ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

Η ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Διπλωματική Εργασία

του

Βογιάκη Γεωργίου

Θεσσαλονίκη, Φεβρουάριος 2024

Η ΜΕΘΟΔΟΛΟΓΙΑ ΤΗΣ ΕΚΤΙΜΗΣΗΣ ΑΝΤΙΚΤΥΠΟΥ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Βογιάκης Γεώργιος

Πτυχίο Νομικής Σχολής, Δημοκρίτειο Πανεπιστήμιο Θράκης, 2020

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπουσες Καθηγήτριες:
Μαρία Μυλώση
Ευγενία Αλεξανδροπούλου

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 04/03/2024

Μαρία Μυλώση	Ευγενία Αλεξανδροπούλου	Ψάννης Κωνσταντίνος
.....	.....	.....

Βογιάκης Γεώργιος

Abstract

With the implementation of the "General Data Protection Regulation", data controllers are faced with new challenges and opportunities to address the risks posed by increasing technological developments. One of the most complex of these is the obligation to carry out a data protection impact assessment. In particular, a Data Protection Impact Assessment has a proactive character and its purpose is to prevent risks at an early stage. The Data Protection Impact Assessment is a 'live' tool and not a one-off procedure, and its methodology is an ongoing process. The effective conduct of impact assessments is expected to be a matter of concern for both science and practice in the coming years, as the risks posed by new technologies are constantly increasing and, as a result, the need to find effective methods to prevent them is of paramount importance. In this paper I present the most popular methodological approaches in Greece, approaching step by step how to conduct a generic personal data impact assessment. The aim of this paper is to identify those common patterns through the methodological approaches and to lay the foundations for a successful impact assessment, i.e. an in-depth and systematic risk study that produces consistent and verifiable results.

Keywords

Data Protection Impact Assessment Methodology, DPIA, Conduct of Data Protection Impact Assessment, Data Protection, Risk, Risk Management, Risk assessment

Περίληψη

Με την εφαρμογή του «Γενικού Κανονισμού για την Προστασία Δεδομένων» οι υπεύθυνοι επεξεργασίας έρχονται αντιμέτωποι με νέες προκλήσεις αλλά και ευκαιρίες για την αντιμετώπιση των κινδύνων που προκαλεί η αυξανόμενη τεχνολογική εξέλιξη. Μία από τις πιο σύνθετες περιπτώσεις αυτών αποτελεί η υποχρέωση για διενέργεια εκτίμησης αντικτύπου προσωπικών δεδομένων. Ειδικότερα, η Εκτίμηση Αντικτύπου έχει προληπτικό χαρακτήρα και σκοπός της είναι να προλάβει κινδύνους σε ένα πρώιμο στάδιο. Η εκτίμηση αντικτύπου προσωπικών δεδομένων αποτελεί ένα «ζωντανό» εργαλείο και όχι μία διαδικασία που διενεργείται άπαξ, ενώ η μεθοδολογία αυτής αποτελεί σημείο το οποίο βρίσκεται υπό εξέλιξη. Η αποτελεσματική διενέργεια εκτίμησης αντικτύπου, αναμένεται τα επόμενα χρόνια να απασχολήσει τόσο την επιστήμη όσο και την πράξη, καθώς οι κίνδυνοι που δημιουργούνται από τις νέες τεχνολογίες αυξάνονται συνεχώς και ως εκ τούτου, η ανάγκη εξεύρεσης

αποτελεσματικών μεθόδων, για την πρόληψη τους, είναι βαρύνουσας σημασίας. Στην παρούσα εργασία παρουσιάζονται οι δημοφιλέστερες μεθοδολογικές προσεγγίσεις στην Ελλάδα, προσεγγίζοντας βήμα – βήμα τον τρόπο που διενεργείται μία γενική («generic») εκτίμηση αντικτύπου προσωπικών δεδομένων. Ζητούμενο της εργασίας αυτής είναι να εντοπίσει εκείνα τα κοινά μοτίβα μέσα από τις μεθοδολογικές προσεγγίσεις και να θέσει τις βάσεις για μία επιτυχημένη εκτίμηση αντικτύπου, δηλαδή μία εις βάθος και συστηματική μελέτη των κινδύνων που παράγει συνεπή και επαληθεύσιμα αποτελέσματα.

Λέξεις-Κλειδιά
Μεθοδολογία Εκτίμησης Αντικτύπου, ΕΑΠΔ, Διενέργεια Εκτίμησης Αντικτύπου, Προστασία Προσωπικών Δεδομένων, Κίνδυνος, Αξιολόγηση Κινδύνου, Μελέτη Εκτίμησης Αντικτύπου

Αφιερώσεις – Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω την διευθύντρια του μεταπτυχιακού προγράμματος «Δίκαιο & Πληροφορική» και όλους τους υπόλοιπους καθηγητές για τις πολύτιμες γνώσεις που μας προσέφεραν.

Ιδιαιτέρως, ωστόσο, θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια μου, κυρία Μυλώση Μαρία, για την πολύτιμη συνεισφορά, βοήθεια και καθοδήγηση της, από την πρώτη στιγμή μέχρι και την τελευταία.

Η εργασία αυτή είναι αφιερωμένη στην οικογένεια μου και στους φίλους μου συναδέλφους και μη, με τους οποίους έχουμε διαμορφωθεί μαζί ως άνθρωποι, ως επιστήμονες και ως πολίτες.

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος **7**

1. Εισαγωγή για την εκτίμηση αντικτύπου **7**

2. Η μεθοδολογία και ο σκοπός της συγκεκριμένης εργασίας **11**

3. Εκτίμηση Αντικτύπου και Λογοδοσία **15**

4. Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση **17**

5. Πριν την μεθοδολογία μίας ΕΑΠΔ **18**

5.1 Οι κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29. 20

5.2 Οι κατευθυντήριες οδηγίες του Ευρωπαίου Επόπτη Προστασίας Δεδομένων. .. 21

6. Έλεγχος για την διενέργεια Εκτίμησης Αντικτύπου (Threshold Analysis – Φάση Εκκίνησης) **21**

6.1 Ποιος έχει την ευθύνη για την εκπόνηση μιας ΕΑΠΔ; 21

6.2 Πότε (χρονικά) πρέπει να διενεργείται μια ΕΑΠΔ. 23

6.3 Πότε (ποιοτικά) πρέπει να διενεργείται μια ΕΑΠΔ – Περιπτωσιολογία 25

6.4 Πότε (ποιοτικά) πρέπει να διενεργείται μια ΕΑΠΔ – Τα κριτήρια της ομάδας του άρθρου 29 27

6.5. Πότε (ποιοτικά) πρέπει να διενεργείται μια ΕΑΠΔ – Το κριτήριο του «Υψηλού Κινδύνου – Ανεξάρτητος Έλεγχος του υπευθύνου επεξεργασίας» 29

7. Η απαραίτητη προεργασία μίας ΕΑΠΔ. **31**

7.1 Δημιουργία αρχείων δραστηριοτήτων επεξεργασίας, καθορισμός των νομικών βάσεων, εντοπισμός των εμπλεκομένων μερών και εκτίμηση της αναγκαιότητας 31

7.2 Οι Στόχοι Προστασίας κατά την «SDM» 36

7.2.1. 1ος Στόχος. Ελαχιστοποίηση των δεδομένων (Data Minimization) 37

7.2.2. 2ος Στόχος. Διαθεσιμότητα (Availability) 38

7.2.3. 3ος Στόχος. Ακεραιότητα (Integrity) 39

7.2.4. 4ος Στόχος. Εμπιστευτικότητα (Confidentiality) 40

7.2.5. 5ος Στόχος. Η μη διασύνδεση των δεδομένων των υποκειμένων (Unlikability) 40

7.2.6. 6ος Στόχος. Διαφάνεια (Transparency) 41

7.2.7. 7ος Στόχος. Δυνατότητα Παρέμβασης (Intervenability) 42

8. Πρώτη φάση της ΕΑΠΔ (Φάση Προετοιμασίας) **43**

8.1 Γενική επισκόπηση της συστηματικής περιγραφής της επεξεργασίας 43

8.1.1. Η προσέγγιση του ICO. 45

8.1.1.1. Περιγραφή της Φύσης της επεξεργασίας 45

8.1.1.2. Περιγραφή του πεδίου εφαρμογής της επεξεργασίας 49

8.1.1.3. Περιγραφή του πλαισίου της επεξεργασίας 51
8.1.1.4. Περιγραφή του σκοπού της επεξεργασίας 53
8.1.2. Η προσέγγιση της CNIL. 53
8.1.3 Η προσέγγιση του Fraunhofer Institute 56
8.1.3.1 Εντοπισμός των υποκειμένων των δεδομένων 57
8.1.3.2. Εντοπισμός λοιπών εμπλεκομένων μερών 58
8.1.3.3. Καθορισμός της ομάδας διενέργειας της ΕΑΠΔ 60
8.1.4 Λοιπές προσεγγίσεις 60
8.1.5 Η προσέγγιση της «Νομολογίας» για την συστηματική περιγραφή 64
8.1.6 Μία λύση στο πρόβλημα της πολυπλοκότητας της συστηματικής περιγραφής. 67
9. Δεύτερη φάση της ΕΑΠΔ (Φάση Υλοποίησης) 69
9.1 Γενική επισκόπηση του κινδύνου στο πλαίσιο της ΕΑΠΔ. 70
9.1.1 Η προσέγγιση του Fraunhofer Institute. 72
9.1.1.1. Συμμετοχική μέθοδος για την ανάλυση της ΕΑΠΔ (Participatory workshop-based method) 73
9.1.1.2. Ο ορισμός του κινδύνου στον ΓΚΠΔ 74
9.1.1.3. Είδη Ζημίας 74
9.1.1.4. Περιπτώσεις «γεγονότων» 76
9.1.1.5. Εντοπισμός και ανάλυση κινδύνου 76
9.1.1.6. Αξιολόγηση κινδύνου 79
9.1.1.7. Επιλογή μέτρων αντιμετώπισης των κινδύνων 79
9.1.1.8. Αξιολόγηση της αναγκαιότητας και της αναλογικότητας 80
9.1.2 Η προσέγγιση του ICO 80
9.1.3 Η προσέγγιση της CNIL 83
9.1.3.1 Ο κίνδυνος σύμφωνα με την προσέγγιση της CNIL 83
9.1.3.2. Πηγές κινδύνου 84
9.1.3.3. Είδη αποτελεσμάτων των απευκταίων γεγονότων 84
9.1.3.4. Απειλές 85
9.1.3.5. Κλίμακα και μεθοδολογία για την εκτίμηση της σοβαρότητας. 86
9.1.3.6. Κλίμακα και μεθοδολογία για την εκτίμηση της πιθανότητας 87
9.1.3.7. Αξιολόγηση των Υφιστάμενων και Προβλεπομένων μέτρων προστασίας. 87
9.1.3.8. Αξιολόγηση του κινδύνου: Πιθανές παραβιάσεις της ιδιωτικότητας. 88
9.1.3.9. Στόχοι για την αντιμετώπιση των κινδύνων 89
9.1.4 ISO 29134 90
9.1.4.1. Εντοπισμός του Κινδύνου 90
9.1.4.2. Ανάλυση του Κινδύνου 91

9.1.4.3. Κατηγοριοποίηση του Κινδύνου 92
9.1.4.4. Επιλογές αντιμετώπισης των κινδύνων 92
9.1.4.5. Καθορισμός των μέτρων αντιμετώπισης 93
10. Τρίτη φάση της ΕΑΠΔ (Φάση Εφαρμογής).....94
11. Τέταρτη φάση της ΕΑΠΔ (Φάση Περιοδικής Επαναξιολόγησης).....94
12. Τελικά συμπεράσματα.....95
12.1 Η συστηματική προσέγγιση της ΕΑΠΔ ως απόρροια της αρχής της Διαφάνειας και της Λογοδοσίας 95
12.2 Η εκτίμηση αντικτύπου δεν είναι ένας απλός έλεγχος νομιμότητας 97
12.3 Το πρόβλημα της αξιολόγησης των ΕΑΠΔ 99
12.4 Το πρόβλημα της ορολογίας..... 100
13. Επίλογος.....100
14. Βιβλιογραφία 101

Πρόλογος

1. Εισαγωγή για την εκτίμηση αντικτύπου.

Κατά τις επιταγές του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ)[1] οι υπεύθυνοι επεξεργασίας οφείλουν να εφαρμόζουν ενδεδειγμένα μέτρα για να διασφαλίζουν και να είναι σε θέση να αποδεικνύουν τη συμμόρφωση προς τον ΓΚΠΔ, λαμβάνοντας υπόψη μεταξύ άλλων «τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων» (άρθρο 24 παράγραφος 1). Η υποχρέωση των υπεύθυνων επεξεργασίας για τη διενέργεια Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων (ΕΑΠΔ) σε ορισμένες περιστάσεις θα πρέπει να εξετάζεται σε σχέση με τη γενική τους υποχρέωση να διαχειρίζονται με ενδεδειγμένο τρόπο τους κινδύνους που ενέχει η επεξεργασία των δεδομένων προσωπικού χαρακτήρα.[2]

[1]Βλ. Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

[2]Βλ. 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. Ομάδα εργασίας άρθρου 29.

Ειδικότερα, σύμφωνα με το άρθρο 35 παρ.1 του ΓΚΠΔ ορίζεται ότι « Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους. »

Έτσι, λοιπόν, θεμελιώνεται η υποχρέωση του υπευθύνου επεξεργασίας κάτω από ορισμένες περιστάσεις και σε συγκεκριμένο χρονικό πλαίσιο να εκπονήσει μία «Εκτίμηση Αντικτύπου». Το ερώτημα που προκύπτει, λοιπόν, τι είναι μία «Εκτίμηση Αντικτύπου». Την απάντηση στο παραπάνω ερώτημα έρχεται να δώσει η ομάδα εργασίας του άρθρου 29 και συγκεκριμένα αναφέρει ότι « Η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων είναι μια διαδικασία που έχει σχεδιαστεί για να περιγράψει την επεξεργασία, να αξιολογήσει την αναγκαιότητα και την αναλογικότητά της και να συνδράμει στη διαχείριση των κινδύνων για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων που συνεπάγεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, με την αξιολόγησή τους και τον καθορισμό μέτρων για την αντιμετώπισή τους»[3]

Στο ίδιο άρθρο και στην παράγραφο επτά (7) ορίζεται μάλιστα και το λεγόμενο «ελάχιστο περιεχόμενό της. Ειδικότερα, η εκτίμηση περιέχει τουλάχιστον:

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

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

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

[3] Βλ. 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. Ομάδα εργασίας άρθρου 29, Σελ 4.

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

Ο νομοθέτης, ωστόσο, επιλέγει να καθορίσει μόνο το ελάχιστο περιεχόμενο μιας Εκτίμησης Αντικτύπου. Αυτό καταδεικνύεται εξάλλου και από την λέξη «τουλάχιστον» που επιλέγει να χρησιμοποιήσει.

Επιπλέον, στην παράγραφο 3 του ίδιου άρθρου ορίζεται ότι:

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

α)συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β)μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ)συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.»

Και σε αυτή την περίπτωση, λοιπόν, ο νομοθέτης επιλέγει να απαριθμήσει ενδεικτικώς («ιδίως») τις περιπτώσεις στις οποίες επιβάλλεται να γίνει μία εκτίμηση αντικτύπου. Παρόλα αυτά, ήδη, από το άρθρο 1 του άρθρου 35 θέτει μια γενική υποχρέωση, σύμφωνα με την οποία ο υπεύθυνος επεξεργασίας υποχρεούται να εκπονήσει μία εκτίμηση αντικτύπου όταν αυτή «ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων»

Τέλος, και πάλι στο άρθρο 35 παράγραφος 1 ο νομοθέτης ορίζει το χρονικό πλαίσιο μέσα στο οποίο πρέπει να εκπονηθεί μία εκτίμηση αντικτύπου. Ειδικότερα, το ως άνω πλαίσιο

ορίζεται ως «πριν από την επεξεργασία**»,** επαληθεύοντας και σε αυτή την περίπτωση τις αρχές By Default και By Design.[4]

Συμπερασματικά, λοιπόν, φαίνεται πως νομοθετικά ρυθμίζεται:

1) Το ελάχιστο περιεχόμενο που θα πρέπει να έχει μία Εκτίμηση Αντικτύπου
2) Το πότε και το ποιος έχει την υποχρέωση να εκπονήσει μία Εκτίμηση Αντικτύπου
3) Το χρονικό σημείο το οποίο θα πρέπει να εκπονηθεί μία ΕΑΠΔ.

Παρόλα αυτά, σε κανένα σημείο του νόμου, τόσο στο σώμα αυτού όσο και στις αιτιολογικές σκέψεις δεν εντοπίζεται ρύθμιση σχετικά με τον τρόπο με τον οποίο πρέπει να εκπονηθεί μια ΕΑΠΔ. Δεν προτείνεται, δηλαδή, κάποιος είδους Μεθοδολογία.

Ως εκ τούτου, δημιουργείται το πρόβλημα του να εντοπιστεί ο κατάλληλος τρόπος εκπόνησης μιας ΕΑΠΔ. Μια πρώτη επίλυση στο παραπάνω κενό θα πρέπει πρώτα από όλα να αναζητηθεί στις οδηγίες που είχε εκδώσει το «ARTICLE 29 DATA PROTECTION WORKING PARTY»[5]. Ειδικότερα, στις παραπάνω οδηγίες αναφέρεται σαφώς και ρητώς ότι οποιαδήποτε μεθοδολογία μπορεί να χρησιμοποιηθεί, οπότε ως προς αυτό δεν υπάρχει κάποια δέσμευση από τον νόμο, με την προϋπόθεση βέβαια ότι θα είναι κατάλληλη για να επιτύχει τον τελικό σκοπό της ΕΑΠΔ, ο οποίος είναι να αποτελεί μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους. Μάλιστα, σε αυτό έρχεται να προστεθεί ότι όχι μόνο επιτρέπεται στον υπεύθυνο επεξεργασίας να επιλέξει όποια μεθοδολογία επιθυμεί, αλλά και να τροποποιήσει την εκάστοτε μεθοδολογία, όπως επιθυμεί. Αυτό καταδεικνύεται και από την απόφαση της ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ) υπ' αριθμόν 30/2023[6] στη σκέψη 17 η οποία αναφέρει ότι «… δεν φαίνεται να υπάρχει απόλυτη συμφωνία με τα βήματα που περιγράφονται σε σχετικά εγχειρίδια της CNIL[7] που είναι διαθέσιμα στο διαδικτυακό της τόπο. Τούτο από μόνο του δεν συνιστά μεν ελλιπή εκπόνηση Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων,

[4] Οι εταιρείες/οργανισμοί ενθαρρύνονται να εφαρμόζουν τεχνικά και οργανωτικά μέτρα, στα αρχικά στάδια του σχεδιασμού των πράξεων επεξεργασίας, με τέτοιον τρόπο ώστε να διασφαλίζονται οι αρχές ιδιωτικού απορρήτου και προστασίας δεδομένων ήδη από την αρχή («προστασία δεδομένων ήδη από τον σχεδιασμό»). Εξ ορισμού, οι εταιρείες/οργανισμοί θα πρέπει να διασφαλίζουν ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία με το υψηλότερο επίπεδο προστασίας της ιδιωτικής ζωής (π.χ. μόνο τα απαραίτητα δεδομένα πρέπει να υποβάλλονται σε επεξεργασία, σύντομη περίοδος αποθήκευσης, περιορισμένη προσβασιμότητα) έτσι ώστε εξ ορισμού τα δεδομένα προσωπικού χαρακτήρα να μην είναι προσβάσιμα από αόριστο αριθμό φυσικών προσώπων («προστασία δεδομένων εξ ορισμού»)

[5] Βλ. 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. Ομάδα εργασίας άρθρου 29.

[6] Βλ. Απόφαση υπ' αριθμόν 30/2023,Αρχή Προστασίας Προσωπικών Δεδομένων, Αθήνα 25-09-2023, Αριθ. Πρωτ.: 2398

[7] Πρόκειται για την Αρχή Προστασίας Προσωπικών Δεδομένων της Γαλλίας.

αφού δεν υπάρχει υποχρέωση υιοθέτησης, από τον υπεύθυνο επεξεργασίας, συγκεκριμένης μεθοδολογίας» . Έτσι, λοιπόν, οι Αρχές Προστασίας Προσωπικών Δεδομένων των χωρών της Ευρωπαϊκής Ένωσης, που αποτελούν τους ισχυρότερους και σημαντικότερους παράγοντες στην προστασία προσωπικών δεδομένων, προσπάθησαν να καλύψουν αυτό το κενό εκδίδοντας σαφείς οδηγίες, τρόπους και μεθοδολογίες κατευθύνοντας τους ενδιαφερομένους για το πως πρέπει να εκπονήσουν μια ΕΑΠΔ. Παράλληλα η ίδια προσπάθεια έγινε και από τον ακαδημαϊκό χώρο. Επιπλέον, για τον ίδιο σκοπό μπορούν να αξιοποιηθούν και τα πρότυπα πιστοποίησης που εκδόθηκαν από τον Διεθνή Οργανισμό Πιστοποίησης (ISO). Παρόλα αυτά, όλες αυτές οι μεθοδολογικές προσεγγίσεις παρά τα κοινά μοτίβα που εμφανίζουν σε κάποια σημεία διαφέρουν πολύ μεταξύ τους, κυρίως όσον αφορά την διαδικασία και τον τρόπο που ερμηνεύουν και εφαρμόζουν τις αφηρημένες απαιτήσεις που προκύπτουν από το άρθρο 5 του ΓΚΠΔ.[8]

Η συγκεκριμένη εργασία έρχεται να αντιμετωπίσει το παραπάνω πρόβλημα. Να οργανώσει, δηλαδή το παραπάνω υλικό, να παραθέσει τις οπτικές των παραπάνω Μεθοδολογιών, ενώ παράλληλος σκοπός είναι να παρουσιάσει την μεθοδολογία της ΕΑΠΔ στον αναγνώστη μέσα από μια εμπειρική – πρακτική σκοπιά.

2. Η μεθοδολογία και ο σκοπός της συγκεκριμένης εργασίας

Η μεθοδολογία που επιλέχθηκε για την εκπόνηση της συγκεκριμένης εργασίας είναι αυτή που προτείνεται από τους Webster & Watson και προέρχεται από τον κλάδο της πληροφορικής με τίτλο «ANALYZING THE PAST TO PREPARE FOR THE FUTURE: WRITING A LITERATURE REVIEW[9]». Ειδικότερα, μελετώντας τις μεθοδολογικές προσεγγίσεις που έχουν αναπτυχθεί για την διενέργεια της εκτίμησης αντικτύπου θεωρήθηκε χρήσιμο να παρουσιαστεί κατ' αρχάς μία ολοκληρωμένη προσέγγιση, με σαφώς καθορισμένα στάδια και βήματα, γεγονός που είναι συνεπές και με την θεματοκεντρική παρουσίαση που επιτάσσει η ως άνω μεθοδολογία, σε αντίθεση με τις εργασίες που αναλύουν την προβληματική τους από μία σκοπιά που θέτουν στο επίκεντρο τους, τους συγγραφείς.

Ο λόγος που επιλέγεται αυτός ο ,ίσως παράδοξος για έναν νομικό, τρόπος εκπόνησης της συγκεκριμένης εργασίας έγκειται στο γεγονός, ότι η μεθοδολογία μιας ΕΑΠΔ, για να επιτύχει

[8] Friedewald, M., Schiering, I., Martin, N., Hallinan, D. (2022). Data Protection Impact Assessments in Practice. In: Katsikas, S., et al. Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science(), vol 13106. Springer, Cham. Σελ. 425

[9] 2 https://web.njit.edu/~egan/Writing_A_Literature_Review.pdf

εν τέλει τον σκοπό της πρέπει να εφαρμοστεί με συστηματικό τρόπο, να παράγει δηλαδή συνεπή, επαληθεύσιμα και αξιολογήσιμα αποτελέσματα. Περαιτέρω, η ΕΑΠΔ αποτελεί ένα σύνθετο κομμάτι για το οποίο έχει χυθεί μελάνι από πολλούς τομείς της επιστήμης και απαιτεί διεπιστημονική προσέγγιση[10]. Επιπλέον, μέσα από την συγκεκριμένη εργασία επιχειρείται να υποδειχθούν σαφή βήματα, καθότι πρόκειται για μεθοδολογία, και όχι μόνον νομικές θεωρίες και επομένως ενδείκνυται ο συγκεκριμένος τρόπος, έτσι ώστε να είναι εφικτό να γίνει μία άμεση παράθεση των μεθοδολογικών προσεγγίσεων, και να εξαχθούν συμπεράσματα για κάθε ένα στάδιο από αυτά. Ως εκ τούτου είναι αναπόφευκτο να μην υπάρξουν συγκρίσεις μεταξύ των μεθοδολογικών προσεγγίσεων. Ωστόσο, σκοπός της συγκεκριμένης εργασίας δεν είναι να συγκρίνει τις εν λόγω μεθοδολογικές προσεγγίσεις αλλά να παρουσιάσει ολιστικά και συνθετικά τον τρόπο που διενεργείται η εκτίμηση αντικτύπου μέσα από σαφή και καθορισμένα βήματα εντοπίζοντας, βέβαια, κοινά μοτίβα και διαφορές.

Τον κορμό της εργασίας θα αποτελέσει η μεθοδολογία που διαμορφώθηκε από ερευνητές στο « Fraunhofer Institute for Systems and Innovation Research ISI » και εκδόθηκε από αυτό με τίτλο «The Data Protection Impact Assessments According to Article 35»[11] (εφεξής μεθοδολογική προσέγγιση Fraunhofer). Ειδικότερα, με την συγκεκριμένη μεθοδολογική προσέγγιση οι συγγραφείς συστηματοποιούν μία προγενέστερη προσέγγιση πάνω στις εκτιμήσεις αντικτύπου η οποία παρουσιάστηκε σε White Paper από το ερευνητικό κονσόρτσιουμ με την ονομασία «Forum Privacy and Self-Determination in a Digital World» [12]. Ο λόγος που προκρίνεται η εν λόγω προσέγγιση είναι ότι αποτελεί μία προσέγγιση με σαφή καθορισμένα βήματα, αλλά και για το γεγονός ότι, όπως αναφέρουν οι συγγραφείς του, έχει διαμορφωθεί μέσα από την εφαρμογή της στον δημόσιο και ιδιωτικό τομέα, μέσα από δώδεκα εργαστήρια και συνεντεύξεις με επιχειρήσεις και αρχές. Φυσικά, ο κορμός αυτός θα συνδυαστεί με τις μεθοδολογίες που αναπτύχθηκαν από τις επιμέρους αρχές των κρατών – μελών της Γαλλίας και της Αγγλίας, με μελέτες από την επιστημονική κοινότητα[13] αλλά και με μεθοδολογίες που αναπτύχθηκαν από τον διεθνή οργανισμό πιστοποίησης (ISO)[14] με σκοπό την ολιστική προσέγγιση του ζητήματος. Σημειώνεται δε, ότι όλες οι μεθοδολογικές προσεγγίσεις που θα αναφερθούν στην παρούσα εργασία, θα μπορούσαν και από μόνες τους,

[10] Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017, Σελ. 104

[11] Βλ. https://publica-rest.fraunhofer.de/server/api/core/bitstreams/e6b91341-71f4-409b-8446-03432231a0d0/content

[12] Βλ. Friedewald, M.; Bieker, F.; Obersteller, H. et al. (2017): Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz. Dritte, überarbeitete Auflage. Karlsruhe: Fraunhofer ISI (Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt)

[13] Βλ. Π.χ. Marie Caroline Oetzel, Sarah Spiekerman, Ingrid Gruning, Harald Kelter and Sabine Mull. Privacy Impact Assessment Guideline for RFID Applications, 2011.

[14] Βλ. ISO 29134:2020

κατά περίπτωση, να καλύψουν τις απαιτήσεις του άρθρου 35 του ΓΚΠΔ. Ωστόσο, σκοπός της συγκεκριμένης εργασίας, όπως αναφέρθηκε και παραπάνω, δεν είναι να συγκρίνει τις μεθοδολογικές προσεγγίσεις μεταξύ τους, αλλά να παρουσιάσει ολιστικά και συνθετικά τον τρόπο που διενεργείται η εκτίμηση αντικτύπου, και να εντοπίσει ομοιότητες και διαφορές μέσα από σαφή και καθορισμένα βήματα.

Οι ίδιοι οι συγγραφείς της προσέγγισης Fraunhofer έχουν «υπερασπιστεί» την αξία της μεθοδολογικής τους προσέγγισης, ασκώντας κάποιου είδους κριτική σε γνωστές μεθοδολογικές προσεγγίσεις. Ειδικότερα, όσον αφορά την πιο δημοφιλή μεθοδολογική προσέγγιση αυτή, δηλαδή, που αναπτύχθηκε από την Γαλλική Αρχή Προστασίας Δεδομένων - Commission nationale de l'informatique et des libertés (CNIL)[15],(εφεξής μεθοδολογική προσέγγιση CNIL) η οποία βασίστηκε πάνω στην μεθοδολογία διαχείρισης κινδύνου EBIOS[16] η οποία με την σειρά της αναπτύχθηκε από την εθνική αρχή κυβερνοασφάλειας και προστασίας πληροφοριακών συστημάτων της Γαλλίας. (ANSSI)[17], αναφέρουν ότι, η συγκεκριμένη μεθοδολογική προσέγγιση είναι μεν λεπτομερής και δομημένη, παρουσιάζεται δε με τη μορφή ερωτο-απαντήσεων τύπου «checklist», ενώ συνοδεύεται και από ένα ηλεκτρονικό υποστηρικτικό εργαλείο, γεγονός που καθιστά το τελικό αποτέλεσμα αυτής της προσέγγισης πολύ διαφορετικό από το νομικό κείμενο. Επιπλέον, σε αυτή την προσέγγιση παρατηρούν ότι η διαβούλευση με τα εμπλεκόμενα μέρη δεν αποτελεί το επίκεντρο της, αλλά ζητάται στο τέλος για την επαλήθευση των αποτελεσμάτων στα οποία κατέληξε ο Υπεύθυνος επεξεργασίας μετά από τον δικό του έλεγχο. Σε γενικές γραμμές σύμφωνα με τους συγγραφείς της προσέγγισης του Fraunhofer η προσέγγιση CNIL χρησιμοποιεί την εκτίμηση αντικτύπου ως ένα μέσον επαλήθευσης της συμμόρφωσης με τον ΓΚΠΔ και τις απαιτήσεις ασφάλειας πληροφοριακών συστημάτων. Αναφέρεται, βέβαια, πως πολλά ιδρύματα και φορείς έχουν ακολουθήσει την συγκεκριμένη μεθοδολογική προσέγγιση, όπως η Γερμανική Ένωση για τις τεχνολογίες Πληροφορικής, τις τηλεπικοινωνίες και των νέων μέσων ενημέρωση «BITKOM»[18] .

Η δεύτερη μεθοδολογική προσέγγιση με εξίσου μεγάλη επιρροή είναι αυτή που αναπτύχθηκε από την Αρχή Προστασίας Προσωπικών Δεδομένων του Ηνωμένου Βασιλείου - Information

[15]Βλ. https://www.cnil.fr/sites/cnil/files/atoms/files/cnil-pia-1-en-methodology.pdf
[16]Βλ. https://cyber.gouv.fr/publications/ebios-risk-manager-method
[17]Βλ. Friedewald, M., Schiering, I., Martin, N., Hallinan, D. (2022). Data Protection Impact Assessments in Practice. In: Katsikas, S., et al. Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science(), vol 13106. Springer, Cham. Σελ. 425 επ.

[18]Βλ. https://www.bitkom.org/sites/default/files/file/import/170919-LF-Risk-Assessment-ENG-online-final.pdf

Commissioner's Office ICO (εφεξής προσέγγιση ICO)[19] και τροποποιήθηκε από άλλες Αρχές Προστασίας Προσωπικών Δεδομένων, όπως αυτή της Ισπανίας[20] . Ειδικότερα, η προσέγγιση ICO βασίζεται πάνω στην «παράδοση» των Εκτιμήσεων αντικτύπου ιδιωτικότητας που είχε αναπτυχθεί στον αγγλοσαξονικό κόσμο ήδη από την δεκαετία του 1990. Ο σημαντικότερος «απόγονος» της προσέγγισης ICO είναι το πρότυπο ISO 29134[21].

Σύμφωνα με τους συγγραφείς της προσέγγισης Fraunhofer η προσέγγιση ICO (και ISO) είναι περισσότερο στοχαστική, κάνοντας περισσότερο ποιοτικές ερωτήσεις, ακόμα και οργανωτικές – κοινωνικές. Η προσέγγιση αυτή είναι πιο ευέλικτη και έχει εφαρμογή σε περισσότερες περιπτώσεις, ενώ σε αντίθεση με αυτή της CNIL φαίνεται ότι η διαβούλευση με τα υποκείμενα των δεδομένων έχει μεγάλη σημασία για την προσέγγιση του ICO. Ωστόσο, αναφέρεται ότι τα αποτελέσματα στα οποία καταλήγει είναι λιγότερο ακριβή και επαληθεύσιμα. Η μεγαλύτερη αδυναμία που αναφέρεται είναι το γεγονός ότι η προσέγγιση ICO δεν εργολειοποιεί τις αρχές που προκύπτουν από το άρθρο 5 του ΓΚΠΔ, και έτσι, σύνθετες νομικές έννοιες όπως η νομιμότητα της επεξεργασίας, η αντικειμενικότητα και η διαφάνεια που συνήθως δεν είναι γνωστές σε μη νομικούς, δεν μπορούν να επεξηγηθούν εύκολα στους υπόλοιπους εμπλεκόμενους φορείς.

Η παραπάνω αδυναμία αναγνωρίστηκε από τις Εποπτικές Αρχές της Γερμανίας[22], ο οποίες πρότειναν το « The Standard Data Protection Model[23]» (εφεξής «SDM»). Το SDM είναι περισσότερο μία μέθοδος για την συνολική συμμόρφωση και τον έλεγχο της προστασίας δεδομένων και του ΓΚΠΔ που βασίζεται στο σενάριο των «στόχων προστασίας», παρά μία μεθοδολογική προσέγγιση για την διενέργεια Εκτίμησης Αντικτύπου. Παρόλα αυτά, περιλαμβάνει σημαντικά στοιχεία τα οποία μπορούν να χρησιμοποιηθούν για να δημιουργηθεί μία μεθοδολογική προσέγγιση διενέργειας εκτίμησης αντικτύπου. Ειδικότερα, το SDM χρησιμοποιεί τους «στόχους προστασίας» αντί για τις Αρχές Προστασίας, όπως αυτές προκύπτουν από το άρθρο 5 του ΓΚΠΔ, έτσι ώστε να μπορέσει να εργαλειοποιήσει τις

[19]Βλ. Information Commissioner's Office (ICO), Wilmslow, UK: Guide to the General Data Protection Regulation (GDPR) (2021). https://ico.org.uk/media/fororganisations/guide-to-data-protection/guide-to-the-general-data-protectionregulation-gdpr-1-1.pdf
[20]Βλ. Agencia Espa˜nola de Protecci´on de Datos (AEPD), Madrid: Gu´ıa pr´actica para las Evaluaciones de Impacto en la Protecci´on de los datos sujetas al RGPD (2018). https://www.aepd.es/sites/default/files/2019-09/guiaevaluaciones-de-impacto-rgpd.pdf
[21] Βλ.ISO/IEC 29134:2023 - Information technology — Security techniques — Guidelines for privacy impact assessment
[22] Η Γερμανία δεν έχει μία κεντρική Εποπτική Αρχή Προστασίας Προσωπικών Δεδομένων, αλλά κάθε μία από τις 16 ομοσπονδίες έχει τη δικιά της Αρχή. (https://www.bfdi.bund.de/EN/Service/Anschriften/Laender/Laender-node.html).
[23]Βλ. Conference of the independent data protection authorities of the Federal and State Governments of Germany: The Standard Data Protection Model: A method for data protection advising and controlling on the basis of uniform protection goals (2020). https://www.datenschutzzentrum.de/uploads/sdm/SDMMethodology V2.0b.pdf

απαιτήσεις του ΓΚΠΔ[24]. Ωστόσο, οι «στόχοι προστασίας» σε δεν έρχονται σε αντίθεση με τις Αρχές Προστασίας του άρθρου 5 του ΓΚΠΔ αλλά αντιθέτως τις εκπληρώνουν πλήρως. Αναλυτικότερα, οι στόχοι αυτοί «μεταφράζουν» τις (ίσως πιο αφηρημένες) αρχές στην γλώσσα του κλάδου της Ασφαλείας Πληροφοριακών Συστημάτων, από όπου και εν τέλει η ιδέα των «στόχων προστασίας» προέρχεται, προσδίδοντας έτσι τις αρχές μία πιο συνοπτική αλλά και περιεκτική μορφή. Πάνω σε αυτή την προσέγγιση βασίζεται και η κεντρική προσέγγιση της παρούσας εργασίας (Προσέγγιση Fraunhofer)

Τέλος, η αξία της μεθοδολογικής προσέγγισης Fraunhofer φαίνεται πως αναγνωρίστηκε και από τον EDPS καθότι ο τελευταίος, προτείνει το White Paper πάνω στο οποίο βασίστηκε η εν λόγω μεθοδολογική προσέγγιση, στο παράρτημα 4, στο κεφάλαιο 4.2. των αντίστοιχων οδηγιών που έχει εκδώσει για την διενέργεια εκτίμηση αντικτύπου[25].

3. Εκτίμηση Αντικτύπου και Λογοδοσία

Με τον ΓΚΠΔ υιοθετήθηκε νέο μοντέλο συμμόρφωσης, κεντρικό μέγεθος του οποίου συνιστά η αρχή της λογοδοσίας στο πλαίσιο της οποίας ο υπεύθυνος επεξεργασίας υποχρεούται να σχεδιάζει, εφαρμόζει και εν γένει λαμβάνει τα αναγκαία μέτρα και πολιτικές, προκειμένου η επεξεργασία των δεδομένων να είναι σύμφωνη με τις σχετικές νομοθετικές προβλέψεις. Επιπλέον δε, ο υπεύθυνος επεξεργασίας πρέπει να αποδεικνύει από μόνος του και ανά πάσα στιγμή τη συμμόρφωση του με τις αρχές του άρθρου 5 παρ. 1 ΓΚΠΔ. Δεν είναι τυχαίο ότι ο ΓΚΠΔ εντάσσει τη λογοδοσία (Άρθρο 5 παρ. ΓΚΠΔ) στη ρύθμιση των αρχών (άρθρο 5 παρ.1 ΓΚΠΔ) που διέπουν την επεξεργασία, προσδίδοντας σε αυτήν, τη λειτουργία ενός μηχανισμού τήρησής τους, αντιστρέφοντας κατ' ουσίαν το «βάρος της απόδειξης» ως προς την νομιμότητα της επεξεργασίας (και εν γένει την τήρηση των αρχών του άρθρου 5 παρ.1 ΓΚΠΔ)

[24]Βλ. Friedewald, M., Schiering, I., Martin, N., Hallinan, D. (2022). Data Protection Impact Assessments in Practice. In: Katsikas, S., et al. Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science(), vol 13106. Springer, Cham. Σελ. 427

[25] Βλ. European Data Protection Supervisor, « Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation».2018, https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf

μεταθέτοντας τη στον υπεύθυνο επεξεργασίας, ώστε να υποστηρίζεται βάσιμα ότι εκείνος φέρει το βάρος της επίκλησης και απόδειξης της νομιμότητας της επεξεργασίας.[26]

Ως εκ τούτου οι υπεύθυνοι επεξεργασίας έχουν υποχρέωση να «επιδείξουν αποτελέσματα» , να είναι σε θέση δηλαδή να αποδείξουν την συμμόρφωση τους, να διατηρούν μία ελευθερία ως προς τον προσδιορισμό των ειδικότερων μέσων με τα οποία θα το επιτύχουν αυτό. Παρόλα αυτά, δεν θα πρέπει αυτή η καινοτομία να δημιουργήσει περαιτέρω γραφειοκρατικό φόρτο, λειτουργώντας εν τέλει ως «δούρειος ίππος».[27]

Μεταξύ των εργαλείων εκπλήρωσης της κατ' άρθρο 5 παρ. 2 σε συνδυασμό με τα άρθρα 24 παρ. 1 και 32 ΓΚΠΔ αρχής της λογοδοσίας , λαμβάνοντας υπόψη την αιτιολογική σκέψη 83 ΓΚΠΔ, είναι η εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ), η οποία προβλέπεται στο άρθρο 35 του ΓΚΠΔ. Η ΕΑΠΔ επιτρέπει στους υπευθύνους επεξεργασίας να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ όποτε σχεδιάζεται ή υλοποιείται επεξεργασία δεδομένων με υψηλό κίνδυνο αλλά και να αποδεικνύουν ότι εφαρμόζουν και εν γένει λαμβάνουν τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσης αυτής[28].

Ως αποτέλεσμα, η παραβίαση της αρχής της λογοδοσίας και ειδικά η παράλειψη εκτίμησης αντικτύπου ή η διενέργεια αυτής με λανθασμένο τρόπο καταλήγει εν τέλει σε μη συμμόρφωση με τον ΓΚΠΔ και κατ' επέκταση στις συνέπειες που επισύρει αυτό. Χαρακτηριστικό παράδειγμα λανθασμένης διενέργειας αποτελεί η απόφαση της Ελληνικής Αρχής υπ' αριθμόν 4/2022[29]. Σύμφωνα με την σκέψη υπ' αριθμόν 16 παρόλο που επιλέχθηκε ως μεθοδολογία, από τον υπεύθυνο επεξεργασίας, εκείνη που είχε προταθεί από την αρχή προστασίας προσωπικών δεδομένων του Ηνωμένου Βασιλείου (ICO) εν τέλει δεν εφαρμόστηκε με ορθό τρόπο, καθώς δεν απαντήθηκαν με σαφήνεια οι ερωτήσεις που έθετε η ως άνω μεθοδολογία και κατ' επέκταση δεν αποδεικνυόταν ότι ο υπεύθυνος επεξεργασίας είχε εξετάσει όλους τους κινδύνους της εν λόγω επεξεργασίας. Σύμφωνα με το άρθρο 83 παρ.4 περ.1 προβλέπεται ότι η παραβίαση του άρθρου 35 μπορεί να επιφέρει πρόστιμο μέχρι και 10.000.000 ευρώ ή σε περίπτωση επιχειρήσεων μέχρι το 2% του παγκόσμιου κύκλου εργασιών σύμφωνα

[26]Βλ. Λ. Μήτρου, Η αρχή της λογοδοσίας σε υποχρεώσεις του Υπευθύνου Επεξεργασίας (Γ. Γιαννόπουλος, Λ. Μήτρου, Γ. Τσόλιας) Συλλογικός τόμος Λ.Κοτσακλή - Κ. Μενουδάκου « Ο ΓΚΠΔ, Νομική διάσταση και πρακτική εφαρμογή», εκδ.Νομική Βιβλιοθήκη, 2018, Σελ 172 επ.
[27]Βλ. ό.π. υποσημ.6
[28]Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Απόφαση υπ' αριθμόν 32/2021, Αθήνα 04-08-2021, Αριθ, Πρω.: 1818
[29] Βλ Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, υπ΄αριθμόν 4/2022, Αθήνα 15-12-2022, Αριθ. Πρωτ:3302Βλ. ΑΠΔΠΧ 32/2021

με το προηγούμενο οικονομικό έτος, ανάλογα ποιο είναι πιο υψηλό. Στο διατακτικό της ιδίας απόφασης επέβαλε πρόστιμο ύψους 1.300.000. για παραβίαση του άρθρου 35 παρ. 7.

