ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΤΗΡΙΟ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ

Μεθοδολογίες Ελέγχου Ιδιωτικότητας και Ασφάλειας σε Ηλεκτρονικά Παρεχόμενες Υπηρεσίες

Μακρή Ελένη-Λασκαρίνα

Διδακτορική Διατριβή

Πειραιάς, 2022

Συμβουλευτική Επιτροπή

Κωνσταντίνος Λαμπρινουδάκης,

Καθηγητής (Επιβλέπων)

Πανεπιστήμιο Πειραιώς

Σωκράτης Κάτσικας,

Καθηγητής

Norwegian University of Science and Technology

Χρήστος Ξενάκης,

Καθηγητής

Πανεπιστήμιο Πειραιώς

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

2022

Εξεταστική Επιτροπή

Κωνσταντίνος Λαμπρινουδάκης, Καθηγητής

Πανεπιστήμιο Πειραιώς

Σωκράτης Κάτσικας, Καθηγητής

Norwegian University of Science and Technology

Χρήστος Ξενάκης, Καθηγητής

Πανεπιστήμιο Πειραιώς

Στέφανος Γκρίτζαλης, Καθηγητής

Πανεπιστήμιο Πειραιώς (Μέλος)

Χρήστος Καλλονιάτης, Αναπληρωτής Καθηγητής

Πανεπιστήμιο Αιγαίου (Μέλος)

Αγγελική Τσώχου, Αναπληρώτρια Καθηγήτρια

Ιόνιο Πανεπιστήμιο (Μέλος)

Βασιλική Διαμαντοπούλου, Επίκουρη Καθηγήτρια

Πανεπιστήμιο Αιγαίου (Μέλος)

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

2022

Περίληψη

Η διδακτορική διατριβή με θέμα "Μεθοδολογίες Ελέγχου Ιδιωτικότητας και Ασφάλειας σε Ηλεκτρονικά Παρεχόμενες Υπηρεσίες" εστιάζει στη διερεύνηση και πειραματική εφαρμογή καινοτόμων λύσεων για την αποτελεσματική προστασία της ιδιωτικότητας των χρηστών ενός οργανισμού και συγκεκριμένα τα δεδομένα που συλλέγει, επεξεργάζεται και αποθηκεύει μέσω των προσφερόμενων υπηρεσιών του.

Εφαλτήριο για τη διατριβή αυτή αποτελεί το γεγονός ότι οι χρήστες δε διστάζουν να αποκαλύπτουν μεγάλο όγκο προσωπικών δεδομένων τους ή ακόμα και δεδομένων ειδικών κατηγοριών προκειμένου να χρησιμοποιήσουν υπηρεσίες ενός οργανισμού, θέτοντας έτσι τον εαυτό τους, αλλά και άλλους σε κίνδυνο. Το βασικό ερώτημα που προκύπτει από τα παραπάνω είναι αν μπορούν οι χρήστες να προστατευθούν πραγματικά όταν «προσφέρουν» τα προσωπικά τους δεδομένα τόσο πρόθυμα προκειμένου να ικανοποιήσουν τις «ψηφιακές ανάγκες» τους. Για να απαντηθεί αυτό το ερώτημα, είναι πρώτα απαραίτητο να εκτιμηθεί ο αντίκτυπος από μια πιθανή παραβίαση της ιδιωτικότητάς τους, χρησιμοποιώντας μια μεθοδολογία Εκτίμησης Αντικτύπου Ιδιωτικότητας (Privacy Impact Assessment - PIA).

Στο πλαίσιο της παρούσας διατριβής, μετά από εκτενή μελέτη, διαπιστώθηκε ότι υπάρχουν πολλές μεθοδολογίες για να διεξάγει ένας οργανισμός μελέτη εκτίμησης αντικτύπου, αλλά δεν έχει καταγραφεί καμία, μέχρι στιγμής, που να κάνει χρήση μετρικών και συνεπώς να αποφέρει μετρήσιμα αποτελέσματα. Επιπλέον, καμία μεθοδολογία από τις καταγεγραμμένες δεν λαμβάνει υπόψη τα χαρακτηριστικά του οργανισμού (μέγεθος, δραστηριότητες, αριθμός πελατών-χρηστών, τύπο προσφερόμενων υπηρεσιών, κτλ.) κάτι το οποίο επηρεάζει την ακρίβεια των αποτελεσμάτων διεξαγωγής της μελέτης.

Αντικείμενο της παρούσας διατριβής, είναι ο σχεδιασμός και η ανάπτυξη μιας μεθοδολογίας, η οποία, λαμβάνοντας σαν είσοδο τις ήδη υπάρχουσες αρχές και απαιτήσεις ιδιωτικότητας καθώς και τις κατηγορίες δεδομένων που χρησιμοποιεί ένας οργανισμός και τα χαρακτηριστικά του, αποφασίζει κατά πόσο ο συγκεκριμένος οργανισμός προστατεύει αποτελεσματικά την ιδιωτικότητα των χρηστών του και συγκεκριμένα τα δεδομένα που συλλέγει, επεξεργάζεται και αποθηκεύει μέσω των προσφερόμενων υπηρεσιών του.

Θεματική Περιοχή: Μεθοδολογίες Ελέγχου Ιδιωτικότητας και Ασφάλειας

Λέξεις Κλειδιά: Απαιτήσεις Ιδιωτικότητας, Απαιτήσεις Ασφάλειας, Εκτίμηση Αντικτύπου Ιδιωτικότητας, Γενικός Κανονισμός για την Προστασία των Δεδομένων, Μεθοδολογία Ελέγχου, Μετρικές, Χαρακτηριστικά Οργανισμού, Υπολογιστικό Νέφος

Abstract

The assessment of the potential impact for an organization from a privacy violation incident is important for three main reasons: the organization will have a justified estimate of the cost (financial, reputation or other) that may be raised, will facilitate the selection of the appropriate technical, procedural and organizational protection mechanisms and also will be compliant with the new General Data Protection Regulation (GDPR) that is in effect from May 2018. Today, there are several methods to do a Privacy Impact Assessment (PIA) but none of these quantifies the results using specific metrics and thus can be significantly affected by various subjective parameters. Furthermore, the specific organizational characteristics (size, activities, number of clients, type of offered services etc.) are very rarely accounted, a fact that also affects the accuracy of the results. This thesis proposes a privacy impact assessment method that explicitly takes into account the organizational characteristics and employs a list of well-defined metrics as input, demonstrating its applicability to two Hospital Information Systems with different characteristics.

The above proposed method consists of two separate methodologies. Driven by the fact that there is no way to handle at the same time the elicitation of the security and privacy requirements and of the main privacy principles, the first methodology proposed integrates the basic steps of well-established risk analysis methodologies with those of methodologies used for the elicitation of privacy requirements, considering, at the same time, the most well-known privacy principles. The aim is to assist information system designers to come up with a complete and accurate list of all security and privacy requirements that must be satisfied by the system.

Furthermore, driven by the absence of a widely accepted structured representation of the privacy principles, that makes their adoption or/and satisfaction difficult and in some cases inconsistent, the second methodology proposed consists of discrete steps that organizations can follow for deciding or/and auditing their privacy protection measures. Every step is based on the significance of a privacy principle and on the sequence of the audit procedure.

This thesis also analyses how a cloud computing service provider will achieve compliance with the GDPR by proposing technical and organizational measures demonstrating their applicability on a hospital cloud environment.

Field of Science: Privacy and Security Auditing Methodology

Key Words: Privacy Requirements, Security Requirements, Privacy Impact Assessment, General Data Protection Regulation (GDPR), Audit Methodology, Metrics, Organizational Characteristics, Cloud Computing

Αφιερώνεται με αγάπη

στο Σπύρο &

στη Μαριάννα

«Η εκπαίδευση είναι δύναμη που γιατρεύει την ψυχή»

Πλάτων (427 π.Χ. - 347 π.Χ.)

Ευχαριστίες

Με την ολοκλήρωση της διδακτορικής διατριβής μου, θα ήθελα να ευχαριστήσω προσωπικά όλους όσους στάθηκαν δίπλα μου σε αυτή την προσπάθεια και να εκφράσω την βαθιά ευγνωμοσύνη μου στην ηθική και πνευματική υποστήριξη που μου προσέφεραν.

Πρώτον απ' όλους θα ήθελα να ευχαριστήσω ολόψυχα τον επιβλέποντά μου κ. Κωνσταντίνο Λαμπρινουδάκη, Καθηγητή του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς, ο οποίος με εμπιστεύθηκε, με ενθάρρυνε, με καθοδήγησε στις ερευνητικές μου αναζητήσεις και με στήριξε καθ' όλη τη διάρκεια της ερευνητικής μου προσπάθειας, από τη στιγμή που έγινα δεκτή ως Υποψήφια Διδάκτορας μέχρι και σήμερα. Οι υψηλές απαιτήσεις του και οι καθοριστικές παρατηρήσεις του, αποτέλεσαν για εμένα σημαντικό κίνητρο για την ολοκλήρωση της συγγραφής τόσο των επιστημονικών δημοσιεύσεων όσο και της παρούσας διδακτορικής διατριβής. Τον ευχαριστώ μέσα από την καρδιά μου για τη συνεργασία που είχαμε τόσο σε επιστημονικό και επαγγελματικό επίπεδο όσο και σε επίπεδο ανθρώπινων σχέσεων. Αποτελεί για μένα υπόδειγμα ***Ανθρώπου*** **και** ***Επιστήμονα***.

Παράλληλα, θα ήθελα να ευχαριστήσω ιδιαίτερα τα άλλα δύο μέλη της τριμελούς συμβουλευτικής επιτροπής, τον Καθηγητή κ. Σωκράτη Κάτσικα και τον Καθηγητή κ. Χρήστο Ξενάκη, των οποίων η εποικοδομητική κριτική, η ενεργός συνεισφορά και οι επιστημονικές συμβουλές, υπήρξαν για εμένα πολύτιμες σε όλη τη διάρκεια της διδακτορικής διατριβής μου.

Θερμές ευχαριστίες θα ήθελα να εκφράσω και σε όλα τα μέλη της επταμελούς εξεταστικής επιτροπής μου, κ. Στέφανο Γκρίτζαλη, Καθηγητή στο Πανεπιστήμιο Πειραιώς, κ. Χρήστο Καλλονιάτη, Αναπληρωτή Καθηγητή στο Πανεπιστήμιο Αιγαίου, κα Αγγελική Τσώχου, Επίκουρη Καθηγήτρια στο Ιόνιο Πανεπιστήμιο και κα Βασιλική Διαμαντοπούλου, Επίκουρη Καθηγήτρια στο Πανεπιστήμιο Αιγαίου, για την πρόθυμη συμμετοχή τους στην κρίση της διδακτορικής μου διατριβής.

Ένα μεγάλο ευχαριστώ οφείλω στην συνάδελφο μα πάνω απ' όλα φίλη και συμφοιτήτριά μου Δρ. Ζαφειρούλα Γεωργιοπούλου για τη στήριξη που μου παρείχε σε

αυτή την προσπάθεια, τις πολύτιμες συμβουλές της, τις αγωνίες αλλά και για τις όμορφες στιγμές που ζήσαμε όλα αυτά τα χρόνια.

Τέλος, το πιο μεγάλο "ευχαριστώ" το οφείλω στην οικογένειά μου, που χωρίς την αγάπη και τη στήριξή τους, η εκπόνηση και η ολοκλήρωση της διδακτορικής μου διατριβής δε θα ήταν ποτέ δυνατή. Θα ήθελα να εκφράσω τις ευχαριστίες μου στους γονείς μου, Γιάννη και Εύη καθώς και στην αδελφή μου Κωνσταντίνα για τη συμπαράστασή τους καθ' όλη τη διάρκεια των σπουδών μου. Επίσης, οφείλω ένα τεράστιο "ευχαριστώ" από καρδιάς στον ακούραστο και υπομονετικό σύζυγό μου Σπύρο καθώς και στην κόρη μας Μαριάννα, για την αγάπη, τη διαρκή υποστήριξη και κατανόησή τους για τις ώρες που χρειάστηκε να αφιερώσω, ώστε να ολοκληρωθεί αυτό το ταξίδι.

Με τιμή

Ελένη-Λασκαρίνα Μακρή

(Υπογραφή)

.....

ΜΑΚΡΗ ΕΛΕΝΗ-ΛΑΣΚΑΡΙΝΑ

Διδακτορική Διατριβή, Πανεπιστήμιο Πειραιώς, Τμήμα Ψηφιακών Συστημάτων

Περιεχόμενα

Ευρετήριο Σχημάτων

Ευρετήριο Εικόνων

Ευρετήριο Πινάκων

Ακρωνύμια

Ακρωνύμιο	Επεξήγηση
ΓΚΠΔ	Γενικός Κανονισμός για την Προστασία Δεδομένων (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
ΠΣ	Πληροφοριακό Σύστημα
ΟΟΣΑ	Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης
OECD	Organisation for Economic Co-operation and Development
EC	European Commission
ISACA	Information Systems Audit and Control Association
ENISA	European Network and Information Security Agency
IBM	International Business Machines
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
GPS	Global Privacy Standard
ΣΔ (DS)	Σύνολο Δεδομένων (Data Set)
ID	Identity Document
PP	Privacy Principle (Αρχή Ιδιωτικότητας)
CH	Characteristics (Χαρακτηριστικά)
CRAMM	CCTA Risk Analysis and Management Method
CCTA	Central Computer and Telecommunications Agency
MOR	Measure of Risk
PETs	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
PIAF	A Privacy Impact Assessment Framework
ΤΠΕ	Τεχνολογίες Πληροφοριών και Επικοινωνιών

Πίνακας 1: Ακρωνύμια

1 Κεφάλαιο 1: Εισαγωγή

Η χρήση των τεχνολογιών πληροφορικής έχει αλλάξει ριζικά τον τρόπο με τον οποίο λειτουργεί η σύγχρονη κοινωνία. Η υιοθέτηση των νέων τεχνολογικών εργαλείων, υπηρεσιών και μέσων που προσφέρονται από διάφορους οργανισμούς έχουν επηρεάσει όλες τις μορφές ανθρώπινης δραστηριότητας και έχουν οδηγήσει σε νέες διαδραστικές μορφές επικοινωνίας. Η διαρκώς αυξανόμενη χρήση των ηλεκτρονικών υπηρεσιών έχει σαν αποτέλεσμα τη συλλογή, αποθήκευση, επεξεργασία και μετάδοση τεράστιου όγκου προσωπικών δεδομένων των χρηστών που τις αξιοποιούν [1][2].

