχθηκαν.[141]

Στο τέλος της αναφοράς θα πρέπει να υπάρχουν τα συμπεράσματα και ως αποτέλεσμα των συμπερασμάτων, οι αποφάσεις που πάρθηκαν κατά τη διάρκεια της διαδικασίας DPIA σχετικά με την αποδοχή των υπολειπόμενων κινδύνων για την προστασία της ιδιωτικότητας.

---

[138] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[139] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[140] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[141] Καθώς οι αποφάσεις για τον μετριασμό μέτρα τεκμηριώνονται, η έκθεση της DPIA επιτρέπει στη διοίκηση των οργανισμών να να αποδείξει τη συμμόρφωση με τον ΓΚΠΔ(‘Αρθρο 24)

7.3 Σύνοψη για το κοινό και δημοσιοποίηση της αναφοράς

Παρά το γεγονός ότι ο οργανισμός δεν είναι υποχρεωμένος νομικά να προχωρήσει σε δημοσιοποίηση της αναφοράς που θα συντάξει, υπάρχουν πλεονεκτήματα στο να το πραγματοποιήσει. Παρέχοντας πληροφορίες στα υποκείμενα των δεδομένων για την επεξεργασία και για τους κινδύνους που την συνοδεύουν ,λειτουργούν με περισσότερη διαφάνεια και ενθαρρύνουν την συγκατάθεση των υποκειμένων.

Μέσα στην σύνοψη που θα δημοσιευθεί, δεν χρειάζεται να υπάρχουν εμπορικά ευαίσθητες πληροφορίες που ενδέχεται να υπάρχουν στην πλήρης αναφορά και αρκεί να περιλαμβάνει μόνο τις πληροφορίες που αφορούν τα υποκείμενα των δεδομένων.Πιο συγκεκριμένα η σύνοψη για το κοινό πρέπει να περιέχει τις εξής πληροφορίες και να τις μεταδίδει με έυκολο και κατανοητό τρόπο:

- Τα οφέλη που έχει η επεξεργασία,το πρόγραμμα κλπ. για τα υποκείμενα.
- Τις κατηγορίες των προσωπικών δεδομένων που θα επεξεργαστούν.
- Μια περίληψη της ανάλυσης συμμόρφωσης.
- Μια περίληψη των μέτρων που χρησιμοποιούνται για να επιτευχθεί η συμμόρφωση με τους νόμους και η προστασία των δεδομένων προσωπικού χαρακτήρα.
- Ποιος είναι ο υπεύθυνος επεξεργασίας και ποιοι είναι οι τρόποι που μπορούν να επικοινωνήσουν μαζί τους για να επιλυθούν τα ζητήματα ιδιωτικότητας.

7.4 Επικύρωση της αναφοράς

Η αναφορά DPIA δεν χρειάζεται απαραίτητα να υπογραφτεί από την διοίκηση αλλά αυτό εξαρτάται από την φύση του έργου.Έαν πρόκειται για μια επεξεργασία μεγάλης κλίμακας , συνιστάται να εγκριθεί, πρώτα, από την ανώτερη διοίκηση. Η υπογραφή μπορεί επίσης να βοηθήσει στη διασφάλιση της παρακολούθησης των απαραίτητων ενεργειών προστασίας.[142]

8. ΕΦΑΡΜΟΓΗ ΤΩΝ ΣΧΕΔΙΩΝ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΙΝΔΥΝΟΥ

Μετά την επικύρωση-έγκριση της αναφοράς από τον υπεύθυνο εκτέλεσης της DPIA και την διοίκηση του οργανισμού πρέπει να γίνουν οι εξής ενέργειες,πριν ξεκινήσει η επεξεργασία όπου είναι δυνατόν:

- Ο οργανισμός πρέπει να καθορίσει τους πόρους για την εφαρμογή των μέτρων

[142] Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]

- Ο οργανισμός πρέπει να προσφέρει στα άτομα που θα έχουν συμμετοχή στο έργο επεξεργασίας την κατάλληλη εκπαίδευση αναφορικά με την προστασία της ιδιωτικότητας.
- Ο οργανισμός πρέπει να φροντίσει να είναι διαθέσιμη η ειδοποίηση ιδιωτικότητας για τους πιθανούς χρήστες σε περίπτωση που αρχίσει η επεξεργασία.
- Ο οργανισμός πρέπει να εφαρμόσει το σχέδιο αντιμετώπισης κινδύνου.