Ακόμη ένα χαρακτηριστικό παράδειγμα αποτελεί το πρόστιμο που επέβαλε η Garante[30] σε εταιρεία διανομής γρήγορου φαγητού, ενεργώντας αυτεπάγγελτα, στο πλαίσιο ελέγχου όλων των εταιρειών που δραστηριοποιούνται στον κλάδο του «food delivery» , ύψους 2.600.000 ευρώ. Στην απόφαση της Ιταλικής Αρχής μεταξύ αρκετών πλημμελειών έγινε αναφορά και στη μη διενέργεια ΕΑΠΔ παρά την καινοτομία των συστημάτων που χρησιμοποιούσε σε συνδυασμό με τη λειτουργία ενός συστήματος διαχείρισης των παραγγελιών μέσω αλγορίθμων, που εκ των υστέρων απεδείχθη πως δεν μπορούσε να εγγυηθεί την ακρίβεια και την ορθότητα αναφορικά με την αξιολόγηση των διανομέων ως προς τον αριθμό παραγγελιών που τους δίνει.[31]

4. Εκτίμηση αντικτύπου και προηγούμενη διαβούλευση

Ο ΓΚΠΔ (αρ.36 παρ.1) επιβάλλει διαβούλευση με τον εποπτική Αρχή όταν από την εκτίμηση αντικτύπου υπάρχει ένδειξη ότι η επεξεργασία θα προκαλέσει υψηλό κίνδυνο, λόγω ελλείψεως μέτρων για να μετριασθεί ο κίνδυνος. Σε αυτή την περίπτωση ο υπεύθυνος επεξεργασίας οφείλει να ζητήσει τη γνώμη της εποπτικής αρχής και μάλιστα μέσα σε συγκεκριμένη προθεσμία (αρ.36 παρ.2) παρέχοντας στην αρχή και συγκεκριμένες πληροφορίες (αρ.36 παρ.3 περ. (α) έως (στ). Έτσι φαίνεται ότι ο ΓΚΠΔ επιτρέπει κατά παρέκκλιση την επαναφορά στο καθεστώς της «προηγούμενης άδειας» που ίσχυε πριν από την εφαρμογή του ΓΚΠΔ , για λόγους δημοσίου συμφέροντος, ενώ περιλαμβάνει σε αυτές και την επεξεργασία που σχετίζεται με την κοινωνική προστασία και τη δημόσια υγεία (αρ.36 παρ.5).[32]

Ως εκ τούτου η υποβολή εκτίμησης αντικτύπου αποτελεί ουσιώδη τύπο της διαδικασίας της διαβούλευσης. Προκειμένου να καταλήξει, δηλαδή, ο υπεύθυνος επεξεργασίας στο συμπέρασμα ότι δεν μπορεί να μετριάσει τους κινδύνους με κατάλληλα τεχνικά και οργανωτικά μέτρα, πρέπει να έχει προηγηθεί αυτή η μελέτη. Η διαβούλευση αρχίζει μετά από αίτηση του υπευθύνου επεξεργασίας μιας και στοιχειοθετεί δικό του δικαίωμα. Τρίτος δεν νομιμοποιείται

[30] Πρόκειται για την Ιταλική Αρχή Προστασίας Προσωπικών Δεδομένων
[31]Βλ. ΝοΒ. Στ. Ζουμπουλίδης "Οδηγός συμμόρφωσης μίας μεσαίας επιχείρησης με τον γενικό κανονισμό προστασίας δεδομένων (679/2017 ΕΚ) και η ειδικότερη πτυχή της προστασίας δεδομένων των εργαζομένων», Τόμος 71 – Τεύχος 5 2023, Σελ 1266 και https://gdprhub.eu/index.php?title=Garante_per_la_protezione_dei_dati_personali_(Italy)_-_9675440#English_Summary (Τελευταία επίσκεψη 4.12.2023)
[32]Βλ. Γ. Γιαννόπουλος, Η αρχή της λογοδοσίας σε υποχρεώσεις του Υπευθύνου Επεξεργασίας (Γ. Γιαννόπουλος, Λ. Μήτρου, Γ. Τσόλιας) Συλλογικός τόμος Λ.Κοτσακλή - Κ. Μενουδάκου « Ο ΓΚΠΔ, Νομική διάσταση και πρακτική εφαρμογή», εκδ.Νομική Βιβλιοθήκη, 2018, Σελ 172 επ.

προς τούτο ελλείψει εννόμου συμφέροντος του, αφού εξ ορισμού δεν θα μπορούσε να εξαναγκάσει τον απρόθυμο υπεύθυνο προκαλώντας την έκδοσηση άδειας προς αυτόν. [33]

Παρά την ασαφή διατύπωση του άρθρου 35 παρ. 9 ΓΚΠΔ γίνεται δεκτό ότι επιβάλλεται ως ουσιώδης τύπος της διαδικασίας διαβούλευσης η γνωστοποίηση της και στα υποκείμενα, εφόσον είναι γνωστή τουλάχιστον η κατηγορία των υποκειμένων, τα οποία αφορά η υπό διαβούλευση επεξεργασία. Σύμφωνα με άλλη άποψη, η ανωτέρω θέση καθίσταται υποχρεωτική, ευθέως από το άρθρο 20παρ. 2 του Συντάγματος όπου κατοχυρώνεται το δικαίωμα ακροάσεως τους πριν από την απόφαση της ΑΠΔΠΧ επί της μελέτης αντικτύπου, αφού πρόκειται για τα δικά τους δεδομένα. Η ενημέρωση τους μπορεί να ικανοποιηθεί με οποιονδήποτε τρόπο (π.χ. δια του τύπου, ή με υποβολή ερωτηματολογίου προς τα υποκείμενα ή τους αντιπροσώπους τους, όπως οι ενώσεις καταναλωτών/υποκειμένων)[34]

Παράδειγμα, από την νομολογία περίπτωσης προηγούμενης διαβούλευσης αποτελεί η γνωμοδότηση της Αρχής Προστασίας Προσωπικών Δεδομένων υπ 'αριθμόν 2/2020[35], σύμφωνα με την οποία το Ανώτατο Συμβούλιο Επιλογής Προσωπικού (ΑΣΕΠ) υπέβαλε στην Αρχή αίτημα διαβούλευσης, βάσει του άρθρου 36 ΓΚΠΔ, σχετικά με το υπολειπόμενο κίνδυνο κατά την επεξεργασία που αφορούσε την ανάρτηση στο διαδικτυακό τόπο (www.asep.gr) πινάκων κατάταξης και διοριστέων, οι οποίο δύναται να περιλαμβάνουν και ειδικές κατηγορίες δεδομένων. Ειδικότερα, το ΑΣΕΠ, ζήτησε τη γνώμη της Αρχής διότι η μελέτης εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) την οποία εκπόνησε υπέδειξε ότι, και μετά τη λήψη μέτρων μετριασμού του κινδύνου, η επεξεργασία, δια της ως άνω ανάρτησης ειδικών κατηγοριών δεδομένων, δύναται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

5. Πριν την μεθοδολογία μίας ΕΑΠΔ

Όπως αναδείχθηκε από τα παραπάνω, η εκπόνηση της Εκτίμησης Αντικτύπου δεν εναπόκειται στην διακριτική ευχέρεια του Υπευθύνου επεξεργασίας αλλά είναι υποχρέωση του ,καθώς αποτελεί την ουσιαστικότερη μορφή της αρχής της λογοδοσίας. Ως εκ τούτου, η αποτελεσματική διενέργειά της, και ο ορθός τρόπος εκπόνησής της είναι βαρύνουσας

[33]Βλ. Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2η έκδοση, Σελ. 141
[34]Βλ. Κ. Χριστοδούλου ό.π
[35]Βλ. Αρχή Προστασίας Προσωπικών Δεδομένων, Γνωμοδότηση υπ΄αριθμόν 2/2020, Αθήνα 08-04-2020, Αριθμ.Πρω.: Γ/ΕΞ/2342/08-04-2020

σημασίας. Βέβαια, ο καθορισμός της μεθοδολογίας μιας ΕΑΠΔ είναι ελεύθερος, αρκεί η μεθοδολογία που θα επιλεχθεί να επιτυγχάνει τον τελικό σκοπό της ΕΑΠΔ να αποτελεί, δηλαδή, μια πραγματική αξιολόγηση των κινδύνων, που θα παρέχει στους υπεύθυνους επεξεργασίας τη δυνατότητα να λάβουν μέτρα για την αντιμετώπισή τους. Ο σαφής καθορισμός της μεθοδολογίας που θα επιλεχθεί και θα εφαρμοστεί είναι πρωτίστης σημασίας. Όπως φάνηκε και από την απόφαση υπ' αριθμόν 30/2023 της Αρχής Προστασίας Προσωπικών Δεδομένων (ΑΠΔΠΧ), ήταν πολύ δύσκολο για τον υπεύθυνο επεξεργασίας να καθορίσει τον τρόπο, την μεθοδολογία με την οποία θα εκπονούσε την εκτίμηση αντικτύπου[36] ,και ως εκ τούτου καθυστέρησε να εκπονήσει την Εκτίμηση Αντικτύπου. Παρόλα αυτά, η Αρχή στην σκέψη 16 θεώρησε πως αυτό δεν μπορεί να άρει την υποχρέωση του Υπευθύνου να εκπονήσει την ΕΑΠΔ όποτε αυτό απαιτείται, λαμβάνοντας τα κατάλληλα μέτρα προκειμένου να διασφαλίσει την έγκαιρη εκπόνησης της και έτσι η μη διενέργεια της εκτίμησης στον κατάλληλο χρόνο αποτέλεσε έναν από τους λόγους που επέβαλλε πρόστιμο.

Ωστόσο, πριν αναζητήσει κάποιος την κατάλληλη μεθοδολογία για να εκπονήσει μια ΕΑΠΔ την οποία ,όπως αναφέρθηκε παραπάνω, επέτρεψε την επιλογή αυτής ο ΓΚΠΔ, πρέπει να λάβει, υπόψη του εκείνα τα σημεία που ο ίδιος ο ΓΚΠΔ δεν άφησε περιθώρια επιλογής. Εκτός, όμως, του κανονισμού και του εφαρμοστικού νόμου (Ν.4624/2019[37]), υπάρχουν επίσης επίσημα έγγραφα τα οποία δεσμεύουν τόσο τυπικά όσο και ουσιαστικά τον υπεύθυνο επεξεργασίας. Ειδικότερα, πρόκειται για τις κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29 αλλά και αυτό του Ευρωπαϊκού Επόπτη.[38]

Επιπλέον, είναι προφανές ότι για να γίνει κατανοητό το περιεχόμενο της παρούσης θα πρέπει να είναι από πριν το περιεχόμενο των όρων του ΓΚΠΔ, όπως αυτά περιγράφονται στο άρθρο 4 αυτού.[39], τα οποία δεν φαίνονται σκόπιμα να παρουσιαστούν εδώ.

[36]Βλ. Απόφαση υπ' αριθμόν 30/2023,Αρχή Προστασίας Προσωπικών Δεδομένων, Αθήνα 25-09-2023, Αριθ. Πρωτ.: 2398
[37]Βλ. Νόμος Υπ' Αριθμ. 4624 Τεύχος Α' 137/29.08.2019 - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις
[38]Βλ. European Data Protection Supervisor, « Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation».2018, https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf
[39]Βλ. https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32016R0679#d1e1373-1-1

5.1 Οι κατευθυντήριες οδηγίες της ομάδας εργασίας του άρθρου 29.

Η ομάδα εργασίας του άρθρου 29 συστάθηκε με την ΟΔΗΓΙΑ 95/46/ΕΚ[40] ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ[41] και αποτελούσε ανεξάρτητο σώμα συμβουλετικού χαρακτήρα[42]. Σκοπός του ήταν να εξετάζει οποιοδήποτε θέμα σχετικό με την εφαρμογή των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της οδηγίας, ώστε να συμβάλλει στην ομοιόμορφη εφαρμογή τους, να παρέχει στην Επιτροπή τη γνώμη της σχετικά με το επίπεδο προστασίας στην Κοινότητα και στις τρίτες χώρες, να συμβουλεύει την Επιτροπή για κάθε σχέδιο τροποποιήσεως της παρούσας οδηγίας, κάθε σχέδιο συμπληρωματικών ή ειδικών μέτρων που πρέπει να ληφθούν για τη διασφάλιση των δικαιωμάτων και ελευθεριών των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθώς ,και για κάθε άλλο σχέδιο κοινοτικών μέτρων που έχουν επιπτώσεις επί αυτών των δικαιωμάτων και ελευθεριών, να γνωμοδοτεί επί των κωδίκων δεοντολογίας που εκπονούνται σε κοινοτικό επίπεδο. Η ομάδα εργασίας του άρθρου 29 αντικαταστάθηκε στις 25 Μαΐου 2018 από το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων, σύμφωνα με το άρθρο 68 του ΓΚΠΔ την ημέρα, δηλαδή, που άρχισε να εφαρμόζεται πλέον ο ΓΚΠΔ.

Στις 4 Απριλίου 2017 δημοσιεύτηκε το έγγραφο από την ομάδα εργασίας του άρθρου 29 με τίτλο: «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.»[43] Το συγκεκριμένο έγγραφο, είναι το πρώτο που εκδόθηκε από όργανο της Ευρωπαϊκής Ένωσης και δεσμεύει όλα τα κράτη μέλη. Μάλιστα, κατά την πρώτη συνεδρίαση της ολομέλειας το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων ενέκρινε τις κατευθυντήριες οδηγίες, οι οποίες ισχύουν μέχρι σήμερα.

Ως εκ τούτου καμία μεθοδολογία δεν μπορεί να παραλείπει ή να αντιβαίνει στα όσα αναφέρονται μέσα σε αυτές τις κατευθυντήριες οδηγίες. Αντιθέτως, θα πρέπει πάντα να

[41]Βλ. Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών

[42]Βλ. ό.π. υποσημ. 19

[43] Article 29 Data Protection Working Party. In Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679; Technical Report; The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data: Brussels, Belgium,

διαπιστώνεται και να ελέγχεται αν τα βήματα που ακολουθήθηκαν είναι σύμφωνα με τα όσα έχει ορίσει η ομάδα εργασίας του άρθρου 29.

5.2 Οι κατευθυντήριες οδηγίες του Ευρωπαίου Επόπτη Προστασίας Δεδομένων.

Ο Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ) εποπτεύει τα θεσμικά όργανα, τους φορείς και τους οργανισμούς της Ευρωπαϊκής Ένωσης (θεσμικά όργανα της ΕΕ), ο οποίος ιδρύθηκε με το άρθρο 41 του Ευρωπαϊκού Κανονισμού υπ' αριθ. 45/2001[44].Βέβαια ο ΕΕΠΔ δεν βασίζεται αποκλειστικά στον ΓΚΠΔ. Οι κανόνες προστασίας δεδομένων για τα θεσμικά όργανα της ΕΕ ορίζονται από τον Κανονισμό (ΕΕ) 2018/1725[45]. Είναι, βέβαια, σε μεγάλο βαθμό πανομοιότυπο με τον ΓΚΠΔ που ισχύει για τις ιδιωτικές εταιρείες και τις περισσότερες δημόσιες διοικήσεις στα κράτη μέλη, ενώ ορίζονται ειδικοί κανόνες στους ιδρυτικούς κανονισμούς των οργάνων της ΕΕ που δραστηριοποιούνται στον τομέα της αστυνομίας και της δικαιοσύνης.

Τον Φεβρουάριο του 2018 εκδόθηκε από τον EDPS το έγγραφο με τίτλο «Accountability on the ground: Guidance on documenting processing operations for EU institutions, bodies and agencies»[46] , στο δεύτερο κεφάλαιο του οποίου περιλαμβάνονται οδηγίες για τους υπευθύνους επεξεργασίας και τους Υπευθύνους Προστασίας Προσωπικών Δεδομένων. Παρόλα αυτά θεωρείται σκόπιμο να αναφερθεί ότι καμία μεθοδολογία δεν θα πρέπει να αντιβαίνει στις παρατηρήσεις του EDPS.[47]

6. Έλεγχος για την διενέργεια Εκτίμησης Αντικτύπου (Threshold Analysis – Φάση Εκκίνησης)

6.1 Ποιος έχει την ευθύνη για την εκπόνηση μιας ΕΑΠΔ;

Η αρχή της λογοδοσίας, όπως αναφέρθηκε και παραπάνω, αφορά την υποχρέωση του Υπευθύνου Επεξεργασίας να εγγυάται την εφαρμογή των κανόνων προστασίας προσωπικών δεδομένων και είναι πάντα σε θέση να την αποδείξει,[48]. Ως εκ τούτου, την ευθύνη για την εκπόνηση μιας ΕΑΠΔ την φέρει ο Υπεύθυνος Επεξεργασίας σύμφωνα και με το άρθρο 35

[44] Βλ. Κανονισμός (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 18ης Δεκεμβρίου 2000, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα όργανα και τους οργανισμούς της Κοινότητας και σχετικά με την ελεύθερη κυκλοφορία των δεδομένων αυτών
[45] Βλ. Κανονισμός (ΕΚ) αριθ. 45/2001 ό.π.,
[46] Βλ. European Data Protection Supervisor, « Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation».2018, https://edps.europa.eu/sites/edp/files/publication/18-02-06_accountability_on_the_ground_part_2_en.pdf
[47] Βλ. European Data Protection Supervisor ό,π.
[48] Βλ. Friedewald, M., Schiering, I., Martin, N., Hallinan, D. (2022). Data Protection Impact Assessments in Practice. In: Katsikas, S., et al. Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science(), vol 13106. Springer, Cham

ΓΚΠΔ. Ένα καίριο ζήτημα που προκύπτει είναι το ποιος καθίσταται υπεύθυνος επεξεργασίας. Ως υπεύθυνος επεξεργασίας νοείται αυτός που ελέγχει την επεξεργασία, ήτοι «οποιοδήποτε πρόσωπο φυσικό ή νομικό, ιδιώτης ή δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός καθορίζει τους σκοπούς και τον τρόπο επεξεργασίας, σύμφωνα και με το άρθρο 4 παρ.7 του ΓΚΠΔ.[49] Ωστόσο, η ανάθεση της μπορεί να γίνει και σε άλλο πρόσωπο, εντός η εκτός του οργανισμού. Μπορούν, δηλαδή, να χρησιμοποιηθούν εξωτερικοί συνεργάτες αλλά ο υπεύθυνος επεξεργασίας είναι αυτός που καθίσταται πάντοτε υπόλογος[50]. Έχει κριθεί μάλιστα ότι ακόμα και στην περίπτωση που η μη εκπόνηση της ή η εκπόνηση της εκπρόθεσμα οφείλεται σε εξωτερικό παράγοντα, όπως η δυσκολία άντλησης πληροφοριών από τους αναδόχους, και πάλι την ευθύνη φέρει ο Υπεύθυνος επεξεργασίας από πλευράς δικαίου προστασίας προσωπικών δεδομένων.[51]

Επιπλέον, υπάρχει περίπτωση για την διενέργεια της επεξεργασίας να χρησιμοποιείται κάποιος εκτελών την επεξεργασίας. Ως εκτελών την επεξεργασία ορίζεται από τον ΓΚΠΔ στο άρθρο 4 παρ.8 «οποιοσδήποτε επεξεργάζεται δεδομένα για λογαριασμό» του υπευθύνου επεξεργασίας». Βασικό χαρακτηριστικό, δηλαδή, του εκτελούντος την επεξεργασία είναι ότι ο τελευταίος ενεργεί για λογαριασμό άλλου και υπό αυτή την έννοια οι ενέργειες του εκτελούντος την επεξεργασία ως βοηθού εκπληρώσεως συνεπάγονται και ενδοσυμβατική ευθύνη του υπευθύνου της επεξεργασίας έναντι του υποκειμένου σύμφωνα με το 334ΑΚ, όχι όμως και κατ' ΑΚ 922 ως αδικοπρακτική ευθύνη, καθώς δεν υπάρχει εξάρτηση μεταξύ εκτελούντος και υπευθύνου.[52] Σε περίπτωση που η επεξεργασία γίνεται εν μέρει ή εν τω συνόλω της από κάποιον εκτελούντα την επεξεργασία, ο τελευταίος είναι υποχρεωμένος να συνδράμει τον υπεύθυνο και να του παρέχει κάθε απαραίτητη πληροφορία. Αυτή η υποχρέωση μάλιστα προκύπτει και άμεσα από το Άρθρο 28 παρ.3 περ. στ', όπου αναφέρεται: «…συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία». Σύμφωνα, βέβαια, και με το άρθρο 28 παρ.3 του ΓΚΠΔ ο Εκτελών με τον Υπεύθυνο επεξεργασίας

[49] Βλ. Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2η έκδοση, Σελ. 55
[50] Βλ. Article 29 Data Protection Working Party. In Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679; Technical Report; The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data: Brussels, Belgium, 2017 Σελ.13
[51] Βλ. Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Απόφαση υπ' αριθμόν 30/2023, 25/09/2023, Αριθμ. Πρωτ: 2398
[52] Βλ. Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2η έκδοση, Σελ. 56

πρέπει να έχουν υπογράψει σύμβαση με την οποία ορίζονται σαφώς οι αρμοδιότητες και οι υποχρεώσεις ανάμεσα τους.[53]

Υπάρχει η πιθανότητα ο Υπεύθυνος επεξεργασίας να έχει διορίσει Υπεύθυνο Επεξεργασίας Προσωπικών Δεδομένων (ΥΠΠΔ) σύμφωνα με το άρθρο 37 του ΓΚΠΔ. Τέτοιου είδους υποχρέωση έχουν όσοι υπεύθυνοι επεξεργασίας επεξεργάζονται σε μεγάλη κλίμακα ευαίσθητα δεδομένα, όσοι προβαίνουν σε επεξεργασία συστηματική και σε μεγάλη κλίμακα και οι δημόσιες αρχές εκτός από τα δικαστήρια όταν αυτά ενεργούν υπό τη δικαιοδοτική τους ιδιότητα, προκειμένου να διασφαλίζεται η ανεξαρτησία των δικαστικών λειτουργών κατά την άσκηση των δικαιοδοτικών τους καθηκόντων, περιλαμβανομένης της λήψης αποφάσεων. Σε αυτή την περίπτωση είναι απαραίτητο να ζητηθεί η γνώμη του και αυτή να καταγραφεί στα αρχεία εκπόνησης της (Άρθρο 35 παρ.2 ΓΚΠΔ). Επίσης, σύμφωνα με το άρθρο 39 περ.γ' ο ΥΠΠΔ έχει υποχρέωση να παρέχει τη συμβουλή του, όταν αυτή απαιτηθεί για μια ΕΑΠΔ (και η άποψη του να καταγραφεί στην τελική αναφορά), καθώς και να παρακολουθεί όλα τα στάδια της.

Τέλος, είναι σημαντικό να ληφθεί υπόψη η γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων αυτών**.** Στην παρ.9 του άρθρου 35 ΓΚΠΔ προβλέπεται ότι ο Υπεύθυνος Επεξεργασίας θα πρέπει να ζητεί τη γνώμη των υποκειμένων ή των εκπροσώπων τους. Αυτό μπορεί να γίνει με πολλούς τρόπους, είτε μιλώντας με τους εκπροσώπους εμπορικών/εργατικών σωματείων, εκθέτοντας τους τρόπους, τα μέσα και τους σκοπούς με τους οποίους σχεδιάζει να προβεί σε αυτή τη νέα επεξεργασία, είτε αποστέλλοντας ερωτηματολόγια στο υποψήφιο κοινό το οποίο πρόκειται να χρησιμοποιήσει την εν λόγω υπηρεσία.

6.2 Πότε (χρονικά) πρέπει να διενεργείται μια ΕΑΠΔ.

Η Εκτίμηση Αντικτύπου έχει προληπτικό χαρακτήρα. Ως εξειδίκευση της γενικότερης αρχής της λογοδοσίας σκοπός της είναι να εντοπίσει τους κινδύνους σε ένα πρώιμο στάδιο, ώστε, αυτοί να εκτοπιστούν μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων[54]. Η Εκτίμηση Αντικτύπου πρέπει να εκπονείται *'πριν από την επεξεργασία'* (άρθρο 35 παρ.1 και παρ.10). Εξάλλου, αυτό είναι το συνεπές και με τις αρχές της επεξεργασίας δεδομένων «εξ'

[53] Βλ. Article 29 Data Protection Working Party. In Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is "Likely to Result in a High Risk" for the Purposes of Regulation 2016/679; Technical Report; The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data: Brussels, Belgium, 2017 Σελ.13

[54] Βλ. Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6, 2019, 105342

ορισμού και από τον σχεδιασμό» (« By Default & By Design »), όπως αυτές προβλέπονται στο άρθρο 25 του ΓΚΠΔ και την αιτιολογική σκέψη 78 του ΓΚΠΔ. Η ΕΑΠΔ θα πρέπει να ξεκινά το νωρίτερο δυνατό στον σχεδιασμό της πράξης επεξεργασίας, ακόμη και αν ορισμένες πράξεις επεξεργασίας παραμένουν άγνωστες. Ειδικότερα, η αρχή της επεξεργασίας δεδομένων «εξ' σχεδιασμού» αναφέρεται καταρχήν στον προληπτικό χαρακτήρα της προσέγγισης. Οι σχεδιαστές ενός συστήματος πρέπει να έχουν ως γνώμονα την ιδιωτικότητα ήδη κατά τη σύλληψη, τον προσδιορισμό των χαρακτηριστικών και της αρχιτεκτονικής ενός συστήματος . Ο σχεδιασμός ενός συστήματος έχει εγγενώς κανονιστικά χαρακτηριστικά. Τα συστήματα σχεδιάζονται έτσι ώστε να ανταποκρίνονται σε ανάγκες και απαιτήσεις που έχουν προδιατυπωθεί και – συνακόλουθα - να καταστήσουν δυνατή την εκπλήρωσή τους. Σύμφωνα με την προσέγγιση της ιδιωτικότητας διά του σχεδιασμού, η προστασία της (πληροφοριακής) ιδιωτικότητας πρέπει να συμπεριλαμβάνεται τόσο στις – σχεδιαστικές και λειτουργικές - απαιτήσεις όσο και στους σκοπούς του πληροφοριακού συστήματος. Ιδιαίτερη σημασία για την εναρμόνιση του σχεδιασμού Τεχνολογιών Πληροφορικής (ΤΠΕ) προς τις δικαιικές επιταγές είναι η διαφάνεια ως προς τις σχεδιαστικές επιλογές σε συνάρτηση με τους σκοπούς που επιδιώκονται. Ωστόσο, η προστασία της ιδιωτικότητας δια του σχεδιασμού δεν περιορίζεται στην ανάπτυξη τεχνικών και οργανωτικών «έξυπνων λύσεων» αλλά στην εξέταση, ήδη κατά τη φάση του φάση του σχεδιασμού. Έτσι, Η αξιολόγηση των επιπτώσεων (μιας τεχνολογίας, εφαρμογής, επεξεργασίας, συστήματος, συσκευής κ.ά.) στην ιδιωτικότητα, όπως και η privacy by design, έχει νόημα, εφόσον εφαρμόζεται ήδη πριν από το στάδιο του σχεδιασμού ενός συστήματος ή μιας επεξεργασίας και δεν εξαντλείται σε τυπικό έλεγχο της συμμόρφωσης προς την κείμενη νομοθεσία, αλλά υπεισέρχεται σε πιο ποιοτική αξιολόγηση τόσο των τεχνολογικών προτάσεων όσο και των σκοπών και μέσων της επεξεργασίας με έμφαση στην αρχή της αναλογικότητας . Η αποτίμηση των επιπτώσεων στην ιδιωτικότητα θα πρέπει να συμπεριλαμβάνει και την κατανόηση των κινδύνων που εμπεριέχει η συγκεκριμένη επεξεργασία τόσο σε σχέση με και τις ειδικότερες κατηγορίες προσώπων που επηρεάζονται ή θίγονται από την σχεδιαζόμενη επεξεργασία αλλά και με την κοινωνία εν γένει. Η αποτίμηση των επιπτώσεων δεν μπορεί παρά να συμπεριλαμβάνει και την κατανόηση των εγγυήσεων που προβλέπονται τόσο στο πλαίσιο της έννομης τάξης όσο και σε σχέση με τη σχεδιαζόμενη επεξεργασία υπό εκτίμηση. Η (πληροφοριακή) ιδιωτικότητα θα πρέπει να ενσωματώνεται εκ των προτέρων σε ένα σύστημα, εφαρμογή ή επεξεργασία ως η κατά κανόνα σχεδιαστική επιλογή. Η privacy by default εμπεριέχει δηλ. υπό μία έννοια την απαίτηση της ενσωμάτωσης της ιδιωτικότητας κατά τον σχεδιασμό (by design) αλλά περαιτέρω προσδιορίζει ως ειδικότερο σκοπό τον σχεδιασμό ενός προγράμματος ή μιας εφαρμογής κατά τρόπο ώστε οι χρήστες που

επιθυμούν να προστατεύσουν την ιδιωτικότητα και τα προσωπικά δεδομένα τους να μην χρειάζεται να τροποποιήσουν τις προεπιλεγμένες ρυθμίσεις. Η προσέγγιση αυτή μπορεί μεν να συνιστά ένα ισχυρό εργαλείο καθώς (επιδιώκει) να επαναφέρει τον έλεγχο της πληροφορίας στα πρόσωπα που αυτή αφορά, αλλά ωστόσο προκαλεί μεγάλες τριβές και αντιστάσεις στον ιδιωτικό τομέα καθώς επηρεάζει πρακτικές που είναι ιδιαίτερα προσοδοφόρες, όπως η χρήση των ελεύθερα προσβάσιμων δεδομένων για σκοπούς (άμεσης και στοχευμένης) διαφήμισης[55].

Η ΕΑΠΔ, επιπλέον, δεν είναι μία τυπική και μεμονωμένη διαδικασία αλλά απαιτεί έναν περιοδικό έλεγχο καθ' όλη τη διάρκεια της αλλά και μετά από την ολοκλήρωση της. Υποστηρίζεται, επιπλέον, ότι θα πρέπει να αντιμετωπίζεται λιγότερο ως «εργαλείο» και περισσότερο ως «διαδικασία» η οποία θα πρέπει να εκτείνεται σε όλο τον κύκλο ζωής της επεξεργασίας.[56] Η επικαιροποίηση της ΕΑΠΔ καθ' όλον τον κύκλο ζωής του έργου θα διασφαλίζει ότι λαμβάνονται υπόψη η προστασία δεδομένων και η ιδιωτική ζωή και θα ενθαρρύνει τη δημιουργία λύσεων που προάγουν τη συμμόρφωση. Μπορεί επίσης να απαιτείται η επανάληψη επιμέρους βημάτων της αξιολόγησης καθώς προχωρά η διαδικασία ανάπτυξης, διότι η επιλογή συγκεκριμένων τεχνικών ή οργανωτικών μέτρων μπορεί να επηρεάσει τη σοβαρότητα ή την πιθανότητα επέλευσης των κινδύνων που ενέχει η επεξεργασία. Για παράδειγμα, μπορεί κατά την διενέργεια της να ανακαλυφθεί ότι συλλέγονται δεδομένα τα οποία τελικά δεν χρειάζονται για την επίτευξη του επιδιωκόμενου σκοπού και ως εκ τούτου να μην είναι απαραίτητη πλέον η συλλογή τους. Το γεγονός ότι η ΕΑΠΔ ενδέχεται να χρειαστεί επικαιροποίηση μετά την έναρξη της επεξεργασίας δεν αποτελεί βάσιμο λόγο για την αναβολή ή την παράλειψη διενέργειας ΕΑΠΔ. Η ΕΑΠΔ είναι μια διαρκής διαδικασία, ειδικά όταν η πράξη επεξεργασίας είναι δυναμική και υπόκειται σε διαρκείς μεταβολές. Η ΕΑΠΔ αποτελεί διαρκή διαδικασία και όχι πράξη που διενεργείται άπαξ.[57]

6.3 Πότε (ποιοτικά) πρέπει να διενεργείται μια ΕΑΠΔ – Περιπτωσιολογία

Το βασικό κριτήριο προσδιορισμού της έκτασης των υποχρεώσεων ενός υπευθύνου επεξεργασίας είναι αυτό του κινδύνου. Αποτέλεσμα αυτού είναι ότι η υπαγωγή σε διάφορες υποχρεώσεις εξαρτάται από το είδος της επεξεργασίας και την κλίμακα του κινδύνου. Η

[55] Λ. Μήτρου, «Privacy by Design – Η τεχνολογική διάσταση της προστασίας προσωπικών Δεδομένων, ΔΙΜΕΕ 1/2013.
[56] Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017, Σελ. 104
[57] Βλ. Katerina Demetzou,ό.π.

επιλογή αυτή συνοψίστηκε με τον όρο «προσέγγιση με βάση τον κίνδυνο» (risk based approach).[58]

Ο ΓΚΠΔ δεν απαιτεί να εκπονείται μια ΕΑΠΔ σε κάθε επεξεργασία προσωπικών δεδομένων. Το κριτήριο που θέτει είναι ποιοτικό και έγκειται στο αν η επεξεργασία ενδέχεται να επιφέρει «υψηλό κίνδυνο» για τα δικαιώματα και τις ελευθερίες των υποκειμένων.

Εκτός, όμως, από αυτή την «γενική ρήτρα» του υψηλού κινδύνου (αναλυτικότερα Βλ.5.5) ο νομοθέτης επιλέγει να δώσει μία περιπτωσιολογία με δύο τρόπους, για να βοήθήσει τον εκάστοτε Υπεύθυνο επεξεργασίας να «υποψιαστεί» το πότε είναι πιθανόν να υπάρχει αυτός ο «Υψηλός» κίνδυνος. Ο πρώτος εξ' αυτών είναι ότι ο ίδιος ο ΓΚΠΔ παρέχει κάποιες εξηγήσεις για το πότε μία επεξεργασία μπορεί να επιφέρει υψηλό κίνδυνο.

Ειδικότερα, στο άρθρο 35 παρ.3 αναφέρονται ενδεικτικά κάποια παραδείγματα τα οποία θεωρείται ότι ενδέχεται να επιφέρουν υψηλό κίνδυνο: Αυτά είναι τα εξής:

α) Σε περίπτωση συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα

Ο δεύτερος τρόπος με τον οποίο επιλέγει να αναπτύξει μια περιπτωσιολογία είναι μέσω της παραγράφου 4 του άρθρου 35, με την οποία υποχρεώνει την εποπτική αρχή να καταρτίζει κατάλογο των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για την διενέργεια εκτίμησης αντικτύπου λόγω του υψηλού κινδύνου. Ειδικότερα, στο άρθρο 35 παρ.4 του ΓΚΠΔ αναφέρεται ότι *«Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με*

[58] Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017, Σελ. 95 επ.

την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.» Ως εκ τούτου, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, στις 16 Οκτωβρίου του 2018 δημοσίευσε τον εν λόγω κατάλογο για την Ελλάδα.[59] Σύμφωνα με τον κατάλογο αυτό, τα κριτήρια για την διενέργεια ΕΑΠΔ ομαδοποιούνται στις παρακάτω τρεις κατηγορίες:

- 1η κατηγορία: με βάση τα είδη και τους σκοπούς επεξεργασίας.

- 2η κατηγορία: με βάση το είδος των δεδομένων και/ή τις κατηγορίες των υποκειμένων.

- 3η κατηγορία: με βάση τα πρόσθετα χαρακτηριστικά και/ή τα χρησιμοποιούμενα μμέσα της επεξεργασίας.

Η διενέργεια ΕΑΠΔ κρίνεται υποχρεωτική όταν πληρούνται τουλάχιστον ένα από τα κριτήρια της 1ης ή της 2ης κατηγορίας. Είναι επίσης υποχρεωτική όταν συντρέχει ένα τουλάχιστον κριτήριο ως προς την 3η κατηγορία και η επεξεργασία αφορά είδη και σκοπούς της 1ης κατηγορίας επεξεργασίας ή/και είδη δεδομένων ή/και κατηγορίες υποκειμένων της 2ης κατηγορίας.

6.4 Πότε (ποιοτικά) πρέπει να διενεργείται μια ΕΑΠΔ – Τα κριτήρια της ομάδας του άρθρου 29

Όπως προαναφέρθηκε ο νομοθέτης επέλεξε να παρουσιάσει μία ευρεία περιπτωσιολογία για το πότε είναι απαραίτητη η διενέργεια μίας ΕΑΠΔ. Ωστόσο, ούτε η παρ. 3 του άρθρου 35 ούτε και ο κατάλογος της ΑΠΔΠΧ περιγράφουν εξαντλητικά τις περιπτώσεις στις οποίες απαιτείται η διενέργεια ΕΑΠΔ. Αντιθέτως, και τα δύο βρίσκονται κάτω από την «ομπρέλα» της παραγράφου 1 του άρθρου 35 ΓΚΠΔ. Δηλαδή του κριτηρίου του «κινδύνου» για τα δικαιώματα και τις ελευθερίες των υποκειμένων , όπως εξάλλου γίνεται και στο άρθρο 24 ΓΚΠΔ , όπου και πάλι βάσει του κριτηρίου του κινδύνου υποχρεώνει τον υπεύθυνο να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Γίνεται δεκτό ότι ο κίνδυνος αυτός μπορεί να αφορά, όχι μόνο τα δικαιώματα που άπτονται των προσωπικών δεδομένων αλλά και άλλα θεμελιώδη δικαιώματα, όπως την ελευθερία του λόγου, την ελευθερία της σκέψης, την ελευθερία κυκλοφορίας, την απαγόρευση των διακρίσεων, το δικαίωμα στην ελευθερία

[59] Βλ. Αρχή Προστασίας Προσωπικών Δεδομένων, «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», 16 Οκτωβρίου 2018, Αριθ. Πρωτ.: Γ/ΕΞ/8187/16-10-2018 https://www.dpa.gr/sites/default/files/2019-10/article_35_dpia_list_gr_2.pdf,

συνειδήσεως και θρησκείας . Βάσει, λοιπόν, αυτού του κριτηρίου, ο υπεύθυνος επεξεργασίας υποχρεούται να διενεργήσει μία ανεξάρτητη αξιολόγηση του κινδύνου.

Ως εκ τούτου, η ομάδα εργασίας του άρθρου 29 καθορίζει εννιά κριτήρια τα οποία θα πρέπει να λαμβάνονται δεόντως υπόψη από τον υπεύθυνο επεξεργασίας που είναι ενδεικτικά για το πότε υπάρχει υψηλός κίνδυνος και αναλύονται εκτενώς στις κατευθυντήριες γραμμές που έχει εκδώσει. Τα εννιά αυτά κριτήρια, αφορούν:

1) Την Βαθμολόγηση ή την Αξιολόγηση των υποκειμένων
2) Την διαδικασία λήψης αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα.
3) Την συστηματική παρακολούθηση υποκειμένων
4) Την ευαισθησία και την φύση των δεδομένων
5) Το αν αποτελούν δεδομένα μεγάλης κλίμακας
6) Την αντιστοίχιση και τον συνδυασμό των δεδομένων
7) Το πόσο ευάλωτα είναι τα υποκείμενα των δεδομένων
8) Την καινοτομία της τεχνολογίας και των οργανωτικών λύσεων που χρησιμοποιούνται στην επεξεργασία
9) Το κατά πόσον εμποδίζονται τα υποκείμενα των δεδομένων να ασκήσουν τα δικαιώματά τους.

Αναφέρεται ενδεικτικά ότι ο υπεύθυνος επεξεργασίας μπορεί να θεωρεί ότι υπάρχει υψηλός κίνδυνος όταν πληρούνται τουλάχιστον δύο από τα ανωτέρω κριτήρια. Εν γένει, η ομάδα εργασίας του άρθρου 29 θεωρεί ότι όσο περισσότερα κριτήρια πληρούνται με την επεξεργασία, τόσο πιθανότερο είναι να τίθενται σε υψηλό κίνδυνο τα δικαιώματα και οι ελευθερίες των υποκειμένων των δεδομένων και, ως εκ τούτου, να απαιτείται η διενέργεια ΕΑΠΔ, ανεξάρτητα από τα προβλεπόμενα μέτρα του υπεύθυνου επεξεργασίας. Ωστόσο, σε ορισμένες περιπτώσεις, ο υπεύθυνος επεξεργασίας μπορεί να θεωρήσει ότι σε επεξεργασία στην οποία πληρούνται μόνο ένα από τα εν λόγω κριτήρια απαιτείται η διενέργεια ΕΑΠΔ. Αντιθέτως, σύμφωνα με την ομάδα εργασίας του άρθρου 29 μια πράξη επεξεργασίας που ενδεχομένως αντιστοιχεί στις ανωτέρω αναφερόμενες περιπτώσεις κατά τον υπεύθυνο επεξεργασίας μπορεί να θεωρείται ότι εξακολουθεί να μην ενδέχεται να επιφέρει «υψηλό κίνδυνο». Στις εν λόγω περιπτώσεις, ο υπεύθυνος επεξεργασίας θα πρέπει να δικαιολογεί και να τεκμηριώνει τους λόγους μη διενέργειας ΕΑΠΔ και να περιλαμβάνει/καταγράφει τις απόψεις του υπεύθυνου προστασίας δεδομένων.

Έτσι, λοιπόν, καθίσταται σαφές πως ούτε τα κριτήρια που θέτει η ομάδα εργασίας του άρθρου 29 είναι numerus clausus και δεν περιγράφουν εξαντλητικά τις περιπτώσεις εκείνες στις οποίες είναι υποχρεωτική η διενέργεια εκτίμησης αντικτύπου. Αντιθέτως, όπως αναφέρθηκε και παραπάνω το πότε είναι υποχρεωτική η διενέργεια της εκτίμησης αντικτύπου πρέπει να κρίνεται μέσα από την σκοπιά του Υψηλού Κινδύνου.

6.5. Πότε (ποιοτικά) πρέπει να διενεργείται μια ΕΑΠΔ – Το κριτήριο του «Υψηλού Κινδύνου – Ανεξάρτητος Έλεγχος του υπευθύνου επεξεργασίας»

Παρόλο των ενδεικτικών περιπτώσεων που παραθέτει τόσο ο νομοθέτης απευθείας, όσο και μέσω της υποχρέωσης των εποπτικών αρχών να εκδώσουν τους αντίστοιχους καταλόγους και της ομάδας εργασίας του άρθρου 29 προσπαθώντας να καθορίσει το πότε υπάρχει υψηλός κίνδυνος και πάλι ο υπεύθυνος επεξεργασίας είναι αυτός που θα πρέπει να καθορίσει αν εν τέλει υπάρχει υψηλός κίνδυνος και να αποτυπώσει αυτή τη «μέτρηση», διενεργώντας έναν ανεξάρτητο έλεγχο για τον εντοπισμό του κινδύνου.

Βέβαια, για την υποχρέωση διενέργειας εκτίμησης Αντικτύπου δεν αρκεί ο απλός κίνδυνος. Το κριτήριο του υψηλού βαθμού κινδύνου είναι αυτό που καθίσταται ρητά αποφασιστικό αναφορικά με την υποχρέωση διενέργειας εκτίμησης των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα (αρ.35 παρ.1),[60].Μάλιστα, αυτή η απαίτηση (του υψηλού κινδύνου) είναι συστατικός όρος για την υποχρέωση διενέργειας μιας ΕΑΠΔ, αφού αν εκλείπει αυτός, εκλείπει και η υποχρέωση για την διενέργεια ΕΑΠΔ[61].

Ως εκ τούτου προκύπτουν κρίσιμα ζητήματα και κυρίως α) ποιο είναι το κριτήριο διαβάθμισης του κινδύνου, β) ποιος και με ποια διαδικασία νομιμοποιείται από τη νομοθεσία να προσδιορίσει τη φύση του κινδύνου και κατά συνέπεια να προσδιορίσει την έκταση των υποχρεώσεων και γ) είναι ελεγκτέος αυτός ο προσδιορισμός και πως. Ο κανονισμός αναφέρεται σε «υψηλό κίνδυνο» και το μείζον ζητούμενο είναι ο προσδιορισμός του κινδύνου και των προσδιοριστικών στοιχείων που τον καθιστούν υψηλό. Η απαίτηση της νομικής ασφάλειας επιτάσσει τον προσδιορισμό των κριτηρίων, έστω ενδεικτικά, από τον ίδιο τον νομοθέτη ακόμα

[60]Βλ. Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017, Σελ. 95 επ.
[61] Βλ. Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6, 2019, 105342

και εάν – καταρχήν- εκτίμηση και αξιολόγηση επιφυλάσσεται στον αποδέκτη της ρύθμισης, τον υπεύθυνο επεξεργασίας[62].