Πιθανές παραβιάσεις στην ασφάλεια μπορεί να προκαλέσουν σημαντικές συνέπειες είτε στους οργανισμούς που τηρούν κι επεξεργάζονται τα δεδομένα είτε στην ιδιωτικότητα των χρηστών, ως ιδιοκτήτες των δεδομένων αυτών [3]. Για την αποφυγή παραβιάσεων της ασφάλειας και συνεπώς της ιδιωτικότητας των χρηστών αρκετοί νόμοι, πρότυπα, κανονισμοί και οδηγίες/κατευθυντήριες γραμμές [4] έχουν αναπτυχθεί και εφαρμοστεί σε πολλές χώρες παγκοσμίως. Σκοπός όλων αυτών είναι να υποχρεώσουν τους οργανισμούς να ενημερώνουν πλήρως τους χρήστες των υπηρεσιών για το είδος των δεδομένων που τηρούν και, σε περίπτωση που δεν υπάρχει νομική υποχρέωση, να λαμβάνουν τη ρητή συγκατάθεσή τους πριν από την οποιαδήποτε συλλογή, αποθήκευση και επεξεργασία των δεδομένων τους. Ταυτόχρονα με τα παραπάνω, έχουν οριστεί συγκεκριμένες αρχές για την προστασία της ιδιωτικότητας (privacy principles) [5], απαιτήσεις ιδιωτικότητας (privacy requirements) και απαιτήσεις ασφάλειας (security requirements) [6][7] που βοηθούν στην ανάπτυξη ενός ενοποιημένου πλαισίου για την προστασία της ασφάλειας και της ιδιωτικότητας των χρηστών.

Μια από τις κύριες ανησυχίες των χρηστών είναι η έλλειψη μιας κοινής μεθοδολογίας ελέγχου ασφάλειας και ιδιωτικότητας, γεγονός που οδηγεί στην αβεβαιότητα αν οι πάροχοι υπηρεσιών (service providers) προστατεύουν επαρκώς τα προσωπικά δεδομένα τους. Αυτό επηρεάζει τους παρόχους υπηρεσιών ως προς το γεγονός ότι δεν μπορούν να αποδείξουν ότι εφαρμόζουν αποτελεσματικά τα μέτρα προστασίας που έχουν υιοθετήσει. Ως συνέπεια, τα προσωπικά δεδομένα των χρηστών είναι εκτεθειμένα σε πολλούς κινδύνους. Η ύπαρξη μεθοδολογίας ελέγχου ασφάλειας και ιδιωτικότητας ενθαρρύνει τους

χρήστες να εμπιστευτούν περισσότερο τους παρόχους υπηρεσιών και συνεπώς να χρησιμοποιήσουν τις υπηρεσίες τους.

Παρά το γεγονός ότι πολλές προσπάθειες έχουν γίνει ως προς την ανάπτυξη ενός κοινού πλαισίου ελέγχου ασφάλειας και ιδιωτικότητας των χρηστών ακόμα είναι σε πρώιμο στάδιο. Στο πλαίσιο της παρούσας Διδακτορικής Διατριβής, προτείνεται μια δομημένη μεθοδολογία ελέγχου ασφάλειας και ιδιωτικότητας (structured security and privacy audit methodology), η οποία αποτελείται από συγκεκριμένα βήματα, τα οποία ένας οργανισμός καλείται να ακολουθήσει. Η προτεινόμενη μεθοδολογία περιλαμβάνει συγκεκριμένα διακριτά βήματα και βασίζεται στις ευρέως αποδεκτές αρχές ιδιωτικότητας [8], που προέκυψαν είτε από χώρες, είτε από ιδιωτικούς και δημόσιους φορείς. Παράλληλα με τις αρχές ιδιωτικότητας, λαμβάνει υπόψη τις απαιτήσεις ιδιωτικότητας, τις απαιτήσεις ασφάλειας καθώς και τις κατηγορίες δεδομένων που χρησιμοποιεί ένας οργανισμός.

Ο βασικός στόχος της προτεινόμενης μεθοδολογίας είναι να υποστηρίξει τους οργανισμούς ως προς την αποτελεσματική προστασία της ιδιωτικότητας των χρηστών και της ασφάλειας των δεδομένων που συλλέγουν, επεξεργάζονται και αποθηκεύουν. Προς αυτή τη κατεύθυνση αξιοποιεί μετρικές και ποσοτικοποιεί τα χαρακτηριστικά του οργανισμού, υπολογίζοντας τις συνέπειες που μπορεί να προκύψουν για τον οργανισμό αν δεν ικανοποιείται κάποια απαίτηση ιδιωτικότητας.

1.1 Ορισμός Προβλήματος

Στην εποχή μας όπου η πρόοδος της τεχνολογίας καλπάζει με ρυθμούς που ο μέσος άνθρωπος – χρήστης του Διαδικτύου αδυνατεί να ακολουθήσει, η προστασία της ασφάλειας των δεδομένων του και της ιδιωτικότητάς του αποτελεί τεράστια πρόκληση. Έρευνες και δημοσκοπήσεις έχουν δείξει ότι η προστασία των δεδομένων των χρηστών αποτελεί καθημερινή ανησυχία τους [9].

Η προστασία της ιδιωτικότητας αποτελεί σοβαρό πρόβλημα τόσο για τους χρήστες όσο και για τους οργανισμούς. Για το λόγο αυτό, πολλοί ερευνητές υποστηρίζουν ότι η ιδιωτικότητα θα πρέπει να διατηρείται καθ' όλη τη διάρκεια του κύκλου ζωής ενός πληροφοριακού συστήματος (ΠΣ). Πιο συγκεκριμένα, η ιδιωτικότητα θα πρέπει να λαμβάνεται υπόψη από τη φάση σχεδιασμού ενός ΠΣ μέχρι την εφαρμογή του. Η ιδέα της ιδιωτικότητας κατά το σχεδιασμό (privacy-by-design) υποστηρίχθηκε έντονα από την Ann

Cavoukian [41] και τον Jaap-Henk Hoepman [42][43], ενώ αποτελεί πλέον και βασική απαίτηση του ΓΚΠΔ.

Υπάρχει έντονη προσπάθεια για την ανάπτυξη τρόπων προστασίας των δεδομένων των χρηστών και κατ' επέκταση της ιδιωτικότητάς τους. Από τη μια πλευρά, υπάρχουν νόμοι, πρότυπα, κανονισμοί και οδηγίες/κατευθυντήριες γραμμές, σύμφωνα με τα οποία πολλές χώρες επιβάλλουν στους οργανισμούς που επεξεργάζονται και αποθηκεύουν δεδομένα χρηστών να τα προστατεύουν και να μην τα χρησιμοποιούν αν δεν έχουν ενημερώσει τους χρήστες και δεν έχουν λάβει τη συγκατάθεσή τους. Από την άλλη πλευρά, υπάρχουν πολλοί δημόσιοι ή/και ιδιωτικοί φορείς, οι οποίοι θέλοντας να προστατεύσουν την ιδιωτικότητα των χρηστών έχουν υιοθετήσει συγκεκριμένες αρχές ιδιωτικότητας (privacy principles). Ταυτόχρονα, χρησιμοποιούνται Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy-Enhancing Technologies - PETs), οι οποίες μέσω μιας ποικιλίας μέτρων προστασίας για την ιδιωτικότητα των δεδομένων των χρηστών προσφέρουν τα τεχνικά μέσα για την προστασία τους και επομένως για την αποτροπή περιττής ή ανεπιθύμητης επεξεργασίας [39] [40]. Ωστόσο, τόσο οι αρχές ιδιωτικότητας όσο και τα PETs δεν μπορούν να χρησιμοποιηθούν επαρκώς μόνα τους, αλλά συσχετίζονται και λειτουργούν συμπληρωματικά.

Παρά το γεγονός ότι στο παρελθόν έχουν γίνει αξιοσημείωτες προσπάθειες [35] [42] [43] [44] για να συγκεντρωθούν όλες οι αρχές ιδιωτικότητας και να χρησιμοποιηθούν σε ένα σύστημα από τη φάση του σχεδιασμού του, δεν υπάρχει δημοσιευμένη μεθοδολογία που να συνδυάζει τις υπάρχουσες αρχές ιδιωτικότητας για την υποστήριξη ενός τέτοιου συστήματος. Ένας από τους βασικούς λόγους για αυτό είναι ότι το τεχνολογικό περιβάλλον αλλάζει συνεχώς, κάτι που δυσκολεύει την προσαρμογή των οργανισμών. Ένας άλλος πιθανός λόγος είναι ότι ο όγκος των πληροφοριών είναι τεράστιος και δύσκολα διαχειρίσιμος. Ως εκ τούτου, οι οργανισμοί εξακολουθούν να αποτυγχάνουν να εφαρμόσουν αποτελεσματικούς μηχανισμούς προστασίας της ιδιωτικότητας. Επιπλέον, μέχρι στιγμής δεν έχει γίνει καμία προσπάθεια να δημιουργηθεί ένα πλαίσιο που θα ορίζει τον τρόπο αντιμετώπισης/εφαρμογής των υφιστάμενων αρχών ιδιωτικότητας (δηλαδή είναι ορισμένες αρχές πιο σημαντικές από άλλες; υπάρχει συγκεκριμένη σειρά που κάποιος πρέπει να προσπαθήσει να τις ικανοποιήσει και σε αυτή την περίπτωση ποια είναι αυτή η σειρά; κ.τ.λ.). Αν και υπάρχει εκτεταμένη βιβλιογραφία σχετικά με τις διαφορετικές αρχές

ιδιωτικότητας και τους ορισμούς τους [35] [36] [45] [46], δεν έχει γίνει αναφορά ως προς το ποια αρχή θα πρέπει να εφαρμοστεί πρώτα, ποια θα πρέπει να ακολουθήσει ή ποια θα μπορούσε να χρησιμοποιηθεί ως εισαγωγή στις υπόλοιπες.

Ως εκ τούτου, η απουσία μιας ευρέως αποδεκτής δομημένης αναπαράστασης των αρχών ιδιωτικότητας καθιστά την υιοθέτηση/ικανοποίησή τους δύσκολη και σε ορισμένες περιπτώσεις αδύνατη. Σε κάθε περίπτωση οι «διασκορπισμένες» [17] αρχές ιδιωτικότητας επιβάλλουν σημαντική πρόσθετη πολυπλοκότητα. Κατά συνέπεια, πολύ συχνά οι οργανισμοί αποτυγχάνουν να εφαρμόσουν αποτελεσματικά τις αρχές ιδιωτικότητας και συνεπώς να προστατεύσουν τα προσωπικά δεδομένα των χρηστών τους.

Κατά τη διαδικασία σχεδιασμού ενός πληροφοριακού συστήματος είναι απαραίτητο να λαμβάνεται υπόψη η προστασία της ιδιωτικότητας των χρηστών, όπως αναφέρθηκε παραπάνω, αλλά και η ασφάλεια των δεδομένων τους [28] [41] [42] [43]. Αυτό μπορεί να γίνει με τον εντοπισμό, μέσω των κατάλληλων μεθοδολογιών, των απαιτήσεων ασφάλειας (security requirements) και των απαιτήσεων ιδιωτικότητας (privacy requirements) που πρέπει να πληρούνται. Ωστόσο, δεν υπάρχει καμία μεθοδολογία που να μπορεί να καλύψει τον προσδιορισμό των απαιτήσεων ασφάλειας, των απαιτήσεων ιδιωτικότητας και ταυτόχρονα να λαμβάνει υπόψη τις βασικές αρχές ιδιωτικότητας. Συνεπώς, οι σχεδιαστές ενός πληροφοριακού συστήματος συνήθως ακολουθούν μια ad hoc προσέγγιση για τον προσδιορισμό των απαιτήσεων ασφάλειας / ιδιωτικότητας, αποτυγχάνοντας έτσι να προστατεύσουν τους χρήστες με αποτελεσματικό τρόπο.

Παρά το γεγονός ότι οι χρήστες έχουν έντονες ανησυχίες για τη συλλογή προσωπικών πληροφοριών και την προστασία της ιδιωτικότητάς τους, στην πραγματικότητα η συμπεριφορά τους έρχεται σε αντίθεση με τις προθέσεις και τη στάση τους αυτή. Αυτό το φαινόμενο είναι γνωστό ως το «παράδοξο της ιδιωτικότητας» [10]. Συγκεκριμένα, από τη μια μεριά, οι χρήστες ανησυχούν για το γεγονός ότι δεν έχουν τον έλεγχο των δεδομένων τους και αυτό συνεπάγεται έλλειψη εμπιστοσύνης προς τους οργανισμούς που παρέχουν υπηρεσίες προς τους χρήστες [11]. Από την άλλη μεριά, οι χρήστες δε διστάζουν να αποκαλύπτουν μεγάλο όγκο προσωπικών δεδομένων τους ή ακόμα και δεδομένων ειδικών κατηγοριών προκειμένου να χρησιμοποιήσουν υπηρεσίες ενός οργανισμού, όπως π.χ. χρήση κοινωνικών δικτύων, χρήση e-banking, αποστολή μηνυμάτων ηλεκτρονικού

ταχυδρομείου, εκτέλεση εμπορικών συναλλαγών, κτλ. [9], θέτοντας έτσι τον εαυτό τους, αλλά και άλλους σε κίνδυνο [12].