Ο οργανισμός μπορεί να μην λάβει υπόψη του όλες τις συστάσεις της DPIA, αλλά θα πρέπει να ενημερώνεται ο υπεύθυνος προστασίας δεδομένων του οργανισμού και η ανώτερη διοίκηση για το ποιες συστάσεις θα εφαρμοστούν και ποιες θα παραλειφθούν.

9. ΕΠΑΝΕΞΕΤΑΣΗ ΚΑΙ ΕΛΕΓΧΟΣ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ

Σημαντική ενέργεια που συνιστάται να πραγματοποιηθεί μετά το τέλος εκτίμησης αντικτύπου και της σύνταξης της αναφοράς είναι να γίνει η επανεξέταση και ο έλεγχος ολόκληρης της DPIA.Για να πραγματοποιηθεί σε μια κατάλληλη στιγμή η επανεξέταση και ο έλεγχος , ο οργανισμός συνιστάται να δημιουργήσει μία σχετική πολιτική.

Σε περίπτωση που είναι νομική απαίτηση[143] , μπορεί να χρειαστεί να γίνει εξέταση και έλεγχος από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.Ο υπεύθυνος προστασίας δεδομένων οφείλει να ενημερώσει την αρχή για το έργο επεξεργασίας και για τον υπολειπόμενο κίνδυνο, παρέχοντας και την αναφορά της DPIA.Δεν μπορεί να αρχίσει η επεξεργασία χωρίς την έγκριση της αρχής.

Σε πολλές περιπτώσεις συνιστάται να γίνει επανεξέταση και έλεγχος από έναν ανεξάρτητο τρίτο για να διασφαλιστεί ότι η DPIA πραγματοποιήθηκε σωστά και ότι ο οργανισμός εφαρμόζει τα σχέδια αντιμετώπισης κινδύνου.Αυτή η επανεξέταση και έλεγχος δίνει μία επιπλέον αξιοπιστία στην αναφορά της DPIA και βελτιώνεται και η διαφάνεια.Αν κάποιος εξωτερικός τρίτος έχει πραγματοποιήσει την DPIA εκ μέρους του οργανισμού τότε δεν πρέπει ο ίδιος να κάνει την επανεξέταση.

10.ΕΝΗΜΕΡΩΣΗ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ

Πολλά έργα επεξεργασίας αλλάζουν πριν καν αρχίσουν. Και αφού ξεκινήσουν ενδέχεται να γίνουν αλλαγές σε αυτά εξαιτίας του γεγονότος ότι το περιβάλλον γύρω τους αλλάζει (τεχνολογικά,νομικά, οι απαιτήσεις των υποκειμένων όσον αφορά την

[143] Αν ο υπολειπόμενος κίνδυνος είναι υψηλός – Άρθρο 36 ΓΚΠΔ

ιδιωτικότητα τους μπορεί να αλλάξουν). Η επιχειρηματική δραστηριότητα ακόμα , ενδέχεται να αλλάξει.

Εξαιτίας αυτών των αλλαγών ένας οργανισμός συνιστάται να διαθέτει έναν μηχανισμό για την επικαιροποίηση της Εκτίμησης Αντικτύπου ανάλογα με τις ανάγκες, ιδίως εάν υπάρχουν υπάρχουν σημαντικές αλλαγές στην δραστηριότητα που επηρεάζει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα.[144]Ο οργανισμός πρέπει να εξηγεί επίσης γιατί πραγματοποιήθηκαν αυτές οι αλλαγές.