Ο ενωσιακός νομοθέτης επιδίωξε τον προσδιορισμό της έννοιας και της έντασης των κινδύνων μέσω ποικίλων αναφορών στις αιτιολογικές σκέψεις. Η αιτιολογική σκέψη 75 του Κανονισμού παραθέτει πράγματι έναν ευρύ κατάλογο πιθανών κινδύνων «για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ποικίλης πιθανότητας και σοβαρότητας, η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη ή οποιαδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα ή όταν τα υποκείμενα των δεδομένων θα μπορούσαν να στερηθούν των δικαιωμάτων και των ελευθεριών τους ή να εμποδίζονται από την άσκηση ελέγχου επί των δεδομένων προσωπικών τους χαρακτήρα.[63]

Έτσι, λοιπόν, ο κίνδυνος αποτελεί ένα κρίσιμο κριτήριο που εισάγεται προκειμένου να υπάρξει μια αναλογικότητα στην εκτίμηση από τους υπευθύνους επεξεργασίας ανάλογα και με τις ειδικές συνθήκες επεξεργασίας δεδομένων. Η λέξη «υψηλός» που χρησιμοποιείται στο άρθρο 35 παρ.1 καταδεικνύει ότι υπάρχουν και ποιοτικά κριτήρια αξιολόγησης. Η ομάδα του άρθρου 29 αναφέρει ότι «κίνδυνος είναι ένα σενάριο που περιγράφει ένα γεγονός συμβάν και τις επιπτώσεις του, που έχουν εκτιμηθεί με όρους σοβαρότητας και πιθανότητας επέλευσης»

Προκειμένου ο υπεύθυνος επεξεργασίας δεδομένων να καταλήξει στο συμπέρασμα ότι κάτι θα μπορούσε να συνιστά κίνδυνο (είτε υψηλό, είτε χαμηλό) θα πρέπει πρώτα να εκτιμήσει εάν και πόσο σοβαρός θα είναι ο κίνδυνος και πόσο πιθανό είναι να συμβεί αυτό το γεγονός. Αναφορικά με την αξιολόγηση της «πιθανότητας« και της «σοβαρότητας» του κινδύνου ο Κανονισμός παραπέμπει στην φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενώ επιτάσσει να αξιολογείται ο κίνδυνος «βάσει αντικειμενικής εκτίμησης, με την οποία διαπιστώνεται κατά πόσον οι πράξεις επεξεργασίας δεδομένων συνεπάγονται κίνδυνο ή υψηλό κίνδυνο» (αιτιολογική σκέψη 76)

Ως εκ τούτου, για την αποτύπωση της σοβαρότητας και της πιθανότητας έχουν αναπτυχθεί εργαλεία που καθορίζουν την κλίμακα και την μεθοδολογία για την εκτίμηση τους. Ειδικότερα, με τον όρο σοβαρότητα νοείται το μέγεθος ενός κινδύνου. Η σοβαρότητα του κινδύνου εκτιμάται κυρίως σε σχέση με την έκταση των πιθανών επιπτώσεων (άμεσων και εμμέσων) στα υποκείμενα των δεδομένων, λαμβάνοντας υπόψη τα υφιστάμενα, προγραμματισμένα ή συμπληρωματικά μέτρα (τα οποία πρέπει να αναφέρονται ως αιτιολόγηση

[62]Βλ. Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017
[63]Βλ. Λ. Μήτρου, ό.π.

της σχετικής αξιολόγησης). Με τον όρο «Πιθανότητα» νοείται το κατά πόσο είναι ενδεχόμενη η επέλευση ενός κινδύνου. Η πιθανότητα του κινδύνου εκτιμάται κυρίως με βάση τον βαθμό ευπάθειας των σχετικών υποστηρικτικών στοιχείων και τον βαθμό ικανότητας των πηγών κινδύνων να εκμεταλλευτούν τις ευπάθειες αυτές, λαμβανομένων υπόψη των υφιστάμενων, προγραμματισμένων ή συμπληρωματικών μέτρων (τα οποία και πάλι πρέπει να αναφέρονται ως αιτιολόγηση της σχετικής αξιολόγησης) [64].

Τέλος, επισημαίνεται ότι το συμπέρασμα στο οποίο καταλήγει ο υπεύθυνος επεξεργασίας από τον έλεγχο για το αν τελικά χρειάζεται να διενεργηθεί μία εκτίμηση αντικτύπου πρέπει να καταγραφεί, παρόλο που κάτι τέτοιο δεν είναι δεσμευτικό από τον κανονισμό ή τις οδηγίες της ομάδας εργασίας του άρθρου 29. Εξάλλου, αυτό είναι συνεπές τόσο σχετικά με την αρχή της λογοδοσίας που , όπως αναφέρθηκε και παραπάνω, διαπνέει ολόκληρο τον ΓΚΠΔ και ως εκ τούτου έχει και πρακτική αξία, καθιστώντας τον υπεύθυνο επεξεργασίας σε θέση να αποδείξει τους λόγους που τον οδήγησαν σε οποιαδήποτε απόφαση εν τέλει έλαβε.

7. Η απαραίτητη προεργασία μίας ΕΑΠΔ.

7.1 Δημιουργία αρχείων δραστηριοτήτων επεξεργασίας, καθορισμός των νομικών βάσεων, εντοπισμός των εμπλεκομένων μερών και εκτίμηση της αναγκαιότητας .

Για να επιτευχθεί μία επιτυχημένη εκτίμηση αντικτύπου είναι απαραίτητο να προηγηθεί μία «προεργασία». Αναφέρεται, βέβαια, πως το συγκεκριμένο στάδιο δεν περιγράφεται στις περισσότερες μεθοδολογικές προσεγγίσεις. Ωστόσο, όπως έχει ήδη αναφερθεί, κορμός της παρούσας εργασίας αποτελεί η Μεθοδολογία που αναπτύχθηκε από το Fraunhofer Institute[65], η οποία και περιγράφει το συγκεκριμένο στάδιο. Σε αυτό το στάδιο εμφανίζεται, ίσως, από άποψη δομής, η μεγαλύτερη διαφορά σε σχέση με οποιαδήποτε άλλη μεθοδολογική προσέγγιση καθώς είναι η μόνη που προτείνει ότι για την διενέργεια της εκτίμησης αντικτύπου είναι απαραίτητο να έχει προηγηθεί η δημιουργία των «Αρχείων δραστηριοτήτων επεξεργασίας», όπως αυτά περιγράφονται στο άρθρο 30 του ΓΚΠΔ. Επιπλέον, απαιτείται ο καθορισμός των νομικών βάσεων της επεξεργασίας καθώς και η αξιολόγηση της αναγκαιότητας να διενεργηθούν πριν από την εκκίνηση της διενέργειας της εκτίμησης αντικτύπου, σε αντίθεση με τις περισσότερες μεθοδολογικές προσεγγίσεις που την διενεργούν

[64]Βλ. Δημήτριος Ευ. Τζέλλης, Μαρία Δ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 9 επ.
[65]Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact ssessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag. Σελ. 8 επ.

μετά από το στάδιο της συστηματικής περιγραφή της επεξεργασίας (Βλ. Κεφάλαιο 7). Ειδικότερα, και η μεθοδολογική προσέγγιση του ICO[66] και της CNIL, φαίνεται ότι ακολουθούν την δομή που παρατίθενται στο παράρτημα 2 - κριτήρια του αν μία ΕΑΠΔ είναι αποδεκτή από την ομάδα εργασίας του άρθρου 29[67] αλλά και από τον ίδιο τον ΓΚΠΔ που παραθέτει την εκτίμηση της αναγκαιότητας και της αναλογικότητας στο στοιχείο β' της παραγράφου 7 του άρθρου 35, μετά ,δηλαδή, από το στοιχείο α' που επιβάλλει την συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,. Βέβαια, το γεγονός ότι επιλέγει η μεθοδολογία του Fraunhofer να αλλάξει την σειρά των απαιτούμενων βημάτων μιας ΕΑΠΔ δεν φαίνεται να έρχεται σε αντίθεση ούτε με τον ΓΚΠΔ, ούτε με τις οδηγίες της ομάδα εργασίας του άρθρου 29, καθώς και τα δύο καθιστούν μεν απαραίτητη την διενέργεια των εν λόγω εκτιμήσεων, χωρίς ,όμως, να προκύπτει απαγόρευση ή υποχρέωση διενέργειάς τους με συγκεκριμένη και υποχρεωτική σειρά.

Μεθοδολογικά, αυτή η μεγάλη δομική διαφορά ερείδεται στο γεγονός ότι η συγκεκριμένη μεθοδολογική προσέγγιση βασίζεται πάνω στην προσέγγιση που αναπτύχθηκε από την Γερμανική Αρχή Προστασίας Προσωπικών Δεδομένων «SDM»[68] η οποία για την εξεύρεση και εφαρμογή των κατάλληλων τεχνικών και οργανωτικών μέτρων προτείνει την λειτουργικοποίηση των Αρχών Επεξεργασίας Προσωπικών Δεδομένων και της συστηματοποίησης εν γένει των απαιτήσεων του ΓΚΠΔ, μέσω της επίτευξης επτά (7) «στόχων προστασίας» (Protectional Goals). Σημειώνεται ότι η SDM δεν αποτελεί μεθοδολογική προσέγγιση για την διενέργεια μίας ΕΑΠΔ , αλλά εργαλείο για την εν γένει συμμόρφωση του υπευθύνου επεξεργασίας προσωπικών δεδομένων με τον ΓΚΠΔ.[69]. Σύμφωνα με αυτή τη προσέγγιση όλες οι απαιτήσεις του ΓΚΠΔ συστηματοποιούνται και συμπυκνώνονται σε 7 στόχους, οι οποίοι πρέπει να επιτευχθούν. Βέβαια, αναφέρεται πως ακόμα και αυτή η μεθοδολογική προσέγγιση έχει από μόνη της ένα προαπαιτούμενο και αυτό είναι ο καθορισμός της νομικής βάσης της επεξεργασίας, που πρέπει να προηγηθεί της εφαρμογή της. Έτσι, ο υπεύθυνος επεξεργασίας καλείται πριν προβεί σε οποιαδήποτε επεξεργασία να καθορίσει την νομική βάση της επεξεργασίας, σύμφωνα με το άρθρο 6 του ΓΚΠΔ[70]. Αποτέλεσμα αυτού είναι

[66]Βλ. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/ (STEP 4)
[67] Βλ. 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. Ομάδα εργασίας άρθρου 29. Παράρτημα 2 Σελ. 28 επ.
[68]Βλ. Standard Data Protection Model, German Federal Data Protection Authority, https://www.bfdi.bund.de/EN/Fachthemen/Inhalte/Technik/SDM.html (Τελευταία επίσκεψη 27/11/2023)
[69]Βλ. Standard Data Protection Model, German Federal Data Protection Authority, Σελ. 9
[70]Βλ. Standard Data Protection Model, German Federal Data Protection Authority, Σελ. 8

ότι και στην μεθοδολογική προσέγγιση της εκτίμησης αντικτύπου που έχει βασιστεί πάνω στην προσέγγιση των «στόχων προστασίας» του SDM, ο καθορισμός του σκοπού και της νομικής βάσης πρέπει να προηγηθεί της διενέργειας της ίδιας της εκτίμησης. Για να συμβεί αυτό, οι δημιουργοί της εν λόγω μεθοδολογικής προσέγγισης θεωρούν ότι πρέπει να έχει εκπληρωθεί κατ' αρχάς η υποχρέωση που απορρέει από το άρθρο 30 του ΓΚΠΔ, η δημιουργία, δηλαδή, των «Αρχείων Δραστηριοτήτων Επεξεργασίας»[71], αφού σύμφωνα με την παράγραφο 1 περ. β' του παραπάνω άρθρου θα πρέπει στα αρχεία αυτά να καθορίζεται ο σκοπός της επεξεργασίας. Επιπλέον, ως προς την νομική βάση αναφέρεται ότι σύμφωνα με το άρθρο 5 παράγραφος 1 στοιχείο α) του ΓΚΠΔ, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα απαιτεί νομική βάση. Οποιαδήποτε επεξεργασία που διενεργείται χωρίς αποτελεσματική νομική βάση συνιστά παραβίαση του θεμελιώδους δικαιώματος στην προστασία των δεδομένων σύμφωνα με το άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαικής Ένωσης[72], και, ως εκ τούτου, θεωρείται παραβίαση για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, καθώς και παράβαση του ΓΚΠΔ. Για να αποφευχθεί αυτό, η νομική βάση για την προβλεπόμενη επεξεργασία θα πρέπει να τεκμηριώνεται εκ των προτέρων. Το άρθρο 6 παράγραφος 1 στοιχεία α)-στ) του ΓΚΠΔ απαριθμεί έξι δυνατούς νομικούς λόγους για την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Εάν υποβάλλονται σε επεξεργασία ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα, όπως αναφέρεται στο άρθρο 9 παράγραφος 1 του ΓΚΠΔ, ή δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα σύμφωνα με τον άρθρο 10 ΓΚΠΔ, οι συμπληρωματικοί νομικοί λόγοι που αφορούν αυτούς τους τύπους προσωπικών δεδομένων πρέπει επίσης να λαμβάνονται υπόψη κατά την επεξεργασία. Εάν σε μία πράξη επεξεργασίας εμπλέκονται πολλές χωριστές νομικές οντότητες, οι οποίες επεξεργάζονται επίσης διαφορετικά δεδομένα προσωπικού χαρακτήρα διαφορετικών υποκειμένων των δεδομένων, αυτές οι διαφορετικές πράξεις επεξεργασίας ενδέχεται να πρέπει να βασίζονται σε ξεχωριστές νομικές βάσεις. Θα πρέπει να διασφαλίζεται ότι κάθε συγκεκριμένη πράξη επεξεργασίας, και συνεπώς η επεξεργασία ως στο σύνολό της, καλύπτεται από μια νομική βάση. Σε τέτοιες περιπτώσεις, συνιστούν την κατάρτιση διαγράμματος που να δείχνει τα ενδιαφερόμενα μέρη, τα υποκείμενα των δεδομένων, τις πράξεις επεξεργασίας και τις νομικές σχέσεις (συμπεριλαμβανομένων των υφιστάμενων ροών δεδομένων).

[71]Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact ssessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag. Σελ. 8 επ.

[72]Βλ. Χάρτης των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (2016/C 202/02)

Επιπλέον, σύμφωνα με την μεθοδολογική προσέγγιση του Fraunhofer σε αυτό το στάδιο θα πρέπει να γίνει και η εκτίμηση της αναγκαιότητας των δεδομένων. Ειδικότερα, αυτό είναι συνεπές και με την αρχή της αναλογικότητας, ιδίως ως προς τις εκφάνσεις της αναγκαιότητας και της (υπό στενή εννοία) αναλογικότητας η οποία αποτελεί κατεξοχήν κριτήριο νομιμότητας της επεξεργασίας και κεντρικό άξονα για την εξέταση των σχετικών υποθέσεων από την ΑΠΔΠΧ[73]. Η εκτίμηση αυτή αφορά την αξιολόγηση του κατά πόσον οι πράξεις επεξεργασίας, συμπεριλαμβανομένων των δεδομένων που συλλέγονται γι' αυτές, είναι πραγματικά αναγκαίες για την εκπλήρωση των σκοπών της επεξεργασίας ή αν οι σκοποί θα μπορούσαν να επιτευχθούν με εναλλακτικούς τρόπους που είναι λιγότερο επεμβατικοί στην ιδιωτική ζωή των υποκειμένων και κατ΄ επέκταση επεμβαίνουν λιγότερο στα δικαιώματα και τις ελευθερίες τους. Σύμφωνα με την μεθοδολογική προσέγγιση του Fraunhofer αυτή η αξιολόγηση πρέπει να γίνεται εκ των προτέρων, καθώς κάθε επεξεργασία – ακόμα και αυτές που δεν εμπίπτουν στην υποχρέωση διενέργειας εκτίμησης αντικτύπου – πρέπει να συμμορφώνονται με την εν λόγω αρχή αλλά και επειδή αν η εκτίμηση καταλήξει σε συμπέρασμα ότι παραβιάζεται η εν λόγω αρχή θα είναι πολύ εύκολη η διενέργεια των κατάλληλων τροποποιήσεων.

Επιπλέον, θεωρεί ωφέλιμο αλλά όχι απαραίτητο να διενεργηθεί σε αυτό το σημείο και η εκτίμηση της αρχής της αναλογικότητας. Ωστόσο, αναφέρει ότι η εκτίμηση της αναλογικότητας μπορεί να γίνει μόνον εφόσον προηγηθεί μία στάθμιση των εννόμων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας από την μία και των συνεπειών που θα μπορούσε να έχει η επεξεργασία για τα δικαιώματα και τις ελευθερίες των υποκειμένων από την άλλη. Ως εκ τούτου σε αυτό το στάδιο, που δεν έχει ακόμα εκτιμηθεί ο κίνδυνος για τις ελευθερίες και τα δικαιώματα των υποκειμένων των δεδομένων η συγκεκριμένη εκτίμηση έχει μόνο προαιρετικό χαρακτήρα και διενεργείται μόνο βάσει του προληπτικού χαρακτήρα της ΕΑΠΔ, με σκοπό να προλάβει εξόφθαλμες παραβιάσεις του ΓΚΠΔ, σε καμία περίπτωση, όμως, δεν μπορεί να θεωρηθεί ότι πληροί τις προϋποθέσεις του άρθρου 35 παρ.7 στοιχεία β'.[74]

Πράγματι, σε αντίθεση με τις μεθοδολογικές προσεγγίσεις την CNIL και του ICO φαίνεται ότι η συγκεκριμένη προσέγγιση εναρμονίζεται καλύτερα με τις αρχές επεξεργασίας By Default και By Design, αφού σε αυτό το στάδιο ακόμα δεν έχει σχεδιαστεί πλήρως το σύστημα και οι διαδικασίες (τεχνικά και οργανωτικά) της επεξεργασίας και ως εκ τούτου, διενεργώντας τόσο νωρίς τις ανωτέρω εκτιμήσεις και καθορίζοντας τους σκοπούς και τις νομικές βάσεις είναι

[73]Βλ. Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017, Σελ. 63 επ.
[74]Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact ssessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag. Σελ. 22 επ.

ευκολότερο να εντοπιστούν (κυρίως) οι εξόφθαλμες παραβιάσεις και να διενεργηθούν όσο το δυνατόν νωρίτερα, οι κατάλληλες τροποποιήσεις.

Ειδικότερα, ο ICO απαιτεί να διενεργηθεί η εκτίμηση της αναγκαιότητας και της αναλογικότητας στο στάδιο μετά την συστηματική περιγραφή της επεξεργασίας.[75] Ως προς το πως πρέπει να διενεργηθεί η εκτίμηση της αναγκαιότητας και της αναλογικότητας καλεί τον υπεύθυνο επεξεργασίας να απαντήσει σε ερωτήσεις. Η πρώτη είναι να καταγράψει ποια είναι η νόμιμη βάση για την επεξεργασία, αν αυτή επιτυγχάνει το σκοπό της, αν υπάρχει άλλος τρόπος να επιτευχθεί το ίδιο αποτέλεσμα, πως θα διασφαλιστεί η ποιότητα των δεδομένων και η ελαχιστοποίηση των δεδομένων, αν χρησιμοποιείται τεχνητή νοημοσύνη πως θα αποφευχθεί η μεροληψία, τι πληροφορίες θα παρασχεθούν στα άτομα, πως θα βοηθηθούν τα άτομα στην άσκηση των δικαιωμάτων τους, ποια μέτρα θα χρησιμοποιηθούν για να διασφαλιστεί ότι οι υπεύθυνοι επεξεργασία συμμορφώνονται και πως διασφαλίζονται τυγχόν διεθνείς διαβιβάσεις[76]. Περαιτέρω, παραπέμπει στις οδηγίες της ομάδας εργασίας του άρθρου 29.

Ως προς την δομή και η μεθοδολογική προσέγγιση της CNIL συμβαδίζει με αυτή του ICO, αφού θέτει την εκτίμηση των αρχών της αναλογικότητας και την αναγκαιότητας μετά την συστηματική καταγραφή της επεξεργασίας[77]. Ειδικότερα, μέσα από το ψηφιακό εργαλείο ανοιχτού κώδικα που παρέχει για την υποβοήθηση των υπευθύνων επεξεργασίας καλεί τους τελευταίους να καταγράψουν τις θεμελιώδεις αρχές που διασφαλίζουν την προστασία των δεδομένων. Το στάδιο αυτό χωρίζεται σε δύο μέρη με το πρώτο να είναι η καταγραφή εκείνων των πληροφοριών που διασφαλίζουν την αναγκαιότητα και την αναλογικότητα των δεδομένων, ενώ το δεύτερο τα μέτρα που διασφαλίζουν τα δικαιώματα των υποκειμένων. Σημειώνεται εδώ, ότι αυτή η προσέγγιση φαίνεται να ομοιάζει πολύ στην προσέγγιση των κριτηρίων για την αποδοχή μίας ΕΑΠΔ στο παράρτημα 2 των οδηγιών της ομάδας εργασίας του άρθρου 29.

Ως εκ τούτου, για το πρώτο μέρος καλεί τον υπεύθυνο επεξεργασίας να καταγράψει αν οι σκοποί της επεξεργασίας είναι καθορισμένοι, ρητοί και νόμιμοι .Επιπλέον, ζητά να καθοριστούν οι νομικές βάσεις που καθιστούν την επεξεργασία νόμιμη και να επεξηγηθεί αν τα δεδομένα είναι απαραίτητα, σχετικά και περιορισμένα ως προς τους σκοπούς της επεξεργασίας. Τέλος, για την ολοκλήρωση του πρώτου μέρους απαιτεί να καταγραφούν αν τα

[75]Βλ. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/ (STEP 4)
[76]Βλ. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/dpia-tools/online-retail/step-4-assess-necessity-and-proportionality/
[77]Βλ. The open source PIA software helps to carry out data protection impact assessment, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

δεδομένα είναι ακριβή και ενημερωμένα και ποιοι είναι οι λόγοι που δικαιολογούν τον συγκεκριμένο χρόνο τήρησης των.

Ως προς το δεύτερο μέρος, το πρώτο ζητούμενο είναι να καταγραφεί το πως επιτυγχάνεται η ενημέρωση του υποκειμένου των δεδομένων προσπαθώντας να διασφαλίσει ότι το υποκείμενο των δεδομένων θα ενημερωθεί και ότι δεν εμπίπτει σε κάποιου είδους εξαίρεση. Επιπλέον, ζητά να καταγραφεί το πως διασφαλίζεται ότι το υποκείμενο των δεδομένων έχει δώσει την συγκατάθεση του όταν αυτή θα αποτελεί τη νομική βάση της επεξεργασίας. Παράλληλα, ζητά να καταγραφούν το πως τα υποκείμενα θα ασκούν τα δικαιώματα τους και ειδικότερα για τα δικαιώματα πρόσβασης και φορητότητας, διόρθωσης και διαγραφής, περιορισμού και εναντίωσης, καθώς και το πως διασφαλίζεται ότι οι εκτελούντες την επεξεργασία δεσμεύονται συμβατικώς για την ασφαλή επεξεργασία των δεδομένων. Τέλος, ζητά την καταγραφή των διασυνοριακών διαβιβάσεων και αν αυτές είναι προστατευμένες στο σωστό επίπεδο.

7.2 Οι Στόχοι Προστασίας κατά την «SDM» .

Σε αντίθεση με τις υπόλοιπες μεθοδολογικές προσεγγίσεις, η μεθοδολογία του Fraunhofer δεν προβαίνει στην καταγραφή των Θεμελιωδών αρχών Προστασίας, όπως απαιτεί να πραγματοποιηθεί η αντίστοιχη της CNIL , αφού οι τελευταίες εργαλειοποιούνται μέσα από το πρίσμα των «στόχων προστασίας». Σε καμία περίπτωση, βέβαια, οι στόχοι προστασίας δεν έρχονται σε αντίθεση με τις Αρχές, αλλά αντιθέτως τις «καλύπτουν» όλες τόσο σε έκταση όσο και σε ποιότητα. Οι «στόχοι προστασίας» δεν είναι κάτι νέο, αλλά αντικατοπτρίζουν τους στόχους προστασίας στην ασφάλεια πληροφοριών που έχουν δοκιμαστεί στην πράξη εδώ και πολλά χρόνια[78]. Οι τρείς πρώτοι στόχοι είναι γνωστοί στην επιστήμη της ασφάλειας πληροφοριακών συστημάτων εδώ και δεκαετίες και πρόκειται για την τριάδα CIA, δηλαδή, της Εμπιστευτικότητας (Confidentiality) – Διαθεσιμότητας (Availability) – Ακεραιότητας (Integrity) των δεδομένων. Μαζί με αυτούς τους τρεις στόχους, που ήταν μέχρι σήμερα η βασική τριάδα για την επιστήμη της ασφάλειας των δεδομένων, προστέθηκαν ακόμα τρεις για να καλυφθεί ολόκληρο το φάσμα προστασίας των αρχών προστασίας προσωπικών δεδομένων, όπως προκύπτουν από το άρθρο 5 του ΓΚΠΔ. Έτσι, οι επόμενοι τρεις στόχοι είναι η Διαφάνεια (Transparency), ως προϋπόθεση για να μπορούν το υποκείμενο των δεδομένων και τα υπόλοιπα

[78]Βλ. Standard Data Protection Model, German Federal Data Protection Authority, Σελ.10 επ.

εμπλεκόμενα μέρη να κατανοούν και να ελέγχουν τις πράξεις επεξεργασίας, η ανυπαρξία δυνατότητας διασύνδεσης των δεδομένων (Unlinkability) του ατόμου, ως προϋπόθεση για τον περιορισμού του σκοπού της επεξεργασίας και της αναγκαιότητας των δεδομένων και τέλος η δυνατότητα παρέμβασης (Intervenability) , ως προϋπόθεση για την άσκηση του δικαιώματος των δεδομένων δικαιωμάτων του υποκειμένου των δεδομένων. Τέλος, στο επίκεντρο όλων αυτών των έξι στόχων τίθενται ο έβδομος στόχος, ο οποίος είναι η ελαχιστοποίηση των δεδομένων. Βέβαια, σε αντίθεση με την επιστήμη των υπολογιστών, ο SDM ερμηνεύει τους προστατευτικούς στόχους από την σκοπιά των υποκειμένων των δεδομένων θέτοντας τα τελευταία στο επίκεντρο του, εκπληρώνοντας έτσι ακόμα πιο ολιστικά τον τελικό σκοπό της, αφού συνδυάζει τους- εδώ και χρόνια γνωστούς – στόχους προστασίας της ασφάλειας των πληροφοριών με τις απαιτήσεις προστασίας προσωπικών δεδομένων του ΓΚΠΔ.[79].

7.2.1. **1ος Στόχος. Ελαχιστοποίηση των δεδομένων (Data Minimization)**

Αναλυτικότερα, ο πρώτος στόχος προστασίας που εξετάζεται είναι η ελαχιστοποίηση των δεδομένων, η οποία εργολειοποιεί τη θεμελιώδη αρχή της ελαχιστοποίησης σύμφωνα με την οποία τα δεδομένα πρέπει να περιορίζονται, στο μέτρο του δυνατού, στο αναγκαίο μέτρο για τον σκοπό τον οποίο διενεργείται η επεξεργασία (άρθρο 5 παρ.1 στοιχ. γ' ΓΚΠΔ). Η ελαχιστοποίηση των δεδομένων δεν αφορά μόνο την ποσότητα των δεδομένων αλλά και το πλαίσιο της επεξεργασίας, την διάρκεια αποθήκευσης τους και την προσβασιμότητα σε αυτά. Έτσι, πρέπει να διασφαλίζεται ότι τα δεδομένα τηρούνται με τέτοιο τρόπο ώστε να καθιστούν ταυτοποιήσιμο ένα πρόσωπο μόνο για όσο χρονικό διάστημα είναι απαραίτητο για την επίτευξη των σκοπών της επεξεργασίας (περιορισμός της διάρκειας των δεδομένων – άρθρο 5 παρ. 1 στοιχ. ε' ΓΚΠΔ). Η ελαχιστοποίηση των δεδομένων ξεκινά από τον σχεδιασμό των τεχνολογιών πληροφορικής από τον ίδιο τον κατασκευαστή τους (άρθρο 25 παρ.2 ΓΚΠΔ), συνεχίζει κατά την βασική του λειτουργία και επεκτείνεται μέχρι τις υποστηρικτικές επεξεργασίας, όπως για παράδειγμα την συντήρηση του συστήματος[80]. Ο τρόπος με τον οποίο μπορεί να επιτευχθεί ο στόχος προστασίας της ελαχιστοποίησης είναι μέσω της μείωσης των καταγεγραμμένων χαρακτηριστικών για κάθε υποκείμενο, μείωση των επιλογών επεξεργασίας για κάθε στάδιο της επεξεργασίας, μείωση των πιθανοτήτων απόκτησης γνώσης για τα υφιστάμενα δεδομένα, καθορισμό προεπιλεγμένων ρυθμίσεων για τα υποκείμενα των δεδομένων που περιορίζουν την επεξεργασία στο μέτρο που είναι αναγκαίο για τον σκοπό της επεξεργασίας, προτίμηση αυτοματοποιημένων διαδικασιών (όχι διαδικασιών λήψης αποφάσεων), οι οποίες θα καταστήσουν περιττή την επιπλέον επεξεργασία δεδομένων και ιδίως

[79]Βλ. Standard Data Protection Model, German Federal Data Protection Authority Σελ. 11
[80]Βλ. Standard Data Protection Model, German Federal Data Protection Authority Σελ. 25

δεδομένων που μπορεί να αποκτηθούν μέσω του διαλόγου, εφαρμογή αυτοματοποιημένων διαδικασιών για την ψευδονυμοποίηση των δεδομένων και σαφώς καθορισμένες πολιτικές διαγραφής των δεδομένων, καθορισμός του τρόπου που διαγράφονται τα δεδομένα και τέλος κανονισμούς για την επιτήρηση των διαδικασιών επεξεργασίας και του τρόπου αλλαγής των διαδικασιών επεξεργασίας.[81]

7.2.2. 2ος Στόχος. Διαθεσιμότητα (Availability)

Ο δεύτερος προστατευτικός στόχος είναι αυτός της διαθεσιμότητας. Η διαθεσιμότητα αναφέρεται στην απαίτηση τα δεδομένα να καθίστανται πάντα διαθέσιμα, χωρίς καθυστέρηση και να είναι διαθέσιμα για να χρησιμοποιηθούν καταλλήλως για τους επιδιωκόμενους σκοπούς. Ως εκ τούτου, τα δεδομένα θα πρέπει να είναι προσβάσιμα από τα εξουσιοδοτημένα μέρη και να εφαρμόζονται σε αυτά οι προβλεπόμενες διαδικασίες. Η διαθεσιμότητα επίσης περιλαμβάνει την ευχερή ανάκτηση των δεδομένων από τα συστήματα τα οποία είναι αποθηκευμένα. Έτσι, θα πρέπει να χρησιμοποιούνται για την ανάκτηση τους κατάλληλα εργαλεία διαχείρισης, δομημένες βάσεις δεδομένων, κατάλληλες αλγοριθμικές δομές αναζήτησης καθώς και από τεχνικής άποψης τα δεδομένα να είναι πάντα δυνατόν να αναγνωστούν από ανθρώπους. Ο προστατευτικός στόχος της διαθεσιμότητας, όμως, περιλαμβάνει και την περίπτωση της γρήγορης αποκατάστασης των δεδομένων, σε περίπτωση που αυτά τεθούν λόγω κάποιου γεγονότος μη προσβάσιμα. Επιπλέον, για την επίτευξη του συγκεκριμένου προστατευτικού στόχου, πρέπει να ληφθούν μέτρα τα οποία διασφαλίζουν την αντοχή του συστήματος, όπως σε περίπτωση αυξημένου φόρτου εργασίας στο δίκτυο. Έτσι, λοιπόν, ο συγκεκριμένος στόχος προστασίας καλύπτει τις απαιτήσεις που προκύπτουν από το άρθρο 32 ΓΚΠΔ παρ.1 περ' β, όπου αναφέρεται συγκεκριμένα «…ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων, περιλαμβανομένων, μεταξύ άλλων, κατά περίπτωση: …β) της δυνατότητας διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση,» Οι βασικότεροι τρόποι για να επιτευχθεί η διαθεσιμότητα των δεδομένων είναι μέσω της δημιουργίας αντιγράφων ασφαλείας, της δημιουργίας καθορισμένων σταδίων επεξεργασίας, μέσω καταλλήλων διαμορφώσεων, καταγραφή ιστορικού συναλλαγών.

[81]Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact ssessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag. Σελ. 55 επ.

Επιπλέον, επιτυγχάνεται μέσω προστασίας από εξωτερικές επιρροές (malware, sabotage, force majeure), με την ύπαρξη εφεδρικού εξοπλισμού (hardware, software και υποδομής), με την υιοθέτηση πολιτικών αποφυγής και επισκευής βλαβών και τέλος με τον καθορισμό πολιτικής διαχείρισης εκτάκτου ανάγκης σε περίπτωση που τα δεδομένα καταστούν μη προσβάσιμα.

7.2.3. 3ος Στόχος. Ακεραιότητα (Integrity)

Τρίτο στόχο προστασίας αποτελεί η ακεραιότητα των δεδομένων. Η ακεραιότητα των δεδομένων χωρίζεται κατ' αρχάς σε δύο χαρακτηριστικά τα οποία θα πρέπει να συντρέχουν σωρευτικά για να θεωρηθεί ότι ο στόχος έχει επιτευχθεί. Το πρώτο εξ΄ αυτών αναφέρεται, αφενός, στην απαίτηση ότι οι διαδικασίες και τα συστήματα τεχνολογίας πληροφοριών συμμορφώνονται συνεχώς με τις προδιαγραφές που καθορίστηκαν για να εκτελούν τις προβλεπόμενες λειτουργίες τους. Το δεύτερο σχετίζεται με τα ίδια τα δεδομένα που τίθενται υπό επεξεργασία και ειδικότερα απαιτεί αυτά να παραμένουν ακέραια, πλήρη, ορθά και ενημερωμένα. Αποκλίσεις από αυτά τα χαρακτηριστικά πρέπει να αποκλείονται ή τουλάχιστον να είναι εύκολα ανιχνεύσιμες, ώστε να μπορούν να ληφθούν υπόψη και να διορθωθούν όσο το δυνατόν νωρίτερα. Ο συγκεκριμένος στόχος είναι επίσης σημαντικός στις επεξεργασίες που σχετίζονται με την κατάρτιση προφίλ και της αυτοματοποιημένης λήψεως αποφάσεων. Είναι σημαντικό οποιαδήποτε επεξεργασία μπορεί να δημιουργήσει διακρίσεις για αποφάσεις που θα έχουν έννομες συνέπειες πάνω στα υποκείμενα να εντοπιστούν νωρίς, ώστε με τα τεχνικά και οργανωτικά μέτρα που θα ληφθούν αργότερα, να μετριασθεί ο κίνδυνος τέλεσης αυτού του γεγονότος. Οι βασικότεροι τρόποι να επιτευχθεί ο στόχος της ακεραιότητας είναι οι εξής: Μέσω του περιορισμού της δυνατότητας των χρηστών για συγγραφή και τροποποίηση, μέσω της χρήσης checksums[82], ηλεκτρονικών σφραγίδων και υπογραφών σε συνδυασμό με σύστημα κρυπτογράφησης. Επιπλέο, μέσω της σαφούς καταγραφής των εξουσιοδοτημένων προσώπων και τον ρόλων, μέσω της διαγραφής ή της τροποποίησης των εσφαλμένων δεδομένων, μέσω της κατάλληλης τροποποίησης των συστημάτων, ώστε, να έχουν όσο το δυνατόν γίνεται λιγότερες δευτερεύουσες λειτουργίες, μέσω διαδικασιών για την διατήρηση χρονοδιαγράμματος των δεδομένων, μέσω διαδικασιών για την ταυτοποίηση και πιστοποίηση προσώπων και εξοπλισμού. Τέλος, μέσω του καθορισμού της συμπεριφοράς-στόχου των διεργασιών και της τακτικής εκτέλεσης δοκιμών για τον προσδιορισμό και την τεκμηρίωση της λειτουργικότητας, των κινδύνων, των κενών ασφαλείας και των παρενεργειών των διεργασιών,

[82] Checksum: είναι ένα άθροισμα που προκύπτει από τα bits ενός τμήματος δεδομένων υπολογιστή το οποίο υπολογίζεται πριν και μετά τη μετάδοση ή την αποθήκευση για να διασφαλιστεί ότι τα δεδομένα είναι απαλλαγμένα από σφάλματα ή παραποιήσεις.

καθώς και μέσω του καθορισμού της συμπεριφοράς-στόχου των διεργασιών και των διαδικασιών και τακτική εκτέλεση δοκιμών για την εξακρίβωση ή τον προσδιορισμό των πραγματικών καταστάσεων των διεργασιών.

7.2.4. 4ος Στόχος. Εμπιστευτικότητα (Confidentiality)

Τέταρτο στόχο αποτελεί η Εμπιστευτικότητα των δεδομένων. Η εμπιστευτικότητα αναφέρεται στην απαίτηση του να μην επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα. Τα μη εξουσιοδοτημένα πρόσωπα είναι όχι μόνο τρίτα μέρη εκτός του υπεύθυνου φορέα, αλλά και υπάλληλοι των τεχνικών παρόχων υπηρεσίες οι οποίοι δεν χρειάζονται πρόσβαση σε δεδομένα προσωπικού χαρακτήρα προκειμένου να παρέχουν τις υπηρεσιών, ή πρόσωπα σε οργανωτικές μονάδες που δεν έχουν καμία σχέση με το περιεχόμενο μιας δραστηριότητας επεξεργασίας ή με το υποκείμενο των δεδομένων. Η εμπιστευτικότητα των δεδομένων προσωπικού χαρακτήρα πρέπει επίσης να διασφαλίζεται όταν τα εν λόγω συστήματα και οι υπηρεσίες υπόκεινται σε απροσδόκητα υψηλά φορτία (ανθεκτικότητα). Σε περίπτωση που η εμπιστευτικότητα παραβιάζεται σε εξαιρετικές περιπτώσεις, πρέπει να διασφαλίζεται ότι λαμβάνονται μέτρα για την αποκατάστασή της και μετριασμού της συνοδευτικής παραβίασης της προστασίας των δεδομένων προσωπικού χαρακτήρα (Αποκατάσταση και μετριασμός των παραβιάσεων της προστασίας δεδομένων). Για την επίτευξη του ως άνω στόχου θα πρέπει να καθοριστούν ποια πρόσωπα θεωρούνται εξουσιοδοτημένα και να αποδοθούν ρόλοι στο κάθε ένα από αυτά, λαμβάνοντας υπόψη και την αρχή της αναγκαιότητας. Για να επιτευχθεί αυτό πρέπει προηγουμένως να έχει τεθεί σε λειτουργία ένα σύστημα ασφαλούς πιστοποίησης χρηστών. Έτσι, θα πρέπει να γίνει ένας σχεδιασμός ανάλογα με τα πρόσωπα που θα θεωρούνται εξουσιοδοτημένα με κριτήρια είτε γεωγραφικά είτε επαγγελματικά. Τέλος, θα πρέπει να διασφαλίζονται με το κατάλληλο επίπεδο προστασίας όλες οι υποδομές, οι διαδικασίες και οι πολιτικές του φορέα σε συνδυασμό και με ισχυρά πρωτόκολλα κρυπτογράφησης.

7.2.5. 5ος Στόχος. Η μη διασύνδεση των δεδομένων των υποκειμένων (Unlikability)

Η μη συνδεσιμότητα αναφέρεται στην απαίτηση τα δεδομένα προσωπικού χαρακτήρα να μην συνδυάζονται μεταξύ τους (να μην συνδέονται), ειδικά στην περίπτωση που έχουν συλλεχθεί για διαφορετικούς σκοπούς. Όσο μεγαλύτερη και πιο περιεκτική είναι μία βάση δεδομένων, τόσο μεγαλύτερη μπορεί να είναι η πιθανότητα συνδυασμού των δεδομένων και η χρήση αυτών πέραν του αρχικού σκοπού και καταστρατηγώντας την αρχική νομική βάση. Η

εν λόγω, περαιτέρω, επεξεργασία είναι νομικά επιτρεπτή μόνο υπό αυστηρά καθορισμένες συνθήκες. Η μη συνδεσιμότητα πρέπει να διασφαλίζεται με τα κατάλληλα τεχνικά και οργανωτικά μέτρα. Εκτός από τα μέτρα για την ψευδονυμοποίηση και άλλα μέτρα μπορούν να χρησιμοποιηθούν που επιτρέπουν την περαιτέρω επεξεργασία, χωριστά, από την αρχική επεξεργασία, τόσο από την πλευρά του οργανισμού όσο και από την πλευρά του συστήματος. Οι βάσεις δεδομένων μπορούν να προσαρμοστούν, για παράδειγμα, με συστήματα εξουσιοδότησης και να μειωθεί το περιεχόμενο τους στο βαθμό που είναι απαραίτητο για την επίτευξη του νέου σκοπού.

7.2.6. 6ος Στόχος. Διαφάνεια (Transparency)

Ο προστατευτικός στόχος της διαφάνειας αναφέρεται στην απαίτηση ότι τόσο τα υποκείμενα των δεδομένων, όσο και οι διαχειριστές των συστημάτων καθώς και οι αρμόδιοι εποπτικοί φορείς πρέπει να είναι σε θέση να προσδιορίζουν ποια δεδομένα συλλέγονται και υποβάλλονται σε επεξεργασία, πότε, για ποιο σκοπό και με ποιες διαδικασίες και συστήματα. Επιπλέον, για να θεωρηθεί ότι έχει επιτευχθεί ο συγκεκριμένος στόχος θα πρέπει να καθορίζεται σε κάθε στάδιο της επεξεργασίας ποιος έχει την ευθύνη της και μέχρι ποια έκταση. Ακόμη, η διαφάνεια είναι απαραίτητη για την παρακολούθηση και τον έλεγχο των δεδομένων, των διαδικασιών και των συστημάτων από τη δημιουργία τους έως τη διαγραφή τους και αποτελεί προϋπόθεση για την επεξεργασία δεδομένων σύμφωνα με το νόμο και για την οποία, εφόσον απαιτείται, τα υποκείμενα των δεδομένων μπορούν να δώσουν συγκατάθεση μετά από ενημέρωση. Η διαφάνεια του συνόλου της επεξεργασίας δεδομένων και των εμπλεκόμενων περιπτώσεων μπορεί να συμβάλει ώστε, ιδίως, τα υποκείμενα των δεδομένων και τα εποπτικά όργανα να μπορούν να εντοπίζουν ελλείψεις και, εάν είναι απαραίτητο, να απαιτούν κατάλληλες αλλαγές στην επεξεργασία. Για την επίτευξη του σκοπού αυτού οι βασικότεροι τρόποι είναι μέσω της καταγραφής όλων των σταδίων επεξεργασίας, δημιουργώντας τα αρχεία δραστηριοτήτων επεξεργασίας, σύμφωνα με το άρθρο 30 του ΓΚΠΔ., καταγράφοντας τα παραρτήματα που συμβάλλουν στην επεξεργασία, και ειδικότερα τις εμπορικές διαδικασίες, τις βάσεις δεδομένων, τις ροές δεδομένων, τα σχέδια του δικτύου, τα συστήματα πληροφορικής και γενικότερα τις διαδικασίες επεξεργασίας. Επιπλέον, πρέπει να καταγράφονται η συγκατάθεση των υποκειμένων, τα κριτήρια που χρησιμοποιούνται για την κατάρτιση προφίλ, τα αποτελέσματα από ελέγχους που έχουν γίνει, τα πρωτόκολλα που χρησιμοποιούνται για την επεξεργασία, το πως και ποιες πληροφορίες παρέχονται στα δεδομένα και το πως ικανοποιούνται τα δικαιώματα πληροφόρησης τους. Τέλος, πρέπει να καταγράφονται οι

συμβάσεις που έχουν γίνει με τους εργαζομένους, με εξωτερικούς συνεργάτες αλλά και τρίτους από τους οποίους τα δεδομένα προέρχονται ή κοινολογούνται..

7.2.7. 7ος Στόχος. Δυνατότητα Παρέμβασης (Intervenability)

Ο στόχος προστασίας της δυνατότητας παρέμβασης αναφέρεται στην απαίτηση να ικανοποιούνται τα δικαιώματα των υποκειμένων των δεδομένων. Η ικανοποίηση αυτών των δικαιωμάτων πρέπει να γίνεται άμεσα και αποτελεσματικά, εφόσον συντρέχουν οι νομικές προϋποθέσεις. Ειδικότερα, τα υποκείμενα έχουν τα δικαιώματα ενημέρωσης, πληροφόρησης, διόρθωσης (δυνατότητα διόρθωσης). των δεδομένων), διαγραφής (Διαγραφή δεδομένων), περιορισμού (Περιορισμός της επεξεργασίας δεδομένων), δεδομένων (Φορητότητα δεδομένων), αντίρρησης και εναντίωσης σε αυτοματοποιημένη ατομική λήψη αποφάσεων (Δυνατότητα παρέμβασης σε διαδικασίες αυτοματοποιημένων αποφάσεων). Όταν ο υπεύθυνος επεξεργασίας δεδομένων διαθέτει πληροφορίες που του επιτρέπουν να ταυτοποιήσει τα υποκείμενα των δεδομένων, οφείλει επίσης να λάβει μέτρα για την ταυτοποίηση και την αυθεντικοποίηση των υποκειμένων των δεδομένων που επιθυμούν να ασκήσουν τα δικαιώματά τους. Για την εφαρμογή των δικαιωμάτων των υποκειμένων των δεδομένων και των εποπτικών εντολών και για την αποκατάσταση και τον μετριασμό των παραβιάσεων της προστασίας δεδομένων και οι υπεύθυνοι επεξεργασίας οφείλουν σε κάθε περίπτωση να είναι σε θέση να παρεμβαίνουν στην επεξεργασία δεδομένων, από τη συλλογή έως τη διαγραφή των των δεδομένων. Όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα βασίζεται στη συγκατάθεση των δεδομένων υποκειμένου, πρέπει να λαμβάνονται μέτρα ώστε να διασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία μόνο όταν το υποκείμενο των δεδομένων έχει δώσει συγκατάθεση και σύμφωνα με τις ρυθμίσεις που αυτή προβλέπεται να δοθεί. Για την επίτευξη του συγκεκριμένου στόχους οι βασικότερες

Μέσω των στόχων προστασίας οι νομικοί επιστήμονες και οι επιστήμονες των υπολογιστών βρίσκουν μία «κοινή γλώσσα» σχετικά με το δίκαιο προστασίας προσωπικών δεδομένων και έτσι μπορούν να εγγυηθούν ότι οι νομικές απαιτήσεις του κανονισμού έχουν εφαρμοστεί σε επίπεδο τεχνικό και οργανωτικό. Η βασική αξία αυτή της προσέγγισης των «στόχων προστασίας» είναι ότι μπορούν να «μεταφράσουν» τις (ίσως πιο αφηρημένες) νομικές απαιτήσεις του κανονισμού σε απαιτήσεις (συγκεκριμένες) επιπέδου τεχνικών και οργανωτικών μέτρων. Ωστόσο, για να επιτευχθεί ο τελικός στόχος της ολιστικής προστασίας των δεδομένων, οι στόχοι προστασίας θα πρέπει να διατρέχουν όλο το φάσμα της επεξεργασίας

δηλαδή τις υπηρεσίες, τις διαδικασίες και τα συστήματα με τα οποία διενεργείται η επεξεργασία.