Το βασικό ερώτημα που προκύπτει από τα παραπάνω είναι αν μπορούν οι χρήστες να προστατευθούν πραγματικά όταν «προσφέρουν» τα προσωπικά τους δεδομένα τόσο πρόθυμα προκειμένου να ικανοποιήσουν τις «ψηφιακές ανάγκες» τους. Για να απαντηθεί αυτό το ερώτημα, είναι πρώτα απαραίτητο να εκτιμηθεί ο αντίκτυπος από μια πιθανή παραβίαση της ιδιωτικότητάς τους, χρησιμοποιώντας μια μεθοδολογία Εκτίμησης Αντικτύπου Ιδιωτικότητας (Privacy Impact Assessment - PIA). Έχοντας εκτιμήσει τον αντίκτυπο, οι εμπλεκόμενοι μπορούν να προβούν σε διορθωτικές ενέργειες για την εξάλειψη ή την ελαχιστοποίηση των συνεπειών [47]. Επιπλέον, η μη εφαρμογή μιας μεθοδολογίας PIA μπορεί να οδηγήσει σε παραβίαση των νόμων - κανονισμών περί ιδιωτικότητας. Ένας από αυτούς είναι ο Γενικός Κανονισμός Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (ΓΚΠΔ) (General Data Protection Regulation - GDPR) ο οποίος υιοθετήθηκε επίσημα το Μάϊο του 2018 [4]. Μέσω του ΓΚΠΔ προτείνεται η διεξαγωγή μελέτης εκτίμησης αντικτύπου προκειμένου να αξιολογηθούν οι πιθανές επιπτώσεις για ένα οργανισμό από περιστατικά παραβίασης ιδιωτικότητας των δεδομένων των χρηστών τους. Η αξιολόγηση της πιθανής επίπτωσης για έναν οργανισμό είναι σημαντική για τρεις βασικούς λόγους: ο οργανισμός μπορεί να εκτιμήσει το κόστος από μια πιθανή παραβίαση (οικονομικό, φήμη, κτλ.), να διευκολυνθεί ως προς την επιλογή κατάλληλων τεχνικών μέτρων, διαδικασιών, πολιτικών και μηχανισμών προστασίας και ταυτόχρονα να είναι συμβατός με τον ΓΚΠΔ.

Σήμερα, υπάρχουν πολλές μεθοδολογίες για να διεξάγει ένας οργανισμός μελέτη εκτίμησης αντικτύπου, αλλά καμία δεν έχει καταγραφεί μέχρι στιγμής που να αποφέρει μετρήσιμα αποτελέσματα, χρησιμοποιώντας μετρικές [13] [14] [15]. Επιπλέον, καμία μεθοδολογία από τις καταγεγραμμένες δεν λαμβάνει υπόψη τα χαρακτηριστικά του οργανισμού (μέγεθος, δραστηριότητες, αριθμός πελατών-χρηστών, τύπο προσφερόμενων υπηρεσιών, κτλ.) κάτι το οποίο επηρεάζει την ακρίβεια των αποτελεσμάτων διεξαγωγής της μελέτης.

Στα πλαίσια συμμόρφωσης ενός οργανισμού με τον ΓΚΠΔ, η αποτελεσματική εφαρμογή μιας μελέτης εκτίμησης αντικτύπου είναι ένα αρκετά περίπλοκο, απαιτητικό και χρονοβόρο έργο από μόνο του. Τι γίνεται όμως σε περιβάλλοντα υπολογιστικού νέφους; Η

διαδικασία απλοποιείται ή συνεχίζει να είναι το ίδιο απαιτητική; Η απάντηση σε αυτό το ερώτημα δίνεται μόνο αν δούμε κατά πόσο οι απαιτήσεις που θέτει ο ΓΚΠΔ στο σύνολό τους μπορούν να ικανοποιηθούν. Μέχρι στιγμής δεν έχουν καταγραφεί κατάλληλα μέτρα αντιμετώπισης για τη συμμόρφωση με τον ΓΚΠΔ σε τέτοιου είδους περιβάλλοντα και συγκεκριμένα στις αρχιτεκτονικές υπολογιστικού νέφους (IaaS, PaaS, SaaS) και το ενδιαφέρον της ερευνητικής κοινότητας αποδεικνύεται αρκετά μεγάλο αν κρίνουμε τις μελέτες που αρχίζουν να γίνονται προς αυτή την κατεύθυνση.

1.2 Στόχοι και Συνεισφορά

Ερευνώντας τον τρόπο με τον οποίο οι οργανισμοί αντιλαμβάνονται την έννοια της προστασίας των δεδομένων των χρηστών που διατηρούν αλλά και τον τρόπο με τον οποίο οι ίδιοι οι χρήστες αποκαλύπτουν, ηθελημένα ή μη, τα δεδομένα τους, καταλήξαμε στο συμπέρασμα ότι ο τρόπος αντιμετώπισής τους είναι διαφορετικός για τις δύο πλευρές. Κύριος στόχος της Διδακτορικής Διατριβής είναι η δημιουργία μιας μεθοδολογίας που να γεφυρώνει αυτή τη διαφορά και να μπορεί να υιοθετηθεί από οποιονδήποτε οργανισμό χειρίζεται προσωπικά δεδομένα και δεδομένα ειδικών κατηγοριών, αποτελεσματικά, με απώτερο σκοπό την προστασία της ασφάλειας των δεδομένων και της ιδιωτικότητας των χρηστών. Πιο συγκεκριμένα, οι στόχοι είναι οι εξής:

i. Καταγραφή των αρχών ιδιωτικότητας, των απαιτήσεων ιδιωτικότητας και των απαιτήσεων ασφάλειας είτε μέσω της σχετικής νομοθεσίας, των προτύπων, των κανονισμών και των οδηγιών σχετικά με την προστασία προσωπικών δεδομένων των χρηστών, είτε μέσω δημόσιων και ιδιωτικών φορέων και του προτεινόμενου τρόπου εφαρμογής τους.

ii. Έρευνα και καταγραφή των ήδη υπαρχουσών μεθοδολογιών ελέγχου και τήρησης ιδιωτικότητας των χρηστών και των μεθοδολογιών μελέτης εκτίμησης αντικτύπου προκειμένου να αξιολογηθούν οι πιθανές επιπτώσεις για ένα οργανισμό από πιθανά περιστατικά παραβίασης της ιδιωτικότητας των χρηστών τους.

iii. Καταγραφή των χαρακτηριστικών ενός υπό μελέτη οργανισμού (π.χ. είδος δεδομένων, πλήθος χρηστών, κτλ.) με σκοπό την αποτελεσματικότερη κατανόηση της λειτουργίας και των υπηρεσιών που προσφέρει.

iv. Συνδυασμός των παραπάνω αρχών και απαιτήσεων ιδιωτικότητας με τον αντίκτυπο σε ένα υπό μελέτη οργανισμό από πιθανά περιστατικά παραβίασης ιδιωτικότητας καθώς και των χαρακτηριστικών του οργανισμού, με σκοπό τη δημιουργία δομημένης μεθοδολογίας που θα καταλήγει στην ποσοτικοποίηση των τελικών αποτελεσμάτων σχετικά με τον έλεγχο του επιπέδου προστασίας της ιδιωτικότητας.

v. Αξιολόγηση της απόδοσης και της ακρίβειας των παραγόμενων αποτελεσμάτων της προτεινόμενης μεθοδολογίας (μέσω use cases).

Συνεισφορά της συγκεκριμένης Διδακτορικής Διατριβής αποτελεί ο σχεδιασμός και η ανάπτυξη μεθοδολογίας, η οποία, λαμβάνοντας σαν είσοδο ταυτόχρονα τις αρχές και απαιτήσεις ιδιωτικότητας καθώς και τις κατηγορίες δεδομένων που χρησιμοποιεί ένας οργανισμός και τα χαρακτηριστικά του, ποσοτικοποιεί το επίπεδο προστασίας που ο συγκεκριμένος οργανισμός επιτυγχάνει σε σχέση με την ιδιωτικότητα των χρηστών του και συγκεκριμένα των δεδομένων που συλλέγει, επεξεργάζεται και αποθηκεύει μέσω των προσφερόμενων υπηρεσιών του. Πιο συγκεκριμένα, η επιστημονική συνεισφορά μπορεί να συνοψιστεί στα ακόλουθα:

i. Λεπτομερής καταγραφή και συγκέντρωση όλων των «διασκορπισμένων» [17] αρχών και απαιτήσεων ιδιωτικότητας, που προέκυψαν είτε από χώρες, είτε από ιδιωτικούς και δημόσιους φορείς και ταξινόμησή τους με βάση τη σημαντικότητά τους, με σκοπό το σχεδιασμό συστημάτων που λαμβάνουν υπόψη την ιδιωτικότητα των χρηστών από τα πρώτα στάδια σχεδιασμού ενός συστήματος [16].

ii. Καταγραφή των χαρακτηριστικών του προς εξέταση οργανισμού και των κατηγοριών των δεδομένων που χρησιμοποιεί με σκοπό την ανάλυση των κριτηρίων με βάση τα οποία θα ελεγχθεί το επίπεδο της προστασίας της ιδιωτικότητας των χρηστών.

iii. Επισκόπηση και καταγραφή των προτεινόμενων μεθοδολογιών εκτίμησης αντικτύπου (PIA) που υπάρχουν μέχρι στιγμής στη βιβλιογραφία με σκοπό την μελέτη και ανάλυση των χαρακτηριστικών τους και την εξέταση της αποτελεσματικότητάς τους.

iv. Ανάπτυξη μεθοδολογίας η οποία λαμβάνει σαν είσοδο τις ταξινομημένες αρχές και απαιτήσεις ιδιωτικότητας, τις κατηγορίες δεδομένων (data sets) που χρησιμοποιεί ένας οργανισμός και τα χαρακτηριστικά του οργανισμού, και συνδυάζοντάς τα, ποσοτικοποιεί το επίπεδο προστασίας της ιδιωτικότητας των χρηστών. Η κάθε κατηγορία δεδομένων επιτρέπει την εκτίμηση του αντικτύπου (impact) για τον οργανισμό αν κάτι δεν πάει «καλά». Οι αρχές ιδιωτικότητας, αντίστοιχα, βοηθούν στην εκτίμηση του αντικτύπου για τον οργανισμό αν δεν συμμορφώνεται με κάποια από αυτές. Στη συνέχεια, τα δεδομένα που προκύπτουν από την εκτίμηση του αντικτύπου για τον οργανισμό ποσοτικοποιούνται ορίζοντας μετρικές (metrics). Σκοπός είναι η προτεινόμενη μεθοδολογία, συνδυάζοντας όλες τις μετρικές που ορίστηκαν, να παρουσιάζει, μέσω μιας συνολικής συνδυαστικής μετρικής, το επίπεδο ικανοποίησης της ιδιωτικότητας των χρηστών ενός οργανισμού, κάτι που μέχρι στιγμής είναι σε πρώιμο στάδιο.

v. Εφαρμογή της προτεινόμενης μεθοδολογίας σε δύο διαφορετικούς οργανισμούς με διαφορετικά χαρακτηριστικά και αξιολόγηση της απόδοσής της και της ακρίβειας των παραγόμενων αποτελεσμάτων. Πραγματοποιήθηκαν συνεντεύξεις σε ένα μεγάλο Νοσοκομείο και σε ένα Κέντρο Υγείας. Και στις δύο περιπτώσεις, οι απαντήσεις εισήχθησαν στη μεθοδολογία μας και εφαρμόζοντας τις μετρικές με βάση τα χαρακτηριστικά τους καταλήξαμε ότι και τα δύο Νοσοκομεία θα πρέπει να λάβουν μέτρα προστασίας για τα προσωπικά και ειδικών κατηγοριών δεδομένα των ασθενών που τηρούν, με σκοπό την μεγαλύτερη προστασία των δεδομένων τους.

vi. Μελέτη, ανάλυση και προσδιορισμός των απαιτήσεων του ΓΚΠΔ («Material & territorial scope», «Data protection principles», «Consent», «Children – Parental Consent», «Sensitive data & lawful processing», «Information notices», «Subject access, rectification and portability», «Right to object», «Right to erasure & to restriction of processing», «Profiling and automated decision-taking» and «Accountability, security and breach notification») και τρόποι ικανοποίησής των σε περιβάλλοντα υπολογιστικού νέφους, όσον

αφορά τα τεχνικά, οργανωτικά και διαδικαστικά μέτρα που πρέπει να ληφθούν.

Στον παρακάτω πίνακα φαίνεται η συνεισφορά στην παρούσα διδακτορική διατριβή:

	Σύντομη Περιγραφή	**Συνεισφορά**
i	Συγκέντρωση των αρχών ιδιωτικότητας, των απαιτήσεων ασφάλειας και ιδιωτικότητας και ταξινόμησή τους με βάση τη σημαντικότητά τους. *(Makri Eleni-Laskarina, Lambrinoudakis Costas, Towards a Common Security and Privacy Requirements Elicitation Methodology, "Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security", ICGS3 2015, 151-159, Springer, 2015.)* *(Makri Eleni-Laskarina, Lambrinoudakis Costas, Privacy Principles: Towards a Common Privacy Audit Methodology, "Trust, Privacy and Security in Digital Business", TrustBus 2015, 219-234, Springer, 2015.)*	[22] [23]
ii	Καταγραφή των χαρακτηριστικών του προς εξέταση οργανισμού και των κατηγοριών των δεδομένων που χρησιμοποιεί. (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, Utilizing a privacy impact assessment method using metrics in the healthcare sector, Information & Computer Security, 503-529, 2020.) (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, A proposed privacy impact assessment method using metrics based on organizational characteristics, Computer Security, ESORICS 2019, 122-139, 2019.)	[18] [20]
iii	Επισκόπηση και καταγραφή των προτεινόμενων μεθοδολογιών εκτίμησης αντικτύπου (PIA) που υπάρχουν μέχρι στιγμής στη βιβλιογραφία. (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, Utilizing a privacy impact assessment method using metrics in the healthcare sector, Information & Computer Security, 503-529, 2020.) (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, A proposed privacy impact assessment method using metrics based on	[18] [20]

	Σύντομη Περιγραφή	Συνεισφορά
	organizational characteristics, Computer Security, ESORICS 2019, 122-139, 2019.)	
iv	Ανάπτυξη μεθοδολογίας η οποία λαμβάνει σαν είσοδο τις ταξινομημένες αρχές και απαιτήσεις ιδιωτικότητας, τις κατηγορίες δεδομένων (data sets) που χρησιμοποιεί ένας οργανισμός και τα χαρακτηριστικά του οργανισμού, και συνδυάζοντάς τα, ποσοτικοποιεί το επίπεδο προστασίας της ιδιωτικότητας των χρηστών. (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, Utilizing a privacy impact assessment method using metrics in the healthcare sector, Information & Computer Security, 503-529, 2020.) (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, A proposed privacy impact assessment method using metrics based on organizational characteristics, Computer Security, ESORICS 2019, 122-139, 2019.)	[18] [20]
v	Εφαρμογή της μεθοδολογίας σε δύο διαφορετικούς οργανισμούς με διαφορετικά χαρακτηριστικά και αξιολόγηση της απόδοσής της. (Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, Utilizing a privacy impact assessment method using metrics in the healthcare sector, Information & Computer Security, 503-529, 2020.)	[18]
vi	Προσαρμογή της μεθοδολογίας στις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (ΓΚΠΔ).	[paper to be submitted]
vii	Μελέτη, ανάλυση και προσδιορισμός των απαιτήσεων του ΓΚΠΔ και τρόποι ικανοποίησής των σε περιβάλλοντα υπολογιστικού νέφους, όσον αφορά τα τεχνικά, οργανωτικά και διαδικαστικά μέτρα που πρέπει να ληφθούν. (Georgiopoulou Zafeiroula, Makri Eleni-Laskarina, Lambrinoudakis Costas,	[19] [21]

	Σύντομη Περιγραφή	Συνεισφορά
	GDPR compliance: proposed technical and organizational measures for cloud provider, Information & Computer Security, 665-680, 2020.) (Georgiopoulou Zafeiroula, Makri Eleni-Laskarina, Lambrinoudakis Costas, GDPR Compliance: Proposed Technical and Organizational Measures for Cloud Providers, Information & Computer Security, ESORICS 2019, 181-194, 2019.)	