Ο Υπεύθυνος Προστασίας Δεδομένων μπορεί να ξεκινήσει μια τέτοια ενημέρωση και μάλιστα να ζητήσει νέο κύκλο αξιολόγησης, εάν είναι απαραίτητο. Αυτό θα ικανοποιεί επίσης το άρθρο 24 του ΓΚΠΔ και 25 για την επανεξέταση και την επικαιροποίηση των επιλεγμένων μέτρων[145], λαμβάνοντας υπόψη την τελευταία λέξη της τεχνολογίας και το πλαίσιο και τους κινδύνους της επεξεργασίας.

Εάν οι τροποποιήσεις είναι σημαντικές και οδηγούν σε σημαντικές πρόσθετες επιπτώσεις στην ιδιωτικότητα των υποκειμένων που δεν εξετάστηκαν στην DPIA, μπορεί να απαιτηθεί νέα DPIA, ακολουθώντας τα προαναφερθέντα στάδια.

Το βήμα αυτό ολοκληρώνεται με την νέα αναφορά της DPIA ή με την απόφαση να ξεκινήσει μια νέα DPIA.

[144] ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[145] Άρθρο 24 Παρ.1 ΓΚΠΔ '' Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο.''

11.ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε αυτήν την εργασία αναλύθηκε η διαδικασία εκτίμησης αντικτύπου σχετικά με τα δεδομένα προσωπικού χαρακτήρα όπως αυτή περιγράφεται στο άρθρο 35 του Γενικού Κανονισμού Προστασίας Δεδομένων.Ειδικά , παρέχονται πληροφορίες για το πως να διενεργηθεί η εκτίμηση και ποιος θα εμπλακεί σε αυτήν.

Αναφέρθηκαν οι προϋποθέσεις με τις οποίες θα επιλέξει ο υπεύθυνος ενός οργανισμού αν είναι υποχρεωτική ή όχι η διενέργεια της εκτίμησης αντικτύπου σύμφωνα με τις οδηγίες της Ομάδας Εργασίας του άρθρου 29 και της ελληνικής Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.Μέσα από την ανάλυση σχετικών μεθοδολογιών αναγνωρίστηκαν πρακτικές που παίζουν σημαντικό ρόλο για την επιτυχία της εκτίμησης αντικτύπου καθώς και τα θετικά αποτελέσματα που μπορεί να αποκτήσει ο οργανισμός που την εκτελεί. Η διερεύνηση των θεμάτων για την προστασία της ιδιωτικότητας από τη σκοπιά ενός οργανισμού, για παράδειγμα, οδηγεί σε μια πιο ολοκληρωμένη κατανόηση των κινδύνων που ελλοχεύουν και προτρέπει σε μια καλύτερη προσπάθεια αντιμετώπισης ή πρόληψης των κινδύνων για την προστασία της ιδιωτικότητας. Για να επιτευχθεί η προστασία των προσωπικών δεδομένων μέσω σχεδιασμού(Privacy by Design), είναι επίσης προτιμότερο να εξαλειφθούν τα θέματα ιδιωτικότητας παρά να αντιμετωπιστούν, αξιολογώντας τη διαδικασία επεξεργασίας δεδομένων και αποφασίζοντας να ελαχιστοποιηθεί η επεξεργασία συγκεκριμένων δεδομένων, εάν δεν είναι κρίσιμα για τον επιθυμητό στόχο.

Αργότερα αναλύθηκε ο τρόπος με τον οποίο διενεργείται η εκτίμηση αντικτύπου σύμφωνα με διάφορες μεθοδολογίες.Συγκεκριμένα αναφέρθηκε πως γίνεται η περιγραφή των ροών δεδομένων,πως γίνεται η αναγνώριση και αξιολόγηση κινδύνων και πως εκτιμάται το αντίκτυπο.Είναι σημαντικό να αναφερθεί ότι στην εργασία αναφέρθηκαν ενδεικτικά κάποιοι κινδύνοι αλλά αυτοί οι κίνδυνοι δεν υπάρχουν σε όλους τους επιχειρηματικούς τομείς και ταυτόχρονα, όσο εξελίσσεται η τεχνολογία μπορεί να δημιουργηθούν νέοι κίνδυνοι.