8. Πρώτη φάση της ΕΑΠΔ (Φάση Προετοιμασίας)

8.1 Γενική επισκόπηση της συστηματικής περιγραφής της επεξεργασίας

Η πρώτη φάση της ΕΑΠΔ είναι η συστηματική περιγραφή των πράξεων της επεξεργασίας και της συλλογής των απαραίτητων πληροφοριών που αφορούν την επεξεργασία.(άρθρο 35 παράγραφος 7 στοιχ.α'). Για να μπορέσει να αξιολογηθεί ο κίνδυνος είναι απαραίτητο να γίνεται κατανοητό (από τον ίδιο τον υπεύθυνο επεξεργασίας κατ' αρχάς) για το πως χρησιμοποιούνται τα δεδομένα που συλλέγει. Αν δεν γνωρίζει ο ίδιος ο υπεύθυνος επεξεργασίας, πως χρησιμοποιούνται τα δεδομένα είναι λογικό επακόλουθο να δημιουργούνται ζητήματα ιδιωτικότητας, αφού για παράδειγμα τα δεδομένα μπορεί να συλλέγονται για παράνομους σκοπούς.[83] Ως εκ τούτου, όλες οι μεθοδολογικές προσεγγίσεις έχουν μία φάση/βήμα κατά το οποίο απαιτούν να γίνει η συγκεκριμένη περιγραφή. Αυτή η φάση της ΕΑΠΔ πρέπει να περιλαμβάνει την συστηματική καταγραφή της επεξεργασίας, και αυτή να αποτυπώνεται με απόλυτη ακρίβεια. Για να μπορέσει να επιτευχθεί αυτό, έχουν προταθεί πολλοί τρόποι οι οποίοι είναι αρκετά διαφορετικοί μεταξύ τους. Ειδικότερα, οι μεθοδολογικές προσεγγίσεις που έχουν αναπτυχθεί δεν φαίνεται να ακολουθούν μία κοινή γραμμή. Το κριτήριο, όμως, για να θεωρηθεί επιτυχημένο το συγκεκριμένο στάδιο είναι, πέραν του να αποτυπωθεί ακριβώς ποια δεδομένα συλλέγονται ,να γίνει με τέτοιον τρόπο, ώστε, να καθοριστεί ακριβώς τι πρόκειται να ελεγχθεί στο πλαίσιο εφαρμογής της ΕΑΠΔ, δηλαδή, να καθοριστεί ο ακριβής στόχος της αξιολόγησης και να είναι δυνατό μέσα από αυτή την περιγραφή που θα προκύψει, να προσδιοριστούν με σαφήνεια και κατ' επέκταση, να μπορούν να αξιολογηθούν και να αναλυθούν, σε μετέπειτα επίπεδο, οι κίνδυνοι. Σκοπός, δηλαδή, είναι να καθοριστούν τα όρια του συστήματος μέσα στο οποίο τελείται (ή θα τελεστεί) η επεξεργασία και να εντοπιστούν όλα τα πρόσωπα που θα υποστούν συνέπειες από την εξεταζόμενη επεξεργασία.

[83] Βλ.UK Information Commissioner's Office (ICO) (2014). "Conducting Privacy Impact Assessments: Code of Practice" URL: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of practice.pdf (visited on 2023/09/02)

Ειδικότερα, στην τελική έκθεση της ΕΑΠΔ θα πρέπει να καθορίζονται σαφώς η φύση, η έκταση και το πλαίσιο της επεξεργασίας. Μια εκτίμηση των επιπτώσεων της επεξεργασίας (και των κινδύνων αυτής) μπορεί να είναι τόσο καλή, όσο της επιτρέπει η περιγραφή του πλαισίου και της έκτασης στην οποία διενεργείται.[84]

Εξετάζοντας τη δομή και τις «φάσεις» μίας ΕΑΠΔ, είναι χρήσιμο να αναφερθούν τα κριτήρια που θέτει η ομάδα του άρθρου 29 στο παράρτημα 2, του εγγράφου για τις κατευθυντήριες οδηγίες για τις ΕΑΠΔ, ώστε μία ΕΑΠΔ να είναι αποδεκτή. Ως εκ τούτου το πρώτο και κύριο στάδιο μίας ΕΑΠΔ βάσει αυτού πρέπει να είναι το εξής:

Να παρέχεται μία συστηματική περιγραφή των πράξεων επεξεργασίας._Ως προς αυτό εξειδικεύεται περαιτέρω με τα εξής:

α) λαμβάνονται υπόψη η φύση, η έκταση, το πλαίσιο και οι σκοποί της επεξεργασίας (αιτιολογική σκέψη 90)·

β) καταγράφονται τα δεδομένα προσωπικού χαρακτήρα, οι αποδέκτες και η περίοδος αποθήκευσης των δεδομένων προσωπικού χαρακτήρα·

γ) παρέχεται λειτουργική περιγραφή της πράξης επεξεργασίας·

δ) προσδιορίζονται τα στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα, έντυπα ή δίαυλοι διαβίβασης εντύπων)·

ε) ο λαμβάνεται υπόψη η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας (άρθρο 35 παράγραφος 8)·

Όλες οι μεθοδολογικές προσεγγίσεις έχουν ένα στάδιο κατά το οποίο απαιτούν την καταγραφή της επεξεργασίας, καθώς αυτή η απαίτηση προκύπτει απευθείας από τον νόμο (άρθρο 35 παράγραφος 7 στοιχ.α') Όπως, αναφέρθηκε και προηγουμένως, βέβαια, δεν ακολουθείται μία κοινή γραμμή από όλες, ενώ δεν φαίνεται να υπάρχει καμία που μπορεί να θεωρηθεί ως η μοναδική και απόλυτη λύση. Ξεκινώντας από την εξέταση των μεθοδολογικών προσεγγίσεων κρίνεται σκόπιμο να εξεταστούν αρχικώς οι μεθοδολογίες που αναπτύχθηκαν από τις Εποπτικές Αρχές με την μεγαλύτερη επιρροή. Ως προς την περιγραφή της επεξεργασίας φαίνεται ότι οι Μεθοδολογίες που έχουν προταθεί από τους Information Commmissioner¨s Office (ICO)[85] και Commission nationale de l'informatique et des libertés (CNIL)[86] συγκλίνουν

[84] Βλ. ISO/IEC 29134:2023 - Information technology — Security techniques — Guidelines for privacy impact assessment
[85] Πρόκειται για την Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου, https://ico.org.uk/
[86] Πρόκειται για την Αρχή Προστασίας Δεδομένων της Γαλλίας, https://www.cnil.fr/en

μεταξύ τους αν και δεν ταυτίζονται απόλυτα. Ειδικότερα, και οι δύο προτείνουν σε αυτό το σημείο ότι θα πρέπει να συλλεχθούν και να αποτυπωθούν οι πληροφορίες με παρόμοιο τρόπο, παρόλο που δεν ταυτίζονται απόλυτα. Ειδικότερα, ο ICO προτείνει να αποτυπωθούν κατ΄ αρχάς η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας. Για να το επιτύχει αυτό ο ICO, εξειδικεύει περισσότερο κάθε ζητούμενο καλώντας τον υπεύθυνο επεξεργασίας να απαντήσει σε συγκεκριμένες ερωτήσεις για να εντοπίσει το περιεχόμενο του κάθε ενός από αυτά . Προς αυτή την κατεύθυνση φαίνεται να συμφωνεί και η πρακτική που εφαρμόζεται στην Ολλανδία. Όπως προκύπτει από σχετική έρευνα[87] που διεξήχθη για το πως διενεργούνται οι Εκτιμήσεις Αντικτύπου στην Ολλανδία, φαίνεται πως και εκεί οι περισσότεροι φορείς που διενεργούν εκτιμήσεις αντικτύπου χρησιμοποιούν κάποιου είδους ερωτηματολόγιο για κάθε φάση της ΕΑΠΔ.

8.1.1. Η προσέγγιση του ICO.

Η μεθοδολογία που έχει αναπτύξει ο ICO προτείνει κατ' αρχάς την αποτύπωση της φύσης της επεξεργασίας[88]. Ως φύση της επεξεργασίας νοείται ως το τι σχεδιάζει να κάνει ο υπεύθυνος επεξεργασίας με τα δεδομένα. Για να το επιτύχει αυτό, ο ICO καλεί τον υπεύθυνο επεξεργασίας να απαντήσει σε συγκεκριμένες ερωτήσεις. Στην ιστοσελίδα του ICO υπάρχει παράδειγμα που έχει εφαρμοστεί η μεθοδολογία αυτή και αφορούσε ηλεκτρονικό κατάστημα εμπορίας παιδικών παιχνιδιών[89]

8.1.1.1. Περιγραφή της Φύσης της επεξεργασίας

Ειδικότερα, για την αποτύπωση της φύσης της επεξεργασίας ο ICO ζητά να απαντηθούν μία σειρά ερωτήσεων με την πρώτη από αυτές να αποτελεί το πώς συλλέγονται τα δεδομένα· Στο παράδειγμα του ο ICO εξηγεί ότι τα δεδομένα μπορεί να συλλέγονται με τρείς τρόπους. Ο πρώτος είναι από άμεσες αλληλεπιδράσεις με τους χρήστες, όπως π.χ. όταν οι χρήστες δημιουργούν έναν λογαριασμό, αγοράζουν ένα προϊόν είτε ως κάτοχος λογαριασμού είτε ως επισκέπτης, όταν εγγράφονται για να λαμβάνουν ενημερωτικά δελτία ή όταν επικοινωνούν για μια ερώτηση ή ένα θέμα. Ο δεύτερος τρόπος είναι με την χρήση αυτοματοποιημένων τεχνολογιών δηλαδή cookies ή παρόμοιες τεχνολογίες όταν οι επισκέπτες χρησιμοποιούν τον

[87] Βλ. Puijenbroek, J. van, & Hoepman, J.-H. (2017). Privacy Impact Assessments in Practice: Outcome of a Descriptive Field Research in the Netherlands. IWPE@SP
[88] Βλ. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/dpia-tools/online-retail/step-2-describe-the-processing/ (visited 9-11-2023)
[89] Βλ. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/dpia-tools/online-retail/step-2-describe-the-processing/

ιστότοπο, ενώ ο τρίτος τρόπος είναι από τρίτους δηλ. από τον τρίτο πάροχο cookies ανάλυσης και από τους τρίτους παρόχους υπηρεσιών πρόληψης απάτης.

Η δεύτερη ερώτηση αφορά το πως χρησιμοποιούνται τα δεδομένα. Ο ICO στο παράδειγμα του αναφέρει ότι η κύρια χρήση των προσωπικών δεδομένων είναι η επεξεργασία και η εκτέλεση των παραγγελιών που γίνονται στον ιστότοπο και η αντιμετώπιση των ερωτημάτων των πελατών. Επιπλέον, αναφέρει ότι διεξάγεται περιορισμένη δραστηριότητα μάρκετινγκ μέσω ενημερωτικού δελτίου ηλεκτρονικού ταχυδρομείου, στο οποίο μπορούν να εγγραφούν χρήστες άνω των 13 ετών. Όλα τα ενημερωτικά δελτία ηλεκτρονικού ταχυδρομείου διαθέτουν σύνδεσμο διαγραφής και όλες οι αποχωρήσεις λαμβάνονται υπόψη και γίνονται σεβαστές. Δεν πραγματοποιείται καμία συμπεριφορική διαφήμιση. Ως εκ τούτου, αναφέρει συνοπτικώς ότι χρησιμοποιεί τα προσωπικά δεδομένα για τους εξής σκοπούς: Για την εγγραφή χρηστών που επιλέγουν να δημιουργήσουν λογαριασμό. Για την οικονομική διαχείριση, την τιμολόγηση και την επεξεργασία και παράδοση παραγγελιών. Για τη διαχείριση της σχέσης με τους πελάτες (π.χ. απάντηση σε ερωτήσεις, παράπονα, αίτημα προς τους χρήστες να συμμετάσχουν σε μια έρευνα). Για να μπορέσουν οι χρήστες να συμμετάσχουν σε διαγωνισμούς, κληρώσεις βραβείων κ.λπ. Για τη διαχείριση και προστασία της επιχείρησής και του ιστοτόπου (π.χ. συντήρηση και υποστήριξη του συστήματος, επίλυση προβλημάτων, φιλοξενία δεδομένων). Για την παροχή περιεχομένου ιστοτόπου και διαφημίσεων με βάση το πλαίσιο και τη μέτρηση και κατανόηση της αποτελεσματικότητας αυτών. Για τη διενέργεια αναλύσεων δεδομένων για τη βελτίωση του ιστότοπου, των προϊόντων, του μάρκετινγκ και της εμπειρίας των πελατών στον ιστότοπο. Για να προτείνονται προϊόντα που μπορεί να ενδιαφέρουν τους χρήστες μέσω ηλεκτρονικού ταχυδρομείου και πλαισιωμένης διαφήμισης. Για την παροχή ενημερωτικών δελτίων ηλεκτρονικού ταχυδρομείου στους χρήστες που έχουν εγγραφεί σε αυτή την υπηρεσία. Για τον εντοπισμό και την πρόληψη δόλιων συναλλαγών. Για την επαλήθευση της ταυτότητας του χρήστη και την παροχή ασφαλούς πλατφόρμας. Για τη συμμόρφωση με κανονιστικές ή νομικές υποχρεώσεις, και τέλος για να μπορούν οι χρήστες να μοιράζονται λεπτομέρειες των αγορών τους σε ιστότοπους κοινωνικής δικτύωσης.

Επιπλέον, στην ίδια ερώτηση αναλύει τη χρήση των cookies. Ειδικότερα, αναφέρει ότι ο ιστότοπος χρησιμοποιεί cookies για μια σειρά λειτουργιών. Χρησιμοποιεί βασικά cookies, τα οποία δεν υπόκεινται στην απαίτηση συγκατάθεσης, για τους ακόλουθους σκοπούς: Για την Πιστοποίηση λογαριασμού, την παρακολούθηση της εισόδου του χρήστη για λειτουργίες της υπηρεσίας (π.χ. καλάθι αγορών) και την ασφάλεια και πρόληψη της απάτης. Γενικότερα,

αναφέρεται ότι τα cookies που θεωρούνται απαραίτητα για την λειτουργία ενός ιστοτόπου (Essential Cookies) δεν απαιτούν την συγκατάθεση του χρήστη.

Η τρίτη ερώτηση αφορά τον τρόπο και την περίοδο αποθήκευσης των δεδομένων. Στο παράδειγμα του ο ICO αναφέρει ότι ο ιστότοπος φιλοξενείται στο Ηνωμένο Βασίλειο και όλα τα δεδομένα αποθηκεύονται στο Ηνωμένο Βασίλειο. Ενώ, για τις περιόδους τήρησης των δεδομένων αναφέρει ότι η επιχείρηση διαθέτει μία πολιτική διατήρησης των δεδομένων, η οποία καθορίζει περιόδους αποθήκευσης για κατηγορίες δεδομένων που αντικατοπτρίζουν τις σχετικές νομικές απαιτήσεις και τις περιόδους παραγραφής που ισχύουν για συμβατικές αξιώσεις. Μόλις λήξουν οι περίοδοι διατήρησης, διαγράφονται με ασφάλεια τα δεδομένα και τηρείται αρχείο καταγραφής των διαγραφών.

Η τέταρτη ερώτηση αφορά την κοινολόγηση των δεδομένων και κυρίως με ποιον διαμοιράζονται τα δεδομένα, ποιος έχει πρόσβαση σε αυτά και αν χρησιμοποιούνται εκτελούντες την επεξεργασία. Στο παράδειγμα του ο ICO τα ανωτέρω ερωτήματα απαντούνται ως εξής. Τα δεδομένα κοινοποιούνται για την επεξεργασία δεδομένων ρουτίνας[90] που είναι απαραίτητη για την ασφαλή παροχή της υπηρεσίας. Ένας τρίτος πάροχος υπηρεσιών πληρωμών χρησιμοποιείται για την παροχή της λειτουργίας πληρωμών στον ιστότοπο. Αυτός ο πάροχος υπηρεσιών πληρωμών ενεργεί ως ανεξάρτητος υπεύθυνος επεξεργασίας δεδομένων. Οι πληρωμές γίνονται εξ' ολοκλήρου στον ιστότοπο του παρόχου υπηρεσιών πληρωμής και ως εκ τούτου, στο κατάστημα πώλησης παιδικών παιχνιδιών, δεν αποθηκεύονται δεδομένα που αφορούν τραπεζικά στοιχεία. Στην πολιτική απορρήτου της επιχείρησης διευκρινίζεται ότι ο πάροχος υπηρεσιών πληρωμών λειτουργεί βάσει της δικής του πολιτικής απορρήτου και παραπέμπει τους χρήστες να ανατρέξουν σε αυτήν για λεπτομέρειες σχετικά με την επεξεργασία του. Επιπλέον, γίνεται χρήση ενός τρίτου παρόχου υπηρεσιών ανάλυσης για τη μέτρηση των αλληλεπιδράσεων των χρηστών με τον ιστότοπο. Αυτό γίνεται για να μπορέσει να ελεγχθεί η ποιότητα και η αποτελεσματικότητα της υπηρεσίας και να διασφαλιστεί ότι ανταποκρίνεται στις ανάγκες του χρήστη. Ο πάροχος αναλυτικών υπηρεσιών χρησιμοποιεί cookies και παρόμοιες τεχνολογίες για τη συλλογή πληροφοριών σχετικά με τις αλληλεπιδράσεις των χρηστών όταν επισκέπτονται τον ιστότοπο. Αυτό περιλαμβάνει δεδομένα σχετικά με τη συσκευή ή το πρόγραμμα περιήγησης του χρήστη, τις δραστηριότητές του στον ιστότοπο και ένα μέρος της διεύθυνσης IP του χρήστη. Ο πάροχος επεξεργάζεται αυτές τις πληροφορίες για λογαριασμό του υπευθύνου επεξεργασίας και τις χρησιμοποιεί για να

[90] Τα δεδομένα ρουτίνας αναφέρονται σε δεδομένα που συλλέγονται τακτικά και χρησιμοποιούνται για την παρακολούθηση και την αξιολόγηση των επιδόσεων των συστημάτων, προγραμμάτων και υπηρεσιών.

ετοιμάσει εκθέσεις για τον ιστότοπο σχετικά με τον τρόπο με τον οποίο οι επισκέπτες αλληλοεπιδρούν με τον ιστότοπο. Αυτές οι αναφορές δεν ταυτοποιούν τους χρήστες - πρόκειται για συγκεντρωτικές πληροφορίες σχετικά με όλους τους χρήστες. Ο πάροχος αναλυτικών υπηρεσιών δεν χρησιμοποιεί καμία από αυτές τις πληροφορίες για δικούς του σκοπούς - ενεργεί ως εκτελών την επεξεργασία και λειτουργεί μόνο κατόπιν οδηγιών. Η επεξεργασία αυτή πραγματοποιείται στην ΕΕ. Επιπλέον, χρησιμοποιείται μια πλατφόρμα ηλεκτρονικού εμπορίου. Ο πάροχος ενεργεί ως εκτελών την επεξεργασία και έχει συνάψει μαζί του όρους του άρθρου 28 παράγραφος 3. Γίνεται χρήση της υπηρεσίας πρόληψης απάτης της πλατφόρμας ηλεκτρονικού εμπορίου, η οποία παρέχει βαθμολογίες κινδύνου για να βοηθήσει στην αποφυγή δόλιων συναλλαγών. Η υπηρεσία αυτή παρέχεται από τρίτο μέρος το οποίο ενεργεί ως ανεξάρτητος υπεύθυνος επεξεργασίας. Για τη χρήση αυτής της υπηρεσίας, ορισμένα προσωπικά δεδομένα διαβιβάζονται στον πάροχο (δηλαδή όνομα, αριθμός τηλεφώνου, διευθύνσεις χρέωσης και παράδοσης, διεύθυνση ηλεκτρονικού ταχυδρομείου, διεύθυνση IP). Αυτή η επεξεργασία εξηγείται στην δήλωση απορρήτου του υπευθύνου με σύνδεσμο προς τη δική του πολιτική απορρήτου του παρόχου. Η πολιτική του υπευθύνου για τα cookies παρέχει περισσότερες πληροφορίες σχετικά με τη χρήση των cookies για σκοπούς ανάλυσης. Οι χρήστες μπορούν να επιλέξουν τη χρήση του ελέγχου των cookies και μπορούν να αλλάξουν γνώμη ανά πάσα στιγμή. Χρησιμοποιείται ένα Captcha που παρέχεται από τρίτο μέρος, το οποίο συνεπάγεται τη μεταφορά δεδομένων σχετικά με τη συσκευή ενός χρήστη προς/από τον τρίτο πάροχο. Ο πάροχος ενεργεί ως εκτελών την επεξεργασία και έχει συνάψει μαζί του όρους του άρθρου 28 παράγραφος 3. Μοιράζονται περιορισμένα δεδομένα με ταχυμεταφορείς για να μπορέσουν να παραδοθούν τα προϊόντα τους στους πελάτες. Όλες οι συσκευασίες και η επισήμανση των προϊόντων γίνονται από την εταιρεία. Ο ρόλος της εταιρείας ταχυμεταφορών είναι μόνο η παράδοση των δεμάτων και δεν ασκεί κανέναν έλεγχο σχετικά με τον σκοπό για τον οποίο χρησιμοποιούνται τα προσωπικά δεδομένα των δεμάτων, που του έχουν ανατεθεί ούτε διαθέτει έλεγχο επί των προσωπικών δεδομένων που του έχουν ανατεθεί. Ως εκ τούτου, η εταιρεία ταχυμεταφορών δεν λειτουργεί ως εκτελών την επεξεργασία.

Επιπλέον εξετάζεται το αν διενεργείται κατάρτιση προφίλ. Ειδικότερα, σύμφωνα με το άρθρο 4 του ΓΚΠΔ ως κατάρτιση προφίλ εννοείται ως « οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που συνίσταται στη χρήση δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων προσωπικών πτυχών ενός φυσικού προσώπου, ιδίως για την ανάλυση ή την πρόβλεψη πτυχών που αφορούν την απόδοση στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις, τα

ενδιαφέροντα, την αξιοπιστία, τη συμπεριφορά, τη θέση ή τις μετακινήσεις του εν λόγω φυσικού προσώπου» . Στο παράδειγμα του ο ICO αναφέρει ότι: Η κατάρτιση προφίλ είναι απενεργοποιημένη από προεπιλογή για όλους τους χρήστες. Για τους χρήστες που συναινούν να λαμβάνουν τα ενημερωτικά δελτία, πραγματοποιούνται περιορισμένες δραστηριότητες κατάρτισης προφίλ για να αποστέλλονται με ηλεκτρονικό ταχυδρομείο συστάσεις παρόμοιων προϊόντων στους χρήστες με βάση το ιστορικό των παραγγελιών τους και τις δραστηριότητες περιήγησής τους. Πραγματοποιείται κατάρτιση προφίλ μόνο για χρήστες που έχουν συναινέσει στα σχετικά cookies. Αυτά τα μηνύματα ηλεκτρονικού ταχυδρομείου αποστέλλονται μόνο σε χρήστες που έχουν επιλέξει να συμμετέχουν στην αντίστοιχη υπηρεσία μάρκετινγκ. Στα παιδιά κάτω των 13 ετών δεν δίνεται η δυνατότητα να επιλέξουν την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου μάρκετινγκ, οπότε η κατάρτιση προφίλ παραμένει απενεργοποιημένη για τους χρήστες κάτω των 13 ετών. Τέλος επισημαίνεται ότι καμία εξωτερική διαφήμιση δεν προσφέρεται στους χρήστες της υπηρεσίας.

Τέλος, για την καταγραφή της φύσης της επεξεργασίας ο ICO καλεί τον υπεύθυνο επεξεργασίας να καταγράψει τα μέτρα ασφαλείας που έχει λάβει. Στο σχετικό παράδειγμα του, αναφέρει για αυτά τα εξής: Για την ασφάλεια του ιστοτόπου χρησιμοποιούνται τα εξής μέτρα: Διατηρείται η συνδρομή του λογισμικού ηλεκτρονικού εμπορίου ενημερωμένη. Απαιτείται από τους χρήστες, που δημιουργούν λογαριασμό, να χρησιμοποιούν έναν ισχυρό κωδικό πρόσβασης με αριθμούς, κεφαλαία γράμματα και άλλους χαρακτήρες, ο οποίος πρέπει να έχει μήκος τουλάχιστον 10 χαρακτήρων. Χρησιμοποιείται προστασία SSL στις σελίδες σύνδεσής. Χρησιμοποιείται μια λειτουργία Captcha[91] στη σελίδα "επικοινωνία". Χρησιμοποιείται μια κορυφαία στην αγορά, αξιόπιστη εταιρεία φιλοξενίας ιστοσελίδων. Γίνεται χρήση μιας πολιτική τακτικής διαγραφής οποιωνδήποτε αρχείων, βάσεων δεδομένων ή εφαρμογών από τον ιστότοπο που δεν χρησιμοποιούνται πλέον. Για όλα τα δεδομένα δημιουργούνται τακτικά αντίγραφα ασφαλείας. Εκτελούνται τακτικές σαρώσεις ασφαλείας ιστού για να ελέγχονται τρωτά σημεία του ιστότοπου και του διακομιστή. Χρησιμοποιείται μια υπηρεσία πρόληψης απάτης για τις αγορές που πραγματοποιούνται στον ιστότοπο.

8.1.1.2. Περιγραφή του πεδίου εφαρμογής της επεξεργασίας

Το πεδίο εφαρμογής της επεξεργασίας πρόκειται για την περιγραφή του τι καλύπτει η επεξεργασία. Οι ερωτήσεις που τίθενται προς απάντηση από τον ICO είναι οι εξής: Ποια είναι

[91]Ενα CAPTCHA (/κάπ-τσα/ ένα αρκτικόλεξο των λέξεων "Completely Automated Public Turing test to tell Computers and Humans Apart") είναι ένας τύπος πρόκλησης-απόκρισης ελέγχου που χρησιμοποιήθηκε για τον υπολογισμό για να καθορίσει αν ο χρήστης είναι άνθρωπος ή όχ

η φύση των δεδομένων προσωπικού χαρακτήρα, Ποιος είναι ο όγκος και η ποικιλία των δεδομένων προσωπικού χαρακτήρα, ποια είναι ευαισθησία των δεδομένων προσωπικού χαρακτήρα, ποια είναι έκταση και τη συχνότητα της επεξεργασίας, ποια θα είναι η διάρκεια της επεξεργασίας, ποιος είναι ο αριθμός των εμπλεκόμενων υποκειμένων των δεδομένων και ποια η γεωγραφική περιοχή που καλύπτεται.

Παρά την ασαφή διατύπωση, κατά τη γνώμη του γράφοντος ,της μεθοδολογίας του ICO σε αυτό το σημείο πρέπει να καταγραφούν και τα ίδια τα δεδομένα ανά κατηγορία. Σε σχετικό παράδειγμα που έχει αναρτηθεί στην ιστοσελίδα του[92] που αφορά εκτίμηση αντικτύπου για την λειτουργία καταστήματος που εμπορεύεται παιδικά παιχνίδια, σε αυτό το σημείο ο ICO καταγράφει τα δεδομένα σε συγκεκριμένες κατηγορίες: Ειδικότερα, τα καταγράφει ως εξής: Σε Δεδομένα ταυτότητας: όνομα, όνομα χρήστη, τίτλος, ημερομηνία γέννησης. Σε δεδομένα επικοινωνίας: διεύθυνση χρέωσης και παράδοσης, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμός τηλεφώνου. Σε οικονομικά δεδομένα: στοιχεία κάρτας πληρωμής (τα οποία επεξεργάζεται τρίτος πάροχος υπηρεσιών πληρωμών και δεν αποθηκεύονται από εμάς/τον ιστότοπό μας). Σε δεδομένα συναλλαγής: λεπτομέρειες των προϊόντων που αγοράστηκαν, ποσά, ημερομηνίες κ.λπ. Σε τεχνικά δεδομένα: Διεύθυνση IP, δεδομένα σύνδεσης, τύπος και έκδοση προγράμματος περιήγησης, ρύθμιση ζώνης ώρας και τοποθεσία, τύποι και εκδόσεις πρόσθετων προγραμμάτων περιήγησης, λειτουργικό σύστημα και πλατφόρμα. Σε δεδομένα προφίλ: όνομα χρήστη και κωδικός πρόσβασης, αγορές ή παραγγελίες που πραγματοποιούνται από τους χρήστες, καθώς και οι προτιμήσεις, τα ενδιαφέροντα, τα σχόλια και οι ερωτήσεις τους, όπως συλλέγονται μέσω απαντήσεων σε έρευνες. Σε δεδομένα χρήσης: πληροφορίες σχετικά με τον τρόπο με τον οποίο οι χρήστες χρησιμοποιούν τον ιστότοπο, τα προϊόντα και τις υπηρεσίες μας και τέλος σε δεδομένα μάρκετινγκ και επικοινωνίας: καταγραφή των προτιμήσεων των χρηστών για τη λήψη μάρκετινγκ.

Επιπλέον, αναφέρει ότι δεν υφίστανται επεξεργασία δεδομένα ειδικών κατηγοριών ενώ όσον αφορά τον όγκο των δεδομένων αναφέρει ότι αναμένεται ότι ο ιστότοπος θα έχει περίπου 100.000 χρήστες, εκ των οποίων το 45% θα είναι παιδιά (κάτω των 18 ετών) και το 55% ενήλικες που θα χρησιμοποιούν αυτή την υπηρεσία. Τέλος, για την γεωγραφική περιοχή που θα καλύπτει η επεξεργασίας αναφέρεται ότι τα υποκείμενα των δεδομένων των οποίων τα δεδομένα επεξεργάζονται βρίσκονται στο Ηνωμένο Βασίλειο. Ο ιστότοπος και όλα τα προσωπικά δεδομένα φιλοξενούνται στο Ηνωμένο Βασίλειο. Ο ιστότοπος δεν χρησιμοποιεί

[92] Step 2: Describe the processing | ICO (visited 11/11/2023)

υπηρεσίες τοποθεσίας, όπως ο γεωγραφικός εντοπισμός της διεύθυνσης IP, για την αλλαγή του νομίσματος του καλαθιού αγορών. Η γλώσσα του ιστότοπου είναι τα αγγλικά του Ηνωμένου Βασιλείου και δεν υπάρχουν επιλογές αλλαγής γλώσσας για επισκέπτες εκτός Ηνωμένου Βασιλείου.

8.1.1.3. Περιγραφή του πλαισίου της επεξεργασίας

Το πλαίσιο της επεξεργασίας αναφέρεται στην ευρύτερη εικόνα, συμπεριλαμβανομένων των εσωτερικών και εξωτερικών παραγόντων που θα μπορούσαν να επηρεάσουν τις προσδοκίες ή τον αντίκτυπο. Ο ICO καλεί τον διενεργούντα την εκτίμηση να καταγράψει τις πηγές των δεδομένων, τη φύση της σχέσης με τα άτομα, τον βαθμό που τα άτομα έχουν τον έλεγχο των δεδομένων τους, τον βαθμό που τα άτομα είναι πιθανό να αναμένουν την επεξεργασία, το εάν στα άτομα αυτά περιλαμβάνονται παιδιά ή άλλα ευάλωτα άτομα, το αν υπάρχει τυχόν προηγούμενη εμπειρία από αυτό το είδος επεξεργασίας, τυχόν σχετικές εξελίξεις στην τεχνολογία ή την ασφάλεια, τυχόν τρέχοντα ζητήματα που προκαλούν δημόσιο ενδιαφέρον.

Στο παράδειγμα του ο ICO αρχικά παραθέτει κι άλλα ερωτήματα που θα πρέπει να λάβει υπόψη του ο υπεύθυνος επεξεργασίας. Ειδικότερα, στα ερωτήματα αυτά συγκαταλέγονται το ποια είναι η φύση της υπηρεσίας σας; Το αν αυτή σχεδιάζεται για παιδιά; Εάν όχι, είναι πιθανό να έχουν πρόσβαση σε αυτήν παιδιά κάτω των 18 ετών; Ποιο είναι το πιθανό ηλικιακό εύρος των χρηστών σας; Πόσο έλεγχο θα έχουν; Θα καταλάβαιναν και θα περίμεναν να χρησιμοποιήσετε τα δεδομένα τους με αυτόν τον τρόπο; Χρησιμοποιεί η υπηρεσία σας τεχνικές ώθησης; Υπάρχουν προηγούμενες ανησυχίες σχετικά με παρόμοιες υπηρεσίες ή συγκεκριμένα κενά ασφαλείας; Είναι η υπηρεσία σας καινοφανής με οποιονδήποτε τρόπο; Ποια είναι η τρέχουσα κατάσταση της τεχνολογίας σε αυτόν τον τομέα; Υπάρχουν τρέχοντα ζητήματα δημόσιας ανησυχίας που θα πρέπει να λάβετε υπόψη σας, ιδίως όσον αφορά τους διαδικτυακούς κινδύνους για τα παιδιά; Υπάρχουν σχετικά βιομηχανικά πρότυπα, κώδικες πρακτικής ή δημόσιες οδηγίες στον τομέα αυτό; Ποιες ευθύνες έχετε βάσει της ισχύουσας νομοθεσίας περί ισότητας για την Αγγλία, τη Σκωτία, την Ουαλία και τη Βόρεια Ιρλανδία; Υπάρχει σχετική καθοδήγηση ή έρευνα σχετικά με τις αναπτυξιακές ανάγκες, την ευημερία ή την ικανότητα των παιδιών στην αντίστοιχη ηλικιακή ομάδα; Έχετε προσχωρήσει σε οποιονδήποτε εγκεκριμένο κώδικα δεοντολογίας ή σύστημα πιστοποίησης (εφόσον έχουν εγκριθεί);

Ο ICO απαντάει ότι το «The Toy Shop» είναι ένας νέος διαδικτυακός ιστότοπος που πωλεί προϊόντα για παιδιά έξι ετών και άνω, υποστηρίζοντας τα δικαιώματα των παιδιών στο παιχνίδι και την ανάπτυξη. Η ιστοσελίδα είναι επί του παρόντος ενεργή και ότι χρησιμοποιεί μια εμπορικά διαθέσιμη πλατφόρμα ηλεκτρονικού εμπορίου.

Περαιτέρω, εξετάζει την φύση της υπηρεσίας που παρέχεται και την φύση των χρηστών. Ως προς αυτό αναφέρει ότι στον ιστότοπο οι χρήστες μπορούν να αναζητήσουν και να ενημερωθούν για το εύρος των προϊόντων. Όλοι οι χρήστες έχουν πρόσβαση στις σελίδες πληροφοριών για τα παιχνίδια. Ο ιστότοπος δίνει τη δυνατότητα σε ενήλικες και παιδιά άνω των 13 ετών με χρεωστικές κάρτες στο όνομά τους να παραγγείλουν προϊόντα. Οι χρήστες ηλικίας 13 ετών και άνω μπορούν να εγγραφούν για ενημερωτικά δελτία με τη διεύθυνση ηλεκτρονικού ταχυδρομείου τους μέσω ενός κουτιού επιλογής για την ηλικιακή αυτοδήλωση. Χρησιμοποιείται η εξαίρεση "soft opt-in" για την αποστολή ενημερωτικών δελτίων σε υφιστάμενους πελάτες με λογαριασμούς χρηστών. Οι χρήστες έχουν τη δυνατότητα να δημιουργήσουν λογαριασμό ή να αγοράσουν χωρίς εγγραφή, ως επισκέπτες. Ο ιστότοπος περιλαμβάνει μια λειτουργία "Επικοινωνήστε μαζί μας", η οποία περιλαμβάνει μια φόρμα επικοινωνίας όπου οι χρήστες παρέχουν όνομα, email, θέμα και μήνυμα. Αυτή η πτυχή της υπηρεσίας προστατεύεται από την υπηρεσία Captcha τρίτου μέρους, η οποία περιλαμβάνει τη χρήση cookies ή παρόμοιων τεχνολογιών. Ο ιστότοπος διατηρεί το ιστορικό παραγγελιών και μέσω αυτού πραγματοποιούνται περιορισμένες δραστηριότητες κατάρτισης προφίλ των χρηστών με βάση τη δραστηριότητα που πραγματοποιούν όταν είναι συνδεδεμένοι σε λογαριασμούς πελατών. Χρησιμοποιούνται αυτά τα δεδομένα και τα δεδομένα από τα cookies ανάλυσης, για να προτείνονται παρόμοια προϊόντα σε αυτούς τους χρήστες. Ο ιστότοπος δεν περιλαμβάνει εξωτερικές διαφημίσεις - όλες οι διαφημίσεις είναι συναφείς και παρουσιάζουν προϊόντα εντός του καταλόγου μας.

Τέλος, για την ολοκλήρωση της περιγραφής του πλαισίου της επεξεργασίας ο ICO εξετάζει το πόσο πιθανό είναι τα υποκείμενα των δεδομένων να αναμένουν την επεξεργασία. Ως προς αυτό στο παράδειγμα του αναφέρει ότι θεωρεί ότι η παραπάνω επεξεργασία θα είναι σύμφωνη με τις προσδοκίες των χρηστών. Εξηγείται με σαφήνεια στη δήλωση απορρήτου, η οποία είναι γραμμένη σε απλή, κατανοητή γλώσσα και διατίθεται ως αρχείο ήχου. Πραγματοποιήθηκαν δοκιμές αναγνωσιμότητας της ειδοποίησής για την προστασία των προσωπικών δεδομένων για να επιβεβαιώσουμε ότι θα πρέπει να είναι κατανοητή από τα περισσότερα άτομα άνω των εννέα ετών. Οι περισσότερες επεξεργασίες εκτός της βασικής δραστηριότητας της πώλησης προϊόντων είναι προαιρετικές. Για παράδειγμα, η επεξεργασία

για σκοπούς μάρκετινγκ, η επεξεργασία για σκοπούς απάντησης σε ερωτήματα, η κοινοποίηση αγορών στα μέσα κοινωνικής δικτύωσης. Δεν χρησιμοποιούμε τα δεδομένα με ασυνήθιστους τρόπους που θα θεωρούνταν ότι είναι εκτός των προσδοκιών των χρηστών.

8.1.1.4. Περιγραφή του σκοπού της επεξεργασίας

Ως σκοπός της επεξεργασίας νοείται ο λόγος για τον οποίο επιθυμεί ο υπεύθυνος επεξεργασίας να προβεί στην επεξεργασία. Επιπλέον, ο ICO προτείνει να καταγραφούν τα έννομα συμφέροντα του υπευθύνου επεξεργασίας, κατά περίπτωση, το επιδιωκόμενο αποτέλεσμα για τα άτομα και τα αναμενόμενα οφέλη για τον ίδιο τον υπεύθυνο επεξεργασίας ή το κοινωνικό σύνολο.

Ως προς αυτό στο παράδειγμα του ο ICO αναφέρει τα εξής: Ως επιδιωκόμενο αποτέλεσμα της επεξεργασίας του συγκεκριμένου ιστοτόπου είναι να προσφερθεί ένα ηλεκτρονικό κατάστημα παιχνιδιών που θα επιτρέπει να πωλούνται, και στους πελάτες να αγοράζουν, παιχνίδια σε ένα ηλεκτρονικό περιβάλλον, και να αναπτυχθεί η επιχείρησή και η πελατειακή της βάση. Αναφέρεται, επίσης, ότι μέσω της παροχής πρόσβασης σε ασφαλή και εκπαιδευτικά παιχνίδια, επιτυγχάνεται η προστασία και υποστήριξη της σωματικής, ψυχολογικής και συναισθηματικής ανάπτυξής των παιδιών.

Επιπλέον, ως προς την επιδιωκόμενη επίδραση στα άτομα αναφέρεται ότι είναι να εμπιστευτούν το εμπορικό σήμα του υπευθύνου και να αγοράσουν από το ηλεκτρονικό κατάστημα της εταιρείας.

Τέλος, ως προς τα οφέλη της επεξεργασίας είναι ότι η τελευταία επιτρέπει να λειτουργήσει η επιχείρησή, να προωθηθούν τα προϊόντα και να αυξηθούν οι πωλήσεις. Η επεξεργασία ωφελεί τους πελάτες, συμπεριλαμβανομένων των παιδιών, επειδή τους επιτρέπει να ψωνίζουν προϊόντα μέσω διαδικτύου, συχνά σε φθηνότερες τιμές από ό,τι σε ένα φυσικό κατάστημα, και να ενημερώνονται μέσω πλαισιωμένης διαφήμισης και ενημερωτικού δελτίου (με την προϋπόθεση της συγκατάθεσης ή του soft opt-in) για προϊόντα που μπορεί να τους ενδιαφέρουν.

8.1.2. Η προσέγγιση της CNIL.

Η CNIL μέσα από το λογισμικό ανοιχτού κώδικα που προτείνει[93], καλεί τον υπεύθυνο επεξεργασίας να καταγράψει κατ' αρχάς το γενικό πλαίσιο της επεξεργασίας με σκοπό την παροχή μιας σαφούς εικόνας της επεξεργασίας των δεδομένων. Παρόλα αυτά, χωρίζει το γενικό αυτό πλαίσιο σε δύο μέρη. Στο πρώτο ζητά να καταγραφεί μία επισκόπηση της όλης διαδικασίας της επεξεργασίας και μετέπειτα τα προσωπικά δεδομένα, την διάρκεια τήρησης τους, τους αποδέκτες αυτών και τα υποστηρικτικά στοιχεία που χρησιμοποιούνται για την συντέλεση της. Σημειώνεται δε, ότι υποστηρικτικά στοιχεία μπορεί να είναι τεχνολογικό υλικό, λογισμικό, δίκτυα, άνθρωποι, χαρτί ή κανάλια διαβίβασης χαρτιού.

Ειδικότερα, το πρώτο ζητούμενο αυτής της γενικής επισκόπησης είναι να καταγραφεί η υπό εξέταση επεξεργασία. Ως προς αυτό, ζητά να δοθεί μία σύντομη περιγραφή της εξεταζόμενης επεξεργασίας προσωπικών δεδομένων, της φύσης, του πεδίου εφαρμογής, του πλαισίου, των σκοπών και του διακυβεύματός της. Να προσδιοριστούν ο υπεύθυνος επεξεργασίας και οι εκτελούντες την επεξεργασία. Να αναφερθούν οι τυποποιημένες αναφορές που ισχύουν για την επεξεργασία των προσωπικών δεδομένων, οι οποίες είναι απαραίτητες ή πρέπει να τηρούνται, μεταξύ των οποίων και οι εγκεκριμένοι κώδικες δεοντολογίας (βλέπετε Άρθ. 40 του ΓΚΠΔ) και πιστοποιήσεις σχετικά με την προστασία δεδομένων (βλέπετε Άρθ. 42 του ΓΚΠΔ)

Επιπλέον, ζητάται να καταγραφούν οι ευθύνες που συνδέονται με την επεξεργασία. Να καταγραφούν δηλαδή ποιες είναι ευθύνες που έχουν οι υπεύθυνοι επεξεργασίας, οι τυχόν εκτελούντες την επεξεργασίας και οι από κοινού υπεύθυνοι επεξεργασίας.

Τέλος, καλεί να καταγραφούν τα πρότυπα (αν υπάρχουν) βάσει των οποίων θα διενεργείται η επεξεργασίας, όπως κώδικες δεοντολογίας ή πιστοποιήσεις επεξεργασίας δεδομένων.