2 Κεφάλαιο 2: Ερευνητική επισκόπηση: Προσδιορισμός αρχών ιδιωτικότητας, απαιτήσεων ασφάλειας και απαιτήσεων ιδιωτικότητας

2.1 Εισαγωγή

Κατά τη διάρκεια των τελευταίων δεκαετιών η χρήση του διαδικτύου έχει αυξηθεί δραματικά. Όλο και περισσότεροι άνθρωποι χρησιμοποιούν το διαδίκτυο και τις υπηρεσίες του σε καθημερινή βάση για να ενημερωθούν, να εκπαιδευτούν, να ψυχαγωγηθούν και να ικανοποιήσουν διάφορες ανάγκες τους. Προκειμένου οι χρήστες να χρησιμοποιήσουν τις διαδικτυακές υπηρεσίες, αποκαλύπτουν τα προσωπικά τους δεδομένα αγνοώντας τις συνέπειες. Ως αποτέλεσμα, πολύ συχνά παραβιάζεται η ιδιωτικότητα των χρηστών αφού τα προσωπικά τους δεδομένα είναι εκτεθειμένα στον οποιονδήποτε. Η έννοια της *Ιδιωτικότητας του Διαδικτύου (Internet Privacy)* περιλαμβάνει τον τρόπο με τον οποίο τα προσωπικά δεδομένα χρησιμοποιούνται, αποθηκεύονται, επεξεργάζονται, είναι εκμεταλλεύσιμα από τρίτους, κτλ. Στόχος είναι η προστασία των χρηστών από μη ηθελημένη αποκάλυψη των προσωπικών τους δεδομένων.

Η υποενότητα 2.2 που ακολουθεί παρέχει μια επισκόπηση της βιβλιογραφίας σχετικά με τις αρχές ιδιωτικότητας που έχουν θεσπιστεί και χρησιμοποιούνται είτε από χώρες είτε από δημόσιους και ιδιωτικούς φορείς προκειμένου να προστατεύσουν τα δεδομένα των χρηστών τους. Η υποενότητα 2.3 παραθέτει τις πιο ευρέως αποδεκτές από την επιστημονική κοινότητα απαιτήσεις ασφάλειας, όπως αυτές προκύπτουν από μελέτες ανάλυσης επικινδυνότητας, ενώ η υποενότητα 2.4 παραθέτει τις πιο ευρέως υιοθετούμενες απαιτήσεις ιδιωτικότητας.

2.2 Αρχές ιδιωτικότητας

Είναι δεδομένο ότι έχει γίνει μεγάλη ερευνητική προσπάθεια για την ανάπτυξη τρόπων προστασίας των προσωπικών δεδομένων των χρηστών. Από τη μια πλευρά, πολλοί νόμοι και οδηγίες/κατευθυντήριες γραμμές σχετικά με την προστασία της ιδιωτικότητας των χρηστών, υπάρχουν σε πολλές χώρες, επιβάλλοντας σε οργανισμούς που αποθηκεύουν προσωπικά δεδομένα να μην τα χρησιμοποιούν χωρίς προηγούμενη ενημέρωση των χρηστών και την απόκτηση συγκατάθεσής τους. Από την άλλη πλευρά, υπάρχουν πολλοί

δημόσιοι ή/και ιδιωτικοί φορείς, οι οποίοι ενδιαφέρονται να προστατεύσουν την ιδιωτικότητα των χρηστών και για το λόγο αυτό έχουν δημοσιεύσει αρκετές αρχές ιδιωτικότητας. Ταυτόχρονα, χρησιμοποιούνται οι *Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies - PETs)*, μια ποικιλία μέτρων προστασίας της ιδιωτικότητας των πληροφοριών προσφέροντας τα τεχνικά μέσα για την προστασία των προσωπικών δεδομένων του χρήστη και επομένως για την αποτροπή της μη απαραίτητης ή της μη ηθελημένης επεξεργασίας [39][40]. Ωστόσο, τόσο οι αρχές ιδιωτικότητας όσο και τα PETs δεν μπορούν να σταθούν από μόνα τους, αλλά συσχετίζονται και λειτουργούν συμπληρωματικά.

Εδώ και πολλά χρόνια, η προστασία της ιδιωτικότητας των χρηστών αποτελεί βασική τους ανησυχία και για το λόγο αυτό έχουν υιοθετηθεί συγκεκριμένες αρχές ιδιωτικότητας προκειμένου να αποφευχθεί η αποκάλυψη των προσωπικών δεδομένων τους. Από το 1980 [5], ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) (Organisation for Economic Co-operation and Development - OECD) έχει ορίσει ένα κοινό πλαίσιο προστασίας της ιδιωτικότητας, το οποίο περιλαμβάνει τις πιο ευρέως χρησιμοποιούμενες αρχές ιδιωτικότητας. Οι οκτώ αρχές ιδιωτικότητας, που προτάθηκαν τη δεκαετία του '80, εξακολουθούν να χρησιμοποιούνται. Διακεκριμένοι επιστήμονες, όπως η Ann Cavoukian και η ομάδα της [40] [41] έχουν βασιστεί σε αυτές τις αρχές για τη διεξαγωγή της έρευνάς τους και πολλοί οργανισμοί τις έχουν εφαρμόσει προκειμένου να διασφαλίσουν προστασία της ιδιωτικότητας.

Οι αρχές ιδιωτικότητας έχουν συμβάλει/εμπνεύσει μια σειρά από νομοθετικές πρωτοβουλίες. Το 1995, η Ευρωπαϊκή Επιτροπή (European Commission - EC) εισήγαγε την Οδηγία για την Προστασία Δεδομένων (Οδηγία 95/46/ΕΚ) [48][49] προκειμένου να ενισχύσει τους νόμους περί προστασίας δεδομένων, με στόχο την προστασία των ατόμων σε σχέση με την επεξεργασία προσωπικών δεδομένων και με την ελεύθερη κυκλοφορία των δεδομένων αυτών [48]. Οι αρχές ιδιωτικότητας του OECD (1980) και η Οδηγία 95/46/ΕΚ (1995) ήταν από τις πρώτες σοβαρές προσπάθειες που έγιναν επιβάλλοντας περιορισμούς στους τρόπους με τους οποίους ένας οργανισμός μπορεί να συλλέγει, να αποθηκεύει και να επεξεργάζεται προσωπικά δεδομένα.

Τον Μάρτιο του 1996 [50], αναπτύχθηκε το Εθνικό Πρότυπο του Καναδά «Μοντελοποίηση Κώδικα για την Προστασία των Προσωπικών Πληροφοριών» βασιζόμενο

στις οδηγίες/κατευθυντήριες γραμμές του OECD. Δύο επιπλέον αρχές ιδιωτικότητας (συναίνεση και συμμόρφωση) προστέθηκαν για την ενίσχυση της προστασίας των προσωπικών πληροφοριών. Επιπλέον, το Υπουργείο Εμπορίου των Ηνωμένων Πολιτειών ανέπτυξε το Safe Harbor [38], ένα νομικό πλαίσιο που επέτρεπε στους οργανισμούς των ΗΠΑ να συμμορφώνονται με την Οδηγία της Ευρωπαϊκής Επιτροπής για την προστασία δεδομένων [5]. Το Safe Harbor περιλάμβανε αρχές ιδιωτικότητας που βασίστηκαν σε αυτές που ορίζει ο OECD (1980).

Παράλληλα με τους νόμους, τις οδηγίες/κατευθυντήριες γραμμές και τα πρότυπα περί ιδιωτικότητας, υπάρχουν και ορισμένοι οργανισμοί που προσπαθούν να υποστηρίξουν την προστασία της ιδιωτικότητας των χρηστών. Βασιζόμενος στις αρχές ιδιωτικότητας του OECD (1980), ο Information Systems Audit and Control Association (ISACA) δημοσίευσε τις αρχές ιδιωτικότητας ISACA/OECD το 2009 [52]. Επιπλέον, ο ISACA πρότεινε μια λίστα με ενδεικτικούς ελέγχους ιδιωτικότητας για την προστασία και τη διατήρηση της ιδιωτικότητας των προσωπικών δεδομένων των χρηστών. Άλλοι οργανισμοί όπως ο European Network and Information Security Agency (ENISA) [37] ή η International Business Machines (IBM) [51] έχουν επίσης λάβει μέτρα για την προστασία της ιδιωτικότητας προτείνοντας κατάλληλους μηχανισμούς.

Το 2011 [36], ο Διεθνής Οργανισμός Τυποποίησης (International Organization for Standardization - ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission - IEC), παρείχαν ένα πλαίσιο ιδιωτικότητας βασισμένο σε έντεκα αρχές ιδιωτικότητας που περιλάμβαναν τις ήδη υπάρχουσες αρχές που αναπτύχθηκαν από κράτη, χώρες και διεθνείς οργανισμούς. Σύμφωνα με το ISO/IEC 29100:2011, οι αρχές ιδιωτικότητας θα πρέπει να χρησιμοποιούνται για την καθοδήγηση του σχεδιασμού, της ανάπτυξης και της εφαρμογής των πολιτικών και ελέγχων ιδιωτικότητας.

Με το πέρασμα του χρόνου, το τεχνολογικό περιβάλλον στο οποίο εφαρμόστηκαν οι αρχές ιδιωτικότητας έχει υποστεί σημαντικές αλλαγές, οι σημαντικότερες από τις οποίες αφορούσαν τον όγκο των προσωπικών δεδομένων που συλλέγονται, αποθηκεύονται και υφίστανται επεξεργασία. Επιπλέον, τα προσωπικά δεδομένα γίνονται σταδιακά διαθέσιμα παγκοσμίως ενώ ταυτόχρονα υπάρχουν πολύ περισσότερες απειλές ιδιωτικότητας. Ως εκ τούτου, για τα ήδη υπάρχοντα και πιο απαιτητικά τεχνολογικά περιβάλλοντα, ήταν

απαραίτητη η ύπαρξη νέων μέτρων προστασίας. Η ανάγκη επικαιροποίησης της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ οδήγησε την Ευρωπαϊκή Επιτροπή να προτείνει μια σημαντική μεταρρύθμιση του νομικού πλαισίου της ΕΕ για την προστασία των προσωπικών δεδομένων, το 2014 [53]. Οι νέες προτάσεις ενίσχυσαν τα δικαιώματα των χρηστών και ταυτόχρονα αντιμετώπισαν τις προκλήσεις της παγκοσμιοποίησης και των νέων τεχνολογιών [46]. Για τους ίδιους λόγους, το 2013 [35] ο OECD πρότεινε συμπληρωματικές αρχές προστασίας της ιδιωτικότητας, προσθέτοντας οκτώ ακόμη αρχές.

Παράλληλα, αρκετές μεμονωμένες προσπάθειες γίνονται από πολλές χώρες και άλλους δημόσιους ή ιδιωτικούς φορείς. Τον Νοέμβριο του 2006, η Ann Cavoukian [44] πρότεινε το Παγκόσμιο Πρότυπο Προστασίας Ιδιωτικότητας (Global Privacy Standard - GPS), στόχος του οποίου ήταν η δημιουργία ενός κοινού παγκόσμιου πλαισίου ιδιωτικότητας για την προστασία της ιδιωτικότητας των χρηστών σε παγκόσμιο επίπεδο. Το πρότυπο GPS περιλάμβανε δέκα αρχές ιδιωτικότητας, οι οποίες προήλθαν από τη συλλογική γνώση και την πρακτική σοφία της διεθνούς κοινότητας προστασίας δεδομένων και, ως εκ τούτου, ήταν η πρώτη ομαδική δουλειά προς ένα παγκόσμιο πλαίσιο ιδιωτικότητας.

Στις μέρες μας, η ιδιωτικότητα αποτελεί σοβαρό πρόβλημα τόσο για τους χρήστες όσο και για τους οργανισμούς. Για το λόγο αυτό, πολλοί ερευνητές υποστηρίζουν ότι η ιδιωτικότητα θα πρέπει να διατηρείται καθ' όλη τη διάρκεια του κύκλου ζωής ενός συστήματος πληροφορικής. Με άλλα λόγια, η ιδιωτικότητα θα πρέπει να λαμβάνεται υπόψη από τη φάση σχεδιασμού ενός συστήματος πληροφορικής μέχρι το τέλος ολόκληρου του κύκλου ζωής του. Η ιδέα της ιδιωτικότητας κατά το σχεδιασμό (privacy-by-design) ως η φιλοσοφία για την προστασία της ιδιωτικότητας καθ' όλη τη διαδικασία της τεχνολογικής ανάπτυξης, από τη σύλληψη της ιδέας ενός νέου συστήματος μέχρι την υλοποίησή του, υποστηρίχθηκε έντονα από την Ann Cavoukian [41] και τον Jaap-Henk Hoepman [42][43].