Έπειτα, αναφέρθηκε η αξιολόγηση των μέτρων ασφαλείας καθώς και πως γίνεται η πρόταση νέων μέτρων, καθώς και πως δημιουργείται το σχέδιο για την εφαρμογή των μέτρων αυτών.Τέλος αναφέραμε πως συντάσσεται η αναφορά της εκτίμησης αντικτύπου καθώς και ο τελικός έλεγχος της.

Συμπερασματικά, η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι μια νομική υποχρέωση για τις εταιρείες και αποτελεί έναν τρόπο για να προστατευθούν τα προσωπικά δεδομένα και η ιδιωτικότητα των ατόμων.Για αυτόν τον λόγο είναι σημαντικό να διενεργείται σωστά.

12. ΒΙΒΛΙΟΓΡΑΦΙΑ

[1].Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679&from=EL

[2].Οδηγία (ΕΕ) 2016/680 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EN

[3].Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα - 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 Διαθέσιμο: https://www.dpa.gr/sites/default/files/2019-10/article_35_dpia_list_gr_2.pdf [Πρόσβαση 05-04-2022]

[4].ISO/IEC 29134 (2017) - Code of practice for personally identifiable information protection - BSI Standards Publication

[5].Νόμος υπ'αριθ. 3979/2011 - Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις

[6].ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ ΤΟΥ ΑΡΘΡΟΥ 29 ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ-Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679. WP 248(2017)

[7].Wright D., & de Hert P. eds. Privacy Impact Assessment. Springer, Dordrecht, 2012

[8].Katerina Demetzou – Data Protection Impact Assessment:A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation – Elsevier (2019)

[9].Office of the Victorian Information Commissioner. Privacy by Design: Effective Privacy Management in the Victorian public sector , Cavoukian, A

[10].van Dijk, N., Gellert, R. and Rommetveit, K. 'A Risk to a Right: Beyond Data Protection Risk Assessments' (2016) Volume 32, Issue 2

[11].Article 29 Data Protection Working Party, 'Opinion 05/2014 on Anonymisation Techniques' Διαθέσιμο: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf [Πρόσβαση 30-11-2021]

[12].Guide to undertaking privacy impact assessments (PIA Guide) – Office of the Australian Information Commissioner Διαθέσιμο:

https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments [Πρόσβαση 28-12-2021]
[13].Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) methodology" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf [Πρόσβαση 29-11-2021]
[14].Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) template" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf [Πρόσβαση 29-11-2021]
[15].Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) Knowledge Bases" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases [Πρόσβαση 30-11-2021]
[16].Commission Nationale de l'Informatique et des Libertes (CNIL) (2018), "Privacy impact assessment (PIA) Application to Connected Objects" Διαθέσιμο: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf [Πρόσβαση 30-11-2021]
[17].ENISA – Risk Management – Glossary Διαθέσιμο: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary
[18].International Organization for Standardization (ISO), Information Technology – Security Techniques – Information Security Risk Management, International Standard, ISO/IEC 27005:2008(E), First edition, 15 Ιουνιίου 2008
[19].Κοινωνική μηχανική - Βικιπαίδεια (wikipedia.org) < https://el.wikipedia.org/wiki/Κοινωνική_μηχανική > Accessed 31-12-2021
[20].Yoichi Seto – Application of Privacy Impact Assessment in the Smart City - Electronics and Communications in Japan, Vol. 98, No. 2, 2015 (Translated from Denki Gakkai Ronbunshi, Vol. 133-C, No. 7, July 2013, pp. 1427–1435)
[21].What Is Data Protection And Why Is It Important? - The Freeman Online [n.d] Διαθέσιμο στο : https://www.thefreemanonline.org/what-is-data-protection-and-why-is-it-important [Πρόσβαση 05-01-2022]
[22].4 Ways Data Protection can increase your Competitive Advantage - Debb Gannaway(2019) Διαθέσιμο: https://dgtechllc.com/4-ways-data-protection-can-increase-your-competitive-advantage/ [Πρόσβαση 05-01-2022]
[23].Cisco – What is penetration Testing Διαθέσιμο https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html [Πρόσβαση 06-01-2022]
[24].John J. Fay, David Patterson, in Contemporary Security Management (Fourth Edition), 2018 Διαθέσιμο: https://www.sciencedirect.com/topics/computer-science/vulnerability-assessment [Πρόσβαση 06-01-2022]
[25].DHS, PIAs: The Privacy Office Official Guidance Περισσότερα : https://www.dhs.gov/privacy-impact-assessments [Πρόσβαση 06-01-2022]