Στο δεύτερο στάδιο της παρούσας φάσης η CNIL καλεί τον διενεργούντα την επεξεργασία να καταγράψει το ποια προσωπικά δεδομένα υφίστανται επεξεργασία. Επεξηγεί περαιτέρω ότι πρέπει να καταγραφούν τα δεδομένα που συλλέγονται και τυγχάνουν επεξεργασίας, να καθοριστούν οι διάρκειες αποθήκευσης τους, οι αποδέκτες τους και τα άτομα που έχουν πρόσβαση σε αυτά. Σε αυτό προσθέτει ότι πρέπει να καθοριστούν και να περιγραφούν λεπτομερώς το πεδίο εφαρμογής, δηλαδή, τα σχετικά προσωπικά δεδομένα, τους παραλήπτες τους και τις διάρκειες αποθήκευσής τους.

[93] The open source PIA software helps to carry out data protection impact assessment, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment

Επιπλέον, ζητά να καταγραφεί το πως λειτουργεί ο κύκλος ζωής των δεδομένων από την συλλογή δεδομένων έως την καταστροφή δεδομένων, τα διάφορα στάδια επεξεργασίας και την αρχειοθέτηση, ενώ προτείνει τη δημιουργία ενός διαγράμματος ροής δεδομένων. Παράλληλα, ζητάται να καταγραφούν οι διαδικασίες που διεξάγονται για την επεξεργασία των δεδομένων.

Σε αυτό το σημείο κρίνεται σκόπιμο να αναφερθεί ότι η CNIL θέτει έναν πιο σαφή και ασφαλή διαχωρισμό των δεδομένων, σε σχέση με αυτόν του ICO. Σε γενικές γραμμές διακρίνει τα δεδομένα ως εξής:

Πρώτη κατηγορία είναι τα λεγόμενα «απλά». Ενδεικτικώς, ληξιαρχικά στοιχεία ταυτότητας, δεδομένα ταυτοποίησης, προσωπική ζωή (Συνήθειες διαβίωσης, οικογενειακή κατάσταση κτλ), επαγγελματική ζωή (βιογραφικό σημείωμα, εκπαίδευση και επαγγελματική κατάρτιση, επιβραβεύσεις κτλ.), οικονομικές και χρηματοοικονομικές πληροφορίες (εισόδημα, οικονομική κατάσταση, φορολογική κατάσταση κτλ), δεδομένα τοποθεσίας (μετακινήσεις, δεδομένα GPS, δεδομένα GSM, κτλ)

Η δεύτερη κατηγορία αφορά προσωπικά δεδομένα που εκλαμβάνονται ως ευαίσθητα. Παράδειγμα, Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ), βιομετρικά δεδομένα, δεδομένα τραπεζικής φύσεως.

Τρίτη κατηγορία είναι προσωπικά δεδομένα ειδικών κατηγοριών. Πρόκειται για τα λεγόμενα «ευαίσθητα» προσωπικά δεδομένα (αρ. 9 του ΓΚΠΔ). Πρόκειται για δεδομένα που αποκαλύπτουν Φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, συμμετοχή σε συνδικαλιστική οργάνωση, γενετικά δεδομένα, βιομετρικά δεδομένα με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένα που αφορούν την υγεία ή δεδομένα που αφορούν στην σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.

Τέλος, τελευταία κατηγορία αποτελούν τα δεδομένα που αφορούν σε ποινικές καταδίκες και αδικήματα (αρ.10 του ΓΚΠΔ), όπως ποινικές καταδίκες, αδικήματα και μέτρα ασφαλείας.[94]

Στο τελευταίο στάδιο για να ολοκληρωθεί η καταγραφή του γενικού πλαισίου της επεξεργασίας, είναι να καταγραφούν εκείνα τα στοιχεία που υποστηρίζουν τα δεδομένα. Ως

[94] Βλ.Δημήτριος Ευ. Τζέλλης, Μαρία Δ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 6 επ.

προς αυτό επεξηγεί ότι ο διενεργών την εκτίμηση αντικτύπου πρέπει να καταγράψει τα λειτουργικά συστήματα, τις επιχειρηματικές εφαρμογές, τα συστήματα διαχείρισης βάσεων δεδομένων, τις σουίτες γραφείου, τα πρωτόκολλα και τις διαμορφώσεις.

Ως προς αυτό το στάδιο έχει ασκηθεί κριτική στην μεθοδολογική προσέγγιση της CNIL. Ειδικότερα, έχει υποστηριχθεί ότι για το στάδιο της συστηματικής περιγραφής η CNIL δεν κατορθώνει να προσεγγίσει την περιγραφή συστηματικά και να καθορίσει το πως αυτή διενεργείται, παρόλο που κατηγοριοποιεί και περιγράφει τις διαδικασίες της επεξεργασίας.[95]

8.1.3 Η προσέγγιση του Fraunhofer Institute

Σύμφωνα με αυτή την προσέγγιση το συγκεκριμένο στάδιο θεωρείται ότι πληροί τις απαιτήσεις του άρθρου 35 παρ.7 περ.1 όταν γίνει μια περιγραφή της προβλεπόμενης επεξεργασίας και των σκοπών της επεξεργασίας. Διευκρινίζεται, βέβαια, ότι η καταγραφή του σκοπού της επεξεργασίας θα πρέπει να έχει προηγηθεί αυτού του σταδίου και ειδικότερα να έχει εκπονηθεί, όπως προαναφέρθηκε, κατά την απαραίτητη προεργασία. Ωστόσο, είναι πιθανό σε αυτό το στάδιο ή και σε κάποιο επόμενο να ανακαλυφθούν εναλλακτικοί ή νέοι σκοποί επεξεργασίας. Ως εκ τούτου θα πρέπει να προστεθούν σε αυτό το στάδιο και αυτοί οι σκοποί και να τροποποιηθούν καταλλήλως και τα αρχεία δραστηριοτήτων επεξεργασίας περιλαμβάνοντας, πλέον, αυτούς τους νέους σκοπούς. Επιπλέον, σε περίπτωση που ανακαλυφθούν νέοι σκοποί θα πρέπει να γίνει και μία νέα εκτίμηση κατά πόσον αυτοί είναι συνεπείς και με την νομική βάση πάνω στην οποία βασίζεται η επεξεργασία και να αξιολογηθεί αν θα πρέπει και αυτή να τροποποιηθεί.

Για να επιτύχει την συστηματική περιγραφή των προβλεπόμενων πράξεων η συγκεκριμένη μεθοδολογική προσέγγιση προτείνει ότι αυτή πρέπει να γίνει από μία τεχνική, νομική και οργανωτική σκοπιά.. Θεωρεί, λοιπόν, ότι για να καταστεί δυνατή η καταγραφή των προβλεπόμενων διαδικασιών επεξεργασίας να καταγραφούν οι εξής κατηγορίες πληροφοριών[96].

[95] Bisztray, T., Gruschka, N. (2019). Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In: Askarov, A., Hansen, R., Rafnsson, W. (eds) Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science(), vol 11875. Springer, Cham., σελ. 9

[96]Βλ. Fraunhofer Institute for Secure Information Technology. (n.d.). Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz.: https://publica-rest.fraunhofer.de/server/api/core/bitstreams/0a2cec45-c81d-4cee-806c-d2ba2f1afb61/content [Accessed 7 Nov. 2023].

Η πρώτη εξ' αυτών αφορά τα υποκείμενα των δεδομένων, τα προσωπικά δεδομένα που τελούν υπό επεξεργασία, οι ροές δεδομένων, τα εμπλεκόμενα μέρη/ πρόσωπα και οι προβλεπόμενες επεξεργασίας. Η δεύτερη κατηγορία αφορά την καταγραφή των προβλεπόμενων τεχνικών προδιαγραφών, της τεχνικής υποδομής καθώς και τα τεχνικά και οργανωτικά μέτρα. Ενώ, τέλος, όπου κρίνεται απαραίτητο πρέπει να καταγραφούν οι εκπρόσωποι των υποκειμένων των δεδομένων (εργατικά σωματεία, εργατικές ενώσεις, ενώσεις ασθενών κτλ.) οργανώσεις, εκτελούντες την επεξεργασία, από κοινού υπεύθυνοι επεξεργασίας, συμβάσεις με αυτούς κτλ. Επιπλέον, προτείνεται η δημιουργία ενός διαγράμματος ροής δεδομένων το οποίο να τεκμηριώνει ολόκληρη την επεξεργασία από την συλλογή των δεδομένων, την αποθήκευση, την χρήση, την διαβίβαση έως και την διαγραφή τους. Επιπλέον, στα έγγραφα που θα περιλαμβάνεται η σχετική καταγραφή θα πρέπει να περιλαμβάνονται τα συστήματα, τα δίκτυα, οι τεχνικές υποδομές και τα σχέδια για την υλοποίηση της επεξεργασίας. Πάντως, και σε αυτή την μεθοδολογική προσέγγιση αναφέρεται ότι τελικός σκοπός της συγκεκριμένης φάσης είναι να μπορέσει σε μετέπειτα πεδίο, η ομάδα που θα διενεργήσει την ΕΑΠΔ να είναι σε θέση με βάση αυτές τις πληροφορίες να προσδιορίσει και να αναλύσει τις πιθανές ζημίες για τα υποκείμενα των δεδομένων στο πλαίσιο της εξεταζόμενης επεξεργασίας.

8.1.3.1 Εντοπισμός των υποκειμένων των δεδομένων

Εκτός από την περιγραφή του συστήματος και των σκοπών, η συγκεκριμένη μεθοδολογική προσέγγιση απαιτεί να γίνει μία καταγραφή των υποκειμένων των δεδομένων. Σύμφωνα με το άρθρο 4 παρ.1 ΓΚΠΔ, υποκείμενο των δεδομένων είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Σύμφωνα με την αιτιολογική σκέψη υπ' αριθμόν 14 τα Νομικά πρόσωπα δεν είναι υποκείμενα των δεδομένων και ως εκ τούτου δεν απολαμβάνουν προστασίας εκ του ΓΚΠΔ.

Εξαιτίας των μεθόδων ανάλυσης δεδομένων που χρησιμοποιούνται σήμερα και της δυνατότητας σύνδεσης συνόλων δεδομένων, είναι δυνατόν ακόμη και δεδομένα που δεν σχετίζονται άμεσα με ένα φυσικό πρόσωπο να μπορούν να συνδεθούν με ένα φυσικό πρόσωπο. Τα δεδομένα GPS των οχημάτων, για παράδειγμα, ή τα δεδομένα καταγραφής των μηχανών μπορούν συχνά να συνδεθούν με ένα συγκεκριμένο πρόσωπο. Ακόμη και αν τα δεδομένα αυτά

συλλέχθηκαν για τη διαχείριση ενός στόλου οχημάτων μιας εταιρείας, ή για να παρακολουθείται η αποδοτικότητα ενός μηχανήματος ή για να παράσχουν πληροφορίες σχετικά με το πότε πρέπει να γίνει συντήρηση, παρόλα αυτά συχνά μπορεί να είναι σε θέση να συνδεθούν με ένα πρόσωπο, έτσι ώστε να υφίστανται επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά την έννοια του ΓΚΠΔ.

Για να καταστεί αξιόπιστος, λοιπόν, ο εντοπισμός των υποκειμένων είναι χρήσιμο να απαντηθούν τρείς ερωτήσεις. Η πρώτη αφορά το «από ποιους θα πρέπει να συλλέγονται δεδομένα». Η δεύτερη, αφορά το «αν συλλέγονται επιπλέον δεδομένα εμμέσως ή παρεμπιπτόντως» και τέλος «ποιος είναι πιθανό να ταυτοποιηθεί από τα συλλεχθέντα είτε τα επεξεργασθέντα δεδομένα;»

Επιπλέον, παρατίθενται κάποιες τυπικές κατηγορίες υποκειμένων δεδομένων. Η πρώτη αφορά τους εργαζομένους του οργανισμού και το προσωπικό των πελατών, των προμηθευτών και των συνεργατών αυτού. Δεύτερη κατηγορία αποτελούν οι πελάτες ή οι χρήστες (όταν πρόκειται για ψηφιακά προϊόντα) των υπηρεσιών του οργανισμού καθώς και οι συγγενικά τους πρόσωπα , όπως η οικογένεια, οι φίλοι και άλλα πρόσωπα που έρχονται σε επαφή με αυτά τα προϊόντα (π.χ. πρόσωπα που υπάρχουν σε έναν χώρο στον οποίο χρησιμοποιούνται συσκευές αναγνώρισης φωνής, οι συνεπιβάτες σε έξυπνα οχήματα κτλ.). Τρίτη κατηγορία αφορά τους ασθενείς, τους ενοίκους σε οίκους ευγηρίας, μαθητές σχολείων, τους αποδέκτες κρατικών επιδομάτων καθώς και τα συγγενικά πρόσωπα όλων των παραπάνω. Τέταρτη κατηγορία αποτελούν οι ασφαλισμένοι ή οι αποδέκτες άλλων ασφαλιστικών – χρηματοοικονομικών προϊόντων και τελευταία κατηγορία οι εντελώς αμέτοχοι πολίτες που απλώς τυγχάνει να διασχίζουν μία περιοχή (π.χ. στην περίπτωση βιντεοεπιτήρησης)

8.1.3.2. Εντοπισμός λοιπών εμπλεκομένων μερών

Επιπλέον, η συγκεκριμένη μεθοδολογική προσέγγιση προκρίνει τον εντοπισμό όλων των εμπλεκομένων μερών που σχετίζονται με την επεξεργασία. Ειδικότερα, ως εμπλεκόμενα μέρη θεωρεί ότι είναι όλοι οι οργανισμοί - εσωτερικοί και εξωτερικοί, φυσικά και νομικά πρόσωπα (επιχειρήσεις, κρατικά ιδρύματα, μη κυβερνητικές οργανώσεις, εξωτερικοί επιτιθέμενοι, άλλοι), καθώς και οργανωτικές μονάδες χωρίς νομική προσωπικότητα (π.χ. άλλα τμήματα της εταιρείας) - που έχουν ήδη πρόσβαση στα δεδομένα που χρησιμοποιούνται στην επεξεργασία, συστήματα ΤΠΕ και λειτουργίες επεξεργασίας, ή που θα μπορούσαν εύλογα να έχουν πρόσβαση σε αυτά ή δυνητικά να τα επηρεάσουν. Ο ουδέτερος όρος "εμπλεκόμενος" επιλέχθηκε σκόπιμα από τους συγγραφείς της συγκεκριμένης μεθοδολογικής προσέγγισης, αφού, η ιδιότητα του «εμπλεκομένου» δεν σημαίνει, ούτε υπονοεί κανενός είδους παράνομη

συμπεριφορά ή "κακόβουλη πρόθεση". Όλα τα πρόσωπα, τα ιδρύματα και οι οργανισμοί που έχουν απολύτως νόμιμη πρόσβαση είναι επίσης εμπλεκόμενα μέρη. Παρ' όλα αυτά, τα εμπλεκόμενα μέρη αποτελούν συχνά την πιο σημαντική πηγή κινδύνου για τα υποκείμενα των δεδομένων. Οι προβληματικές δραστηριότητες των εμπλεκομένων μερών δεν είναι απαραίτητο να ανάγονται σε κακόβουλη πρόθεση, αλλά μπορεί ακόμη και να έχουν το αντίθετο κίνητρο (π.χ. στο πλαίσιο της φροντίδας), να θέλουν να βοηθήσουν τα υποκείμενα των δεδομένων. Επομένως, είναι σημαντικό να εντοπιστούν - χωρίς να κριθούν ακόμη σε αυτή την φάση - όλα τα υφιστάμενα ή δυνητικά, άμεσα και έμμεσα, εσωτερικά και εξωτερικά εμπλεκόμενα μέρη.

Ο προσδιορισμός των εμπλεκομένων μερών θα πρέπει να περιλαμβάνει την ανάλυση των κινήτρων, των συμφερόντων τους, και των ικανοτήτων τους να αποκτήσουν πρόσβαση στα δεδομένα και τις πράξεις επεξεργασίας ή να επηρεάσουν τα δεδομένα και τις πράξεις επεξεργασίας. Οι πληροφορίες αυτές είναι σημαντικές για τον εντοπισμό και την ανάλυση των κινδύνων που θα λάβει χώρα αργότερα. Σε αυτό τον εντοπισμό ,επίσης, θα πρέπει να εξετάζονται τα πιθανά κίνητρα των εμπλεκομένων μερών που συμμετέχουν νόμιμα όταν εμπλέκονται στην επεξεργασία και υπερβαίνουν τον σκοπό της επεξεργασίας.

Τέλος, θα πρέπει να ληφθεί υπόψη ότι μια επιρροή που μπορεί να ασκήσει ένα εμπλεκόμενα μέρος μπορεί να συμβεί και χωρίς να υπάρχει κίνητρο ακόμη και ακούσια. Για παράδειγμα, οι εργαζόμενοι μπορούν να αποκτήσουν πρόσβαση χωρίς πρόθεση σε δεδομένα, επειδή, οι επιχειρηματικοί εταίροι τους στέλνουν δεδομένα με ακατάλληλο τρόπο και χωρίς να έχουν ζητηθεί ή ανακοινωθεί. Εάν ένα τέτοιο σενάριο συμβεί, οι εν λόγω υπάλληλοι θα πρέπει να θεωρούνται εμπλεκόμενα μέρη - ακόμη και αν δεν το επιθυμούν!

Για τον αποτελεσματικό εντοπισμό των λοιπών εμπλεκόμενων μερών η μεθοδολογική προσέγγιση Fraunhofer προτείνει ότι θα πρέπει να απαντηθούν κάποιες ερωτήσεις, όπως και προηγουμένως στον εντοπισμό των υποκειμένων. Η πρώτη εξ' αυτών είναι ποια ενδιαφερόμενα μέρη (εσωτερικά ή εξωτερικά) περιλαμβανομένων και των εκτελούντων την επεξεργασία συμμετέχουν ενεργά στην επεξεργασία. Ποιος άλλος έχει πρόσβαση στα δεδομένα και τις διαδικασίες επεξεργασίας (χωρίς να συμμετέχει ενεργά στην επεξεργασία) ή ειδάλλως θα μπορούσε να επηρεάσει ή να εκμεταλλευτεί την επεξεργασία; Τι κίνητρα θα μπορούσαν να έχουν οι ανωτέρω εμπλεκόμενοι να επηρεάσουν την επεξεργασία, χρησιμοποιώντας τα δεδομένα ή επηρεάζοντας την επεξεργασία; Ποιοι άλλοι θα μπορούσαν να ήθελαν να έχουν πρόσβαση στην επεξεργασία και θα ενδιαφέρονταν ή θα επεδίωκαν να αποκτήσουν πρόσβαση στα δεδομένα; Ποιος άλλος, ίσως, αποκτήσει πρόσβαση στα δεδομένα ακόμα και ακούσια και πως;

Επιπλέον, παρατίθενται κάποιες χαρακτηριστικές κατηγορίες εμπλεκομένων μερών. Η πρώτη εξ' αυτών αφορά εσωτερικά μέρη, όπως εργαζομένους, στελέχη και επιθεωρητές, τμήματα που έχουν συχνά πρόσβαση σε προσωπικά δεδομένα όπως τμήμα προσωπικού, marketing, product development, IT και επισκέπτες. Η δεύτερη κατηγορία αφορά εξωτερικά μέρη, όπως παρόχους υπηρεσιών πληροφορικής, συστημάτων και υποδομών, προμηθευτές, τράπεζες και ασφαλιστικές εταιρείες, διαφημιστικές εταιρείες, υπηρεσίες χρεωστικών καρτών, παρόχους τεχνολογιών αιχμής, λογιστές, υπηρεσίες ασφαλείας, υπηρεσίες στατιστικών ερευνών, οργανισμούς υγείας όπως νοσοκομεία και γηροκομία και τέλος οργανισμούς από τον τομέα της έρευνας όπως πανεπιστήμια ή ερευνητικούς φορείς.

8.1.3.3. Καθορισμός της ομάδας διενέργειας της ΕΑΠΔ

Τέλος, πρέπει να καθοριστεί η ομάδα που θα διενεργήσει την ΕΑΠΔ. Ειδικότερα, το πιο λογικό είναι πως μία ΕΑΠΔ θα διενεργηθεί από μία ομάδα και όχι από ένα άτομο μόνο, καθώς είναι δύσκολο να βρεθεί ένας και μόνο άνθρωπος που να κατέχει όλη την γνώση για να μπορέσει να τη διενεργήσει μόνος του. Ως καλύτερη πρακτική προκρίνεται εκείνη που θα περιλάβει στην ως άνω ομάδα κατ' αρχάς τους πιο ειδικούς από κάθε τμήμα (ως εκπρόσωπο όλων των εργαζομένων στο συγκεκριμένο τμήμα) που θα συντελεί στην υπό εξέταση επεξεργασία. Επιπλέον, θα πρέπει να λάβουν μέρος οι εξής: Ένας εξειδικευμένος νομικός ειδικά στον τομέα των προσωπικών δεδομένων. Ο Υπεύθυνος προστασίας Προσωπικών Δεδομένων, ένας εξειδικευμένος επαγγελματίας στον τομέα της πληροφορικής. Όπου είναι δυνατό εκπρόσωποι των εκτελούντων την επεξεργασία και των παρόχων των τεχνολογιών πληροφορικής, καθώς και οι εκπρόσωποι των εργαζομένων.

8.1.4 Λοιπές προσεγγίσεις

Ως λοιπές προσεγγίσεις νοούνται αυτές που δεν έχουν αναπτυχθεί από Εποπτικές Αρχές.

M. Caroline Oetzel & S. Spiekermann

Ειδικότερα, η πρώτη εξ αυτών προσέγγιση αναπτύχθηκε από τους δύο ερευνητές (Oetzel & Spiekermann) του Πανεπιστημίου Οικονομικών & Επιχειρήσεων της Βιέννης[97] το 2014, το υπόβαθρο των οποίων είναι ο κλάδος της πληροφορικής. Σύμφωνα με την εν λόγω

[97] Βλ. Marie Caroline Oetzel, Sarah Spiekerman, Ingrid Gruning, Harald Kelter and Sabine Mull. Privacy Impact Assessment Guideline for RFID Applications, 2011

προσέγγιση για να καθοριστούν τα όρια της επεξεργασίας, η συστηματική περιγραφή της επεξεργασίας πρέπει να γίνει βασιζόμενη σε τέσσερις οπτικές. Αυτές είναι:

1) Την οπτική του συστήματος. Η οποία αποτελείται από τις εφαρμογές, τα συστατικά μέρη του συστήματος, το υλικό, το λογισμικό, την διεπαφή (interface) και την αρχιτεκτονική δικτύου.
2) Την λειτουργική οπτική. Η οποία αποτελείται τις διαδικασίες του φορέα, τις περιπτώσεις εφαρμογής, τους τεχνικούς ελέγχους τους ρόλους και τους χρήστες.
3) Την οπτική των δεδομένων. Η οποία περιλαμβάνει κατηγορίες δεδομένων οι οποίες τίθενται υπό επεξεργασία, διαγράμματα ροής (εξωτερικά και εσωτερικά) περιλαμβάνοντας τα πρόσωπα
4) Την οπτική του φυσικού Περιβάλλοντος: Η οποία περιλαμβάνει την φυσική προστασία και τους τεχνικούς ελέγχους όπως την δημιουργία αντιγράφων ασφαλείας και τα σχέδια δράσης σε περίπτωση έκτακτης ανάγκης.

Ως εκ τούτου, σύμφωνα με αυτή την μεθοδολογική προσέγγιση, για να ολοκληρωθεί το συγκεκριμένο στάδιο η περιγραφή πρέπει να περιλαμβάνει και τις τέσσερις αυτές οπτικές, καθώς και όλες τις διεπαφές, τα κομμάτια του συστήματος που συντελούν στην επεξεργασία, τις διαδικασίες επεξεργασίας και τις διαβιβάσεις των προσωπικών δεδομένων. Επιπλέον, κάθε διεπαφή του συστήματος πρέπει να ελέγχεται για το αν επιτρέπει στον χρήστη να έχει πρόσβαση σε κάποιο άλλο σημείο του συστήματος, καθώς και τα διαγράμματα ροής δεδομένων να περιλαμβάνουν όλους τους ρόλους και τα εμπλεκόμενα πρόσωπα της επεξεργασίας

S. Joyee De & D. Le Métayer (BEMS SYSTEM)

Εμπνεόμενη από την παραπάνω προσέγγιση, διαμορφώθηκε και η παρακάτω η οποία εφαρμόστηκε σε εκτίμηση αντικτύπου που διενεργήθηκε πάνω σε έξυπνο σύστημα διαχείρισης ενέργειας (BEMS)[98]. Η έρευνα αυτή αναπτύχθηκε από τους ερευνητές S. Joyee De & D. Le Métayer στο πανεπιστήμιο της Λυόν της Γαλλίας και δημοσιεύτηκε το 2016, ενώ και οι δύο ερευνητές έχουν τεχνολογικό υπόβαθρο.

Στην συγκεκριμένη Εκτίμηση, λοιπόν , ό,τι αφορούσε το σύστημα και τις προδιαγραφές αυτού αποτυπώθηκε πάνω σε έξη βασικούς άξονες:

[98] Βλ. Sourya Joyee De, Daniel Le Métayer, Privacy Risk Analysis, Springer Cham,https://doi.org/10.1007/978-3-031-02349-1,

1. Την λειτουργική προδιαγραφή του συστήματος. Θα πρέπει δηλαδή να περιγραφούν οι λειτουργίες που έχει σκοπό να επιτελεί το σύστημα, και οι πιθανές χρήσεις του.
2. Τα τεχνικά και οργανωτικά μέτρα που έχουν ληφθεί για την προστασία των προσωπικών δεδομένων.
3. Τις διεπαφές (interface) του συστήματος, περιλαμβάνοντας όλες τις αλληλεπιδράσεις που έχει αυτό με τον εξωτερικό κόσμο, περιλαμβάνοντας τους χρήστες και άλλα συστήματα που τυχόν έχουν πρόσβαση σε αυτό.
4. Το διάγραμμα ροής δεδομένων, περιγράφοντας το σύστημα «εκ των έσω», περιλαμβάνοντας τα βασικά συστατικά του, την τοποθεσία τους και τα δικαιώματα πρόσβασης που υπάρχουν σε αυτά.
5. Τις υποστηρικτικές υποδομές πάνω στις οποίες βασίζεται το σύστημα, περιλαμβάνοντας το λογισμικό, το υλικό(hardware) και τους εμπλεκόμενους φορείς που τα ελέγχουν.
6. Τους φορείς που έχουν πρόσβαση στο σύστημα και αλληλοεπιδρούν με αυτό, περιλαμβάνοντας τους ρόλους τους και τα δικαιώματα πρόσβασης τους.

ISO 29134:2020

Επιπλέον, στο ISO 29134: 2020[99] προτείνεται ότι το έγγραφο της ΕΑΠΔ θα πρέπει να περιγράφει τουλάχιστον τις προδιαγραφές του συστήματος, το σχεδιασμό του συστήματος, την λειτουργική του περιγραφή και τις πληροφορίες για επιχειρησιακά σχέδια και διαδικασίες δεδομένων. Περαιτέρω τα εξειδικεύει ως εξής:

1) Για τις προδιαγραφές του συστήματος:
   - Τον σκοπό της επεξεργασίας.
   - Τις οργανικές δραστηριότητες τις οποίες υποστηρίζει ή θα υποστηρίζει το σύστημα.
   - Έναν κατάλογο των λειτουργικών απαιτήσεων που έχουν καθοριστεί για το πληροφοριακό σύστημα.
   - Τους στόχους που έχουν τεθεί για την ασφάλεια των πληροφοριών
   - Μία περιγραφή για το πως τα δεδομένα θα συλλεχθούν, από ποιον και γιατί. Η περιγραφή, επίσης, θα πρέπει να καθορίζει το ποιος θα έχει πρόσβαση και να λαμβάνει υπόψη τις βασικές αρχές επεξεργασίας.
   - Αν οι πληροφορίες του συστήματος πρόκειται να κοινολογηθούν σε τρίτους, αν ναι λεπτομέρειες για το ποιοι θα είναι και για ποιον σκοπό

[99] Βλ. ISO/IEC 29134:2023 - Information technology — Security techniques — Guidelines for privacy impact assessment

2) Για τον σχεδιασμό του συστήματος:
   - Μια επισκόπηση της λειτουργικής αρχιτεκτονικής του συστήματος.
   - Μια επισκόπηση της φυσικής αρχιτεκτονικής
   - Την δομή και τις λίστες των βάσεων δεδομένων, πίνακες και πεδία που θα περιέχουν προσωπικά δεδομένα.
   - Ένα διάγραμμα ροής δεδομένων που να περιλαμβάνει τις οντότητες (entities) και την διεπαφή (interface)
   - Ένα διάγραμμα με τον κύκλο ζωής των δεδομένων, π.χ. δημιουργία δεδομένων, χρήση, μεταφορά και καταστροφή τους.
   - Ένα διάγραμμα που να περιγράφει το πότε πρέπει να ειδοποιεί και να λαμβάνει συγκατάθεση
   - Μία λίστα των διεπαφών, καθορίζοντας τα μέρη που είναι συνδεδεμένα.
   - Λεπτομέρειες σχετικά με την κρυπτογράφηση, τις θύρες (ports), τα πρωτόκολλα και τα APIs (Application Programming Interfaces)
3) Για τα επιχειρησιακά σχέδια και τις διαδικασίες επεξεργασίας δεδομένων.
   - Την διαχείριση της ταυτοποίησης των χρηστών για το πληροφοριακό σύστημα. (Την εγγραφή των χρηστών, την εξουσιοδότηση των χρηστών, την διαχείριση των χρηστών, Single Sign- On SSO να παρέχεται, δηλαδή, η δυνατότητα στους χρήστες να συνδέονται σε πολλές εφαρμογές με ένα σύνολο διαπιστευτηρίων, κτλ)
   - Το λειτουργικό σχέδιο του πληροφοριακού συστήματος, περιλαμβάνοντας και μέρη τα οποία λειτουργούν ή φιλοξενούνται εσωτερικά ή εξωτερικά ή σε κάποιο υπολογιστικό νέφος.
   - Το υποστηρικτικό σχέδιο, και ειδικά λίστες με τρίτα μέρη με το όνομα κάθε εμπλεκόμενου στην υποστήριξη του πληροφοριακού συστήματος, τον βαθμό στο οποίο θα έχουν πρόσβαση στα προσωπικά δεδομένα και τις τοποθεσίες από τις οποίες θα υπάρχει πρόσβαση σε αυτό.
   - Το σχέδιο καταγραφής των πληροφοριών και τα σχετικά σχέδια για την διατήρηση και καταστροφή τους.
   - Τα σχέδια για τα αντίγραφα ασφαλείας και ανάκαμψης
   - Την διαχείριση και την προστασία των μετα-δεδομένων

8.1.5 Η προσέγγιση της «Νομολογίας» για την συστηματική περιγραφή

Η σπουδαιότητα της φάσης προετοιμασίας και ειδικά της συστηματικής καταγραφής, έχει αναγνωριστεί και «νομολογιακά» από άποψη Εποπτικής Αρχής. Χαρακτηριστική περίπτωση αποτελεί η Γνωμοδότηση της Ελληνικής Αρχής Προστασίας Προσωπικών Δεδομένων υπ' αριθμόν 3/2022[100], κατά την οποία κλήθηκε η αρχή να γνωμοδοτήσει σχετικά με το Σχέδιο Νόμου του Υπουργείο Εσωτερικών για την ίδρυση και την λειτουργία Κεντρικού Μητρώου Πιστώσεων (ΚΜΠ), σύμφωνα με το οποίο σκοπός του ανωτέρου Μητρώου είναι η αξιολόγηση της πιστοληπτικής ικανότητας των δυνητικών δανειοληπτών και της εν γένει συνδρομής στη λήψη τεκμηριωμένων αποφάσεων χρηματοδότησης με απώτερο στόχο «την ενίσχυση της χρηματοδότησης από το ελληνικό χρηματοπιστωτικό σύστημα της πραγματικής οικονομίας και τη διασφάλιση της χρηματοπιστωτικής σταθερότητας».

Ως εκ τούτου, μέσα από τη συγκεκριμένη γνωμοδότηση της αρχής ζήτησε να καθοριστούν κρίσιμα τεχνικά, οργανωτικά και νομικά ζητήματα, ώστε να διενεργηθεί μία ΕΑΠΔ. Πράγματι, δηλαδή, ζήτησε για την ανάγκη διενέργειας της ΕΑΠΔ να παρασχεθούν και να καταγραφούν πληροφορίες σχετικά με τα δεδομένα, τις τεχνικές και τις οργανωτικές δομές του ανωτέρου συστήματος.

Ειδικότερα, η Αρχή κατ' αρχάς διαπίστωσε την ανάγκη διενέργειας εκτίμησης αντικτύπου, σύμφωνα με το άρθρο 35 παρ.4 σε συνδυασμό με τον εθνικό κατάλογο[101] με τα είδη των πράξεων επεξεργασία που υπόκεινται στην απαίτηση για διενέργεια ΕΑΠΔ και ειδικότερα στην κατηγορία: «1.1 Συστηματική αξιολόγηση, βαθμολόγηση, πρόβλεψη, πρόγνωση και κατάρτιση προφίλ, ιδίως πτυχών που αφορούν την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή ενδιαφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή τις κινήσεις ή την πιστοληπτική ικανότητα των υποκειμένων των δεδομένων».

Από το πρώτο άρθρο (στο οποίο καθιερώνεται ο σκοπός και η σύσταση του εν λόγω Μητρώου) του υποβληθέντος Σχεδίου Νόμου, και ειδικά στις παραγράφους 4 και 5 η Αρχή παρατηρεί ότι γίνεται λόγος για δυνατότητα διαλειτουργικότητα του εν λόγω συστήματος με άλλα συστήματα και ως εκ τούτου επεσήμανε την ανάγκη προσδιορισμού του τρόπου της εν

[100] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Γνωμοδότηση υπ' αριθμόν 3/2022, Αθήνα 25-08-2022, Αριθ. Πρωτ.: 2110

[101] Βλ. απόφαση Αρχής 65/2018, διαθέσιμη στην ιστοσελίδα της Αρχής: https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf

λόγω διαλειτουργικότητας, ίδιως, του τεχνικού τρόπου διασύνδεσης των αναφερομένων συστημάτων στην Εκτίμηση Αντικτύπου.

Επιπλέον, στο δεύτερο εδάφιο της παραγράφου 4 του ΣχΝ προβλεπόταν η δυνατότητα προσφυγής του ΚΜΠ «στα πληροφοριακά συστήματα της Ανεξάρτητης Αρχής Δημοσίων Εσόδων (ΑΑΔΕ), του Γενικού Εμπορικού Μητρώου (ΓΕΜΗ), της ΕΡΓΑΝΗ και εν γένει σε πληροφοριακά συστήματα φορέων του δημόσιου τομέα» χωρίς να εξειδικεύονται περαιτέρω τα επιπλέον πληροφοριακά συστήματα του δημοσίου τομέα. Η Αρχή επεσήμανε την ανάγκη εξειδίκευσης των πληροφοριακών συστημάτων του δημοσίου που προβλεπόταν να υπάρξει δυνατότητα προσφυγής χαρακτηρίζοντας την συγκεκριμένη διατύπωση μη επαρκώς ορισμένη και γενική.

Ακόμη, στην παράγραφο 5 προβλεπόταν, επίσης, η δυνατότητα διασύνδεσης του ΚΜΠ για ανάπτυξη συνεργασιών με αντίστοιχα ΚΜΠ της αλλοδαπής, χωρίς να προσδιορίζεται, εάν αυτά βρίσκονται εκτός ή εντός ΕΕ. Ως εκ τούτου, η Αρχή παρατήρησε ότι έπρεπε να προσδιορισθεί αυτό στη σχετική ΕΑΠΔ, και να αναφερθούν οι κανόνες του κεφαλαίου V βάσει των οποίων θα λάμβανε χώρα η διασυνοριακή μεταβίβαση.

Επιπρόσθετα, στο άρθρο 3 παρ.3 του υποβληθέντος ΣχΝ ορίζεται η Τράπεζα της Ελλάδος (ΤτΕ) ως υπεύθυνος επεξεργασίας και προσδιορίζονταν οι ειδικότερες αρμοδιότητες της. Η Αρχή πρότεινε να προστεθεί στην εν λόγω παράγραφο και η υποχρέωση της ΤτΕ ως υπευθύνου επεξεργασίας για διενέργεια ΕΑΠΔ, Όπως, αναφέρθηκε εξάλλου σε αυτή τη φάση πρέπει να καθοριστούν τα ενδιαφερόμενα – εμπλεκόμενα μέρη και να αποδοθούν σε καθένα από αυτά οι ευθύνες που έχουν σε σχέση με την επεξεργασία προσωπικών δεδομένων. Ως εκ τούτου, η Αρχή επεσήμανε την τροποποίηση της εν λόγω παραγράφου για μεγαλύτερη ασφάλεια δικαίου.

Περαιτέρω, με το άρθρο 4 προσδιορίζεται η διαδικασία και οι προϋποθέσεις παροχής δεδομένων στο ΚΜΠ από τους πιστωτές. Η Αρχή επισήμανέ, κατ' αρχάς, ότι θα πρέπει να προσδιορισθεί στο ΣχΝ ο τρόπος διαβίβασης των προς καταχώριση δεδομένων σε ηλεκτρονική μορφή και να προσδιορισθούν αντιστοίχως στην ΕΑΠΔ τα σχετικά μέτρα ασφαλείας για την εν λόγω διαβίβαση. Επιπλέον, στην παράγραφο 3 προβλεπόταν υποχρέωση των πιστωτών για ηλεκτρονική σύνδεση με το ΚΜΠ. Η Αρχή παρατήρησε ότι δεν αναφερόταν στο ΣχΝ ο τρόπος της εν λόγω σύνδεσης και ως εκ τούτου επεσήμανε ότι στην ΕΑΠΔ θα πρέπει να συμπεριληφθούν οι σχετικές απαιτήσεις ασφαλείας. Περαιτέρω, για την υποχρέωση παροχής επιπρόσθετων δεδομένων από τους πιστωτές προς την Τράπεζα μετά από αίτημα της τελευταίας

επισημαίνεται ότι θα πρέπει να διευκρινισθεί ειδικότερα η εν λόγω διαδικασία (καθώς και οι γενικότερες απαιτήσεις ασφαλείας στην ΕΑΠΔ) και να οριστεί στο ΣχΝ ότι τα εν λόγω δεδομένα θα παρέχονται σε μορφή που δεν επιτρέπει ταυτοποίηση υποκειμένων φυσικών προσώπων, καθώς ο σκοπός της εν λόγω επιπρόσθετης παροχής είναι η εκπόνηση οικονομικών αναλύσεων και στατιστικών μελετών. Η αρχή επεσήμανε ότι στην ΕΑΠΔ αυτονοήτως θα πρέπει να αναφέρεται η ως άνω μορφή καθώς και οι σχετικές τεχνικές διαδικασίες.

Στο άρθρο 6 του υποβληθέντος ΣχΝ καθορίζονται οι φορείς που έχουν πρόσβαση στα δεδομένα οικονομικής συμπεριφοράς του ΚΜΠ. Η Αρχή παρατήρησε ότι θα πρέπει να διευκρινιστεί ένα όλοι οι υπάλληλοι του πιστωτή έχουν δικαίωμα πρόσβασης στο ΚΜΠ ή υπάρχει σχετικός περιορισμός, καθώς και αν παρέχονται ατομικοί ή ομαδικού λογαριασμού πρόσβασης και αντίστοιχα αν γίνεται καταγραφή προσωποποιημένης (ατομικής) πρόσβασης.

Επιπλέον, στο άρθρο 7 του υποβληθέντος ΣχΝ προβλεπόταν η διαδικασία χορήγησης από την ΤτΕ της Πιστωτικής Έκθεσης στον αιτούνται και καθορίζονταν οι σχετικοί όροι. Επιπλέον, στο τέλος της παραγράφου 1 του άρθρου παρεχόταν μια γενική αναφορά στο σύνολο των δικαιωμάτων του ΓΚΠΔ. Η Αρχή επεσήμανε ότι πρέπει να γίνει σαφής αναφορά και την υποχρέωση της ΤτΕ ως υπευθύνου επεξεργασίας για ενημέρωση του υποκειμένου για την εν λόγω αίτηση προκειμένου το υποκείμενο να είναι σε θέση να ασκήσει τα εν λόγω δικαιώματα.

Στο άρθρο 8 του ΣχΝ προβλεπόταν η αυτοματοποιημένη συλλογή των δεδομένων οικονομικής συμπεριφοράς και εξειδικεύονταν περαιτέρω οι λειτουργίες του ΚΜΠ. Παρόλα αυτά, στην παράγραφο 2 του εν λόγω άρθρου γινόταν μόνο ενδεικτική απαρίθμηση των ειδικότερων λειτουργιών. Ως εκ τούτου η Αρχή επεσήμανε ότι η απαρίθμηση δεν θα έπρεπε να διατυπώνεται ενδεικτικά αλλά αποκλειστικά με σαφώς προσδιορισμένους στο ΣχΝ σκοπούς. Επιπροσθέτως, επεσήμανε την εξειδίκευση και προσδιορισμού στην ΕΑΠΔ του τρόπου με τον οποίο θα διενεργούνταν η αυτοματοποιημένη επεξεργασία.

Με το άρθρο 9 προσδιορίζονταν τα δικαιώματα των υποκειμένων των δεδομένων κατ' εφαρμογή των διατάξεων 12 – 22 ΓΚΠΔ και τα αντίστοιχα του ν.4624/2018 των άρθρων 33-35 για την άσκηση των οποίων, όπως προβλεπόταν στο εν λόγω άρθρο, θα ενημερώνονταν σχετικά, χωρίς ωστόσο να προσδιορίζεται ειδικότερα σε ποιο στάδιο και με ποιον τρόπο θα γινόταν η εν λόγω ενημέρωση. Η Αρχή επεσήμανε την ανάγκη προσδιορισμού των υποχρεώσεων της ΤτΕ, ως υπευθύνου επεξεργασία, για την εκπλήρωση των σχετικών ως άνω δικαιωμάτων των υποκειμένων των δεδομένων, ενώ προσθέτει ότι όσον αφορά την

ηλεκτρονική υποβολή αιτήσεων προς εκπλήρωση των ως άνω δικαιωμάτων πρέπει να περιληφθούν στην ΕΑΠΔ τα μέτρα εκείνα που εγγυώνται την ασφάλεια της διαδικασίας.

Στο άρθρο 10 του ΣχΝ προβλεπόταν η δυνατότητα του ΚΜΠ να διαλειτουργεί και να ανταλλάσσει πληροφορίες «με βάση δεδομένων του δημοσίου τομέα ή φορέων ιδιωτικού τομέα ή φορέων πιστοληπτικής αξιολόγησης, καθώς και με κάθε άλλο ηλεκτρονικό σύστημα δημοσίου ή άλλου φορέα ή με αρμόδιες υπηρεσίες για την παροχή πληροφριών στο πλαίσιο εκπόνησης οικονομικών αναλύσεων ή στατιστικών μελετών με βάση τα δεδομένα που τηρεί», ενώ οι ως άνω πληροφορίες δεν θα επέτρεπαν τον προσδιορισμό της ταυτότητας των υποκειμένων των δεδομένων οικονομικής συμπεριφοράς. Η Αρχή επεσήμανε, λοιπόν, ότι έπρεπε να επεξηγηθεί στην ΕΑΠΔ ο τρόπος που θα επιτυγχάνονταν η εν λόγω διαλειτουργικότητα και να εξειδικευθεί η μορφή των δεδομένων, έτσι ώστε να είναι σαφές ότι δεν θα προέκυπτε ταυτοποίηση φυσικών προσώπων.

Τέλος, στο άρθρο 11 του ΣχΝ προτείνονταν να προστεθεί στο σώμα του ίδιου του νόμου η υποχρέωση διενέργειας ΕΑΠΔ καθώς και η εκπόνηση Αλγοριθμικής Εκτίμησης Αντικτύπου.

Φαίνεται, λοιπόν, και από την εν λόγω γνωμοδότηση της Αρχής, ότι, όντως, το ζητούμενο της συστηματικής περιγραφής πρέπει να προσεγγίζεται ολιστικά από μία τεχνική, οργανωτική και νομική σκοπιά. Συνοψίζοντας, η Αρχή έθεσε στο επίκεντρο αυτής, τόσο ζητήματα τεχνικά (π.χ. πως επιτυγχάνεται η διαλειτουργικότητα του συστήματος, ποια είναι εκείνα τα τεχνικά μέτρα ασφαλείας που εγγυώνται την ασφάλεια, με ποιο τρόπο θα έχουν πρόσβαση οι χρήστες κτλ.), όσο λειτουργικά – οργανωτικά (π.χ. να καθοριστούν οι ευθύνες των εμπλεκόμενων μερών, να καθοριστούν τα μέρη που θα έχουν πρόσβαση στο εν λόγω σύστημα) και νομικά (π.χ. να παρέχεται ενημέρωση στα υποκείμενα των δεδομένων, να αποδοθούν ευθύνες στα εμπλεκόμενα μέρη κτλ.).