Παρά το γεγονός ότι έγιναν αξιοσημείωτες προσπάθειες [35][42][43][44] για να συγκεντρωθούν όλες οι αρχές ιδιωτικότητας και να χρησιμοποιηθούν σε ένα κοινό σύστημα το οποίο λαμβάνει υπόψη την ιδιωτικότητα κατά το σχεδιασμό, δεν υπάρχει δημοσιευμένη μεθοδολογία που να συνδυάζει τις υπάρχουσες αρχές ιδιωτικότητας για την υποστήριξη του σχεδιασμού ενός Συστήματος Διατήρησης Ιδιωτικότητας (a Privacy Preserving System). Ένας από τους βασικούς λόγους για αυτό είναι ότι το τεχνολογικό

περιβάλλον αλλάζει συνεχώς, κάτι που δυσκολεύει την προσαρμογή των οργανισμών. Ένας άλλος πιθανός λόγος είναι ότι ο όγκος των πληροφοριών είναι τεράστιος και δύσκολα διαχειρίσιμος. Επιπλέον, τα τρέχοντα πληροφοριακά συστήματα απαιτούν παγκόσμια διαθεσιμότητα προσωπικών δεδομένων για να λειτουργήσουν, ενώ παράλληλα, οι απειλές για την ιδιωτικότητα έχουν αυξηθεί και οι οργανισμοί δεν μπορούν να τις καλύψουν λόγω της ταχείας αλλαγής/μεταμόρφωσής τους. Όλα τα παραπάνω είναι μερικοί από τους πιο σημαντικούς λόγους για τους οποίους οι τρέχουσες αρχές ιδιωτικότητας είναι απαραίτητες.

Η πλειοψηφία των υφιστάμενων πλαισίων ιδιωτικότητας βασίζεται στις παρακάτω οκτώ αρχές ιδιωτικότητας [5][8] του ΟΟΣΑ:

- **Αρχή Καθορισμού του Σκοπού (Purpose Specification Principle):** Ο οργανισμός πρέπει να καθορίσει έναν συγκεκριμένο σκοπό για τη συλλογή δεδομένων. Τα προσωπικά δεδομένα θα πρέπει να συλλέγονται και να χρησιμοποιούνται μόνο για συγκεκριμένους σκοπούς. Ο χρήστης θα πρέπει να ειδοποιείται/ενημερώνεται για το λόγο ή τους λόγους που τα προσωπικά δεδομένα του συλλέγονται και χρησιμοποιούνται.

- **Αρχή Περιορισμού της Συλλογής (Collection Limitation Principle):** Ο οργανισμός θα πρέπει να συλλέγει, με νόμιμα μέσα, προσωπικά δεδομένα που εξυπηρετούν συγκεκριμένους σκοπούς. Με αυτό τον τρόπο, μόνο τα απαραίτητα δεδομένα θα συλλέγονται χωρίς πλεονάζοντες προσωπικές πληροφορίες. Επίσης, η συλλογή δεδομένων θα πρέπει να πραγματοποιείται μόνο μετά τη συγκατάθεση του χρήστη, εάν φυσικά δεν υπάρχει κάποια άλλη νομική βάση για τη συλλογή τους.

- **Αρχή Διατήρησης Ποιότητας των Δεδομένων (Data Quality Principle):** Ο οργανισμός θα πρέπει να διατηρεί τα προσωπικά δεδομένα που συλλέγονται και χρησιμοποιούνται ακριβή, πλήρη και ενημερωμένα. Η ποιότητα των πληροφοριών θα πρέπει να διατηρείται καθ’ όλη τη διάρκεια χρήσης των προσωπικών δεδομένων.

- **Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης (Use, Retention and Disclosure Limitation Principle):** Τα προσωπικά δεδομένα θα πρέπει να χρησιμοποιούνται μόνο με τη συγκατάθεση του χρήστη ή υπό νόμιμες συνθήκες. Ο οργανισμός θα πρέπει να περιορίσει τη χρήση προσωπικών δεδομένων χωρίς να τα

αποκαλύπτει ή να τα καθιστά διαθέσιμα για οποιονδήποτε άλλο λόγο εκτός από τον σκοπό για τον οποίο συλλέχθηκαν.

- **Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας (Security Safeguards Principle):** Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται από πιθανά περιστατικά παραβίασης της ασφάλειας ή/και της ιδιωτικότητας [29] μέσω της εφαρμογής των μέτρων προστασίας ασφάλειας. Με αυτό τον τρόπο, τα προσωπικά δεδομένα θα είναι προστατευμένα από απειλές ασφάλειας και ιδιωτικότητας.

- **Αρχή Διαφάνειας (Openness Principle):** Οι πρακτικές, πολιτικές, διεργασίες και διαδικασίες που αφορούν τα προσωπικά δεδομένα των χρηστών θα πρέπει να είναι εύκολα προσβάσιμες και η διαφάνειά τους θα πρέπει να διατηρείται σε κάθε στάδιο της συλλογής και χρήσης τους.

- **Αρχή Ατομικής Συμμετοχής (Individual Participation Principle):** Ο ιδιοκτήτης των προσωπικών δεδομένων θα πρέπει να συμμετέχει στη διαδικασία συλλογής και χρήσης τους. Ο χρήστης θα πρέπει να έχει το δικαίωμα να παρεμβαίνει οπουδήποτε είναι απαραίτητο εκτός από την περίπτωση που κάτι τέτοιο απαγορεύεται ρητά από το νόμο.

- **Αρχή Λογοδοσίας (Accountability Principle):** Ο Υπεύθυνος Επεξεργασίας Δεδομένων (Data Controller) θα πρέπει να είναι υπεύθυνος για τη συμμόρφωση με τους μηχανισμούς προστασίας που έχουν προκύψει από την εφαρμογή των παραπάνω αρχών ιδιωτικότητας.

Οι παραπάνω αρχές ιδιωτικότητας είναι μεταξύ των πιο ευρέως υιοθετούμενων [5][8] για την προστασία των προσωπικών πληροφοριών. Παρ' όλα αυτά, δεν υπάρχουν καλές πρακτικές, οδηγίες/κατευθυντήριες γραμμές ή δομημένες διαδικασίες για την εφαρμογή τους, ούτε από την πλευρά του οργανισμού, ούτε από την πλευρά του χρήστη.

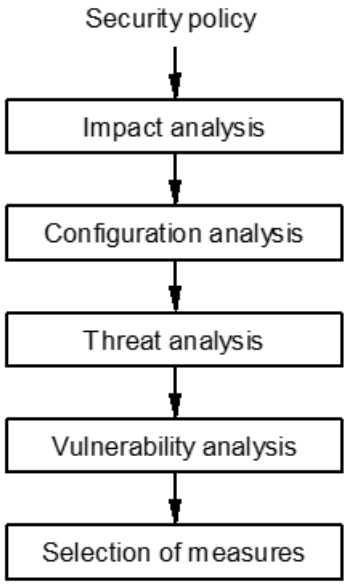
Μερικές καλές πρακτικές και συμβουλές στον τρόπο με τον οποίο οι αρχές ιδιωτικότητας θα πρέπει να ληφθούν υπόψη κατά το σχεδιασμό ενός συστήματος μπορεί κάποιος να βρει σε ιστολόγια (blogs), φόρουμ (fora) και ιστοτόπους (websites) [17]. Παρόλα αυτά, η πληροφορία παραμένει «διασκορπισμένη» και ακόμα μη επίσημη. Επομένως, είναι ιδιαίτερα δύσκολο και για έναν οργανισμό και για έναν χρήστη να

αποφασίσει την αποτελεσματικότητα και συνέπεια των εφαρμοζόμενων μηχανισμών προστασίας της ιδιωτικότητας. Η ύπαρξη μιας δομημένης διαδικασίας μπορεί να βοηθήσει τους οργανισμούς να εφαρμόσουν τις αρχές ιδιωτικότητας, και την ίδια στιγμή, να βοηθήσει τους χρήστες να εξασφαλίσουν ότι οι προσωπικές τους πληροφορίες είναι επαρκώς προστατευμένες. Επιπλέον, μια τέτοια δομημένη διαδικασία μπορεί να βοηθήσει τους Ελεγκτές Ιδιωτικότητας (Privacy Auditors) να ελέγξουν αν η ιδιωτικότητα προστατεύεται αποτελεσματικά. Ο έλεγχος είναι μια από τις πιο σημαντικές διαδικασίες σε έναν οργανισμό, από τη στιγμή που μπορεί να επηρεάσει τη φήμη του είτε θετικά είτε αρνητικά. Κατά συνέπεια, μπορεί είτε να αυξήσει την εμπιστοσύνη των χρηστών είτε την ανασφάλειά τους.

2.3 Ανάλυση επικινδυνότητας και Απαιτήσεις ασφάλειας

Για την επιλογή αντιμέτρων (countermeasures) μπορεί κανείς να επιλέξει μεταξύ μιας βασικής προσέγγισης, η οποία χρησιμοποιεί λίστες ελέγχου (checklists), και μιας πιο ενδελεχούς προσέγγισης, η οποία βασίζεται σε (ποιοτική) ανάλυση κινδύνου [26] [27].

Η ποιοτική ανάλυση κινδύνου (qualitative risk analysis) ενός πληροφοριακού συστήματος περιλαμβάνει τα ακόλουθα στάδια (Σχήμα 1):



Σχήμα 1: Ενδεικτικές φάσεις μιας μεθοδολογίας ανάλυσης επικινδυνότητας

- Impact analysis: Ανάλυση αντικτύπου για τον καθορισμό των απαιτήσεων ασφαλείας που επιβάλλονται στο πληροφοριακό σύστημα και τα επιμέρους στοιχεία (components) του, με βάση την πιθανή ζημιά στα επιμέρους στοιχεία και

στις επιχειρησιακές διαδικασίες (business processes) που χρησιμοποιούν το πληροφοριακό σύστημα.

- Configuration analysis: Ανάλυση ρυθμίσεων για να καθοριστεί ποια επιμέρους στοιχεία υπάρχουν στο πληροφοριακό σύστημα και ποιες σχέσεις υπάρχουν μεταξύ τους.
- Threat analysis: Ανάλυση απειλών για να εντοπιστούν οι σχετιζόμενες απειλές.
- Vulnerability analysis: Ανάλυση ευπαθειών για τον καθορισμό της ευπάθειας των επιμέρους στοιχείων σε σχέση με τις εντοπισθείσες απειλές.
- Selection of measures: Επιλογή μέτρων ασφαλείας που είναι ικανά να μειώσουν τους μη αποδεκτούς κινδύνους.

Μια ενδεικτική μεθοδολογία ανάλυσης επικινδυνότητας είναι η CRAMM (CCTA Risk Analysis and Management Method). Αναπτύχθηκε αρχικά από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών του Ηνωμένου Βασιλείου (CCTA - Central Computer and Telecommunications Agency) για χρήση από την κυβέρνηση του Ηνωμένου Βασιλείου. Αργότερα, αναπτύχθηκαν εκδόσεις για εμπορική χρήση και σε άλλες γλώσσες. Μια μελέτη ανάλυσης επικινδυνότητας με την CRAMM (αναθεώρηση-review) αποτελείται από τρία στάδια:

- **Στάδιο 1**: Το στάδιο αποτίμησης αγαθών
- **Στάδιο 2**: Το στάδιο ανάλυσης επικινδυνότητας, και
- **Στάδιο 3**: Το στάδιο διαχείρισης επικινδυνότητας

Το *πρώτο στάδιο* (στάδιο αποτίμησης αγαθών) ξεκινά με τον ορισμό του πεδίου εφαρμογής της μελέτης. Στη συνέχεια, η αξία του συστήματος που υπόκειται στη μελέτη καθορίζεται με την κατασκευή ενός μοντέλου αγαθών το οποίο αναλύει το σύστημα στα επιμέρους στοιχεία του (τοποθεσίες, εξοπλισμός, λογισμικό και δεδομένα) και τις σχέσεις μεταξύ των στοιχείων. Επίσης, καθορίζεται το κόστος αντικατάστασης κάθε επιμέρους στοιχείου (άμεσο κόστος). Η ζημία (αντίκτυπος) που προκαλείται στον οργανισμό από μια πιθανή παραβίαση στην εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα του συστήματος (επακόλουθο κόστος) προσδιορίζεται με τη διεξαγωγή συνεντεύξεων. Για κάθε

αντίκτυπο στο υπό εξέταση σύστημα, ο ερωτώμενος πρέπει να υποδεικνύει τη ζημία που εκτιμά ότι θα προκληθεί στον οργανισμό.

Οι ζημιές ταξινομούνται σε μια κλίμακα από το 1 έως το 10. Για να αντιστοιχιστούν οι πραγματικές ζημίες σε τιμές CRAMM, η CRAMM περιλαμβάνει έναν αριθμό πινάκων. Κάθε ένας από αυτούς τους πίνακες περιέχει δέκα περιγραφές ορισμένων τύπων ζημιών (για παράδειγμα: οικονομική ζημία ή βλάβη στη φήμη ενός οργανισμού) και τις αντίστοιχες τιμές CRAMM. Ο ερωτώμενος επιλέγει το κατάλληλο σενάριο ζημίας για κάθε αντίκτυπο και επιλέγει την κατάλληλη περιγραφή από τον πίνακα ζημιών του σεναρίου. Η αντίστοιχη τιμή είναι η τιμή ζημίας CRAMM.

Στο τέλος του πρώτου σταδίου, η CRAMM υπολογίζει το σχετικό αντίκτυπο και τις σχετικές ζημίες για κάθε επιμέρους στοιχείο με βάση το μοντέλο αγαθών, τον αντίκτυπο που θεωρήθηκε σχετικός για το σύστημα στο σύνολό του και τη ζημία που θα προκαλούσε κάθε αντίκτυπος.