[26].Transparency - European Data Protection Supervisor Διαθέσιμο :https://edps.europa.eu/data-protection/our-work/subjects/transparency_en [Πρόσβαση 06-01-2022]
[27].ICO – Transparency < https://ico.org.uk/for-organisations/accountability-framework/transparency/#:~:text=Transparency%20is%20a%20key%20data%20protection%20principle%20which,complex%20or%20if%20it%20relates%20to%20a%20child. > [Πρόσβαση 07-01-2022]
[28].ISO/IEC 29100 (2011) - Privacy framework
[29].Guide to undertaking privacy impact assessments (PIA Guide) – Office of the Australian Information Commissioner(OAIC) Διαθέσιμο: <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments> [[Πρόσβαση 28-12-2021]
[30].PIA Framework for RFID Applications(2011), Διαθέσιμο https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf [Πρόσβαση 15-01-2022]
[31].Privacy, Data Breach and Reputation Management – Data Privacy Manager 2020 https://dataprivacymanager.net/data-breach-and-reputation-management/ [Πρόσβαση 03-01-2022]
[32].Stewart, Blair, Privacy Impact Assessment Handbook, Office of the Privacy Commissioner, Auckland, 2015 Διαθέσιμο: https://privacy.org.nz/publications/guidance-resources/privacy-impact-assessment-handbook/ [Πρόσβαση 05-01-2022]
[33].Office of the Privacy Commissioner,2015 Privacy Impact Assessment Toolkit – Part 2 How to do a Privacy Impact Assessment Διαθέσιμο: https://privacy.org.nz/assets/New-order/Resources-/Publications/Guidance-resources/Privacy-Impact-Assessment-Part-2-FA.pdf [Πρόσβαση 03-03-2022]
[34]. Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Version 2.0, 2009 Διαθέσιμο: https://www.academia.edu/1321883/ICO_Privacy_Impact_Assessment_Handbook
[35].Stefan Strauß - Privacy and Identity in a Networked Society Refining Privacy Impact Assessment-Routledge (2019)
[36].Information and Privacy Office, Management Board Secretariat, Ontario, Privacy Impact Assessment: A User's Guide, June 2001
[37].Clarke, Roger, "Privacy Impact Assessment Guidelines", Xamax Consultancy Pty Ltd, February 1998. < http://www.xamax.com.au/DV/PIA.html> [Πρόσβαση 30 19-01-2022]
[38].Information Commissioner's Office (ICO) - Conducting privacy impact assessments – Code Of Practice [n.d] Διαθέσιμο: https://ico.org.uk/media/about-the-ico/consultations/2052/draft-conducting-privacy-impact-assessments-code-of-practice.pdf [Πρόσβαση 20-01-2022]
[39].Vemou, K. and Karyda, M. (2020), "Evaluating privacy impact assessment methods: guidelines and best practice", Information and Computer Security, Vol. 28 No. 1, pp. 35-53.Διαθέσιμο: https://doi.org/10.1108/ICS-04-2019-0047

[40].Majed Alshammari and Andrew Simpson - Towards an Effective Privacy Impact and Risk Assessment Methodology: Risk Analysis – Springer (2018)