Ως εκ τούτου, η προσέγγιση της Αρχής φαίνεται να επαληθεύει τις μεθοδολογικές προσεγγίσεις που αναπτύχθηκαν παραπάνω, χωρίς όμως, όπως προαναφέρθηκε, να είναι δυνατόν να θεωρηθεί μόνον μία προσέγγιση ως «πανάκια». Για αυτό τον λόγο το συγκεκριμένο στάδιο δημιουργεί σαφές πρόβλημα στους διενεργούντες την ΕΑΠΔ, καθώς αποτελεί το πιο πολύπλοκο κομμάτι της διαδικασίας.

8.1.6 Μία λύση στο πρόβλημα της πολυπλοκότητας της συστηματικής περιγραφής.

Ένα μεγάλο πρόβλημα που μπορεί να δημιουργηθεί κατά το στάδιο της συστηματικής περιγραφής της επεξεργασίας είναι να καθορίσει ο διενεργών την επεξεργασία το πόσο

λεπτομερής πρέπει να είναι η περιγραφή της όλης επεξεργασίας. Αυτό είναι λογικό, καθώς το επίπεδο της αφαιρετικής σκέψης μπορεί να είναι πολύ διαφορετικό τόσο μεταξύ των ανθρώπων που θα διενεργήσουν την περιγραφή, όσο και για το πως θα γίνει αυτή. Ο διενεργών αυτού του σταδίου, λοιπόν, μπορεί να βρεθεί αντιμέτωπος με το πρόβλημα μέχρι ποιο βαθμό πρέπει να περιγράψει την επεξεργασία. Γενικά, αναφέρεται ότι η περιγραφή δεν θα πρέπει να είναι ούτε υπερβολικά λεπτομερής και να «χάνεται» η ουσία σε αμέτρητες τεχνικές λεπτομέρειες, αλλά ούτε και πρόχειρη[102]. Είναι δύσκολο να βρεθεί ένας γενικός κανόνας, που να επιλύει αυτό το πρόβλημα. Όπως αναφέρθηκε και παραπάνω, σκοπός της περιγραφής θα πρέπει πάντα να είναι να καθοριστεί το πλαίσιο και τα όρια της επεξεργασίας και να προκύπτουν από αυτή αξιόπιστα αποτελέσματα, πάνω στα οποία θα μπορέσει να βασιστεί ο εντοπισμός, η ανάλυση και η εκτίμηση των κινδύνων, λαμβάνοντας υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

Η τεχνολογική ανάπτυξη και η ενσωμάτωση από όλους τους φορείς ολοένα και πιο σύνθετων τεχνολογικών υποδομών, όπως οι υπηρεσίες υπολογιστικού νέφους και τεχνολογίες αιχμής, καθιστά την καταγραφή της επεξεργασίας ολοένα και πιο περίπλοκη στην πράξη για τους υπευθύνους επεξεργασίας. Ειδικότερα, η χρήση των εν λόγω τεχνολογιών δημιουργεί δυσκολίες για τους υπευθύνους επεξεργασίας στο να αποκτήσουν τις απαιτούμενες πληροφορίες για να κατανοήσουν (και εν τέλει να αποτυπώσουν) τον τρόπο με τον οποίο τελείται η επεξεργασία. Αυτό αφορά κυρίως επεξεργασίες, όπου χρησιμοποιούνται για την πραγματοποίηση τους, εκτελούντες την επεξεργασία πολυεθνικές εταιρείες που παρέχουν τυποποιημένες υπηρεσίες ΤΠΕ, όπως υπηρεσίες υπολογιστικού νέφους (standard cloud services). Ως εκ τούτου, δεν είναι εύκολο να αποτυπωθεί από τους διενεργούντες την εκτίμηση αντικτύπου ο τρόπος με τον οποίο διενεργείται η επεξεργασία με έναν διαφανή και επαληθεύσιμο τρόπο.

Η παραπάνω αδυναμία εντοπίστηκε από την διοίκηση της Ολλανδίας. Βασισμένη στο πρότυπο της Autoritet Persoongevens[103], το Υπουργείο Δικαιοσύνης της Ολλανδίας σε συνεργασία με τις εταιρείες Google, Microsoft και Amazon διενήργησαν εκτίμηση Αντικτύπου τύπου «Ομπρέλα»[104]. Ειδικότερα, η εν λόγω ΕΑΠΔ διενεργήθηκε για να εκτιμήσει τους κινδύνους που δημιουργούνται από την χρήση των υπηρεσιών που προσφέρονται από την εταιρεία AMAZON AWS και από τα προϊόντα της τελευταίας, Amazon Elastic Compute Cloud

[102]Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact Assessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag.
[103] Πρόκειται για την Αρχή Προστασίας Προσωπικών Δεδομένων της Ολλανδίας, https://autoriteitpersoonsgegevens.nl/en
[104] Voer titel in (slmmicrosoftrijk.nl) (Τελευταία επίσκεψη 23/11/2023)

(Amazon EC2), Amazon Simple Storage Service (Amazon S3) και Amazon RDS λειτουργώντας με μία βάση δεδομένων MySQL. Τα συγκεκριμένα προϊόντα αποτελούν υποστηρικτικά στοιχεία τα οποία χρησιμοποιεί ολόκληρο το Ολλανδικό κράτος για να υποστηρίζει τις λειτουργίες των πληροφοριακών του συστημάτων και πάνω στα οποία μπορεί να βασιστούν μετέπειτα επεξεργασίες κάθε αρμόδιας αρχής για το κράτος της Ολλανδίας. Ως εκ τούτου, η συγκεκριμένη εταιρεία λειτουργεί ως Εκτελών την Επεξεργασία για κάθε έναν υπεύθυνο επεξεργασίας που χρησιμοποιεί τα προϊόντα της για να αναπτύξει περαιτέρω εφαρμογές. Η συγκεκριμένη ΕΑΠΔ δεν καλύπτει την υποχρέωση κάθε ξεχωριστού Υπευθύνου Επεξεργασίας (δημόσιας αρχής/φορέα)[105] να διενεργήσει από μόνη της ΕΑΠΔ όταν αυτή απαιτείται, αλλά διενεργήθηκε με σκοπό να βοηθήσει τους υπευθύνους επεξεργασίας να κατανοήσουν ,μέσα από αυτή, τον τρόπο λειτουργίας τους και μέσω αυτού να κατανοήσουν τον τρόπο επεξεργασίας για να μπορέσουν να διενεργήσουν με την σειρά τους την ΕΑΠΔ, όπου και όποτε αυτό απαιτείται.

9. Δεύτερη φάση της ΕΑΠΔ (Φάση Υλοποίησης)

Έχοντας ολοκληρώσει όλα τα προηγούμενα στάδια, πλέον, είναι δυνατόν να εξεταστούν οι κίνδυνοι, που εκτιμάται ότι θα προκαλέσει η σχεδιαζόμενη επεξεργασία, αξιοποιώντας όλη την πληροφορία που έχει συλλεχθεί κατά το προηγούμενο στάδιο. Ειδικότερα, ο Υπεύθυνος επεξεργασίας βασιζόμενος πάνω στην συστηματική καταγραφή της πληροφορίας που έχει προηγηθεί, πρέπει να εκτιμήσει τους κινδύνους που μπορεί να προκαλέσει η υπό εξέταση επεξεργασία.

Είναι χρήσιμο να παρατεθούν τα κριτήρια που καθιστούν μία ΕΑΠΔ αποδεκτή, όπως τα θέτει η ομάδα εργασίας του άρθρου 29 για το συγκεκριμένο στάδιο. Ειδικότερα, μία ΕΑΠΔ θα πρέπει να θέτει υπό διαχείριση τους κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και ειδικότερα να έχουν αξιολογηθεί η προέλευση, η φύση, η ιδιαιτερότητα και η σοβαρότητα των κινδύνων (αιτιολογική σκέψη 84) ή ειδικότερα κάθε κίνδυνος (αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση, και εξαφάνιση δεδομένων) από την οπτική των υποκειμένων των δεδομένων. Να έχουν ληφθεί υπόψη οι πηγές των κινδύνων (αιτιολογική σκέψη 90)· Να εξακριβώνονται οι δυνητικές επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων σε περιπτώσεις συμβάντων που περιλαμβάνουν

[105] Ό.π.σελ.11

αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων. Να εξακριβώνονται απειλές που θα μπορούσαν να επιφέρουν αθέμιτη πρόσβαση, ανεπιθύμητη τροποποίηση και εξαφάνιση δεδομένων. Να εκτιμώνται η πιθανότητα και η σοβαρότητα (αιτιολογική σκέψη 90). Να καθορίζονται τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (άρθρο 35 παράγραφος 7 στοιχείο δ) και αιτιολογική σκέψη 90)·

Η εκτίμηση και η διαχείριση του κινδύνου υπάρχει, ήδη, εδώ και πολλές δεκαετίες σε διάφορους τομείς της επιστήμης και της οικονομίας (π.χ. στον Τραπεζικό τομέα, στην Ναυτιλία, στην Πληροφορική, στην Οικονομία, στον κλάδο των τροφίμων κτλ.)[106] και ως εκ τούτου έχουν δημιουργηθεί πολλά πρότυπα διαχείρισης κινδύνων. Ωστόσο, στα περισσότερα από αυτά οι διεργασίες εκτίμησης αντικτύπου για την προστασία των δεδομένων δεν περιλαμβάνονται και δεν είναι συχνά ενσωματωμένες στο ευρύτερο πλαίσιο διαχείρισης κινδύνου ενός οργανισμού, ενώ είναι ακόμη λιγότερο συσχετισμένες με τις εσωτερικές του διαδικασίες (Business, Organizational processes)[107]. Επιπλέον, αυτά τα μοντέλα δεν θέτουν στο επίκεντρο τους τα υποκείμενα των δεδομένων αλλά τους οργανισμούς και τα στοιχεία αυτών. Προσπαθούν, δηλαδή, να περιορίσουν τον κίνδυνο με επίκεντρο, όμως, τα περιουσιακά στοιχεία των οργανισμών, σε αντίθεση με την ΕΑΠΔ που εξετάζει τον κίνδυνο με επίκεντρο τα υποκείμενα των δεδομένων, τις ελευθερίες και τα δικαιώματά τους.

Ο ΓΚΠΔ δεν επιτάσσει να χρησιμοποιηθεί ένας συγκεκριμένος τρόπος για την διαχείριση του κινδύνου. Ως εκ τούτου ο υπεύθυνος επεξεργασίας είναι αυτός που φέρει το «βάρος» να διαμορφώσει τον τρόπο με τον οποίο θα εκτιμήσει τους κινδύνους της επιδιωκόμενης επεξεργασίας[108].

9.1 Γενική επισκόπηση του κινδύνου στο πλαίσιο της ΕΑΠΔ.

Πριν την ανάπτυξη της συγκεκριμένης φάσης μέσα από την οπτική των μεθοδολογικών προσεγγίσεων, θεωρείται αναγκαίο να αναπτυχθεί πρωτίστως η έννοια του κινδύνου, όπως αυτός παρουσιάζεται στον ΓΚΠΔ, μέσα από το πρίσμα του νόμου και της θεωρίας.

[106]Βλ. π.χ. X. Huang, Yuanqiao Wen, F. Zhang, H. Han, Y. Huang, Z. Sui,A review on risk assessment methods for maritime transport,Ocean Engineering,Volume 279, 2023,114577, ISSN 0029-8018,. (Στη συγκεκριμένη εργασία αξιολογήθηκαν 1181 papers που έχουν γραφτεί σχετικά με την διαχείριση κινδύνου στον τομέα της Ναυτιλίας)

[107] ΔιΤΕ. Ν. Λουκάς, «Η Έννοια και η Διαχείριση του «Κινδύνου» στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).

[108] Βλ.UK Information Commissioner's Office (ICO) (2014). "Conducting Privacy Impact Assessments: Code of Practice, Σελ 21 – 22.URL: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of practice.pdf (visited on 12-12-2023)

Ως σημείο εκκίνησης, λοιπόν, πρέπει να θεωρηθεί κατ' αρχάς το γεγονός ότι εξ' ορισμού κάθε επεξεργασία προσωπικών δεδομένων είναι μια διαδικασία που δημιουργεί κινδύνους. Η ολοένα και μεγαλύτερη ανάπτυξη της τεχνολογίας κατ΄ επέκταση δημιουργεί ολοένα και μεγαλύτερους κινδύνους για τα υποκείμενα, και ολοένα και περισσότεροι νόμοι εκδίδονται, ώστε, να αποτρέψουν την επέλευση τους, καθορίζοντας νέα δικαιώματα ή τροποποιώντας καταλλήλως παλαιότερα δικαιώματα, ώστε, να ρυθμίσουν νέους κινδύνους και να παρέχουν πιο αποτελεσματική προστασία (Μία τέτοια περίπτωση είναι και ο ΓΚΠΔ.)[109] Ο νομοθέτης εξάλλου, υπογραμμίζει την παραπάνω θέση στο άρθρο 24 του ΓΚΠΔ σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να αποδεικνύει ότι η επεξεργασία γίνεται σύμφωνα με τον ΓΚΠΔ, λαμβάνοντας, όμως, υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο, τους σκοπούς της επεξεργασίας καθώς και τους κινδύνους διαφορετικής πιθανότητας προέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Έτσι, λοιπόν, ο νομοθέτης θέτει τον κίνδυνο ως καθοριστικό κριτήριο για τον καθορισμό των μέτρων που πρέπει να παρθούν. Οι νομικές υποχρεώσεις, λοιπόν, του υπευθύνου επεξεργασίας βασίζονται πάνω στους κινδύνους που μπορεί να επιφέρει η επεξεργασία που διενεργεί, προσδίδοντας έτσι μία κλιμάκωση στις υποχρεώσεις που απορρέουν γενικά από τον ΓΚΠΔ. Αυτή ακριβώς η κλιμάκωση είναι άρρηκτα συνδεδεμένη με την Αρχή της Λογοδοσίας. Αφού, λοιπόν, δεν εμφανίζουν όλες οι επεξεργασίας τον ίδιο βαθμό κινδύνου, έτσι δεν χρειάζεται να λαμβάνουν ακριβώς τα ίδια μέτρα, ώστε, να διασφαλίζουν ότι συμμορφώνονται με τον ΓΚΠΔ. Χαρακτηριστικότερο παράδειγμα αυτής της έκφανσης του κινδύνου αποτελεί η υποχρέωση διενέργειας εκτίμησης αντικτύπου, καθώς είναι ο πιο βασικός λόγος να θεωρηθεί ότι ο υπεύθυνος επεξεργασίας παραβιάζει τον κανονισμό, καθώς δεν εκτίμησε σωστά τους κινδύνους.

Παρόλα αυτά, η νομική υποχρέωση που απορρέει από το άρθρο 35 του ΓΚΠΔ, η υποχρέωση δηλαδή διενέργειας εκτίμησης αντικτύπου , απαιτεί ο κίνδυνος να είναι υψηλός. Η συστηματική προσέγγιση του κινδύνου (μέσω της ΕΑΠΔ) είναι μια πρωτοπορία που εισάγει ο ΓΚΠΔ από την άποψη ότι ο κίνδυνος στον τομέα του δικαίου προσωπικών δεδομένων πρέπει να εκτιμηθεί πρωτίστως μέσα στο γενικό πλαίσιο των «δικαιωμάτων και των ελευθεριών των φυσικών προσώπων» και δευτερευόντως μεθοδολογικά μέσω των εργαλείων διαχείρισης κινδύνων (τα οποία όπως προαναφέρθηκε είναι γνωστά σε πολλούς κλάδους της επιστήμης και

[109] Βλ. Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of 'high risk' in the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6, 2019, 105342

του επιχειρείν εδώ και χρόνια)[110]. (Αυτός είναι και ο βασικός λόγος που προηγείται μία προσέγγιση της φύσης του κινδύνου στο πλαίσιο του δικαίου προστασίας δεδομένων, όπως προαναφέρθηκε)

Λεπτομερέστερα, στην περίπτωση της ΕΑΠΔ το γεγονός του ότι πρέπει ο κίνδυνος να είναι υψηλός προκειμένου να ενταχθεί ο υπεύθυνος επεξεργασίας στην υποχρέωση διενέργειας εκτίμησης αντικτύπου, καταδεικνύει ότι υπάρχουν ποιοτικά κριτήρια. Σύμφωνα με την ομάδα εργασίας του άρθρου 29, «ο κίνδυνος είναι ένα υποθετικό σενάριο που περιγράφει ένα γεγονός και τις συνέπειες του εκτιμώντας την σοβαρότητα και την πιθανότητα. Μάλιστα, το γεγονός ότι η σοβαρότητα και η πιθανότητα πρέπει να ληφθούν υπόψη καταδεικνύεται και από τις αιτιολογικές σκέψεις του ΓΚΠΔ. υπ' αριθμόν 75 και 76. Έτσι, προκειμένου ο Υπεύθυνος Επεξεργασίας να φθάσει στο συμπέρασμα ότι κάποιο γεγονός αποτελεί κίνδυνο πρέπει πρωτίστως να αξιολογήσει πόσο σοβαρό και πιθανό είναι να επέλθει. Ωστόσο, αυτό μόνο δεν αρκεί, καθώς είναι κρίσιμο να καθοριστεί ο τρόπος με τον οποίο θα γίνει η αξιολόγηση της σοβαρότητας και της πιθανότητας. Έτσι, λοιπόν, γίνεται μία τριπλή αξιολόγηση η πρώτη εκ των οποίων ανάγεται στο «Τι αποτελεί κίνδυνο» ενώ η δεύτερη και η Τρίτη στο πόσο υψηλός είναι αυτός με τα κριτήρια της σοβαρότητας και της πιθανότητας αντίστοιχα. Επιπλέον, ο νομοθέτης απαιτεί η προαναφερθείσα τριπλή αξιολόγηση να είναι αντικειμενική.[111] Το ερώτημα που δημιουργείται, λοιπόν, είναι το πως θα επιτευχθεί αυτή η αντικειμενικότητα δεδομένου ότι τα σενάρια που εξετάζονται ως κίνδυνοι (η σοβαρότητα και η πιθανότητα αυτών) είναι υποθετικά. Ως εκ τούτου, το ζητούμενο της αξιολόγησης των κινδύνων είναι μέσα από την συστηματική προσέγγιση της εκτίμηση αντικτύπου να προκύψουν αξιόπιστα, επαληθεύσιμα, έμπιστα και αμφισβητήσιμα συμπεράσματα.[112] Όποια μεθοδολογική προσέγγιση, λοιπόν, και να εφαρμόσει ο Υπεύθυνος επεξεργασίας για να θεωρηθεί επιτυχής θα πρέπει να πληροί τα ανωτέρω κριτήρια.

9.1.1 Η προσέγγιση του Fraunhofer Institute.

Ξεκινώντας με την μεθοδολογική προσέγγιση Fraunhofer αναφέρεται εξ αρχής ότι η συγκεκριμένη φάση έχει τρεις σκοπούς. Ο πρώτος από αυτούς είναι να αξιολογηθεί ο κίνδυνος της σχεδιαζόμενης επεξεργασίας σε σχέση με τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων (αρ.35 παρ.7 περ. γ΄ ΓΚΠΔ), ενώ δεύτερο στόχο αποτελεί η επιλογή των

[110] Βλ. Ό.π. K. Demetrzou, Σελ. 5
[111] Βλ. Αιτιολογική Σκέψη 76 ΓΚΠΔ.: «… Ο κίνδυνος θα πρέπει να αξιολογείται βάσει αντικειμενικής εκτίμησης, με την οποία διαπιστώνεται κατά πόσον οι πράξεις επεξεργασίας δεδομένων συνεπάγονται κίνδυνο ή υψηλό κίνδυνο.»
[112] Βλ. Ό.π. K. Demetrzou, Σελ. 6

κατάλληλων μέτρων για την αντιμετώπιση των κινδύνων και την διασφάλιση της ασφαλούς επεξεργασίας,. Ο τρίτος στόχος είναι η αξιολόγηση της αναγκαιότητας και της καταλληλόλητας, η οποία (αξιολόγηση) σε αυτή την φάση πληροί τα κριτήρια του νόμου σύμφωνα με το άρθρο 35 παρ.7. περ. β', σε αντίθεση με την ίδια αξιολόγηση που είχε προηγηθεί κατά το στάδιο της απαραίτητης προεργασίας, που, όπως αναλύθηκε, γίνεται μονάχα για να προληφθούν εξόφθαλμες παραβιάσεις.

9.1.1.1. Συμμετοχική μέθοδος για την ανάλυση της ΕΑΠΔ (Participatory workshop-based method)

Η συγκεκριμένη μεθοδολογική προσέγγιση θέτει στο επίκεντρο της, την συμμετοχή στην διενέργεια εκτίμησης αντικτύπου όλων των εμπλεκόμενων φορέων (ή έστω αντιπροσώπων τους) και θεωρεί πως αυτή η συμμετοχική προσέγγιση μειώνει τις πιθανότητες του να παραλειφθεί από την μελέτη κάποιος ουσιώδης παράγοντας (π.χ. κάποιο εμπλεκόμενο μέρος στην επεξεργασία) . Ως εκ τούτου θεωρεί ότι στη συγκεκριμένη φάση πρέπει να «ενωθεί» ολόκληρη η ομάδα που θα διενεργήσει την ΕΑΠΔ η οποία θα περιλαμβάνει, εκτός από τους ειδικούς, και αντιπροσώπους των εμπλεκόμενων φορέων και των υποκειμένων που πρόκειται να επηρεάσει η σχεδιαζόμενη επεξεργασία για να διενεργηθεί η εκτίμηση του κινδύνου στο πλαίσιο ενός «εργαστηρίου».

Ως εκ τούτου, το υλικό που έχει συλλεχθεί κατά την πρώτη και δεύτερη φάση πρέπει να είναι διαθέσιμο σε όλα τα μέλη του εργαστηρίου και να αποτελέσουν την βάση πάνω στην οποία θα θεμελιωθεί και η εκτίμηση των κινδύνων. Έτσι, καθίσταται σαφές ότι όλα τα μέλη που απαρτίζουν την ομάδα διενέργειας της εκτίμησης αντικτύπου έχουν κοινή αντίληψη και κοινές βάσεις για την σχεδιαζόμενη επεξεργασία, γεγονός που είναι απαραίτητο για την εκπλήρωση της απαίτησης

Την παραπάνω προσέγγιση φαίνεται να επαληθεύει και η Αρχή με την γνωμοδότηση υπ' αριθμόν 4/2020 της, όπου και επεσήμανε ότι όταν εμπλέκονται κατά το στάδιο σύνταξης της ΕΑΠΔ (καθώς και στην δημοσίευση της) τα υποκείμενα των δεδομένων και έμπειροι φορείς αυξάνεται η διαφάνεια και επιτυγχάνεται ως εκ τούτου μεγαλύτερη εμπιστοσύνη στην επεξεργασία.[113] Επιπλέον, θα πρέπει να είναι σαφές το ποια πρόσωπα συμμετείχαν στην διαδικασία και με ποια ιδιότητα αλλά και σε ποιο συγκεκριμένο στάδιο. Έτσι, λοιπόν, δεν αρκεί μία απλή αναφορά στο ότι συμμετείχαν εκπρόσωποι των εκτελούντων ή των υποκειμένων,

[113]Βλ.ΑΠΔΠΧ, Γνωμοδότηση υπ' αριθμόν 4/2020, Αριθμ. Πρωτ.: Γ/ΕΞ/6031/07-09-2020, σελ 20.

αλλά θα πρέπει να προσδιορίζονται οι ρόλοι, το στάδιο της διαδικασίας και η ιδιότητα των συμμετεχόντων.[114]

9.1.1.2. Ο ορισμός του κινδύνου στον ΓΚΠΔ

Παρόλο που ο ΓΚΠΔ δεν δίνει έναν σαφή ορισμό του τι είναι ο κίνδυνος, η μεθοδολογία του Fraunhofer επιχειρεί να δώσει έναν ορισμό, ο οποίος προκύπτει από τις αιτιολογικές σκέψεις υπ' αριθμόν 75 και 94 του ΓΚΠΔ και από το Short Paper No.18 όπως αυτό προέκυψε από το «Data Protection Conference »[115]. Ειδικότερα, ο ορισμός διαμορφώνεται ως εξής: «Κίνδυνο κατά την έννοια του ΓΚΠΔ αποτελεί η ύπαρξη της πιθανότητας ενός γεγονότος το οποίο από μόνο του αποτελεί ζημία (περιλαμβάνοντας της αδικαιολόγητη παρέμβαση στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων) ή που μπορεί να οδηγήσει σε περαιτέρω ζημία σε ένα ή περισσότερα φυσικά πρόσωπα. Έχει δύο διαστάσεις, η πρώτη εκ των οποίων αποτελεί ή σοβαρότητα της ζημίας και την δεύτερη η πιθανότητα να επέλθει το γεγονός και να προκληθεί η ζημία».

Βάσει αυτού του ορισμού εγείρονται τρία κρίσιμα ερωτήματα τα οποία θα πρέπει να απαντηθούν. Πρώτον, τι αποτελεί «Ζημία» (περιλαμβάνοντας την αδικαιολόγητη παρέμβαση στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων), τι αποτελεί «γεγονός» και πως αξιολογείται η σοβαρότητα και η πιθανότητα. Ως εκ τούτου, αυτά αναλύονται κατωτέρω.

9.1.1.3. Είδη Ζημίας

Στο δίκαιο της Ένωσης με τον όρο «Δικαιώματα και Ελευθερίες των φυσικών προσώπων» νοούνται όλα τα θεμελιώδη δικαιώματα που περιλαμβάνει ο Χάρτης των Θεμελιωδών Δικαιωμάτων και η Ευρωπαϊκή Σύμβαση για τα δικαιώματα του Ανθρώπου. Όπως έχει ήδη αναφερθεί, το άρθρο 35 του ΓΚΠΔ απαιτεί η εκτίμηση αντικτύπου να λαμβάνει υπόψη όλα αυτά τα δικαιώματα που περιλαμβάνονται στα ανωτέρω νομοθετήματα.

Παρόλο που εκ πρώτης όψεως η απαίτηση του άρθρου 35 μπορεί να θεωρηθεί κάπως ασαφής (καθώς δεν παρέχει κάποια διευκρίνιση με τα είδη της ζημίας), η λύση έρχεται λαμβάνοντας υπόψη την αιτιολογική σκέψη υπ' αριθμόν 75 που δίνει σαφή παραδείγματα και περιπτώσεις για το τι αποτελεί εν τέλει ζημία σε σχέση με τις ελευθερίες και τα δικαιώματα των υποκειμένων. Η αιτιολογική σκέψη 75 προβαίνει σε μία πρώτη μεγάλη διάκριση που γίνεται σε τρεις βασικές κατηγορίες. Πρώτη κατηγορία αποτελούν οι σωματικές βλάβες, δεύτερη οι υλικές βλάβες και τρίτη οι μη υλικές βλάβες.

[114]Βλ. ΑΠΔΠΧ, Ό.π. σελ.21

[115] Πρόκειται επιτροπή που αποτελείται από όλες τις ανεξάρτητων αρχές των κρατιδίων της Γερμανίας και συνεδριάζει δύο φορές τον χρόνο με κυλιόμενη προεδρεία.

Ως εκ τούτου, σύμφωνα με την προσέγγιση Fraunhofer στις σωματικές βλάβες περιλαμβάνονται περιπτώσεις όπου τα δεδομένα υγείας κάποιου υποκειμένου είναι λανθασμένα και ως εκ τούτου οδηγούν σε λανθασμένη ιατρική γνωμάτευση ή αγωγή – θεραπεία. Επιπλέον, σε αυτή την κατηγορία θα μπορούσε να υποπέσει και η περίπτωση ψυχολογικών επιπτώσεων, όπως στην περίπτωση που αποκαλυφθούν, παρανόμως, δεδομένα σε σχέση με την θρησκεία, τον σεξουαλικό προσανατολισμό ή των ποινικών διώξεων που έχουν ασκηθεί σε κάποιο φυσικό πρόσωπο.

Η δεύτερη κατηγορία αποτελείται από τις υλικές βλάβες, ο οποίες σχετίζονται κυρίως με βλάβες που έχουν οικονομικές συνέπειες. Πλέον, και ειδικά όσο η οικονομία ψηφιοποιείται, η παραβίαση των αρχών προστασίας προσωπικών δεδομένων μπορούν να οδηγήσουν σε τέτοιου είδους βλάβες. Χαρακτηριστικό παράδειγμα αποτελούν τα ψηφιακά φορολογικά στοιχεία τα οποία, αν είναι αναληθή, μπορούν να οδηγήσουν σε αδικαιολόγητα πρόστιμα. Επιπλέον, σε αυτή την κατηγορία περιλαμβάνεται η κλοπή ταυτότητας με σκοπούς εξαπάτησης ή ξέπλυμα «βρώμικου» χρήματος. Ακόμη, ζημίες που σχετίζονται με την εργασία εμπίπτουν στην συγκεκριμένη κατηγορία, όπως για παράδειγμα όταν ελέγχονται οι υπάλληλοι ή παρανόμως παρακολουθούνται και ως εκ τούτου κρίνονται από μη διαφανείς διαδικασίες για την παραμονή τους στον εκάστοτε εργοδότη ή για την προαγωγή τους. Τέλος πολύ σημαντικές οικονομικές ζημίες μπορεί να προκληθούν αν υπάρξει παραβίαση των δεδομένων στα μεγάλα τραπεζικά ψηφιακά συστήματα με αποτέλεσμα να παραβιασθούν οι τραπεζικοί λογαριασμοί των υποκειμένων, γεγονός με πολύ σοβαρές οικονομικές συνέπειες.

Τρίτη και τελευταία κατηγορία αποτελούν οι μη υλικές ζημίες. Οι ζημίες αυτές μπορεί να είναι ποικίλων συνεπειών και ως εκ τούτου η προσέγγιση Fraunhofer τις ομαδοποιεί σε τέσσερις υποκατηγορίες. Αυτές είναι οι εξής:

Η πρώτη κατηγορία αφορά τις ζημίες που προκαλούν κοινωνικές συνέπειες και σχετίζονται κυρίως με την φήμη του ατόμου, την εξευτελισμό, την κοινωνική διάκριση καθώς και τον κοινωνικό αποκλεισμό που μπορεί να υποστεί (π.χ. σε περίπτωση αδικαιολόγητου αποκλεισμού σε κάποιον λογαριασμό). Δεύτερη κατηγορία αποτελούν οι ζημίες που αφορούν την ιδιωτικότητα του ατόμου και σχετίζεται με την αίσθηση του ατόμου ότι δεν έχει έλεγχο πάνω στα δεδομένα του. Έτσι, το άτομο μπορεί να αναπτύξει ένα αίσθημα δυσφορίας και να νιώθει ότι συνεχώς ελέγχεται και παρακολουθείται. Αυτό συμβαίνει κυρίως αν χρησιμοποιούνται τεχνολογίες αναγνώρισης προσώπου (και γενικότερα τεχνολογίες βιομετρικής αναγνώρισης), ή δημιουργίας προφιλ και βιντεοεπιτήρησης. Τρίτη κατηγορία αποτελούν οι ζημίες που έχουν συνέπειες στην ελευθερία της έκφρασης και του λόγου. Αφορά

περιπτώσεις που το άτομα δεν νιώθουν ασφαλή να ασκήσουν τα δικαιώματά τους (όπως το να εκφράσουν πολιτικό λόγο) περιορίζοντας το δικαίωμα τους στην ελεύθερη ανάπτυξη της προσωπικότητας. Τέλος, η τελευταία κατηγορία αφορά ζημίες που προκαλούνται από αδικαιολόγητη παρέμβαση στα δικαιώματα και τις ελευθερίες των υποκειμένων. Αναλυτικότερα, οποιαδήποτε επεξεργασία προσωπικών δεδομένων μπορεί να θεωρηθεί ένα είδους παρέμβασης στο δικαίωμα που έχουν τα φυσικά πρόσωπα στο να προστατεύονται τα προσωπικά τους δεδομένα. Ως εκ τούτου όταν μία επεξεργασία διενεργείται χωρίς, πρωτίστως, να υπάρχει κάποια νομική βάση ως προς αυτή, είτε χωρίς να είναι πλήρως συμμορφωμένη με τις αρχές που απορρέουν του ΓΚΠΔ (Άρθρο 5), είτε χωρίς να ικανοποιούνται τα δικαιώματα που απορρέουν από τα άρθα 12-22 ή αυτό γίνεται με λανθασμένο τρόπο, δημιουργούν ζημία, ακόμη και αν οι συνέπειες αυτής δεν είναι και τόσο «απτέ», αφού παραβιάζουν το δικαίωμα στην ιδιωτικότητα.

9.1.1.4. Περιπτώσεις «γεγονότων»

Ως γεγονός η προσέγγιση Fraunhofer ορίζει την αιτία που προκαλούν την εμφάνιση μίας ζημίας και ως εκ τούτου στην πραγμάτωση του κινδύνου. Τις περισσότερες φορές οφείλονται στη μη συμμόρφωση με τις αρχές προστασίας των δεδομένων (Άρθρο 5 ΓΚΠΔ), στην μη ικανοποίηση των δικαιωμάτων υποκειμένων (άρθρα 12 – 22 ΓΚΠΔ) ή σε άλλες παραβάσεις του ΓΚΠΔ. Ως τα πιο συχνά γεγονότα παραθέτει την επεξεργασία που είναι αντίθετη με τις αρχές επεξεργασίας, την επεξεργασία η οποία δεν είναι διαφανής για τα υποκείμενα των δεδομένων, την μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη των δεδομένων, την τυχαία βλάβη, την απώλεια ή την καταστροφή των δεδομένων, την άρνηση ή την αδυναμία ικανοποίησης των δικαιωμάτων των υποκειμένων, την χρήση των δεδομένων για παράνομους σκοπούς, την επεξεργασία κατηγοριών δεδομένων τα οποία δεν ήταν προβλεπόμενο να υφίστανται επεξεργασία, την επεξεργασία λανθασμένων ή μη επικαιροποιημένων δεδομένων, σφάλματα που προκύπτουν κατά την επεξεργασία (είτε τεχνικά, είτε σφάλματα που περιλαμβάνουν τον ανθρώπινο παράγοντα), την επεξεργασία που γίνεται μετά το πέρας του προβλεπόμενου χρόνου τήρησης των δεδομένων και τέλος την ίδια την επεξεργασία όταν αυτή είναι παράνομη, γιατί δεν βασίζεται σε κάποια νομική βάση ή έχει παράνομους σκοπούς.

9.1.1.5. Εντοπισμός και ανάλυση κινδύνου

Στη συνέχεια, σύμφωνα με την παρούσα προσέγγιση πρέπει να ξεκινήσει ο εντοπισμός και η ανάλυση του κινδύνου. Κατ' αρχάς η προσέγγιση Fraunhofer για τον συγκεκριμένο σκοπό χρησιμοποιεί τους «στόχους προστασίας», όπως αυτοί εκτέθηκαν παραπάνω. Με αυτή την προσέγγιση φαίνεται να συμφωνεί και η προσέγγιση που αναπτύχθηκε από τους M. Caroline

Oetzel & S. Spiekermann[116], καθώς και οι τελευταίοι θεωρούν πως οι σχετικά αφηρημένες «νομικές» αρχές, πρέπει να μεταφραστούν σε πιο συγκεκριμένους, επαληθεύσιμους και τεχνικά (και λειτουργικά) εφαρμόσιμους στόχους προστασίας

Η προσέγγιση fraunhofer προτείνει ότι η ο εντοπισμός και η ανάλυση των κινδύνων πρέπει να γίνει σε δύο βήματα, καθώς υποστηρίζει ότι αυτό είναι χρήσιμο για να εντοπιστεί το πως, από ποιον ή τι και κάτω από ποιες περιστάσεις θα μπορούσε να προκληθεί ζημία στα φυσικά πρόσωπα και η συμμόρφωση με ποιους στόχους προστασίας (άρα και αρχές επεξεργασίας) θα μπορούσαν να τεθούν σε κίνδυνο.

Το πρώτο βήμα είναι να αναπτυχθούν σενάρια, τα οποία σε συνδυασμό με το συλλεχθέν υλικό που έχει προηγηθεί (τα εντοπισθέντα εμπλεκόμενα μέρη, τα συστήματα που χρησιμοποιούνται για την επεξεργασία, την λειτουργική περιγραφή του συστήματος, τη φύση, το πεδίο εφαρμογής και τους σκοπούς της επεξεργασίας κτλ.), θα μπορούσαν να οδηγήσουν σε ζημία. Για να εκτελεστεί το συγκεκριμένο στάδιο με μία συστηματική προσέγγιση θα πρέπει για κάθε προσδιορισμένη ομάδα υποκειμένων των δεδομένων να διευκρινιστεί το σε ποιο βαθμό οι ενέργειες των λοιπών εμπλεκομένων μερών, ή άλλων γεγονότων (π.χ.τεχνικά σφάλματα, ανωτέρα βία) θα μπορούσαν να οδηγήσουν σε σωματική, υλική ή μη – υλική ζημία. Επιπλέον, για κάθε σενάριο που θα αναπτυχθεί και για κάθε ομάδα υποκειμένων ξεχωριστά θα πρέπει να εντοπιστεί το ποιοι στόχοι προστασίας θα επηρεαστούν και με ποιον τρόπο.

Για να δημιουργηθούν τα προαναφερθέντα σενάρια σύμφωνα με το οποία μπορεί να προκληθεί ζημία, η προσέγγιση Fraunhofer θέτει τρία κρίσιμα ερωτήματα τα οποία πρέπει να απαντηθούν. Η πρώτη εξ' αυτών αφορά το ποιες ζημίες θα μπορούσαν να προκύψουν για τα υποκείμενα που έχουν εντοπισθεί, σύμφωνα με την προβλεπόμενη επεξεργασία. Η δεύτερη ερώτηση αφορά το ποιες ενέργειες και υπό ποιες προυποθέσεις μπορούν να οδηγήσουν στις αντίστοιχες ζημίες, δηλαδή, πρέπει να εξεταστούν το ποιοι είναι οι εμπλεκόμενοι φορείς και οι πηγές του κινδύνου. Ενώ, τελευταία ερώτηση αφορά το αν τα μέτρα ασφαλείας που ήδη τηρούνται επαρκούν για την διασφάλιση της ασφάλειας ή πρέπει να σχεδιαστούν καινούργια.

Για την συστηματική δημιουργία αυτών των σεναρίων πρέπει να εξεταστούν για κάθε ομάδα υποκειμένων χωριστά, και οι αντίστοιχες κατηγορίες και υποκατηγορίες ζημιών. Θα πρέπει, δηλαδή, να εξεταστεί για κάθε ομάδα υποκειμένων πως θα την επηρεάσει η επεξεργαία,

[116]Βλ. Marie Caroline Oetzel, Sarah Spiekerman. A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach. European Journal of Information Systems, 2014. Σελ. 133

ποιοι είναι οι εμπλεκόμενοι φορείς και τι είδους ζημίες μπορεί επέλθουν (σωματικές, υλικές, ή μη-υλικές). Επιπλέον, στο σημείο αυτό θα πρέπει να εντοπιστούν το ποιοι εμπλεκόμενοι φορείς, ποιοι, δηλαδή, είναι αυτοί που μπορεί να ενδιαφερθούν για αυτά τα δεδομένα και θα είχαν κίνητρο, ίσως, να επέμβουν στην επεξεργασία. Ακόμη, θα πρέπει να ληφθούν υπόψη και οι λοιποί παράγοντες που μπορούν να δημιουργήσουν ζημίες, όπως τα λανθασμένα δεδομένα, οι τεχνικές αστοχίες ή κάποιου είδους ανωτέρα βία. Έτσι, τα μέτρα αντιμετώπισης των κινδύνων, που έχουν ήδη ληφθε,ί θα πρέπει να προσαρμοστούν πάνω σε αυτά τα σενάρια ή θα πρέπει να σχεδιαστούν νέα μέτρα αντιμετώπισης τους. Είναι σημαντικό να είναι απόλυτα διασαφηνισμένο ποια μέτρα έχουν προγραμματιστεί για να εφαρμοστούν στο μέλλον και ποια μέτρα, ήδη, εφαρμόζονται. Συνοπτικά, η πληροφορία που πρέπει να καταγραφεί για κάθε ένα σενάριο είναι τα εξής: μία περιγραφή του σεναρίου, τα υποκείμενα που εξετάζονται, τα προσωπικά δεδομένα που εξετάζονται, οι εμπλεκόμενοι φορείς, η πιθανή ζημία/ες για τα υποκείμενα, οι στόχοι προστασίας που επηρεάζονται, τα στοιχεία εκείνα που διαμορφώνουν τα αίτια για να προκληθεί η ζημία και τέλος τα ήδη υπάρχοντα τεχνικά και οργανωτικά μέτρα που διασφαλίζουν την αποτροπή της ζημίας. Η προσέγγιση frauhofer προτείνει ότι τα προηγούμενα πρέπει να καταγραφούν σε μορφή πίνακα, ενώ με την ολοκλήρωση αυτού ολοκληρώνεται και το πρώτο στάδιο της ανάλυσης και του εντοπισμού του κινδύνου.

Το δεύτερο βήμα του εντοπισμού και της ανάλυσης του κινδύνου ξεκινάει με τους στόχους προστασίας. Ειδικότερα, για κάθε στόχο προστασίας και σε συνάρτηση με την εκάστοτε ομάδα υποκειμένων των δεδομένων πρέπει να απαντηθούν τρία ερωτήματα. Πρέπει, κατ' αρχάς η να απαντηθεί αν η σχεδιαζόμενη επεξεργασία συμμορφώνεται με τον αντίστοιχο στόχο προστασίας, πρέπει επιπλέον, να καθοριστεί κάτω υπό ποιες περιστάσεις θεωρείται ότι υπάρχει παραβίαση του εν λόγω στόχου προστασίας που εξετάζεται και ποιος ή τι μπορεί να την προκαλέσει και τέλος τι είδους ζημίας θα προκληθεί, αν εν τέλει, παραβιασθεί ο συγκεκριμένος κανόνας προστασίας. Βέβαια, αναφέρεται ότι κάποιοι από τους στόχους προστασίας βρίσκονται μεταξύ τους σε μία σχέση αντιστρόφως ανάλογου. Για παράδειγμα, μεγαλύτερη διαφάνεια μπορεί να οδηγεί σε μικρότερη εμπιστευτικότητα, ή μεγαλύτερη διαθεσιμότητα σε ασθενέστερη αξιοπιστία και το αντίστροφο. Ως εκ τούτου, πρέπει να αναλυθεί και το ποιος από τους στόχους θεωρείται σημαντικότερος και ως εκ τούτου να δοθεί αντίστοιχη προτεραιότητα, πάντα με γνώμονα την προστασία των ελευθεριών και των δικαιωμάτων των υποκειμένων των δεδομένων. Αυτή η «κατηγοριοποίηση» τον στόχων προστασίας είναι απαραίτητη για την ορθή επιλογή των κατάλληλων μέτρων για την αντιμετώπιση των κινδύνων, σε μετέπειτα επίπεδο.

9.1.1.6. Αξιολόγηση κινδύνου

Πλέον, έχοντας ολοκληρώσει το στάδιο του εντοπισμού, καταγραφής και ανάλυσης του κινδύνου μέσω των σεναρίων και των στόχων προστασίας πρέπει να γίνει η αξιολόγηση του. Το επίπεδο του κινδύνου είναι αποτέλεσμα, όπως προαναφέρθηκε, της σοβαρότητας της ζημίας που προκαλεί και της πιθανότητας να επέλθει το γεγονός το οποία συνιστά την ζημία. Για την κατηγοριοποίηση της σοβαρότητας και της πιθανότητας του κινδύνου, η προσέγγιση fraunhofer συνιστά την δημιουργία ενός «Risk Matrix» κάτι που αποτελεί κοινό χαρακτηριστικό όλων των μεθοδολογικών προσεγγίσεων. Πρόκειται για έναν πίνακα που οπτικοποιεί τον κίνδυνο λαμβάνοντας υπόψη τις μεταβλητές της σοβαρότητας από την μία πλευρά και της πιθανότητας από την άλλη.