Στο *δεύτερο στάδιο* (στάδιο ανάλυσης επικινδυνότητας), οι απειλές αντιστοιχίζονται σε αντίκτυπο και επιμέρους στοιχεία, υποδεικνύοντας ότι μια συγκεκριμένη απειλή επηρεάζει ένα συγκεκριμένο επιμέρους στοιχείο και θα προκαλέσει ένα συγκεκριμένο αντίκτυπο εάν πραγματοποιηθεί. Η CRAMM περιέχει μια στάνταρ αντιστοίχιση απειλών για αντίκτυπο και απειλών για επιμέρους στοιχεία, την οποία ο χρήστης μπορεί να επεξεργαστεί για την τρέχουσα ανάλυση, για παράδειγμα λόγω περιορισμών που θέτει ο σκοπός. Στη συνέχεια, το επίπεδο κάθε απειλής καθορίζεται με τη διεξαγωγή συνεντεύξεων πολλαπλών επιλογών για κάθε απειλή για κάθε επιμέρους στοιχείο. Οι απαντήσεις στη συνέντευξη καθορίζουν το επίπεδο αυτής της απειλής για το συγκεκριμένο επιμέρους στοιχείο. Τέλος, το επίπεδο ευπαθειών ενός επιμέρους στοιχείου για μια απειλή καθορίζεται με τη διεξαγωγή συνεντεύξεων για τις ευπάθειες. Οι συνεντεύξεις για απειλές και ευπάθειες διεξάγονται συνήθως ταυτόχρονα, για να περιοριστεί ο αριθμός των συνεντεύξεων. Παρόμοια επιμέρους στοιχεία ομαδοποιούνται στην αρχή του δεύτερου σταδίου, για να περιοριστεί ο αριθμός των σχέσεων απειλής-επιμέρους στοιχείου που πρέπει να καθοριστούν. Τα επίπεδα απειλής και ευπάθειας ορίζονται για αυτές τις ομάδες στο σύνολό τους, περιορίζοντας περαιτέρω τον αριθμό των συνεντεύξεων που πρέπει να διεξαχθούν.

Αφού καταχωρηθούν όλες αυτές οι πληροφορίες, η CRAMM υπολογίζει μια τιμή Μέτρησης Κινδύνου (Measure of Risk - MOR) για κάθε συνδυασμό ομάδας αγαθών, απειλών και αντίκτυπου. Η τιμή MOR υποδεικνύει το επίπεδο κινδύνου, βασιζόμενη στην πιθανότητα να υλοποιηθεί η απειλή, στην πιθανότητα αυτό να επηρεάσει την ομάδα αγαθών (με βάση την ευπάθεια αυτής της ομάδας αγαθών για αυτήν την απειλή) και να προκαλέσει τον αντίκτυπο.

Στο *τρίτο στάδιο* (στάδιο διαχείρισης επικινδυνότητας), η CRAMM επιλέγει αυτόματα αντίμετρα από τη βάση δεδομένων της, βασιζόμενη στα αποτελέσματα από τα προηγούμενα στάδια και ιδιαίτερα στο μοντέλο αγαθών και τις τιμές MOR. Τα επιλεγμένα αντίμετρα πρέπει να συγκριθούν με τα υπάρχοντα μέτρα. Συνεπώς, η κατάσταση κάθε επιλεγμένου αντιμέτρου μπορεί να καθοριστεί ως εξής: έχει ήδη εφαρμοστεί (εάν υπάρχει υπάρχον αντίμετρο που αντιστοιχεί στο επιλεγμένο αντίμετρο), να εφαρμοστεί ή αποδοχή κινδύνου (εάν ο οργανισμός έχει επιλέξει να μην εφαρμόσει αυτό το αντίμετρο και αποδεχτεί τον κίνδυνο).

Οι πιο κοινές απαιτήσεις ασφαλείας που προκύπτουν από την ανάλυση επικινδυνότητας είναι:

- **Εμπιστευτικότητα**: Μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στα δεδομένα
- **Ακεραιότητα**: Μόνο εξουσιοδοτημένοι χρήστες μπορούν να τροποποιήσουν / διαγράψουν τα δεδομένα
- **Διαθεσιμότητα**: Η παρεχόμενη υπηρεσία θα πρέπει να είναι διαθέσιμη όποτε ζητηθεί.
- **Μη αποποίηση**: Συσχέτιση συγκεκριμένων χρηστών με συγκεκριμένες ενέργειες.

2.4 Απαιτήσεις ιδιωτικότητας

Προκειμένου τα προσωπικά δεδομένα ενός πληροφοριακού συστήματος να είναι προστατευμένα, εκτός από τους νόμους περί ιδιωτικότητας και τους κανονισμούς που πρέπει να εφαρμόζονται, υπάρχουν πολλές μεθοδολογίες απαιτήσεων ιδιωτικότητας που έχουν προταθεί στη βιβλιογραφία [28] [29]. Οι υπάρχουσες μεθοδολογίες απαιτήσεων ιδιωτικότητας υιοθετούν έννοιες από τον τομέα της ασφάλειας οι οποίες χρησιμοποιούνται

για να αντιπροσωπεύουν ρητά τις απαιτήσεις ασφαλείας (οι οποίες περιλαμβάνουν επίσης απαιτήσεις ιδιωτικότητας) και καθορίζουν τον τρόπο με τον οποίο αυτές οι απαιτήσεις μπορούν να μετατραπούν σε συγκεκριμένες πολιτικές για ένα υπό κατασκευή σύστημα [28]. Με άλλα λόγια, οι μεθοδολογίες ιδιωτικότητας, που παρουσιάζονται παρακάτω, στοχεύουν να ενσωματώσουν βασικές έννοιες για τη σαφή αναπαράσταση των απαιτήσεων ιδιωτικότητας κατά το σχεδιασμό ενός συστήματος.

Η πλειοψηφία αυτών των μεθοδολογιών ακολουθούν συγκεκριμένα βήματα/φάσεις προκειμένου να επιτύχουν τον στόχο τους και να προστατεύσουν την ιδιωτικότητα. Ενδεικτικά, θα παρουσιαστούν τα βήματα της μεθόδου PriS, ως παράδειγμα μιας τέτοιας μεθοδολογίας [28] [29] [30] [31] [32] [33], η οποία αποτελείται από τρία βήματα. Στο *πρώτο βήμα*, καθορίζονται οι στόχοι για την επίτευξη της ιδιωτικότητας, που σχετίζονται με έναν οργανισμό. Κατά τη διάρκεια αυτού του βήματος συμμετέχουν αρκετοί εμπλεκόμενοι προκειμένου να εντοπιστούν οι βασικές ανησυχίες σχετικά με την ιδιωτικότητα του πληροφοριακού συστήματος του οργανισμού. Στο *δεύτερο βήμα*, αρχικά, προσδιορίζεται και αναλύεται ο αντίκτυπος των στόχων ιδιωτικότητας σε σχέση με τους στόχους του οργανισμού. Δεύτερον, εξετάζονται οι στόχοι ιδιωτικότητας και προσδιορίζονται οι διαδικασίες που αναγνωρίζουν τους στόχους που σχετίζονται με την ιδιωτικότητα και χαρακτηρίζονται ως διαδικασίες σχετιζόμενες με την ιδιωτικότητα. Στη συνέχεια, μοντελοποιούνται χρησιμοποιώντας πρότυπα διαδικασιών ιδιωτικότητας. Στο *τρίτο βήμα*, η μεθοδολογία ορίζει την αρχιτεκτονική του συστήματος και στη συνέχεια προσδιορίζει τις κατάλληλες τεχνικές υλοποίησης που υποστηρίζουν καλύτερα τις αντίστοιχες διαδικασίες.

Αυτός ο τύπος μεθοδολογιών επιτυγχάνει την προστασία της ιδιωτικότητας μέσω της ικανοποίησης των απαιτήσεων ιδιωτικότητας που πρέπει να υιοθετήσει ένα πληροφοριακό σύστημα προκειμένου να προστατεύει την ιδιωτικότητα. Ενδεικτικά, οι πιο συνηθισμένες απαιτήσεις ιδιωτικότητας παρατίθενται παρακάτω:

- **Αυθεντικοποίηση (Authentication):** Η αυθεντικοποίηση χρησιμοποιείται περισσότερο ως απαίτηση ασφαλείας παρά ως απαίτηση ιδιωτικότητας σε ένα πληροφοριακό σύστημα. Ωστόσο, έχει σημαντική συνεισφορά και στην ιδιωτικότητα. Μέσω της διαδικασίας αυθεντικοποίησης επιβεβαιώνεται η ταυτότητα των χρηστών.

- **Εξουσιοδότηση (Authorization):** Μέσω της διαδικασίας εξουσιοδότησης οι χρήστες αποκτούν δικαιώματα και έχουν πρόσβαση στις υπηρεσίες ενός πληροφοριακού συστήματος. Με αυτόν τον τρόπο διασφαλίζεται η ιδιωτικότητα.
- **Ταυτοποίηση (Identification):** Η διαδικασία ταυτοποίησης δεν επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση σε προσωπικά δεδομένα που είναι αποθηκευμένα σε ένα πληροφοριακό σύστημα.
- **Προστασία Δεδομένων (Data Protection):** Τα προσωπικά δεδομένα των χρηστών θα πρέπει να προστατεύονται σύμφωνα με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΕΕ) 2016/679 [4].
- **Ανωνυμία / Ψευδωνυμία (Anonymity / Pseudonymity):** Ο οργανισμός θα πρέπει να μπορεί να παρέχει στους χρήστες ψευδώνυμα, εργαλεία ανωνυμοποίησης (anonymisers) ή ανώνυμα στοιχεία δεδομένων (data credentials) κ.τ.λ., προκειμένου να παραμείνουν ανώνυμοι και έτσι να προστατεύσουν την ιδιωτικότητά τους.
- **Μη συνδεσιμότητα (Unlinkability):** Ο οργανισμός θα πρέπει να παρέχει μηχανισμούς που δεν επιτρέπουν καμία σύνδεση μεταξύ των χρηστών ή μεταξύ ενός χρήστη και ενός γεγονότος.
- **Μη παρατηρησιμότητα (Unobservability):** Η μη παρατηρησιμότητα αποτρέπει τους κακόβουλους χρήστες να βρουν ίχνη (traces) των χρηστών ενός πληροφοριακού συστήματος όταν έχουν πρόσβαση σε υπηρεσίες του πληροφοριακού συστήματος ή σε υπηρεσίες μέσω διαδικτύου.

3 Κεφάλαιο 3: Μεθοδολογία εξαγωγής απαιτήσεων ασφάλειας και ιδιωτικότητας

3.1 Εισαγωγή

Τα τελευταία χρόνια υπάρχει μια σημαντική εξέλιξη στον τρόπο χρήσης των πληροφοριακών συστημάτων και των συστημάτων επικοινωνιών. Σήμερα, τα προσωπικά δεδομένα είναι διαθέσιμα ή/και μπορούν να συλλεχθούν από διαφορετικούς ιστότοπους σε όλο τον κόσμο. Παρόλο που η χρήση των προσωπικών πληροφοριών οδηγεί σε πολλά πλεονεκτήματα, συμπεριλαμβανομένων βελτιωμένων υπηρεσιών πελατών, αυξημένων εσόδων και χαμηλότερου επιχειρηματικού κόστους, μπορεί να γίνει κατάχρηση με διάφορους τρόπους και μπορεί να οδηγήσει σε περιστατικά ασφάλειας ή/και σε παραβίαση της ιδιωτικότητας.

Στα πλαίσια του ηλεκτρονικού εμπορίου, αρκετοί οργανισμοί, προκειμένου να εντοπίσουν τις προτιμήσεις των πελατών τους και να προσαρμόσουν ανάλογα τα προϊόντα τους, προωθώντας έτσι τις πωλήσεις τους μέσω Διαδικτύου, αναπτύσσουν νέες μεθοδολογίες συλλογής και επεξεργασίας προσωπικών δεδομένων. Συχνά, αυτό γίνεται κατά το αρχικό στάδιο της σύνδεσης του πελάτη (φάση εγγραφής) με τον ιστότοπο του πωλητή. Για παράδειγμα, οι πιστωτικές κάρτες αφήνουν ένα ίχνος στα μέρη που επισκέπτονται οι κάτοχοί τους, σε σχέση με το πού ψωνίζουν και τι αγοράζουν. Οι σύγχρονες τεχνικές εξόρυξης δεδομένων μπορούν στη συνέχεια να χρησιμοποιηθούν για την περαιτέρω επεξεργασία των συλλεγόμενων δεδομένων, δημιουργώντας βάσεις δεδομένων με τα προφίλ των καταναλωτών μέσω των οποίων μπορούν να εντοπιστούν μοναδικά οι προτιμήσεις κάθε ατόμου.

Ένα άλλο παράδειγμα είναι αυτό των ιστοτόπων που παρέχουν στους χρήστες ιατρικές πληροφορίες και συμβουλές. Οποιοσδήποτε μπορεί, μέσω Διαδικτύου, να απευθύνει ένα συγκεκριμένο αίτημα στον ιατρικό ιστότοπο και να λάβει τις πληροφορίες που θέλει, εφόσον έχει εγγραφεί. Ο οργανισμός που διατηρεί τον ιατρικό ιστότοπο μπορεί εύκολα να δημιουργήσει «προφίλ χρηστών», παρακολουθώντας πόσο συχνά ένας συγκεκριμένος χρήστης επισκέπτεται τον ιστότοπο και επιπλέον το είδος των ιατρικών πληροφοριών που τον ενδιαφέρουν. Ως εκ τούτου, αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για παραβίαση της ιδιωτικότητας των χρηστών και κατ' επέκταση του

ΓΚΠΔ για την προστασία των ατόμων σε σχέση με την επεξεργασία προσωπικών και ειδικών κατηγοριών δεδομένων.

Οι ηλεκτρονικές συναλλαγές έχουν αναδείξει το κύριο πρόβλημα της προστασίας της ιδιωτικότητας των χρηστών. Επιπλέον, έχουν αυξήσει σημαντικά τον αριθμό των απειλών στις οποίες είναι ευάλωτοι. Η πιθανότητα οι απειλές να υλοποιηθούν και να οδηγήσουν σε περιστατικό ασφαλείας συνεπάγεται την ύπαρξη ορισμένων κινδύνων. Προκειμένου να αποφευχθεί η σύγχυση, είναι σημαντικό να τονιστεί η διαφορά μεταξύ ιδιωτικότητας και ασφάλειας. Πιο συγκεκριμένα, μια πληροφορία είναι ασφαλής όταν προστατεύεται το περιεχόμενό της, ενώ είναι ιδιωτική όταν προστατεύεται η ταυτότητα του ιδιοκτήτη της. Είναι σημαντικό για κάθε πληροφοριακό σύστημα να επιτυγχάνει επαρκές επίπεδο ασφάλειας για τα δεδομένα του και επίσης να προστατεύει την ιδιωτικότητα των χρηστών του. Για αυτό το λόγο είναι απαραίτητη η εφαρμογή κατάλληλων αντιμέτρων. Λαμβάνοντας υπόψη ότι οι συμβατικοί μηχανισμοί ασφαλείας, όπως η κρυπτογράφηση, δεν μπορούν να διασφαλίσουν την προστασία της ιδιωτικότητας (για παράδειγμα, η κρυπτογράφηση μπορεί να προστατεύσει μόνο την εμπιστευτικότητα του μηνύματος), έχουν αναπτυχθεί νέες πρόσθετες Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies - PETs).