[41].Βικιπαίδεια Διαθέσιμο: https://en.wikipedia.org/wiki/COMPAS_(software) [Πρόσβαση 22-10-21]/

[42].'Data matching: concepts and techniques for record linkage, entity resolution, and duplicate detection''- Peter Christen - Springer-Verlag Berlin Heidelberg(2012)

[43].Sam Corbett-Davies, Emma Pierson, Avi Feller and Sharad Goel (2016)- A computer program used for bail and sentencing decisions was labeled biased against blacks. It's actually not that clear. – The Washington post Διαθέσιμο:https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/ [Πρόσβαση 22-10-21]

[44].Sourya Joyee De and Daniel Le M´etayer "A Refinement Approach for the Reuse of Privacy Risk Analysis Results " (2016) – Morgan & Claypool Publishers

[45].Reuben Binns - Data protection impact assessments: a meta-regulatory approach International Data Privacy Law (2017) 7 (1): 22-35. DOI: https://doi.org/10.1093/idpl/ipw027 Published: 28 April 2017

[46].Βικιπαίδεια (Wikipedia) Διαθέσιμο: https://el.wikipedia.org/wiki/Συνάρτηση_κατατεμαχισμού [Πρόσβαση 04-04-2022]

[47].Injection – Owasp (2021) https://owasp.org/Top10/A03_2021-Injection/

[48].H.M.A. van Beek, E.J. van Eijk, R.B. van Baar, M. Ugen, J.N.C. Bodde, A.J. Siemelink, Digital forensics as a service: Game on, Digital Investigation, Volume 15, 2015, Pages 20-38, https://doi.org/10.1016/j.diin.2015.07.004. (https://www.sciencedirect.com/science/article/pii/S1742287615000857)

[49].Cloudflare – What is a DDoS attack Διαθέσιμο: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ [Πρόσβαση 06-02-2022]

[50].ENISA - Handbook on Security of Personal Data Processing (2017) Διαθέσιμο: https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing [Πρόσβαση 20-04-2022]

[51].David Wright – The state of the art in privacy impact assessment – Elsevier (2012)

[52].A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation -Felix Bieker , Michael Friedewald , Marit Hansen, Hannah Obersteller, and Martin Rost – Springer (2016)

[53].Why you need Privacy Awareness Training- Information Managers Διαθέσιμο : https://informationmanagers.ca/privacy-awareness-training/ [Πρόσβαση 10-02-2022]

[54].Larry G. Wlosinski - The Benefits of Information Security and Privacy Awareness Training Programs – ISACA(2019) Διαθέσιμο: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2019/volume-1/the-benefits-of-information-security-and-privacy-awareness-training-programs_joa_eng_0219.pdf [Πρόσβαση 07-04-2022]

[55].Van Blarkom GW, Borking JJ, Olk JGE (eds.) (2003) The handbook of privacy and privacy enhancing technologies: the case of intelligent software agents.The Hague, Hes R, Borking J (eds) (2000) Privacy-enhancing technologies: the path to anonymity
[56].Types of Authentication Methods – OptimalIdm Διαθέσιμο: https://optimalidm.com/resources/blog/types-of-authentication-methods/ [Πρόσβαση 05-04-2022]
[57].Office of the Australian Information Commissioner - Part 3: Responding to data breaches — four key steps Διαθέσιμο: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-3-responding-to-data-breaches-four-key-steps [Πρόσβαση 08-04-2022]
[58].Data Processing Agreement (DPA) -GDPRregister [n.d] Διαθέσιμο: https://www.gdprregister.eu/gdpr/data-processing-agreement-dpa/ [Πρόσβαση 25-04-2022]
[59].Βικιπαίδεια(Wikipedia) - Σκάνδαλο δεδομένων Facebook-Cambridge Analytica Διαθέσιμο: https://el.wikipedia.org/wiki/Σκάνδαλο_δεδομένων_Facebook-Cambridge_Analytica [Πρόσβαση 05-03-2022]
[60].ICO – Security Διαθέσιμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ [Πρόσβαση 05-05-2022]