Η σοβαρότητα της ζημίας αξιολογείται από τις σωματικές, υλικές ή μη υλικές συνέπειες που θα προκαλέσει στα υποκείμενα των δεδομένων όταν αυτή επέλθει. Μεταξύ των κριτηρίων της αξιολόγησης της σοβαρότητας της ζημίας θα πρέπει να λαμβάνεται υπόψη και το πόσο εύκολο ή δύσκολο είναι να αντιστραφεί αυτή. Ως εκ τούτου, όσο περισσότερο χρόνο, χρήματα ή προσπάθεια χρειάζεται για να αντιστραφεί κάποια ζημία, τόσο πιο σοβαρή θεωρείται.

Τέλος, για την αξιολόγηση της πιθανότητας επέλευσης της ζημίας είναι σημαντικό να λαμβάνονται υπόψη το πόσο δύσκολο είναι να επέλθει ο κίνδυνος, τι μέσα χρειάζονται για αυτό, λαμβάνοντας υπόψη και την ανθεκτικότητα των συστημάτων και των διαδικασιών του οργανισμού.

9.1.1.7. Επιλογή μέτρων αντιμετώπισης των κινδύνων

Έχοντας, πλέον, ολοκληρώσει τα στάδια εντοπισμού, ανάλυσης, και αξιολόγησης των κινδύνων, σκοπός είναι οι τελευταίοι να μετριασθούν ή αν είναι δυνατόν να εξαλειφθούν εντελώς. Αν κάτι τέτοιο θεωρηθεί ότι δεν είναι αδύνατον η σχεδιαζόμενη επεξεργασία, είτε θα πρέπει να τροποποιηθεί, είτε να ακυρωθεί. Το πρόβλημα που γεννάται είναι ότι δεν καθορίζεται από τον ΓΚΠΔ μέχρι ποιο σημείο πρέπει να μετριασθεί ο κίνδυνος. Γενικά, γίνεται αποδεκτό ότι κάθε κίνδυνος που θεωρείται υψηλός θα πρέπει να μετριασθεί σε ένα επίπεδο «κανονικού κινδύνου», χωρίς, όμως, να είναι απόλυτα ευδιάκριτο ότι δεν θα πρέπει να μετριασθεί σε επίπεδο «χαμηλού κινδύνου». Ως εκ τούτου αυτά θα πρέπει να εξετάζεται κάθε φορά ανά περίπτωση.

Επιπλέον, όσον αφορά τα μέτρα αντιμετώπισης των κινδύνων, για να θεωρηθούν κατάλληλα θα πρέπει να ταιριάζουν με τα όσα αναφέρθηκαν στην ανάλυση του κινδύνου. Αν, για παράδειγμα, εντοπισθεί ένα σενάριο που θα μπορούσε να προκαλέσει ζημία στην ακεραιότητα των δεδομένων, τότε κατάλληλο μέτρο θα ήταν αυτό που θα μετριάσει την ζημία

σχετικά με την ακεραιότητα. Τα μέτρα αυτά μπορεί να είναι τόσο τεχνικά όσο και οργανωτικά, ενώ μπορεί να μην είναι καινούργια μέτρα αλλά να θεωρηθεί αρκετό η ενίσχυση των ήδη υπαρχόντων μέτρων.

Σε αυτό το σημείο, ίσως, εμφανίζεται και το μεγαλύτερο μειονέκτημα της προσέγγισης Fraunhofer, αφού η ίδια δεν παρέχει κανένα παράδειγμα μέτρων για τον μετριασμό του κινδύνου. Παραθέτει βέβαια, την SDM η οποία περιλαμβάνει λίστα με τα σημαντικότερα μέτρα αντιμετώπισης κινδύνων, αλλά, και την CNIL[117] η οποία διαθέτει μεγάλη και συστηματική λίστα με μέτρα αντιμετώπισης κινδύνων.

Τα μέτρα αντιμετώπισης που επιλέχθηκαν πρέπει να μετριάζουν τον κίνδυνο σε ένα αποδεκτό επίπεδο. Αν ο κίνδυνος παραμένει υψηλός τότε είτε η επεξεργασία πρέπει να ακυρωθεί, είτε να εφαρμοστεί το άρθρο 36 του ΓΚΠΔ και να ξεκινήσει η διαδικασία διαβούλευσης με την Αρχή, όπως αναλύθηκε στο αντίστοιχο κεφάλαιο της παρούσας εργασίας. Σε καμία περίπτωση, δεν θα πρέπει να συνεχιστεί η επεξεργασία αν δεν διασφαλιστεί το χαμηλό επίπεδου κινδύνου.

9.1.1.8. Αξιολόγηση της αναγκαιότητας και της αναλογικότητας

Βασιζόμενοι πάνω στον κίνδυνο, όπως αυτός προκύπτει μετά την ολοκλήρωση όλων των προηγούμενων βημάτων, πλέον, είναι δυνατή η αξιολόγηση της αναγκαιότητας και της αναλογικότητας όπως απαιτεί το ά.35 παρ.7 περ' β. του ΓΚΠΔ. Τέσσερα κριτήρια πρέπει να πληρούνται για να θεωρηθεί ότι η επεξεργασία είναι αναγκαία και αναλογική, σύμφωνα με την προσέγγιση Fraunhofer. Πρώτον, ότι διασφαλίζεται ότι η επεξεργασία είναι νόμιμη σύμφωνα με το άρθρο 6 παρ.1 του ΓΚΠΔ. Δεύτερον, ότι όλες οι αρχές του ΓΚΠΔ όπως περιγράφονται στο α.5 ΓΚΠΔ έχουν γίνει σεβαστές και υιοθετούνται στην επεξεργασία. Τρίτον, ότι όλα τα υπόλοιπα ζητούμενα του ΓΚΠΔ (π.χ. να παρέχονται όλα τα δικαιώματα κτλ.) ικανοποιούνται και τα προσωπικά δεδομένα των υποκειμένων είναι ασφαλή και, τέλος ,ότι όλοι οι κίνδυνοι που προκύπτουν από την επεξεργασία έχουν μετριασθεί σε αποδεκτό βαθμό και δεν υπάρχει υψηλός κίνδυνος.

9.1.2 Η προσέγγιση του ICO

[117] CNIL Privacy Impact Assessment: Knowledge Bases: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

Η προσέγγιση του ICO για την συγκεκριμένη φάση είναι πολύ πιο λακωνική και, μάλλον, παρουσιάζει μία λιγότερη συστηματική προσέγγιση. Δεν φαίνεται να αναλύει τα είδη της ζημίας, ούτε όμως προβαίνει σε κάποια περαιτέρω εισήγηση για την φύση του κινδύνου. Ο ICO, όπως έχει ήδη προαναφερθεί, προσπαθεί να είναι πρακτικός και μέσω ερωτημάτων να κατευθύνει τον ενδιαφερόμενο. Ειδικότερα, όπως παρουσιάζεται στο βήμα 4 και 5[118] της μεθοδολογίας που έχει δημοσιευμένη στον διαδικτυακό του ιστότοπο, η εν λόγω φάση παρουσιάζεται σε δύο βήματα. Το πρώτο εξ ΄αυτών, αφορά στον τρόπο με τον οποίο εντοπίζεται και αξιολογείται ο κίνδυνος, ενώ το δεύτερο αφορά την επιλογή μέτρων αντιμετώπισης του κινδύνου.

Ως προς το πρώτο βήμα, του εντοπισμού και της αξιολόγησης του κινδύνου ο ICO υποδεικνύει ότι κατ' αρχάς θα πρέπει να ληφθεί υπόψη το ποιες συνέπειες θα έχει η επεξεργασία για τα άτομα και ποιες ζημίες μπορεί να προκαλέσει η σχεδιαζόμενη επεξεργασία, είτε πρόκειται για σωματική, συναισθηματική ή υλική βλάβη. Ως εκ τούτου δίνει απτά παραδείγματα για να κατευθύνει τον/ τους διενεργούντα/ες την εκτίμηση αντικτύπου, τα οποία είναι η αδυναμία άσκησης δικαιωμάτων (συμπεριλαμβανομένων των δικαιωμάτων στην προστασία της ιδιωτικής ζωής), την απώλεια ελέγχου της χρήσης των προσωπικών δεδομένων, τις διακρίσεις, την κλοπή ταυτότητας και την απάτη, την σωματική βλάβη, την απώλεια εμπιστευτικότητας, την αδυναμία πρόσβασης σε υπηρεσίες ή ευκαιρίες, την ζημία στην φήμη και οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα.

Επιπλέον, στο παρόν στάδιο, η προσέγγιση ICO φαίνεται πως ταυτίζεται με τις οδηγίες της ομάδας εργασίας του άρθρου 29 και διασαφηνίζει ότι θα πρέπει να ληφθούν υπόψη και να αξιολογηθούν οι κίνδυνοι ασφαλείας, καθώς και οι πηγές των κινδύνων και οι επιπτώσεις κάθε είδους παραβίασης (συμπεριλαμβανομένης της παράνομης πρόσβασης, τροποποίησης ή απώλειας δεδομένων προσωπικού χαρακτήρα).

Για την αξιολόγηση του κινδύνου η προσέγγιση ICO δεν πρωτοπορεί, και προτρέπει τους διενεργούντες να χρησιμοποιήσουν τα κριτήρια της πιθανότητας και της σοβαρότητας της πιθανής βλάβης, αναφέροντας ότι η αξιολόγηση αυτή θα πρέπει να είναι αντικειμενική. Ως εκ τούτου και η προσέγγιση ICO προτρέπει με την σειρά της στην δημιουργία ενός «Risk Matrix» στην οπτικοποίηση, δηλαδή, του κινδύνου με τις μεταβλητές της πιθανότητας και της σοβαρότητας. Ειδικότερα, στην προσέγγιση ICO οι μεταβλητές τίθενται ως εξής: Στον άξονα

[118] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/how-do-we-do-a-dpia/#how10 (Step 5: How do we identify and assess risks? & Step 6: How do we identify mitigating measures?)

Χ τίθενται η πιθανότητα ενώ στον άξονα Ψ τίθεται η σοβαρότητα. Οι τιμές που μπορούν να δοθούν στην πιθανότητα είναι η «Λιγότερο πιθανό», η «Εύλογα πιθανό» και «Πιο πιθανό να συμβεί από το να μην συμβεί», ενώ στην μεταβλητή της σοβαρότητας είναι από κάτω προς τα πάνω οι «Μικρό αντίκτυπο», «Κάποιο αντίκτυπο», «Σοβαρό αντίκτυπο». Ως εκ τούτου, εκτιμώντας τον κίνδυνο και δίνοντας τις κατάλληλες τιμές στις δύο αυτές μεταβλητές το σημείο συνάντησης τους θα καθορίσει και το επίπεδο κινδύνου δημιουργώντας εννιά σενάρια. Τρία από αυτά αποτελούν υψηλό κίνδυνο τα οποία είναι οι περιπτώσεις που υπάρχει Μεγάλη πιθανότητα με σοβαρό αντίκτυπο, μεγάλη πιθανότητα με κάποιο αντίκτυπο και εύλογη πιθανότητα με σοβαρό αντίκτυπο. Ως εκ τούτου, και στα τρία αυτά σενάρια ο κίνδυνος είναι μεγάλος και θα πρέπει οπωσδήποτε να μετριασθεί. Το ζήτημα που δημιουργείται αφορά κυρίως την περίπτωση, όπου η και η σοβαρότητα και η πιθανότητα λαμβάνουν την μεσαία τιμή, αυτή δηλαδή της εύλογης πιθανότητας και του «Κάποιου αντικτύπου» που οδηγεί στο ότι ο κίνδυνος είναι μέτριος. Σε αυτή την περίπτωση, ωστόσο, θεωρείται ότι μάλλον είναι ασφαλέστερο να γίνουν προσπάθειες ο κίνδυνος να μετριασθεί σε ένα χαμηλότερο επίπεδο και μόνον αν αυτό δεν είναι δυνατό να συνεχιστεί η διαδικασία, έχοντας όμως καταγράψει το αποτέλεσμα της συγκεκριμένης διαδικασίας.

Ολοκληρώνοντας αυτό το στάδιο ο κίνδυνος έχει εντοπιστεί και αξιολογηθεί. Ως εκ τούτου, η προσέγγιση ICO στο επόμενο στάδιο προτείνει πλέον την επιλογή των κατάλληλων μέτρων αντιμετώπισης του κινδύνου με σκοπό αυτός να μετριασθεί. Ωστόσο, ούτε η προσέγγιση ICO περιλαμβάνει κάποιον κατάλογο με ενδεδειγμένα μέτρα αντιμετώπισης του κινδύνου, με εξαίρεση από μία ενδεικτική λίστα με πολύ γενικά μέτρα.

Ως εκ τούτου, στο παράδειγμα που έχει δημοσιευμένο στην ιστοσελίδα του ο ICO[119] (που αφορά ηλεκτρονικό κατάστημα πώλησης παιδικών παιχνιδιών), στο συγκεκριμένο στάδιο έχει εντοπίσει και αναλύσει οχτώ διαφορετικά σενάρια κινδύνου, τα τέσσερα εκ των οποίων έχουν χαρακτηριστεί ως «υψηλοί» ενώ οι υπόλοιποι ως «μέτριοι». Ωστόσο, δεν περιγράφεται ούτε ο τρόπος με τον οποίο δημιουργήθηκαν αυτά τα σενάρια, ούτε ειδικότερα κριτήρια για την αξιολόγηση της πιθανότητας και της σοβαρότητας τους. Ενδεικτικά, ένα από τα σενάρια υψηλού κινδύνου αποτελεί αυτό που θέτει σε κίνδυνο παιδιά να πέσουν θύματα παρακολούθησης ή παρενόχλησης λόγω της από προεπιλογής («by default») κοινολόγησης δεδομένων τους με άλλους χρήστες υπηρεσιών. Ως εκ τούτου, στο επόμενο στάδιο της επιλογής μέτρων αντιμετώπισης αυτού του κινδύνου, ως ενδεδειγμένο μέτρο για να

[119] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/dpia-tools/connected-toy/step-5-identify-and-assess-risks/

αντιμετωπισθεί αυτός ο κίνδυνος, έχει επιλεχθεί από τους διενεργούντες την εκτίμηση, το να μην υπάρχει η δυνατότητα κοινολόγησης βίντεο ή φωτογραφιών και να ληφθούν μέτρα ασφαλείας που να εμποδίζουν την πρόσβαση σε τρίτους. Καταληκτικά, αναφέρει ότι ότι ο κίνδυνος έχει μετριασθεί σε επίπεδο χαμηλού κινδύνου και, πλέον, είναι αποδεκτός. Παρόλα αυτά, και πάλι δεν αναφέρεται με ποια κριτήρια επιλέχθηκαν τα συγκεκριμένα μέτρα αντιμετώπισης και από που αντλήθηκε η σχετική πληροφορία.

9.1.3 Η προσέγγιση της CNIL

Η προσέγγιση CNIL στο συγκεκριμένα στάδιο παρουσιάζει μία εκτενή και συστηματική ανάλυση, ενώ παρέχει έναν πολύ μεγάλο και οργανωμένο κατάλογο[120] για την υποβοήθηση των διενεργούντων την εκτίμηση αντικτύπου. Αποτελεί αναμφίβολα την πιο ολοκληρωμένη προσέγγιση, για την παρούσα φάση, μεταξύ των εξεταζόμενων στην παρούσα εργασία.

Ειδικότερα, σκοπός του συγκεκριμένου σταδίου σύμφωνα με την προσέγγιση της CNIL είναι η κατανόηση των αιτιών από τους οποίους προκαλούνται οι κίνδυνοι και οι συνέπειες που θα έχουν αυτοί.

9.1.3.1 Ο κίνδυνος σύμφωνα με την προσέγγιση της CNIL

Ο κίνδυνος σύμφωνα με την CNIL είναι ένα υποθετικό σενάριο που περιγράφει ένα απευκταίο γεγονός[121] και όλες τις απειλές που θα επέτρεπαν αυτό να συμβεί.. Ως εκ τούτου για την κατανόηση της έννοιας του κινδύνου όπως αυτή περιγράφεται στην προσέγγιση της CNIL έχουν πολύ μεγάλη σημασία οι έννοιες του «απευκταίου γεγονότος» και της «απειλής» καθώς αυτές οι δύο έννοιες αποτελούν τον κίνδυνο.

Ως εκ τούτου, η απειλή απαρτίζεται από την μελέτη του πως οι πηγές κινδύνου (π.χ. η δωροδοκία ενός υπαλλήλου από έναν ανταγωνιστή) θα μπορούσαν να εκμεταλλευτούν ευπάθειες των υποστηρικτικών στοιχείων[122] (π.χ. το σύστημα διαχείρισης αρχείων που επιτρέπει παρέμβαση στα δεδομένα) σε ένα πλαίσιο απειλών (π.χ. μέσω της λανθασμένης χρήσης email). Κατ' επέκταση το απευκταίο γεγονός απαρτίζεται από το τι αποτέλεσμα θα είχαν τα ανωτέρω αν πραγματώνονταν και το πως θα οδηγούσαν στην πραγμάτωση ενός απευκταίου γεγονότος (π.χ. παράνομη πρόσβαση) στα προσωπικά δεδομένα (π.χ. στα αρχεία

[120]Βλ. CNIL, Privacy Impact Assessment (PIA) Knowledge Bases, 2018
[121]Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, όπου και έχει αποδοθεί στην ελληνική ο όρος «απευκταίο γεγονός» για τον όρο «feared event»
[122]Υπενθυμίζεται ότι υποστηρικτικό στοιχεία κατά την CNIL μπορεί να είναι άνθρωποι, τεχνολογικό υλικό, λογισμικό, δίκτυα, άνθρωποι, χαρτί ή κανάλια διαβίβασης χαρτιού.

ενός πελάτη) και ως εκ τούτου τι συνέπειες στην ιδιωτικότητα των υποκειμένων των δεδομένων θα δημιουργούσαν(π.χ. ανεπιθύμητες προτροπές, συναισθήματα, παραβίαση ιδιωτικής ζωής, προσωπικά ή επαγγελματικά προβλήματα.).

Τα ανωτέρα είναι πολύ σημαντικά και για την αξιολόγηση του επιπέδου του κινδύνου, καθώς σύμφωνα με την προσέγγιση της CNIL η «απειλή» που απαρτίζει τον κίνδυνο εκτιμάται με το κριτήριο της πιθανότητας. Πόσο πιθανό, δηλαδή είναι οι πηγές του κινδύνου να εκμεταλλευτούν ευπάθειες των υποστηρικτικών στοιχείων[123]. Από την άλλη πλευρά το απευκταίο γεγονός που μπορεί να οδηγήσουν οι ως άνω απειλές εκτιμώνται με το κριτήριο της σοβαρότητας. Πόσο σοβαρή είναι ,δηλαδή, η πιθανή παραβίαση των προσωπικών δεδομένων και πόσο επιζήμιες θα είναι συνέπειες τους στα υποκείμενα των δεδομένων;

Ως εκ τούτου η CNIL διαχωρίζει την εξέταση του κινδύνου σε δύο αλληλένδετες φάσεις. Η πρώτη φάση αποτελεί των εντοπισμό των απειλών, δηλαδή το σενάριο που εξετάζει το πως οι πηγές κινδύνου μπορούν να εκμεταλλευτούν τις ευπάθειες των υποστηρικτικών στοιχείων της επεξεργασίας και κατ' επέκταση αν πραγματωθεί εν τέλει αυτή η απειλή σε ποιο απευκταίο γεγονός θα οδηγήσει και τι συνέπειες θα έχει αυτό για την ιδιωτικότητα των υποκειμένων; Για την ολοκληρωμένη κατανόηση της έννοιας του κινδύνου στην προσέγγιση της, η CNIL δίνει εκτενή παραδείγματα μέσω των οποίων επεξηγεί τις εν λόγω έννοιες. Ειδικότερα:

9.1.3.2. Πηγές κινδύνου

Οι πηγές κινδύνου αποτελούνται από τρία είδη τα οποία είναι: Οι εσωτερικές ανθρωπογενείς πηγές (π.χ. εργαζόμενοι, διευθυντές) , οι εξωτερικές ανθρωπογενείς πηγές (π.χ. αποδέκτες προσωπικών δεδομένων, πάροχοι υπηρεσιών, επισκέπτες, πρώην υπάλληλοι, υπεύθυνοι συντήρησης κτλ.) και οι μη ανθρωπογενείς πηγές (π.χ. κακόβουλος κώδικας άγνωστης προελεύσεως, νερό, εύφλεκτα και διαβρωτικά υλικά κτλ.)[124]

9.1.3.3. Είδη αποτελεσμάτων των απευκταίων γεγονότων

Από την άλλη πλευρά ως απευκταίο γεγονός νοείται η πιθανή παραβίαση των προσωπικών δεδομένων που προκαλούν διάφορες επιπτώσεις στην ιδιωτικότητα των υποκειμένων. Ειδικότερα, σύμφωνα με την προσέγγιση της CNIL υπάρχουν τρία απευκταία γεγονότα, το κάθε ένα από τα οποία έχει συγκεκριμένες συνέπειες. Έτσι, πρώτο απευκταίο γεγονός είναι η Αθέμιτη πρόσβαση σε προσωπικά δεδομένα και το αποτελέσματα που

[123] Αυτό εξαρτάται κυρίως από το πόσο μεγάλες είναι οι ευπάθειες που παρουσιάζουν τα υποστηρικτικά στοιχεία και τις ικανότητες που έχουν οι πηγές του κινδύνου για να τις εκμεταλλευτούν.
[124] Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 7.

δημιουργείται από την πραγμάτωση του είναι είτε «επουσιώδες» (δηλαδή αποκτούν πρόσβαση άνθρωποι που δεν χρειάζεται να τα γνωρίζουν αλλά δεν κάνουν χρήση τους), είτε να πραγματοποιείται «Αποθήκευση» τους (δηλαδή, τα δεδομένα να αντιγράφονται και να αποθηκεύονται σε άλλη τοποθεσία αλλά να μην χρησιμοποιούνται), είτε να πραγματοποιείται «Διάδοση» τους (δηλαδή, τα δεδομένα να διαδίδονται πέραν του απαραίτητου μέτρου προς τον σκοπό τους ή/και πέρα από τον έλεγχο των υποκειμένων τους), είτε τέλος να γίνεται «Χρήση» αυτών (δηλαδή, τα δεδομένα να χρησιμοποιούνται για άλλο σκοπό διαφορετικό από εκείνο που αρχικά προβλέπονταν ή συσχετίζονται με άλλα δεδομένα, όπως για παράδειγμα συσχέτιση της διεύθυνσης διαμονής και δεδομένων γεωεντοπισμού με διεύθυνση διαμονής σε πραγματικό χρόνο.)

Το επόμενο απευκταίο γεγονός που περιγράφεται στην CNIL είναι η Ανεπιθύμητη τροποποίηση προσωπικών δεδομένων. Ειδικότερα, το συγκεκριμένο απευκταίο γεγονός οδηγεί σε δύο κύρια αποτελέσματα το πρώτο εκ των οποίων είναι η «Δυσλειτουργία» τους (δηλαδή, τα δεδομένα μετατρέπονται σε άλλα έγκυρα ή μη έγκυρα δεδομένα, τα οποία δεν θα χρησιμοποιηθούν σωστά δημιουργώντας σφάλματα στην επεξεργασία ή να μην παρέχει πλέον την αναμενόμενη υπηρεσία. Το δεύτερο αποτέλεσμα στο οποίο μπορεί να οδηγήσει το ως άνω απευκταίο γεγονός είναι να γίνει «Χρήση» αυτών (δηλαδή, τα δεδομένα να μετατρέπονται σε άλλα έγκυρα δεδομένα, με τρόπο ώστε να γίνεται ή να δύναται να γίνει κατάχρηση της επεξεργασίας).

Τρίτο και τελευταίο απευκταίο γεγονός αποτελεί η «Μη διαθεσιμότητα προσωπικών δεδομένων» το οποίο γεγονός μπορεί να έχει δύο αποτελέσματα. Το πρώτο εξ' αυτών είναι να οδηγήσει στην «Δυσλειτουργία» των δεδομένων (δηλαδή, να εκλείψουν δεδομένα και να προκληθούν σφάλματα στην επεξεργασία, ή δυσλειτουργίες από την αναμενόμενη επεξεργασία) και το δεύτερο είναι να οδηγήσει σε «Αποκλεισμό» (δηλαδή, να εκλείπουν δεδομένα για την επεξεργασία προσωπικών δεδομένων η οποία δεν μπορεί πλέον να παρέχει το προσδοκόμενα αποτέλεσμα, όπως για παράδειγμα να εκλείψουν ιατρικοί φάκελοι και ως εκ τούτου να μην είναι δυνατή η παροχή ιατρικής περίθαλψης, ή να εκλείψουν δεδομένα και να μην δύνανται τα υποκείμενά τους να ασκήσουν τα δικαιώματά τους.) [125]

9.1.3.4. Απειλές

Η προσέγγιση της CNIL, για την πληρέστερη κατανόηση του τι συνιστά απειλή, παρέχει εκτενή παραδείγματα για συγκεκριμένες κατηγορίες απειλών. Ειδικότερα, η CNIL παρέχει

[125] Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 8.

καθοδήγηση για τον καθορισμό απειλών που μπορούν να οδηγήσουν σε αθέμιτη πρόσβαση, σε ανεπιθύμητη τροποποίηση καθώς και σε μη διαθεσιμότητα των δεδομένων, μέσω εκτενών παραδειγμάτων. Σε κάθε ένα από αυτά, εξετάζεται ποιο είδος υποστηρικτικού στοιχείου αφορά η εν λόγω απειλή (π.χ. Υλισμικό, λογισμικό, Άνθρωποι, Έγχαρτα έγγραφα), τι επίδραση θα έχει (π.χ. Ακατάλληλη χρήση, υπερφόρτωση, τροποποίηση, χειραγώγηση, βλάβη, απώλεια) ενώ δίνονται και παραδείγματα απειλών κατά της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας αντίστοιχα για κάθε κατηγορία απειλών. Τέλος, για κάθε μία από αυτές τις περιπτώσεις εξετάζεται τα τρωτά σημεία των υποστηρικτικών στοιχείων που αφορά η εκάστη απειλή.[126]

Ως εκ τούτου, η μεθοδολογία της CNIL παρουσιάζει μία συστηματική μέθοδο για τον εντοπισμό και την ανάλυση του κινδύνου. Ωστόσο, πάνω στην ίδια βάση πρέπει να γίνει και η αξιολόγηση του κινδύνου. Ειδικότερα, η CNIL έχει αναπτύξει μία λεπτομερέστερη κλίμακα και μία σαφέστερη μεθοδολογία για την αξιολόγηση του κινδύνου. Όπως, ήδη, αναφέρθηκε ο κίνδυνος στην προσέγγιση της CNIL εκτιμάται μέσω της πιθανότητας να επέλθει η απειλή (πόσο πιθανό είναι δηλαδή οι πηγές του κινδύνου να εκμεταλλευτούν ευπάθειες των υποστηρικτικών στοιχείων) και κατ΄επέκταση σε ποιο απευκταίο γεγονός θα οδηγήσει, δηλαδή με ποιον τρόπο θα επηρεαστούν τα δεδομένα και τι συνέπειες θα έχει αυτό για τα υποκείμενα.

9.1.3.5. Κλίμακα και μεθοδολογία για την εκτίμηση της σοβαρότητας.

Ειδικότερα, «σοβαρότητα» είναι το μέγεθος ενός κινδύνου και εκτιμάται σε συνάρτηση με την έκταση των επιπτώσεων στα υποκείμενα των δεδομένων, αφού ληφθούν υπόψη τα υφιστάμενα, προγραμματισμένα ή συμπληρωματικά μέτρα. Ειδικότερα, η κλίμακα που χρησιμοποιεί η προσέγγιση CNIL για την αξιολόγηση τους περιλαμβάνει τέσσερις διαφορετικές τιμές που μπορεί να λάβει η αξιολόγηση της σοβαρότητας. Έτσι, η σοβαρότητα μπορεί να αξιολογηθεί ως «αμελητέα», αν δεν ενδέχεται τα υποκείμενα να επηρεαστούν ή να αντιμετωπίσουν κάποια πρόβλημα και ακόμα και αν αντιμετωπίσουν να το ξεπεράσουν χωρίς καμία δυσχέρεια, ως «περιορισμένη» αν τα υποκείμενα των δεδομένων αντιμετωπίσουν μεν σοβαρά προβλήματα αλλά θα μπορέσουν να τα ξεπεράσουν εύκολα, ως «Σημαντική» αν τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές συνέπειες τις οποίες αναμένεται να ξεπεράσουν, αλλά με πραγματικές και σοβαρές δυσκολίες και τέλος ως

[126] Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 16-29

«Μέγιστη» αν τα υποκείμενα των δεδομένων ενδέχεται να αντιμετωπίσουν σημαντικές ή ακόμη και μη αναστρέψιμες συνέπειες τις οποίες ενδεχομένως να μην ξεπεράσουν.[127]

Επιπλέον, σε αυτό το σημείο η προσέγγιση της CNIL, μέσω παραδειγμάτων, παρουσιάζει τα είδη των επιπτώσεων. Ως εκ τούτου, σύμφωνα με την προσέγγιση της CNIL οι επιπτώσεις διακρίνονται σε σωματικές (σωματικές βλάβες, παραμόρφωση του σώματοσκλπ), υλικές (οικονομική ζημία, απώλεια εισοδήματος) και ηθικές (ηθική βλάβη, συναισθηματική ταλαιπωρίακ κτλ)[128]

9.1.3.6. Κλίμακα και μεθοδολογία για την εκτίμηση της πιθανότητας.

Με τον όρο «πιθανότητα» νοείται το κατά πόσο είναι ενδεχόμενη η επέλευση ενός κινδύνου. Η πιθανότητα του κινδύνου εκτιμάται κυρίως με βάση τον βαθμό ευπάθειας των σχετικών υποστηρικτικών στοιχείων και τον βαθμό ικανότητα των πηγών κινδύνου να εκμεταλλευτούν τις ευπάθειες αυτές, λαμβανομένων υπόψη των υφιστάμενων, προγραμματισμένων ή συμπληρωματικών μέτρων. Ειδικότερα, και σε αυτή την περίπτωση όπως και στην εκτίμηση της σοβαρότητας οι τιμές της αξιολόγησης είναι τέσσερις και μάλιστα είναι οι ίδιες. Ωστόσο, διαφέρουν ως προς το περιεχόμενό τους. Έτσι, η πιθανότητα μπορεί να εκτιμηθεί ως «αμελητέα» αν φαίνεται απίθανό οι εξεταζόμενες πηγές κινδύνου να προκαλέσουν την επέλευση του κινδύνου εκμεταλλευόμενες τις ιδιότητες των υποστηρικτικών στοιχείων, ως «περιορισμένη» αν είναι δύσκολο, ως «σημαντική» αν είναι πιθανό και ως «Μέγιστη» αν είναι εξαιρετικά εύκολο. Για τον ευχερέστερο καθορισμό του επιπέδου της πιθανότητας, η CNIL υποδεικνύει ότι πρέπει να ληφθούν υπόψη τα αν υπάρχει ανοικτή πρόσβαση στο διαδίκτυο, το αν γίνεται διαβίβαση δεδομένων στο εξωτερικό, η διασύνδεση ή μη με άλλα συστήματα, η ετερογένεια του συστήματος, η μεταβλητότητα ή η σταθερότητα του συστήματος και εικόνα που έχει ο οργανισμός προς τα έξω.

9.1.3.7. Αξιολόγηση των Υφιστάμενων και Προβλεπομένων μέτρων προστασίας.

Ως εκ τούτου, αφού πλέον έχει καθοριστεί ο κίνδυνος μέσω της συστηματικής προσέγγισης που περιγράφεται στα ανωτέρω βήματα, πλέον πρέπει να γίνει η αξιολόγηση του κινδύνου. Η αξιολόγηση του κινδύνου σύμφωνα με την προσέγγιση της CNIL χωρίζεται σε δύο βήματα. Το πρώτο εξ αυτών είναι η αξιολόγηση των υφιστάμενων και των προβλεπόμενων

[127] Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 10-13
[128] Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 9

μέτρων προστασίας σε συνάρτηση με τους κινδύνους που εντοπίσθηκαν, ενώ το δεύτερο στάδιο είναι ο εντοπισμός των πιθανών παραβιάσεων της ιδιωτικής ζωής.[129]

Ως εκ τούτου, κατά ο πρώτο στάδιο πρέπει να εντοπιστούν και να καθοριστούν τα ήδη υπάρχοντα ή τα ήδη σχεδιαζόμενα μέτρα προστασίας, τα οποία, σύμφωνα με την προσέγγιση CNIL, διαχωρίζονται σε τρία είδη. Το πρώτο εξ ΄αυτών αφορά τα μέτρα που εφαρμόζονται στα υπό επεξεργασία δεδομένα (π.χ. κρυπτογράφηση, ανωνυμοποίηση, έλεγχος πρόσβασης κτλ), το δεύτερο είδος αφορά τα γενικά μέτρα ασφαλείας που αφορούν το συγκεκριμένο σύστημα στο οποίο γίνεται η επεξεργασία (π.χ. Λειτουργική ασφάλεια, αντίγραφα ασφαλείας, ασφάλεια υλικού κλπ.) και το τρίτο μέρος αποτελούν τα οργανωτικά μέτρα (όπως πολιτικές, οργάνωση προσωπικού, πολιτικές διαχείρισης παραβιάσεων, σχέση με τρίτα μέρη κτλ).

Ο διενεργών την επεξεργασία πρέπει να ελέγξει ότι το κάθε μέτρο ασφαλείας συμβαδίζει με τις βέλτιστες πρακτικές ασφαλείας, να διασφαλίσει ότι αυτό έχει περιγραφθεί με σαφήνεια μέσα στην αναφορά της Εκτίμησης αντικτύπου και να κρίνει, εν τέλει, την καταλληλόλητά του. Αφού, έχουν εντοπισθεί και αναλυθεί πλέον και τα υφιστάμενα μέτρα προστασίας πρέπει να γίνει η τελική αξιολόγηση του κινδύνου.

9.1.3.8. Αξιολόγηση του κινδύνου: Πιθανές παραβιάσεις της ιδιωτικότητας.

Για την τελική αξιολόγηση του κινδύνου, η προσέγγιση της CNIL προβλέπει ότι για κάθε απευκταίο γεγονός (δηλαδή, για την Αθέμιτη πρόσβαση σε δεδομένα, για την Ανεπιθύμητη τροποποίηση των δεδομένων και την μη διαθεσιμότητα των δεδομένων) πρέπει να καθορισθούν οι συνέπειες που θα έχει, αν αυτό πραγματωθεί, για την ιδιωτικότητα των υποκειμένων. Περαιτέρω, πρέπει να εκτιμηθούν η σοβαρότητα ιδίως ανάλογα με το επιζήμιο χαρακτήρα των συνεπειών και κατά περίπτωση των μέτρων ασφαλείας που ενδέχεται να την τροποποιήσουν, ενώ παράλληλα, πρέπει να εντοπισθούν οι απειλές στα υποστηρικτικά στοιχεία της επεξεργασίας τα οποία θα μπορούσαν να οδηγήσουν στην πραγμάτωση ενός απευκταίου γεγονότος και οι πηγές κινδύνων που θα μπορούσαν να τις προκαλέσουν καθώς και να εκτιμηθεί η πιθανότητα σε συνάρτηση με το επίπεδο ευπάθειας που παρουσιάζουν τα υποστηρικτικά στοιχεία της επεξεργασίας και την ικανότητα των πηγών του κινδύνου να εκμεταλλευτούν αυτές.

[129] CNIL (Commission Nationale de l'Informatique et des Libert´es): Privacy Impact Assessment: Methodology (how to carry out a PIA). CNIL (2015). Σελ. 7

Οι κίνδυνοι, λοιπόν, που θα εντοπισθούν μέσω αυτής της συστηματικής διαδικασίας και σε συνάρτηση με τα υπάρχοντα μέτρα προστασίας μπορούν να αξιολογηθούν και να θεωρηθούν αποδεκτοί ή μη. Στην περίπτωση δε που δεν θεωρείται ότι είναι αποδεκτοί θα πρέπει να προταθούν καινούργια μέτρα προστασίας και να επαναληφθεί αυτό το στάδιο μέχρι ο κίνδυνος να φτάσει σε ένα αποδεκτό επίπεδο.

Αξίζει να σημειωθεί ότι στον κατάλογο που έχει δημοσιεύσει η CNIL περιέχεται ένας πολύ μεγάλος αριθμός εξειδικευμένων μέτρων προστασίας, που μπορούν να φανούν ιδιαίτερα χρήσιμα για την υποβοήθηση στο στάδιο της επιλογής των κατάλληλων μέτρων προστασίας. Ωστόσο, αυτό που παρατηρείται είναι ότι η προσέγγιση της CNIL θέτει στην αξιολόγηση της ως πρώτο στόχο τον καθορισμό των επιπτώσεων που θα έχει η πραγμάτωση ενός απευκταίου γεγονότος. Παρόλα αυτά, για να αξιολογηθεί η επίπτωση θα πρέπει πρώτα να αξιολογηθούν η σοβαρότητα και η πιθανότητα. Ως εκ τούτου, φαίνεται ότι τα συγκεκριμένα βήματα είναι σε λανθασμένη σειρά και θα πρέπει να προηγηθεί η αξιολόγηση της σοβαρότητας και της πιθανότητας (για κάθε απειλή και κάθε απευκταίο γεγονός) και ύστερα να αξιολογηθούν οι επιπτώσεις, ενώ το ίδιο πρόβλημα φαίνεται να επαναλαμβάνεται και στο υποστηρικτικό εργαλείο που παρέχει η συγκεκριμένη μεθοδολογική προσέγγιση.[130]

9.1.3.9. Στόχοι για την αντιμετώπιση των κινδύνων

Μία από τις σημαντικότερες καινοτομίες που εισάγονται με την μεθοδολογική προσέγγιση CNIL είναι ότι καθορίζονται σχετικώς οι στόχοι που πρέπει να επιτευχθούν σε συνάρτηση με το επίπεδο του κινδύνου. Ειδικότερα, πρώτη περίπτωση αποτελεί όταν υπάρχει κίνδυνος με υψηλή σοβαρότητα και υψηλή πιθανότητα. Στην περίπτωση αυτή οι κίνδυνοι θα είναι και πολύ πιθανόν να επέλθουν αλλά και οι επιπτώσεις τους θα είναι πολύ σοβαρές. Ως εκ τούτου, πρέπει οπωσδήποτε να αποφευχθούν ή να περιοριστούν με την εφαρμογή μέτρων ασφαλείας που θα μειώσουν την σοβαρότητα και την πιθανότητα τους. Δεύτερη περίπτωση αποτελούν οι κίνδυνοι με υψηλή σοβαρότητα αλλά χαμηλή πιθανότητα. Ειδικότερα, για αυτούς τους κινδύνους αναφέρεται ότι αυτοί μπορούν να γίνουν αποδεκτοί αλλά μόνο εάν αποδειχθεί ότι δεν είναι δυνατόν με κανένα τρόπο να μειωθεί η σοβαρότητα τους και υπό την ταυτόχρονη προϋπόθεση ότι η σοβαρότητα τους είναι αμελητέα. Τρίτη περίπτωση αποτελούν οι κίνδυνοι με χαμηλή σοβαρότητα αλλά υψηλή πιθανότητα. Όπως και προηγουμένως, έτσι και σε αυτή την περίπτωση οι κίνδυνοι μπορούν να γίνουν αποδεκτοί, μόνον, όμως, εφόσον συντρέχουν

[130] Βλ. Bisztray, T., Gruschka, N. (2019). Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In: Askarov, A., Hansen, R., Rafnsson, W. (eds) Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science(), vol 11875. Springer, Cham.

σωρευτικώς οι προυποθέσεις ότι η σοβαρότητά τους είναι αμελητέα και η πιθανότητά τους δεν μπορεί να μειωθεί με κανέναν τρόπο. Τέλος, η περίπτωση που οι κίνδυνοι έχουν χαμηλή και πιθανότητα και σοβαρότητα μπορούν να γίνουν αποδεκτοί.[131]

9.1.4 ISO 29134

Για την αξιολόγηση του κινδύνου το ISO 29134:2020 έχει την δομή (όπως γενικότερα συνηθίζουν οι πιστοποιήσεις ISO) «Αντικείμενο» – «είσοδος» – «επιδιωκόμενο αποτέλεσμα» (Objective – input – expect outpout). Ειδικότερα, στην φάση μελέτης του κινδύνου το ISO ζητά από τον διενεργούντα την επεξεργασία να θέσει ως «είσοδο», δηλαδή, ως δεδομένο της εν λόγω φάσης την συστηματική περιγραφή της επεξεργασίας, όπως αυτή προέκυψε από την αντίστοιχη προγενέστερη φάση, ενώ για κάθε επόμενο στάδιο τίθεται ως είσοδος το προηγούμενο στάδιο. Ως εκ τούτου, για την αξιολόγηση του κινδύνου το ISO 29134 κατ' αρχάς θεωρεί ότι ο κίνδυνος πρέπει να εντοπιστεί, στην συνέχεια να αναλυθεί, ύστερα να αξιολογηθεί και τέλος να εντοπιστούν εκείνα τα κατάλληλα μέτρα που θα τον περιορίσουν.

9.1.4.1. Εντοπισμός του Κινδύνου

Κατ΄ αρχάς για τον εντοπισμό του κινδύνου το ISO υποδεικνύει στους διενεργούντες την εκτίμηση να χρησιμοποιήσουν τα κατάλληλα εργαλεία και τεχνικές εντοπισμού κινδύνων, χωρίς να εξηγεί περαιτέρω ποια είναι αυτά. Παρόλα αυτά, αναφέρει ότι οι κίνδυνοι συνήθως, αλλά όχι αποκλειστικά, περιλαμβάνουν την Αθέμιτη πρόσβαση (έλλειψη εμπιστευτικότητας), την αθέμιτη τροποποίηση των δεδομένων (έλλειψη ακεραιότητας) και την μη διαθεσιμότητα των δεδομένων (έλλειψη διαθεσιμότητας). Σε αντίθεση, όμως, με την μεθοδολογική προσέγγιση της CNIL, το ISO 29134 θεωρεί πως οι εν λόγω κίνδυνοι δεν είναι οι μόνοι και θα πρέπει να ληφθούν υπόψη και άλλες παράμετροι, όπως η συλλογή περισσότερων δεδομένων από αυτά που είναι απαραίτητα για την επίτευξη του σκοπού της επεξεργασίας, την μη εξουσιοδοτημένη ή της απαγορευμένης διασύνδεσης δεδομένων, την λανθασμένη ενημέρωση των υποκειμένων για τους σκοπούς της επεξεργασίας (έλλειψη διαφάνειας), την μη ικανοποίηση των δικαιωμάτων των υποκειμένων, την επεξεργασία δεδομένων χωρίς να το γνωρίζουν τα υποκείμενα των δεδομένων ή χωρίς να έχουν δώσει την συγκατάθεση τους (όπου αυτό απαιτείται), την λανθασμένη κοινολόγηση δεδομένων σε τρίτους, ή την σωστή μεν κοινολόγηση αλλά την περαιτέρω επεξεργασία για διαφορετικούς από τους προβλεπόμενους

[131] Βλ. Δ. Τζέλλης, Μ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022, σελ 9

σκοπούς και τέλος την διατήρηση δεδομένων για μεγαλύτερο διάστημα από αυτό που έχει προβλεφθεί .

Για τον εντοπισμό αυτών των κινδύνων το ISO29134 υποδεικνύει ότι θα πρέπει να γίνει από ανθρώπους που έχουν γνώση στον εντοπισμό κινδύνων σχετικά με την ιδιωτικότητα. Αναφέρει επίσης ότι αφού εντοπιστεί, το τι αναμένεται να γίνει μέσω ανάπτυξης, πρέπει για κάθε σενάριο να εντοπιστεί και τι επιπτώσεις θα είχε αυτό, αν τελικά πραγματωθεί.

9.1.4.2. Ανάλυση του Κινδύνου

Σκοπός του συγκεκριμένου σταδίου είναι να αναλυθούν οι συνέπειες που θα έχουν στην ιδιωτικότητα των υποκειμένων οι εντοπισθέντες στο προηγούμενο στάδιο κίνδυνοι, και να αξιολογηθεί η σοβαρότητα και η πιθανότητα τους.