Η ιδιωτικότητα και η ασφάλεια θα πρέπει να θεωρούνται ως κύρια ζητήματα κατά τη διαδικασία σχεδιασμού ενός πληροφοριακού συστήματος και θα πρέπει να λαμβάνονται υπόψη από την αρχή [28] [41] [42] [43]. Αυτό μπορεί να γίνει εντοπίζοντας, μέσω των κατάλληλων μεθοδολογιών, αρκετά νωρίς στο σχεδιασμό, τις απαιτήσεις ασφάλειας και ιδιωτικότητας που πρέπει να ικανοποιούνται.

Ωστόσο, μέχρι στιγμής, δεν υπάρχει καμία μεθοδολογία που να μπορεί να καλύψει τον προσδιορισμό των απαιτήσεων ασφάλειας και ιδιωτικότητας και ταυτόχρονα να λαμβάνει υπόψη τις βασικές αρχές ιδιωτικότητας. Ως συνέπεια οι σχεδιαστές ενός πληροφοριακού συστήματος συνήθως ακολουθούν μια ad hoc προσέγγιση για τον προσδιορισμό των απαιτήσεων ασφάλειας / ιδιωτικότητας, αποτυγχάνοντας έτσι να προστατεύσουν τους χρήστες με αποτελεσματικό τρόπο. Η κύρια ιδέα πίσω από την προτεινόμενη μεθοδολογία είναι η ενσωμάτωση των βασικών βημάτων των καθιερωμένων μεθοδολογιών ανάλυσης επικινδυνότητας με εκείνα των μεθοδολογιών που χρησιμοποιούνται για τον προσδιορισμό των απαιτήσεων ιδιωτικότητας, λαμβάνοντας

ταυτόχρονα υπόψη τις πιο γνωστές αρχές ιδιωτικότητας. Η προτεινόμενη μεθοδολογία στοχεύει να βοηθήσει τους σχεδιαστές πληροφοριακών συστημάτων να καταλήξουν σε μια πλήρη και ακριβή λίστα όλων των απαιτήσεων ασφάλειας και ιδιωτικότητας που πρέπει να πληροί το σύστημά τους.

Η υποενότητα που ακολουθεί παρουσιάζει/προτείνει μια ενιαία μεθοδολογία ασφάλειας και ιδιωτικότητας που μπορεί να ακολουθήσει ένας οργανισμός για να διασφαλίσει την ασφάλεια του πληροφοριακού συστήματός του και της προστασίας της ιδιωτικότητας των χρηστών.

3.2 Μεθοδολογία ασφάλειας και ιδιωτικότητας

Η μεθοδολογία που παρουσιάζεται στο παρακάτω σχήμα (Σχήμα 2), συνδυάζει τα αποτελέσματα (απαιτήσεις ασφαλείας) μιας μελέτης ανάλυσης επικινδυνότητας με τα αποτελέσματα (απαιτήσεις ιδιωτικότητας) μιας μεθοδολογίας εξαγωγής απαιτήσεων ιδιωτικότητας και τις αρχές ιδιωτικότητας του ΟΟΣΑ. Το σημαντικό είναι ότι η ενοποίηση αυτών των ετερογενών προσεγγίσεων πραγματοποιείται σε ανεξάρτητα και καλά καθορισμένα διακριτά βήματα που ακολουθούν μια συγκεκριμένη σειρά.

Πιο συγκεκριμένα, όταν ένας οργανισμός θέλει να εφαρμόσει την προτεινόμενη μεθοδολογία προκειμένου να προστατεύσει τα προσωπικά δεδομένα και την ιδιωτικότητα των χρηστών, θα πρέπει:

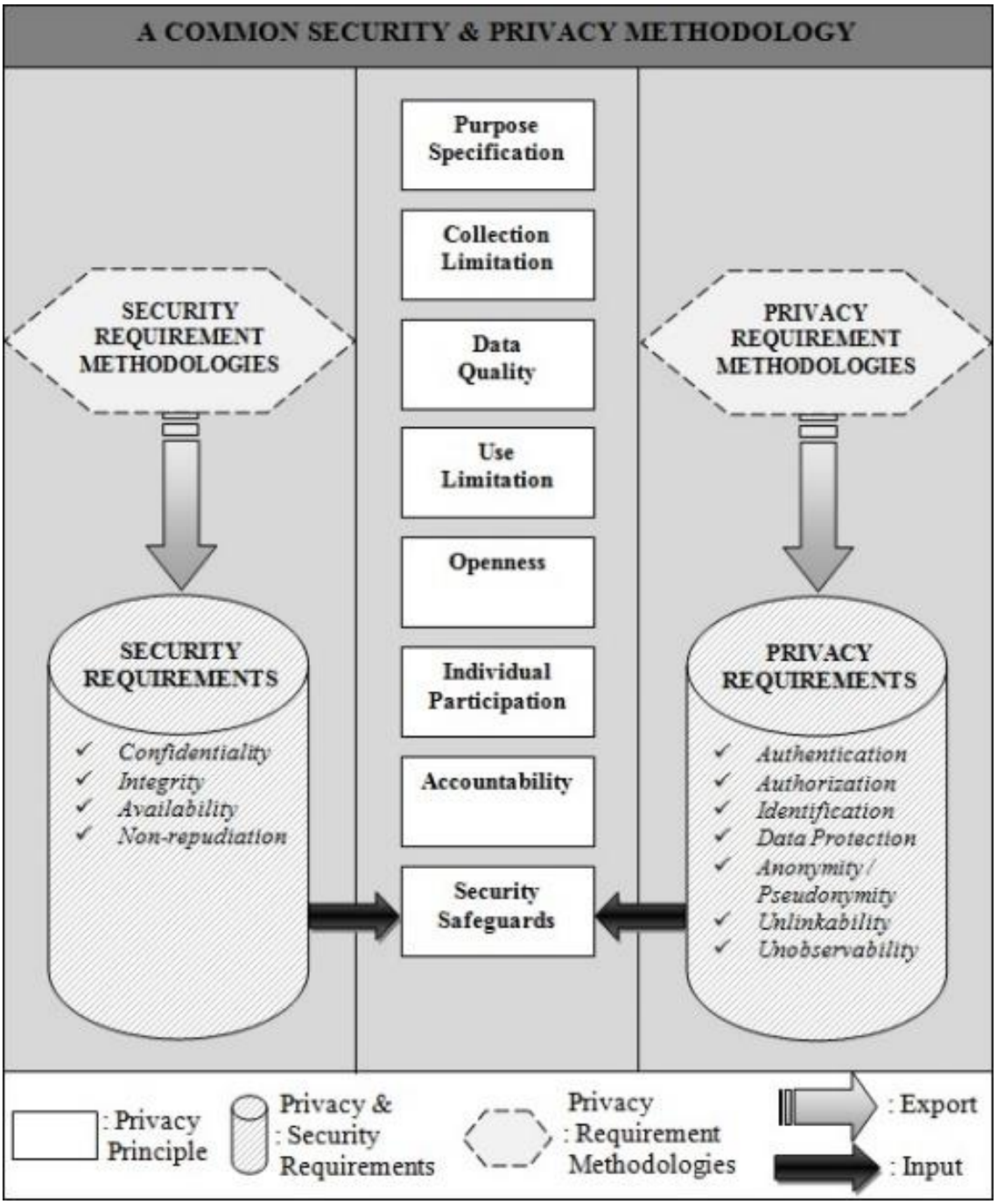
- **Να ικανοποιήσει πρώτα όλες τις αρχές ιδιωτικότητας** (μεσαία στήλη στο Σχήμα 2) σύμφωνα με διάφορους δημόσιους και ιδιωτικούς φορείς [5] [17] [36] [37] [38]. Κάθε αρχή ιδιωτικότητας θα πρέπει να εφαρμόζεται με τη σειρά που εμφανίζεται στο παρακάτω σχήμα.

- **Να προσδιορίσει τις απαιτήσεις ασφαλείας** (αριστερή στήλη στο Σχήμα 2) μέσω κάποιας μεθοδολογίας ανάλυσης επικινδυνότητας.

- **Να προσδιορίσει τις απαιτήσεις ιδιωτικότητας** (δεξιά στήλη στο Σχήμα 2) μέσω κάποιας κατάλληλης μεθοδολογίας.

- Σε αυτό το στάδιο, ο οργανισμός θα πρέπει να **επιλέξει τα κατάλληλα μέτρα ασφάλειας** για την ικανοποίηση όλων των απαιτήσεων ασφάλειας και

ιδιωτικότητας και, κατά συνέπεια, την προστασία των προσωπικών δεδομένων των χρηστών από πιθανά περιστατικά παραβίασης της ασφάλειας και της ιδιωτικότητας. Αυτά τα μέτρα ασφάλειας θα εφαρμοστούν κατά την υλοποίηση της «Αρχής Εφαρμογής Μέτρων Προστασίας Ασφάλειας».



Σχήμα 2: Μια κοινή μεθοδολογία ασφάλειας και ιδιωτικότητας

3.3 Συμπεράσματα

Με γνώμονα τις πιο ευρέως γνωστές απαιτήσεις ασφάλειας και ιδιωτικότητας, καθώς και τις αρχές ιδιωτικότητας, που έχουν αναπτυχθεί είτε από χώρες είτε από δημόσιους/ιδιωτικούς φορείς, η προτεινόμενη μεθοδολογία είναι μια κοινή μεθοδολογία ασφάλειας και ιδιωτικότητας που μπορούν να ακολουθήσουν οι οργανισμοί για την ασφάλεια των συστημάτων τους και τη προστασία της ιδιωτικότητας των χρηστών τους. Η εφαρμογή της προτεινόμενης μεθοδολογίας ασφάλειας και ιδιωτικότητας σε πραγματικό περιβάλλον, αναδεικνύει τη σημασία της τόσο για τους οργανισμούς όσο και για τους χρήστες.

4 Κεφάλαιο 4: Δομημένη μεθοδολογία ελέγχου της ιδιωτικότητας

4.1 Εισαγωγή

Η ερευνητική επισκόπηση της υποενότητας 2.2 αποκάλυψε ότι, αν και υπάρχει εκτεταμένη βιβλιογραφία σχετικά με τις διαφορετικές αρχές ιδιωτικότητας και τους ορισμούς τους [36][35][53][46], μέχρι στιγμής δεν έχει γίνει καμία προσπάθεια να δημιουργηθεί ένας οδικός χάρτης για το πώς θα πρέπει να εφαρμοστούν οι υφιστάμενες αρχές ιδιωτικότητας (δηλαδή είναι ορισμένες αρχές πιο σημαντικές από άλλες; υπάρχει συγκεκριμένη σειρά που κάποιος πρέπει να προσπαθήσει να τις ικανοποιήσει και σε αυτή την περίπτωση ποια είναι αυτή η σειρά; κτλ.) για τη διευκόλυνση του σχεδιασμού συστημάτων που «θέλουν» να είναι συνεπή με τις αρχές αυτές.

Η απουσία μιας ευρέως αποδεκτής δομημένης αναπαράστασης των αρχών ιδιωτικότητας καθιστά την υιοθέτηση/ικανοποίησή τους δύσκολη και σε ορισμένες περιπτώσεις ασυνεπή. Λαμβάνοντας υπόψη ότι η προστασία της ιδιωτικότητας από μόνη της δεν είναι εύκολη υπόθεση για έναν οργανισμό, οι «διασκορπισμένες» [17] αρχές ιδιωτικότητας επιβάλλουν σημαντική πρόσθετη πολυπλοκότητα. Κατά συνέπεια, πολύ συχνά οι οργανισμοί αποτυγχάνουν να εφαρμόσουν αποτελεσματικά τις αρχές ιδιωτικότητας και επομένως να προστατεύσουν τα προσωπικά δεδομένα των χρηστών. Σαν αποτέλεσμα, η ανάγκη δημιουργίας ενός δομημένου οδικού χάρτη για την εκπλήρωση των αρχών ιδιωτικότητας είναι απολύτως απαραίτητη.

Ο δομημένος οδικός χάρτης, που αναφέρθηκε παραπάνω, θα μπορούσε επίσης να χρησιμοποιηθεί ως βάση μιας μεθοδολογίας ελέγχου για τη χρήση των PETs από έναν οργανισμό. Η ανάγκη για μια κοινή μεθοδολογία ελέγχου της ιδιωτικότητας δεν είναι κάτι καινούριο, αφού το 2004 μια ομάδα επιστημόνων [16] τόνισε την απουσία της. Ωστόσο, μέχρι σήμερα δεν έχει γίνει καμία σημαντική προσπάθεια προς αυτή την κατεύθυνση.

Η απουσία μιας μεθοδολογίας ελέγχου ιδιωτικότητας αποτελεί μία από τις κυριότερες ανησυχίες των χρηστών και συνεπώς προκαλεί αβεβαιότητα για το εάν οι πάροχοι υπηρεσιών προστατεύουν επαρκώς τα προσωπικά δεδομένα των χρηστών τους ή όχι. Επιπλέον, η απουσία μιας μεθοδολογίας ελέγχου του επιπέδου προστασίας της ιδιωτικότητας επηρεάζει τους παρόχους υπηρεσιών, καθώς δεν μπορούν να εξασφαλίσουν την πληρότητα και την αποτελεσματικότητα των μέτρων προστασίας ιδιωτικότητας που

έχουν υιοθετήσει. Κατά συνέπεια, τα προσωπικά δεδομένα των χρηστών εκτίθενται σε πολλούς διαφορετικούς κινδύνους. Η ύπαρξη μιας μεθοδολογίας ελέγχου ιδιωτικότητας, βοηθά τους χρήστες να εμπιστεύονται περισσότερο τους παρόχους υπηρεσιών και κατά συνέπεια να αξιοποιούν περισσότερο τις προσφερόμενες υπηρεσίες τους.