Ειδικότερα, σε αυτό το στάδιο το ISO29134 φαίνεται να ομοιάζει αρκετά με την προσέγγιση της CNIL, αφού θεωρεί ότι η ανάλυση του κινδύνου βασίζεται πάνω σε μία λεπτομερή ανάλυση του προγράμματος, του συστήματος ή της επεξεργασίας. Πιο συγκεκριμένα, αναφέρει ότι η ανάλυση του κινδύνου περιλαμβάνει τον εντοπισμό των προσωπικών δεδομένων και των υποστηρικτικών στοιχείων τα οποία βρίσκονται σε κίνδυνο, παρουσιάζουν, δηλαδή, ευπάθειες που μπορούν κάποιοι (ή κάτι) μέσω απειλών να εκμεταλλευτούν. Επιπλέον, η ανάλυση του κινδύνου περιλαμβάνει και την αξιολόγηση της πιθανότητας και της σοβαρότητας αυτά να συμβούν, ενώ πρέπει να ληφθούν υπόψη τα υπάρχοντα μέτρα αντιμετώπισης τους και το κατά πόσο είναι ικανά να αντιμετωπίσουν τους εντοπισθέντες κινδύνους. Όπως και στην προσέγγιση της CNIL, έτσι και εδώ αναφέρεται ότι για την εκτίμηση της πιθανότητας του κινδύνου πρέπει να ληφθεί υπόψη η ικανότητα των πηγών του κινδύνου να εκμεταλλευτούν τις ευπάθειες των υποστηρικτικών στοιχείων και των ήδη υπαρχόντων μέτρων προστασίας (το πόσο ικανά, δηλαδή, είναι να αποτρέψουν αυτή την «εκμετάλλευση»)

Για κάθε κίνδυνο που εντοπίζεται πρέπει επίσης να καθοριστούν ποιες είναι οι πηγές του κινδύνου (παραπέμπει στο ISO Guide 73:2009, 3.5.1.5), ποιες είναι οι πιο πιθανές απειλές και ποια είναι τα ήδη υφιστάμενα μέτρα προστασίας και πως βοηθούν στην αντιμετώπιση αυτών των κινδύνων;

Μία καινοτομία, ωστόσο, που φαίνεται να παρουσιάζεται στο ISO 29134 είναι ότι για την ανάλυση των κινδύνων θα πρέπει να ληφθεί υπόψη και η ευαισθησία των δεδομένων και ο βαθμός εμπιστευτικότητας τους και να συζητηθούν αυτά με τα υπόλοιπα εμπλεκόμενα μέρη.

Γενικότερα, το ISO 29134 φαίνεται να ομοιάζει με την προσέγγιση Fraunhofer στο σημείο που θέτει στο επίκεντρο την συζήτηση μεταξύ των εμπλεκομένων μερών.

9.1.4.3. Κατηγοριοποίηση του Κινδύνου

Επίσης μία καινοτομία που εισάγεται με το ISO 29134 είναι ότι το τελευταίο υποδεικνύει ότι οι εντοπισθέντες κίνδυνοι θα πρέπει να κατηγοριοποιηθούν. Έτσι, οι πόροι του οργανισμού θα μπορέσουν να κατανεμηθούν σωστά, περισσότεροι πόροι δηλαδή για τους πολύ μεγάλης σημασίας κινδύνους και λιγότερους πόρους για τους κινδύνους με λιγότερη σημασία αντίστοιχα. Αυτή η κατηγοριοποίηση των κινδύνων πρέπει να προκύψει μέσα από την αξιολόγηση, για κάθε κίνδυνο της πιθανότητας και της σοβαρότητας του, να επέλθει.

9.1.4.4. Επιλογές αντιμετώπισης των κινδύνων

Σύμφωνα με το ISO 29134:2020 η αντιμετώπιση των κινδύνων μπορεί να περιλαμβάνει, χωρίς να περιορίζεται σε αυτό βέβαια, την αναδιάρθρωση της όλης διαδικασίας. Η επιλογή των κατάλληλων μέτρων αντιμετώπισης των κινδύνων πρέπει να περιλαμβάνει μία στάθμιση μεταξύ της υποχρέωσης της προστασίας των δεδομένων από την μία και του κόστους και της προσπάθειας που χρειάζεται για αυτό από την άλλη. Ως εκ τούτου, ένας οργανισμός μπορεί να μην θελήσει όχι απλώς να αναδιαρθρώσει την προβλεπόμενη επεξεργασία, αλλά να μην λάβει ούτε επιπλέον μέτρα προστασίας, αν θεωρηθεί ότι αυτά που ήδη υφίστανται επαρκούν για την αντιμετώπιση των κινδύνων.

Αυτό που επισημαίνεται, ωστόσο, είναι ότι ο υπεύθυνος επεξεργασίας θα πρέπει να αναζητήσει ενεργά την συμμετοχή των εμπλεκόμενων μερών στην επεξεργασία και είναι διαφανές και κατανοητό από όλους οι λόγοι που οδηγούν στις εν λόγω αποφάσεις.

Ως εκ τούτου, το ISO 29134 παρουσιάζει τέσσερις επιλογές για την αντιμετώπιση των κινδύνων. Αυτές είναι η μείωση του κινδύνου, η διατήρηση του κινδύνου, η αποφυγή του κινδύνου, και η μεταφορά του κινδύνου.

Αναλυτικότερα, όσον αφορά την πρώτη επιλογή, την μείωση του κινδύνου, αυτή μπορεί να επιτευχθεί μέσω της επιλογής κατάλληλων ελέγχων, χωρίς βέβαια να αναφέρεται ποιοι ακριβώς είναι αυτοί οι έλεγχοι. Επισημαίνεται, ωστόσο, ότι και αν ακόμα μετά την επιλογή αυτών των μέτρων παραμένει κίνδυνος, ο οργανισμός θα πρέπει να αξιολογήσει αν αυτός ο κίνδυνος είναι αποδεκτός ή όχι και αν όχι να επιλέξει εκ νέου νέα μέτρα μέχρι ο κίνδυνος να φτάσει σε αποδεκτά επίπεδα. Ειδικότερα, τα μέτρα για την μείωση του κινδύνου μπορεί να

ποικίλλουν και να περιλαμβάνουν αλλαγές στην επεξεργασία, αλλαγές στην οργανωτική μορφή (όπως αλλαγή στην πολιτική και στις διαδικασίες επεξεργασίας των δεδομένων) ή αλλαγές στα προσόντα του εργασιακού δυναμικού (εκπαίδευση του προσωπικού, απόκτηση πιστοποιητικών κτλ). Επιπλέον, μπορεί να χρειασθεί τροποποίηση στα υποστηρικτικά στοιχεία της επεξεργασίας είτε αυτά θα είναι προληπτικά μέτρα, μέτρα εντοπισμού σφαλμάτων ή διορθωτικά μέτρα.

Δεύτερη επιλογή είναι η διατήρηση του κινδύνου. Ειδικότερα, όταν οι κίνδυνοι είναι εντός των αποδεκτών ορίων τότε δεν χρειάζεται να ληφθούν επιπλέον μέτρα και πρέπει να διατηρηθούν τα ήδη υφιστάμενα για να διατηρηθεί ο κίνδυνος σε αυτό το επίπεδο.

Τρίτη επιλογή είναι η αποφυγή του κινδύνου. Ειδικότερα, όταν ο κίνδυνος αξιολογηθεί ως πολύ υψηλός και δεν φαίνεται πως υπάρχουν σαφή μέτρα που εγγυώνται την μείωση του τότε η επεξεργασία θα πρέπει να ακυρωθεί, ώστε να αποφευχθούν και οι κίνδυνοι που προέρχονται από αυτόν.

Τέλος, τελευταία επιλογή είναι η μεταφορά του κινδύνου που αφορά περιπτώσεις όπου ο κίνδυνος μοιράζεται μεταξύ περισσότερων οργανισμών. Αυτή η επιλογή περιλαμβάνει περιπτώσεις όπου λαμβάνεται απόφαση (συνήθως μέσω υπεργολαβίας) να αναλάβει άλλος οργανισμός την ασφάλεια των πληροφοριακών συστημάτων. Η συγκεκριμένη επιλογή αφορά οργανισμούς οι οποίοι είτε θεωρούν ότι δεν έχουν επαρκή γνώση και κατάρτιση για την αντιμετώπιση των κινδύνων, είτε έχουν θέσει πολύ υψηλούς στόχους προστασίας και ως εκ τούτου θεωρούν ωφέλιμο να αναθέσουν αυτό το έργο σε πολύ εξειδικευμένους συνεργάτες.

9.1.4.5. Καθορισμός των μέτρων αντιμετώπισης

Έχοντας πλέον εντοπίσει, αναλύσει και αξιολογήσει τους κινδύνους, πρέπει πλέον να γίνει η επιλογή των κατάλληλων μέτρων αντιμετώπισης των κινδύνων. Ο τρόπος για να γίνει αυτό σύμφωνα με το ISO 29134 είναι μέσω της συλλογής των ήδη υφισταμένων και γνωστών μέτρων αντιμετώπισης των κινδύνων και ο έλεγχος αυτών του κατά πόσον επαρκούν για την αντιμετώπιση των εντοπισμένων κινδύνων. Εναλλακτικά μέτρα αντιμετώπισης πρέπει να προστεθούν στα ήδη υπάρχοντα μέχρι ο κίνδυνος να αξιολογηθεί ότι είναι εντός αποδεκτών ορίων. Ως εκ τούτου, η αξιολόγηση αυτή, του αποδεκτού δηλαδή, του κινδύνου σε σχέση με τα μέτρα προστασίας πρέπει να γίνει για τις εξής κατηγορίες. Πρώτον, σχετικά με τα προσωπικά δεδομένα τα μέτρα αυτά πρέπει να εγγυώνται ότι είναι σχεδιασμένα έτσι, ώστε, να προλαμβάνουν παραβιάσεις του συστήματος, να εντοπίζουν τέτοιες παραβιάσεις ή να αποκαταστούν την ασφάλεια τους. Αν αυτά δεν επαρκούν τότε θα πρέπει να μειωθούν οι

συνέπειες, δηλαδή το αποτέλεσμα των ανωτέρω (αν αυτά πραγματωθούν) να μην επηρεάζει σημαντικά την επεξεργασία την ίδια αλλά και τα υποκείμενα των δεδομένων. Αν και αυτό δεν επαρκεί, τότε τα μέτρα αντιμετώπισης θα πρέπει να επικεντρωθούν στις πηγές των κινδύνων και να καταστήσουν αυτές ανίκανες να εκμεταλλευτούν τις ευπάθειες του συστήματος. Στο τέλος, αν ούτε και αυτά τα μέτρα επαρκούν, τα μέτρα πρέπει να επικεντρωθούν στα υποστηρικτικά στοιχεία της επεξεργασίας και αναμφίβολα να είναι ικανά να αποτρέπουν και να προλαμβάνουν τους κινδύνους που προκύπτουν από την εκμετάλλευση των ευπαθειών του συστήματος.

Ως εκ τούτου, στο τέλος αυτής της διαδικασίας πρέπει ο κίνδυνος να είναι πλέον εντός αποδεκτών ορίων. Αν όχι, τότε είτε πρέπει να επιλεχθούν εναλλακτικά μέτρα είτε η επεξεργασία να εγκαταλειφθεί.

10. Τρίτη φάση της ΕΑΠΔ (Φάση Εφαρμογής)

Αφότου, έχουν εντοπισθεί και αξιολογηθεί οι κίνδυνοι και έχουν επιλεχθεί τα κατάλληλα μέτρα αντιμετώπισης τους, τα τελευταία πρέπει, πλέον, να εφαρμοστούν. Αφού εφαρμοστούν, τα μέτρα αυτά πρέπει να δοκιμαστούν σε πραγματικό περιβάλλον πλέον, ως προς την ικανότητα τους να αντιμετωπίσουν τους κινδύνους. Η αξιολόγηση αυτή θα πρέπει να γίνει με συστηματικό τρόπο και τα αποτελέσματά της να καταγραφούν. Η αξιολόγηση αυτή, πρέπει να γίνεται τακτικά, ώστε, να διασφαλίζεται ότι δεν έχει αλλάξει το οτιδήποτε που μπορεί να επηρεάσει την ασφάλεια της διαδικασίας.[132]

11. Τέταρτη φάση της ΕΑΠΔ (Φάση Περιοδικής Επαναξιολόγησης)

Έχοντας, πλέον, ολοκληρώσει όλα τα προηγούμενα στάδια πρέπει να ληφθούν μέτρα για την διαχρονική διασφάλιση της βιωσιμότητάς του. Οι κίνδυνοι θα πρέπει συνεχώς να βρίσκονται υπό εποπτεία και να γίνονται τακτικοί έλεγχοι της αποτελεσματικότητα των μέτρων προστασίας. Αν προκύψουν νέοι κίνδυνοι που συνδέονται με την επεξεργασία, θα πρέπει να γίνει επανεκτίμηση του κινδύνου και να ληφθούν νέα μέτρα για τον μετριασμό τους, όπως

[132] Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact ssessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag. Σελ. 51

εξάλλου πρεσβεύει και η παράγραφος 11 του άρθρου 35 του ΓΚΠΔ. Η τελική έκθεση της ΕΑΠΔ δύναται να αποτελέσει την βάση για την καινούργια αυτή μελέτη και να ληφθεί υπόψη η τεκμηρίωση σχετικά με τους κινδύνους. Έτσι, θα πρέπει να επαναληφθεί η διαδικασία για τον εντοπισμό, την ανάλυση και την αξιολόγηση του κινδύνου, καθώς και για την εφαρμογή εύρεση των κατάλληλων μέτρων προστασίας[133]. Η ΕΑΠΔ αποτελεί μία διαρκή διαδικασία και όχι μία πράξη που διενεργείται άπαξ.

12. Τελικά συμπεράσματα

12.1 Η συστηματική προσέγγιση της ΕΑΠΔ ως απόρροια της αρχής της Διαφάνειας και της Λογοδοσίας

Όπως ήδη αναφέρθηκε η υποχρέωση για την διενέργεια εκτίμησης αντικτύπου προκύπτει και είναι άρρηκτα συνδεδεμένη με την αρχή της λογοδοσίας. Από την άλλη, η αρχή της διαφάνειας είναι άρρηκτα συνδεδεμένη με την αρχή της λογοδοσίας καθώς και οι δύο αποτελούν βασικές αρχές μέσω των οποίων μπορεί να αποδειχθεί η συμμόρφωση.

Ειδικότερα, η αρχή της διαφάνειας, στο πλαίσιο του δικαίου προσωπικών δεδομένων προκύπτει από την ενσωμάτωση της στον ΓΚΠΔ στο άρθρο 5 παρ.1 περ.1 όπου προβλέπεται ότι τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»). Στο πλαίσιο της προστασίας προσωπικών δεδομένων, παρότι δεν υπάρχει σαφής ορισμός της διαφάνειας, η οποία είναι νομικά σύνθετη έννοια, πρέπει να ερμηνεύεται μέσω του άρθρου 39 το οποίο παρέχει πληροφορίες σχετικά με την έννοια και το προσδοκώμενο αποτέλεσμα της εφαρμογής της. Έτσι, η διαφάνεια διατρέχει όλα τα δικαιώματα του υποκειμένου και προσδίδει διαυγές, φανερό και κατανοητό περιεχόμενο στην παρεχόμενη πληροφορία χωρίς αμφιβολία ή αμφισημία[134].

Από την άλλη πλευρά, η αρχή της λογοδοσίας, όπως ήδη αναφέρθηκε, απαιτεί από τον υπεύθυνο επεξεργασίας να συμμορφώνεται με τις αρχές του άρθρου 5 του ΓΚΠΔ και να είναι σε θέση να αποδείξει αυτή τη συμμόρφωση. Η συμμόρφωση αυτή, διαμορφώνεται με

[133] Βλ. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact ssessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag. Σελ. 52

[134] Βλ. Μ. Μυλώση, Ε. Αλεξανδροπούλου – Αιγυπτιάδου, «Η ενημέρωση του υποκειμένου προσωπικών δεδομένων σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων και τον Ν.4624/2019 – Κριτικές σκέψεις», ΔiΜΜΕ, 2/2020, σελ. 188- 189

διάφορους τρόπους και βασίζεται στην πολυπλοκότητα και την φύση της επεξεργασίας. Μεταξύ αυτών των τρόπων, όμως, είναι ,κυρίως, η τήρηση των αρχών προστασίας και των υπόλοιπων υποχρεώσεων του ΓΚΠΔ κατά τη διάρκεια ολόκληρου του κύκλου της επεξεργασίας και ως εκ τούτου και κατά τη διενέργεια εκτίμησης αντικτύπου.

Έτσι, λοιπόν, λόγω της άρρηκτης σύνδεσης μεταξύ της διαφάνειας και της λογοδοσίας προκύπτει ότι και η διαφάνεια διατρέχει όλο το φάσμα της επεξεργασίας τόσο στις εκ των προτέρων (ex-ante), όσο και στις εκ των υστέρων (ex-post) διαδικασίες που αποσκοπούν στην συμμόρφωση με την προστασία των δεδομένων, άρα και κατά την διενέργεια της εκτίμησης αντικτύπου. Όσον αφορά, όμως, την διαφάνεια σε σχέση με την μεθοδολογία για την διενέργεια εκτίμησης αντικτύπου, η διαφάνεια πρέπει να γίνει κατανοητή υπό μία πιο στενή έννοια. Ως εκ τούτου, στο πλαίσιο αυτό η εκπλήρωση της αρχής της διαφάνειας πρέπει να θεωρηθεί ότι απαιτεί την κατανόηση της διαδικασίας, των λόγων και του τρόπου με τον οποίο διενεργείται η εκτίμηση του κινδύνου, από τα υποκείμενα των δεδομένων και κατ' επέκταση από τις εποπτικές αρχές[135].

Ως εκ τούτου, και σύμφωνα με τα επιμέρους στοιχεία στα οποία αναλύεται περαιτέρω η αρχή της διαφάνειας στο πλαίσιο του δικαίου προστασίας προσωπικών δεδομένων, καταδεικνύεται ότι η εκτίμηση του κινδύνου που περιλαμβάνεται σε μία ΕΑΠΔ πρέπει να είναι αξιολογήσιμη, λογικά και σαφώς καθορισμένη καθώς και κατανοητή[136]. Συνοψίζοντας, η εκτίμηση του κινδύνου (η δεύτερη φάση μίας ΕΑΠΔ δηλαδή) πρέπει να περιέχει δύο στοιχεία. Πρώτον Θα πρέπει να υπάρχει σαφής ένδειξη της μεθοδολογίας που χρησιμοποιήθηκε για την αξιολόγηση του κινδύνου προστασίας δεδομένων, η οποία θα προσδιορίζει τις διαδικασίες και τα κριτήρια για την αξιολόγηση του κινδύνου με συστηματικό και αναγνωρίσιμο τρόπο. Δεύτερον, θα πρέπει οι εμπλεκόμενοι φορείς με τους οποίους διεξάγεται διαβούλευση κατά τη διαδικασία της εκτίμησης του κινδύνου, να είναι σαφώς καθορισμένοι και οι προτάσεις τους να προσδιορίζονται και να αντικατοπτρίζονται όπου αυτό προβλέπεται. Επιπλέον, θα πρέπει να προκύπτει ο βαθμός κατά τον οποίο προσδιορίζεται ο κίνδυνος ως αποτέλεσμα των εν λόγω διαβουλεύσεων με τα εμπλεκόμενα μέρη,[137].

Αυτός είναι ο βασικότερος λόγος που θα πρέπει μία ΕΑΠΔ να έχει σαφώς καθορισμένα βήματα, και ειδικά στην δεύτερη φάση (στην αξιολόγηση δηλαδή του κινδύνου) να προκύπτει

[135] Βλ. I. Nwankwo, Towards a transparent and systematic approach to conducting risk assessment under Article 35 of the GDPR, 2021, σελ. 85
[136] Βλ.I. Nwankwo, ό.π., σελ 86 εκτενής ανάλυση της αρχής της διαφάνειας
[137] Βλ. I. Nwankwo, ό.π., σελ. 86

με μεγάλη σαφήνεια το πως ο κίνδυνος εντοπίστηκε, αναλύθηκε και εν τέλει αξιολογήθηκε. Όμως, εκτός από την δεύτερη φάση (η οποία αποτελεί αναμφισβήτητα τον πυρήνα της ΕΑΠΔ) και οι υπόλοιπες φάσεις που αποτελούν την βάση (όπως η πρώτη φάση και η φάση εκκίνησης) πάνω στην οποία θα στηριχθεί η αξιολόγηση του κινδύνου, πρέπει να εκτελεστούν με προσοχή και να υλοποιηθούν με γνώμονα τον προσδιορισμό του κινδύνου που προκύπτει από την επεξεργασία σε μεταγενέστερο επίπεδο. Έτσι, τα αποτέλεσμα αυτής της προσέγγισης θα παρέχουν συνοχή, σαφήνεια και τα κατάλληλα κριτήρια για τη μέτρηση της ορθότητας ή μη, της εκ των προτέρων εκτίμησης κινδύνου που περιέχεται σε μια ΕΑΠΔ και θα καταστήσει τη διαδικασία επαληθεύσιμη, συμμορφούμενη και με την αρχή της διαφάνειας.

Εξ αυτού του λόγου, γίνεται λόγος και για «συστηματική προσέγγιση», η οποία παρόλο που δεν αποτελεί αυτοτελή αρχή του ΓΚΠΔ, είναι ζητούμενο του τελευταίου. Επιτάσσεται δηλαδή, να εφαρμόζονται, οι κανόνες του ΓΚΠΔ συστηματικά και με συνέπεια. Αυτό εξάλλου, καταδεικνύεται και από το μηχανισμό συνεκτικότητας που υιοθετεί στο σύνολό του ο ΓΚΠΔ και ειδικά μέσω του μηχανισμού που επιτρέπει (ή επιτάσσει) στις Αρχές να εκδίδουν «λευκές» και «μαύρες» λίστες σύμφωνα με τις παραγράφους 3 και 4 του άρθρου 35 ΓΚΠΔ. Επιπλέον, κατά μία άποψη η συστηματική προσέγγιση ορίζεται ως μία μεθοδική, επαναλαμβανόμενη και ικανή να διδαχθεί με μία βήμα προς βήμα διαδικασία. Στην ουσία, όμως, πρόκειται για μία διαδικασία που αποσκοπεί στον "εντοπισμό των πιο αποτελεσματικών μέσων για τη δημιουργία συνεπώς και βέλτιστων αποτελεσμάτων". [138]

Αυτό έχει πολύ μεγάλη σημασία για την διενέργεια της ΕΑΠΔ, γιατί η τελευταία όταν χρειαστεί, θα τεθεί υπό εξέταση. Όσο, λοιπόν, πιο συστηματική προσέγγιση έχει μία ΕΑΠΔ τόσο πιο εύκολο θα είναι να αξιολογηθεί εν τέλει και από την Αρχή, όταν αυτό απαιτηθεί, δημιουργώντας έτσι τόσο στον υπεύθυνο επεξεργασίας, όσο και στα λοιπά εμπλεκόμενα μέρη την αυτοπεποίθηση, ότι δεν θα βρεθούν αντιμέτωποι με αναπάντεχες συνέπειες.

12.2 Η εκτίμηση αντικτύπου δεν είναι ένας απλός έλεγχος νομιμότητας

Τα όσα αναλύθηκαν ανωτέρω έχουν πολύ μεγάλη σημασία από την στιγμή που δεν υπάρχει μία κοινώς αποδεκτή μεθοδολογική προσέγγιση για την διενέργεια εκτίμησης αντικτύπου. Από την μελέτη της βιβλιογραφίας, μάλιστα, προκύπτει ότι συνεχώς αναπτύσσονται νέες έρευνες που εντοπίζουν ελλείψεις στις ήδη υπάρχουσες προσεγγίσεις ή αναπτύσσουν νέες, γεγονός που δημιουργεί ακόμα μεγαλύτερη ανασφάλεια στο πλαίσιο της

[138] Βλ. I. Nwankwo, ό.π., σελ. 35

εκτίμησης αντικτύπου. Παρόλα αυτά, τα όσα αναπτύχθηκαν ως άνω, αποτελούν χαρακτηριστικά κάθε προσέγγισης που θεωρείται αποδεκτή. Πρόκειται, δηλαδή, για επιχειρήματα που συνηγορούν στο ότι μία ΕΑΠΔ πρέπει να διενεργείται με συστηματικό τρόπο. Αυτό μπορεί να γίνει ακόμα πιο σαφές αναλύοντας τι δεν αποτελεί μία σωστή ΕΑΠΔ.

Μία ΕΑΠΔ δεν σχετίζεται με έναν απλό νομικό έλεγχο συμμόρφωσης της επεξεργασίας, όπως συνέβαινε παλαιότερα με τις προσεγγίσεις για την αξιολόγηση της ιδιωτικότητας (PIA). Αυτές οι προσεγγίσεις, εξάλλου, κρίθηκαν από μερίδα ειδικών ότι δεν υπαγόρευαν μια μεθοδική προσέγγιση για την εκτίμηση της ιδιωτικότητας παρά αποτελούσαν περισσότερο ένα είδος ελέγχου τύπου λίστας.[139] Αντιθέτως, η ΕΑΠΔ παρόλο που περιλαμβάνει και αυτή τον νομικό έλεγχο, δεν περιορίζεται σε αυτό, αλλά όπως έχει προαναφερθεί, αποτελεί μία συστηματική και εις βάθος αναζήτηση, ανάλυση και αξιολόγηση των κινδύνων καθώς και εντοπισμού προς εφαρμογή μέτρων προστασίας για να αντιμετωπιστούν οι εντοπισθέντες κίνδυνοι. Έτσι, λοιπόν, αυτές οι δύο μελέτες μπορούν να εκπονηθούν παράλληλα σε μία κοινή διαδικασία, όπως αυτή της ΕΑΠΔ. Αυτό που είναι σημαντικό, όμως, είναι να μην επικαλύπτει η μία την άλλη, αλλά να αλληλοσυμπληρώνονται. [140]

Ένας ακόμη κίνδυνος τον οποίο διατρέχουν οι διενεργούντες την εκτίμηση αντικτύπου είναι να αντιμετωπίσουν με διακπεραιωτικό και όχι ουσιαστικό τρόπο τα πρότυπα (templates) για την εκτίμηση αντικτύπου. Πρέπει να επισημανθεί, δηλαδή, ότι τα συγκεκριμένα υποδείγματα που έχουν αναπτυχθεί από διαφορετικές πλευρές (π.χ. Εθνικές Αρχές Προστασίας, Επιστημονικά Ινστιτούτα κτλ) έχουν ως σκοπό, κυρίως, να κατευθύνουν τους διενεργούντες την επεξεργασία και να θέσουν κάποιες βασικές κατευθυντήριες γραμμές. Σε καμία περίπτωση, όμως, δεν μπορεί να θεωρηθεί ότι επειδή, απλώς, συμπληρώθηκαν τα κενά ή απαντήθηκαν οι ερωτήσεις των εν λόγω υποδειγμάτων, μπορεί να θεωρηθεί η ΕΑΠΔ ολοκληρωμένη. Μία τέτοια προσέγγιση, οδηγεί στην αντιμετώπιση της ΕΑΠΔ και πάλι ως μία λύση τύπου checklist. Αντιθέτως, όπως αναπτύχθηκε και παραπάνω, η προσέγγιση θα πρέπει να είναι συστηματική και συνεπής προσδίδοντας μέσω της κατάλληλης μεθοδολογίας διαφάνεια, συνέπεια και επαληθευσιμότητα.

Παρά την φτωχή, μέχρι στιγμής, νομολογία που υπάρχει στην χώρας μας σχετικά με την εκτίμηση αντικτύπου και ακόμα περισσότερο σχετικά με την μεθοδολογία αυτής, φαίνεται πως την παραπάνω άποψη, υιοθετεί και η ΑΠΔΠΧ. Αυτό καταδεικνύεται από την αιτιολογική

[139] Στην βιβλιογραφία περιγράφονται ως (Checklist, Checkboxes, tickboxes)
[140]Βλ. Dariusz Kloza, Niels van Dijk, Paul De Hert,Chapter 2 - Assessing the European Approach to Privacy and Data Protection in Smart Grids, 2015, Pages 11-47, ISBN 9780128021224, https://doi.org/10.1016/B978-0-12- 02122-4.00002-X. (https://www.sciencedirect.com/science/article/pii/B978012802122400002X)

σκέψη υπ΄αριθμόν 16 της υπ΄αριθμόν 4/2022 απόφαση της. Ειδικότερα, η Αρχή αναγνώρισε μεν πως ο υπεύθυνος επεξεργασίας είχε εκπονήσει ΕΑΠΔ βασισμένη σε ένα πρότυπο που είχε εκδώσει ο ICO που έγκειται στην απάντηση συγκεκριμένων ερωτήσεων, αλλά αναγνώρισε πως οι απαντήσεις που παρείχε ο υπεύθυνος επεξεργασίας δεν ήταν τεκμηριωμένες και ως εκ τούτου, δεν αποδεικνυόταν ότι έχουν εξεταστεί όλοι οι κίνδυνοι. Ενδεικτικό παράδειγμα που παρατίθεται και στην απόφαση είναι το εξής: σε ερώτηση «Είναι εφικτή η επίτευξη του σκοπού χωρίς την συγκεκριμένη επεξεργασία;» δίνεται η απάντηση «Όχι, δεν είναι δυνατόν να εξυπηρετηθούν τα αιτήματα βλαβοδιαχείρισης των συνδρομητών χωρίς την επεξεργασία των συγκεκριμένων προσωπικών δεδομένων»). Σε συνέχεια, αυτού, η ΑΠΔΠΧ εκτίμησε ότι το περιεχόμενο της ΕΑΠΔ δεν ήταν επαρκές, ειδικά ως προς την εκτίμηση της αναγκαιότητας και της αναλογικότητας της επεξεργασίας και επέβαλλε πρόστιμο στον υπεύθυνος επεξεργασίας.

Καταληκτικά, αναφέρεται πως ο διενεργών την επεξεργασία, ανεξαρτήτως του ποια μεθοδολογική προσέγγιση θα επιλέξει, θα πρέπει να την εφαρμόσει με κατάλληλο τρόπο. Επιπλέον, οι περισσότερες μεθοδολογικές προσεγγίσεις (όπως και αυτές που παρουσιάστηκαν στην παρούσα) αποτελούν γενικές μεθοδολογικές προσεγγίσεις. Ως εκ τούτου, είναι πολύ πιθανόν, για να είναι κατάλληλες για συγκεκριμένους τομείς, να πρέπει τροποποιηθούν με τον κατάλληλο τρόπο.

12.3 Το πρόβλημα της αξιολόγησης των ΕΑΠΔ

Ένα ακόμα πρόβλημα που προκύπτει είναι ότι δεν είναι ξεκάθαρος ο τρόπος με τον οποίο αξιολογείται μία ΕΑΠΔ στο σενάριο που αυτή τεθεί υπό την κρίση ΑΠΔΠΧ. Το ερώτημα που γεννάται είναι το πως η Αρχή θα αξιολογήσει την ΕΑΠΔ και ειδικά το πως θα αξιολογήσει την μεθοδολογία, την διαφάνεια, το πεδίο εφαρμογής και τους εν γένει παράγοντες που λαμβάνονται υπόψη. Ποιους δείκτες θα λάβει υπόψη της, ειδικά από τη στιγμή που κάθε υπεύθυνος επεξεργασίας μπορεί να υιοθετεί διαφορετική προσέγγιση; Η μόνη ασφαλής λύση που φαίνεται να υπάρχει, μέχρι σήμερα, είναι αυτή που αναλύθηκε ανωτέρω, να υιοθετηθεί, δηλαδή, μία συστηματική προσέγγιση η οποία αποδεικνύοντας βήμα – βήμα τη λογική της και καθορίζοντας τα κριτήρια βάσει των οποίων έχει προβεί στις αξιολογήσεις της, έχοντας καθορίσει το ποιοι εμπλεκόμενοι φορείς έχουν συμμετάσχει και μέχρι ποιο βαθμό, θα επιτύχει εν τέλει τον τελικό της σκοπό, να παράξει, δηλαδή, αποτελέσματα με συνοχή, διαφάνεια και συνέπεια καθιστώντας εν τέλει την διαδικασία επαληθεύσιμη και από τα υποκείμενα των δεδομένων αλλά και από την ΑΠΔΠΧ. Μέσω αυτής της συστηματικής προσέγγισης θα

επιτευχθεί, επιπλέον, και η αντικειμενικότητα που είναι ζητούμενο, αφού θα είναι δυνατό να εξακριβωθεί ο τρόπος με τον οποίο έγινε η εξαγωγή των συμπερασμάτων της μελέτης.

12.4 Το πρόβλημα της ορολογίας

Ένα ακόμη πολύ μεγάλο πρόβλημα που εντοπίζεται είναι ότι η ορολογία που χρησιμοποιείται σε κάθε μεθοδολογική προσέγγιση είναι διαφορετική. Ειδικότερα, δεν υπάρχει μία κοινή γραμμή για την έννοια του κινδύνου, των απειλών, των απευκταίων γεγονότων και των ζημιών μεταξύ των μεθοδολογικών προσεγγίσεων. Για την επίλυση αυτού, πρέπει στο μέλλον να διαμορφωθεί μία προσέγγιση η οποία θα χαίρει κοινής αποδοχής σε όλη την Ε.Ε. Μέχρι τότε, μία ασφαλής λύση είναι η κατανόηση του κάθε όρου στο πλαίσιο της αντίστοιχης μεθοδολογικής προσέγγισης. Ως εκ τούτου, αυτή η εργασία προσπαθεί να οργανώσει και να παρουσιάσει τις πιο δημοφιλείς μεθοδολογικές προσεγγίσεις, οι οποίες δεν ομοιάζουν, έτσι, ώστε να καλύψει όσο μεγαλύτερο φάσμα είναι δυνατόν, εντοπίζοντας κοινά μοτίβα και διαφορές μεταξύ αυτών και εξάγοντας συμπεράσματα για την ολοκληρωμένη προσέγγιση της μεθοδολογίας μίας ΕΑΠΔ.

13. Επίλογος

Η παρούσα εργασία πραγματεύεται την μεθοδολογία για την διενέργεια εκτίμησης αντικτύπου στο πλαίσιο της προστασίας προσωπικών δεδομένων. Ειδικότερα, παρουσιάζεται βήμα προς βήμα ο τρόπος διενεργείας μίας ΕΑΠΔ σύμφωνα με την προσέγγιση των δημοφιλέστερων μεθοδολογικών προσεγγίσεων και της νομολογίας, με σκοπό να παρουσιάσει ολοκληρωμένα το ζήτημα. Τελικό συμπέρασμα, είναι ότι ανεξαρτήτως της μεθοδολογικής προσέγγισης που θα επιλεχθεί, η ΕΑΠΔ πρέπει να διενεργείται με συστηματικό τρόπο για να μπορέσει εν τέλει να επιτύχει τον σκοπό της, να καταστεί, δηλαδή, μία πραγματική μελέτη του κινδύνου και των επιπτώσεων του. Αυτό που αξίζει να καταγραφεί είναι ότι ανεξάρτητα από τον υποχρεωτικό της χαρακτήρα, η ΕΑΠΔ αποτελεί ένα πολύ χρήσιμο εργαλείο για τους υπευθύνους επεξεργασίας, ώστε να διασφαλίζουν ότι συμμορφώνονται με τους κανονισμούς που απορρέουν από τον ΓΚΠΔ και ότι ικανοποιούν όλα τα δικαιώματα των υποκειμένων των δεδομένων.

Καταληκτικά, σημειώνεται ο προβληματισμός πως γενικά σε ενωσιακό επίπεδο δεν έχει επιτευχθεί ακόμα μια κοινά αποδεκτή μεθοδολογία που θα δημιουργήσει έναν επαρκή βαθμό

ασφάλειας δικαίου. Μάλιστα, σε μία εποχή που η τεχνολογία αναπτύσσεται με καταιγιστικούς ρυθμούς και δημιουργεί αναπάντεχους κινδύνους για τις ελευθερίες και τα δικαιώματα των υποκειμένων των δεδομένων, τα χρονικά περιθώρια για την ανάπτυξη συστηματικών, συνεπών και συνεκτικών λύσεων, φαντάζουν όλο και πιο στενά.

14. Βιβλιογραφία

Ξενόγλωσση

Article 29 Data Protection Working Party. In Guidelines on Data Protection Impact Assessment (DPIA) and Determining whether Processing Is “Likely to Result in a High Risk” for the Purposes of Regulation 2016/679; Technical Report; The Working Party on the Protection of Individuals With Regard to the Processing of Personal Data: Brussels, Belgium, 2017

1. Bieker, F., Friedewald, M., Hansen, M., Obersteller, H., Rost, M. (2016). A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (eds) Privacy Technologies and Policy. APF 2016. Lecture Notes in Computer Science(), vol 9857. Springer, Cham.

2. Bisztray, T., Gruschka, N. (2019). Privacy Impact Assessment: Comparing Methodologies with a Focus on Practicality. In: Askarov, A., Hansen, R., Rafnsson, W. (eds) Secure IT Systems. NordSec 2019. Lecture Notes in Computer Science(), vol 11875. Springer, Cham.

3. CNIL (Commission Nationale de l’Informatique et des Libert´es): Privacy Impact Assessment: Methodology (how to carry out a PIA). CNIL (2015).

4. Diamantopoulou, Vasiliki, Aggeliki Tsohou, and Maria Karyda. “General Data Protection Regulation and ISO/IEC 27001:2013: Synergies of Activities Towards Organisations’ Compliance.” Trust, Privacy and Security in Digital Business (2019).

5. Demetzou, K. (2018). Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Vienna, Austria, August 20-24, 2018, Revised Selected Papers. Springer International Publishing.

6. Deng, M., Wuyts, K., Scandariato, R. et al. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Eng 16, 3–32 (2011).

7. European Data Protection Supervisor. (2019). Accountability Toolbox.

8. Friedewald, M., Schiering, I., Martin, N., Hallinan, D. (2022). Data Protection Impact Assessments in Practice. In: Katsikas, S., et al. Computer Security. ESORICS 2021 International Workshops. ESORICS 2021. Lecture Notes in Computer Science(), vol 13106. Springer, Cham.

9. Katerina Demetzou, Data Protection Impact Assessment: A tool for accountability and the unclarified concept of ‘high risk’ in the General Data Protection Regulation, Computer Law & Security Review, Volume 35, Issue 6, 2019.

10. Kloza, D., van Dijk, N., Casiraghi, S., Maymir, S. V., Roda, S., Tanas, A., & Konstantinou, I. (2020, October 9). Towards a method for data protection impact assessment: Making sense of GDPR requirements.

11. Marie Caroline Oetzel, Sarah Spiekerman. A Systematic Methodology for Privacy Impact Assessments: A Design Science Approach. European Journal of Information Systems, 2014.

12. Marie Caroline Oetzel, Sarah Spiekerman, Ingrid Gruning, Harald Kelter and Sabine Mull. Privacy Impact Assessment Guideline for RFID Applications, 2011.

13. Martin, N., Friedewald, M., Schiering, I., Mester, B. A., Hallinan, D., & Jensen, M. (2020). The Data Protection Impact Assessment according to Article 35 GDPR: A Practitioner's Manual. Fraunhofer Verlag.

14. Sourya Joyee De, Daniel Le Métayer, Privacy Risk Analysis, Springer Cham.

15. Standard Data Protection Model, German Federal Data Protection Authority.

16. UK Information Commissioner's Office (ICO) (2014). "Conducting Privacy Impact Assessments: Code of Practice" URL: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of practice.pdf (visited on 2023/09/02).

17. van Puijenbroek, J.P.M., Hoepman, J.H.(2017). "Privacy Impact Assessments in Practice: Outcome of a Descriptive Field Research in the Netherlands". In: Ceur Workshop Proceedings, Alamo, J.M. del(ed.), IWPE 2017: International Workshop on Privacy Engineering: Proceedings of the 3rd International Workshop on Privacy Engineering, co-located with 38th IEEE Symposium on Security and Privacy (S&P 2017) San Jose (CA), USA, May 25, 2017, pp. 1-8.

18. Vemou, Konstantina, Karyda, Maria, An evaluation framework for privacy impact assessment methods, 2018/09/28.

19. ISO/IEC 29134:2023 - Information technology — Security techniques — Guidelines for privacy impact assessment

20. I. Nwankwo, Towards a transparent and systematic approach to conducting risk assessment under Article 35 of the GDPR, 2021, Διαθέσιμο στο: https://www.academia.edu/79146536/Towards_a_transparent_and_systematic_approach_to_conducting_risk_assessment_under_Article_35_of_the_GDPR

21. Dariusz Kloza, Niels van Dijk, Paul De Hert,Chapter 2 - Assessing the European Approach to Privacy and Data Protection in Smart Grids, 2015, Pages 11-47, ISBN 9780128021224,https://doi.org/10.1016/B978-0-12-02122-4.00002-X.(https://www.sciencedirect.com/science/article/pii/B9780128021224000 02X)

Ελληνική

1. *Ε. Αλεξανδροπούλου-Αιγυπτιάδου, Προσωπικά δεδομένα, εκδ. Νομ. Βιβλιοθήκη 2016*
2. *Κ. Κόμνιος, Γενικός κανονισμός για την προστασία δεδομένων, Εκδ. Σάκκουλα, 2020*
3. *Λ. Κανέλλος, The GDPR Handbook, Εκδ. Νομική Βιβλιοθήκη, 2020*
4. Λ. Μήτρου, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων, νέο δίκαιο – νέες υποχρεώσεις- νέα δικαιώματα, Εκδ. Σάκκουλα, 2017
5. *Δημήτριος Ευ. Τζέλλης, Μαρία Δ. Μυλώση, «Εκτίμηση Αντικτύπου στην προστασία προσωπικών δεδομένων», Νομική Βιβλιοθήκη 2022*
6. *Ι. Ιγγλεζάκης, Η εκτίμηση αντικτύπου στην προστασία προσωπικών δεδομένων (Data Protection Impact Assessment). Δικαιοπολιτική θεώρηση ενός καινοτόμου εργαλείου προστασίας της ιδιωτικότητας στον 21ο αιώνα, Επιθεώρηση Δικαίου Πληροφορικής, Τομ. 1, Τεύχ. 1, 2020*

7. *Ι.Ιγγλεζάκης, « Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων», 2020, Interactive books, Ady's Publishers*

8. *Συλλογικός τόμος Λ.Κοτσακλή - Κ. Μενουδάκου «Ο ΓΚΠΔ, Νομική διάσταση και πρακτική εφαρμογή», εκδ.Νομική Βιβλιοθήκη, 2018*

9. *ΑΠΔΠΧ, Κατάλογος με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων σύμφωνα με το άρθρο 35 παρ. 4 του ΓΚΠΔ, Αθήνα 16-10-2018 Αριθ. Πρωτ.: Γ/ΕΞ/8187/16-10-2018*

10. *Κ. Χριστοδούλου, Δίκαιο Προσωπικών Δεδομένων, Εκδ. Νομική Βιβλιοθήκη, 2η έκδοση*

11. . NoB. Στ. Ζουμπουλίδης "Οδηγός συμμόρφωσης μίας μεσαίας επιχείρησης με τον γενικό κανονισμό προστασίας δεδομένων (679/2017 ΕΚ) και η ειδικότερη πτυχή της προστασίας δεδομένων των εργαζομένων», Τόμος 71 – Τεύχος 5 2023

12. ΔιΤΕ. Ν. Λουκάς, «Η Έννοια και η Διαχείριση του «Κινδύνου» στον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).

13. Μ. Μυλώση, Ε. Αλεξανδροπούλου – Αιγυπτιάδου, «Η ενημέρωση του υποκειμένου προσωπικών δεδομένων σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων και τον Ν.4624/2019 – Κριτικές σκέψεις», ΔiΜΜΕ, 2/2020, σελ. 188- 189

Ενδεικτικές DPIA's:

1. *NHS, Data Protection Impact Assessment – COVID -19 Vaccine Trials Permission to Contact: https://digital.nhs.uk/coronavirus/ coronavirus-covid-19-response-information-governance-hub/data-protection-impact-assessment---covid-19-vaccine-trials-permission-to-contact-service---v1.0#7-demonstrate-the-fairness-of-the-processing*

2. *DPIA Zoom Education and Enterprise – SURF, February 2022: https://www.surf.nl/files/ 2022-03/dpia-zoom-25-february-2022_0.pdf*
3. *Μελέτη Εκτίμησης Αντικτύπου Σχετικά με την Προστασία Δεδομένων για τις πράξεις επεξεργασίας κατά την παροχή ΣΥΓΧΡΟΝΗΣ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΕΚΠΑΙΔΕΥΣΗΣ (ΤΗΛΕΚΠΑΙΔΕΥΣΗΣ) εκ μέρους του Υπουργείου Παιδείας και Θρησκευμάτων: https://www.minedu.gov.gr/publications/docs2020/DPIA_ΥΠΑΙΘ_sign.pdf*
4. *Data Protection Impact Assessment for the Corona App, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V, April 29, 2020 https://doi.org/10.48550/arXiv.2101.07292*: https://arxiv.org/ftp/arxiv/papers/2101/2101.07292.pdf
5. *Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12 January 2011:* https://digital-strategy.ec.europa.eu/en/library/privacy-and-data-protection-impact-assessment-framework -rfid-applications