Μολονότι έχουν γίνει ορισμένα βήματα προς ένα κοινό πλαίσιο προστασίας της ιδιωτικότητας, μόνο λίγες προσπάθειες έχουν γίνει προς τη δημιουργία μιας δομημένης διαδικασίας ελέγχου της ιδιωτικότητας. Μια τέτοια διαδικασία προτείνεται στις ακόλουθες ενότητες. Στα πλαίσια αυτής της διαδικασίας, όλες οι αρχές και απαιτήσεις ιδιωτικότητας έχουν συγκεντρωθεί και ταξινομηθεί προκειμένου να προσδιοριστεί: α) ο τρόπος με τον οποίο μπορεί να ικανοποιηθεί κάθε απαίτηση ιδιωτικότητας και β) η προτεραιότητα – σειρά με την οποία θα πρέπει να προσδιορίζεται κάθε απαίτηση ιδιωτικότητας.

4.2 Μεθοδολογία ελέγχου ιδιωτικότητας

4.2.1 Οπτική από την πλευρά του οργανισμού

Για τον καθορισμό της μεθοδολογίας ελέγχου ιδιωτικότητας, οι υπάρχουσες αρχές ιδιωτικότητας ταξινομούνται σε τέσσερα επίπεδα βασισμένα στην σημαντικότητά τους και τη σειρά που θα πρέπει να αξιολογούνται βάσει της διαδικασίας ελέγχου. Κάθε επίπεδο σχετίζεται με ένα «Βήμα» της διαδικασίας ελέγχου. Όλα τα βήματα θα πρέπει να ακολουθούνται με αυστηρή σειρά καθώς η αποτυχία ελέγχου οποιουδήποτε βήματος σημαίνει αυτόματα ότι ούτε τα υπόλοιπα βήματα μπορούν να ελεγχθούν, καθώς όλα τα βήματα είναι αλληλένδετα/αλληλεξαρτώμενα μεταξύ τους.

Η προτεινόμενη μεθοδολογία αποτελείται από τέσσερα βήματα ελέγχου. Κάθε ελεγχόμενο βήμα περιλαμβάνει μία ή περισσότερες αρχές ιδιωτικότητας και απεικονίζεται ιεραρχικά. Τα αποτελέσματα ελέγχου κάθε αρχής ιδιωτικότητας μπορούν να χρησιμοποιηθούν ως είσοδος για τον έλεγχο κάποιας άλλης αρχής ιδιωτικότητας στο ίδιο ή σε επόμενο βήμα. Τα συμπαγή βέλη μεταξύ διαφορετικών βημάτων συμβολίζουν την είσοδο από μια αρχή ιδιωτικότητας σε μια άλλη στο επόμενο βήμα ελέγχου. Ταυτόχρονα, έχει εντοπιστεί ότι υπάρχει ανάγκη ορισμένες αρχές ιδιωτικότητας να τηρούνται καθ' όλη τη διάρκεια της διαδικασίας ελέγχου.

ΒΗΜΑ 1:

- **Αρχή Ιδιωτικότητας**: Αρχή Καθορισμού του Σκοπού (**PP-S1-1**)
- **Προαπαιτούμενη Αρχή Ιδιωτικότητας**: -
- **Περιγραφή**: Το πρώτο βήμα ελέγχου περιλαμβάνει την «Αρχή Καθορισμού του Σκοπού» (Σχήμα 3). Όταν ένας οργανισμός θέλει να προστατεύσει την ιδιωτικότητα των χρηστών, το πρώτο βήμα είναι να ορίσει με σαφήνεια και να εξηγήσει το σκοπό της συλλογής και χρήσης των προσωπικών δεδομένων. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 2). Επομένως, όταν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλα τα έγγραφα, τα οποία καθορίζουν το σκοπό και παρουσιάζονται στον παρακάτω πίνακα.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Καθορισμός του Σκοπού	Το έγγραφο που αναφέρει το γενικό σκοπό του οργανισμού.				
	Το έγγραφο που αναφέρει τον βασικό και πιο εξειδικευμένο σκοπό συλλογής των προσωπικών δεδομένων είτε πριν είτε κατά τη στιγμή της συλλογής τους.				
	Τα έγγραφα, τα φυλλάδια, τα βίντεο, τις διαφημίσεις, τα πρακτικά συνεδρίων, τις ειδοποιήσεις μέσω εφαρμογών και οτιδήποτε άλλο χρησιμοποιεί ο οργανισμός για να ενημερώσει τους χρήστες σχετικά με το σκοπό συλλογής των δεδομένων τους.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής καθορισμού του σκοπού και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 2: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Καθορισμού του Σκοπού"

ΒΗΜΑ 2:

- **Αρχή Ιδιωτικότητας**: Αρχή Περιορισμού της Συλλογής (**PP-S2-1**)
- **Προαπαιτούμενη Αρχή Ιδιωτικότητας**: (PP-S1-1)

- **Περιγραφή**: Η πρώτη αρχή ιδιωτικότητας που ανήκει στο δεύτερο βήμα ελέγχου είναι η «Αρχή Περιορισμού της Συλλογής» (Σχήμα 3). Όταν ένας οργανισμός θέλει να προστατεύσει την ιδιωτικότητα των χρηστών, θα πρέπει να μειώσει τη συλλογή και χρήση των προσωπικών δεδομένων. Έχοντας ορίσει το σκοπό της συλλογής και χρήσης στο προηγούμενο βήμα (*ΒΗΜΑ 1*), ο οργανισμός είναι υποχρεωμένος να συλλέγει και να χρησιμοποιεί μόνο εκείνα τα δεδομένα που είναι απαραίτητα για τις προσφερόμενες υπηρεσίες του. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 3). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλα τα έγγραφα και τα μέσα περιορισμού συλλογής δεδομένων που χρησιμοποιούνται από τον οργανισμό. Εάν η «Αρχή Καθορισμού του Σκοπού» δεν έχει ελεγχθεί, ο έλεγχος της «Αρχής Περιορισμού της Συλλογής» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	**ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ**	**ΑΞΙΟΛΟΓΗΣΗ**			**ΕΝΕΡΓΕΙΕΣ**
		Ι	**ΔΙ**	**ΙΜ**	
Περιορισμός της Συλλογής	Το έγγραφο που αναφέρει το σκοπό συλλογής των δεδομένων.				
	Τα έγγραφα, τα φυλλάδια, τα βίντεο, τις διαφημίσεις, τα πρακτικά συνεδρίων, τις ειδοποιήσεις μέσω εφαρμογών και οτιδήποτε άλλο χρησιμοποιεί ο οργανισμός για να ενημερώσει τους χρήστες σχετικά με το σκοπό συλλογής των δεδομένων τους.				
	Το έγγραφο που αναφέρει τις πολιτικές και τις διαδικασίες που χρησιμοποιούνται από τον οργανισμό προκειμένου να χειριστεί και να συλλέξει πληροφορίες.				
	Το έγγραφο που αναφέρει/περιέχει τη συγκατάθεση του χρήστη.				
	Το έγγραφο με τις πολιτικές και τις διαδικασίες του οργανισμού, σχετικά με την καταστροφή προσωπικών δεδομένων, όταν αυτά δεν είναι πλέον χρήσιμα.				
	Τα κατάλληλα τεχνικά μέσα που χρησιμοποιούνται από τα συστήματα του οργανισμού για ελαχιστοποίηση των προσωπικών δεδομένων.				
	Τα νόμιμα μέσα που χρησιμοποιεί ένας οργανισμός προκειμένου να συλλέξει δεδομένα. Η φυσική παρουσία του ελεγκτή κατά τη λειτουργία συστημάτων ή υποσυστημάτων κρίνεται				

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
	απαραίτητη. Τα μέσα μπορεί είτε να είναι τεχνικά είτε όχι.				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής περιορισμού της συλλογής και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 3: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Περιορισμού της Συλλογής"

- **Αρχή Ιδιωτικότητας**: Αρχή Διατήρησης Ποιότητας των Δεδομένων (**PP-S2-2**)
- **Προαπαιτούμενη Αρχή Ιδιωτικότητας**: (PP-S1-1)
- **Περιγραφή**: Η τελευταία αρχή ιδιωτικότητας που ανήκει στο δεύτερο βήμα ελέγχου είναι η «Αρχή Διατήρησης Ποιότητας των Δεδομένων» (Σχήμα 3). Ο οργανισμός είναι υποχρεωμένος να διατηρήσει τα προσωπικά δεδομένα των χρηστών του ακριβή, πλήρη και ενημερωμένα στο βαθμό που αυτό είναι απαραίτητο για το σκοπό συλλογής και χρήσης των δεδομένων. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 4). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλα τα έγγραφα, τα μέσα και τις πολιτικές, τα οποία ο οργανισμός χρησιμοποιεί προκειμένου να διατηρήσει την ποιότητα των προσωπικών δεδομένων. Εάν η «Αρχή Καθορισμού του Σκοπού» δεν έχει ελεγχθεί, ο έλεγχος της «Αρχής Διατήρησης Ποιότητας των Δεδομένων» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Διατήρηση Ποιότητας των Δεδομένων	Το έγγραφο που αναφέρει το σκοπό χρήσης των δεδομένων.				
	Τα κατάλληλα τεχνικά μέσα που χρησιμοποιούνται από τα συστήματα του οργανισμού για να ελέγξουν εάν τα προσωπικά δεδομένα διατηρούνται ακριβή,				

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
	πλήρη και ενημερωμένα.				
	Το έγγραφο με τις πολιτικές και τις διαδικασίες του οργανισμού, σχετικά με την επαναφορά/αποκατάσταση και ενημέρωση των προσωπικών δεδομένων.				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής διατήρησης ποιότητας των δεδομένων και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 4: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Διατήρησης Ποιότητας των Δεδομένων"

ΒΗΜΑ 3:

- **Αρχή Ιδιωτικότητας**: Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης (**PP-S3-1**)
- **Προαπαιτούμενη Αρχή Ιδιωτικότητας**: (PP-S1-1), (PP-S2-1)
- **Περιγραφή**: Το τρίτο βήμα ελέγχου περιλαμβάνει την «Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης» (Σχήμα 3). Ο οργανισμός πρέπει να περιορίσει τη χρήση, τη διατήρηση και την αποκάλυψη προσωπικών πληροφοριών, έτσι ώστε ο χρήστης να έχει το δικαίωμα να παρέμβει όπου είναι απαραίτητο (εκτός εάν αυτό απαγορεύεται από το νόμο). Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 5). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλα τα έγγραφα και τις πολιτικές, τα οποία ο οργανισμός χρησιμοποιεί προκειμένου να περιορίσει τη χρήση, τη διατήρηση και την αποκάλυψη προσωπικών δεδομένων. Εάν η «Αρχή Καθορισμού του Σκοπού» και η «Αρχή Περιορισμού της Συλλογής» δεν έχει ελεγχθεί, ο έλεγχος της «Αρχής Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Περιορισμός της Χρήσης, Διατήρησης και Αποκάλυψης	Το έγγραφο που αναφέρει το σκοπό χρήσης των προσωπικών δεδομένων.				
	Το έγγραφο με τις πολιτικές και τις διαδικασίες του οργανισμού, σχετικά με τον περιορισμό της χρήσης, της διατήρησης και της αποκάλυψης των προσωπικών δεδομένων του χρήστη.				
	Το έγγραφο που αναφέρει τη συγκατάθεση του χρήστη.				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής περιορισμού χρήσης, διατήρησης και αποκάλυψης των δεδομένων και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 5: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης"

ΒΗΜΑ 4:

- **Αρχή Ιδιωτικότητας**: Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας (**PP-S4-1**)
- **Προαπαιτούμενη Αρχή Ιδιωτικότητας**: (PP-S3-1)
- **Περιγραφή**: Το τέταρτο βήμα ελέγχου περιλαμβάνει την «Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας» (Σχήμα 3). Για την προστασία της ιδιωτικότητας των χρηστών, ο οργανισμός πρέπει να εφαρμόσει μέτρα προστασίας ασφάλειας για την αντιμετώπιση της απώλειας ή μη εξουσιοδοτημένης πρόσβασης, καταστροφής, χρήσης, τροποποίησης ή αποκάλυψης των δεδομένων. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 6). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλα τα έγγραφα και τις πολιτικές, τα οποία ο οργανισμός χρησιμοποιεί προκειμένου να εφαρμόσει μέτρα προστασίας ασφάλειας. Εάν η «Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης»

δεν έχει ελεγχθεί, ο έλεγχος της «Αρχής Εφαρμογής Μέτρων Προστασίας Ασφάλειας» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Εφαρμογή Μέτρων Προστασίας Ασφάλειας	Το έγγραφο που αναφέρει τα φυσικά, διοικητικά και τεχνικά μέτρα που εφαρμόζει ο οργανισμός. Για όλα αυτά τα μέτρα, ο ελεγκτής ιδιωτικότητας θα πρέπει να ελέγξει τις εγκαταστάσεις, τους εργαζόμενους και τα τεχνικά μέσα που χρησιμοποιεί ο οργανισμός.				
	Το πρόγραμμα εκπαίδευσης των εργαζομένων.				
	Το έγγραφο με τις πολιτικές και τις διαδικασίες του οργανισμού, σχετικά με την εφαρμογή των μέτρων ασφάλειας για την προστασία των προσωπικών δεδομένων του χρήστη.				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής εφαρμογής μέτρων προστασίας ασφάλειας και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 6: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Εφαρμογής Μέτρων Προστασίας Ασφάλειας"

<u>ΚΑΘΟΛΙΚΕΣ ΑΡΧΕΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ</u>

Οι αρχές ιδιωτικότητας που ακολουθούν δεν έχουν ενταχθεί σε κανένα από τα παραπάνω τέσσερα βήματα ελέγχου αφού θεωρήθηκε ότι ισχύουν καθ' όλη τη μεθοδολογία ελέγχου ιδιωτικότητας (Σχήμα 3). Ως αποτέλεσμα, έχουν χαρακτηριστεί ως «Καθολικές Αρχές Ιδιωτικότητας», που εφαρμόζονται για όλα τα βήματα ελέγχου και θα πρέπει να ελέγχονται αυστηρά καθ' όλη τη διαδικασία ελέγχου. Πρακτικά, η χρηστικότητα αυτών των καθολικών αρχών είναι ότι προσθέτουν ένα επιπλέον βήμα σε καθένα από τα παραπάνω βήματα της μεθοδολογίας (δηλαδή για την «Αρχή Περιορισμού της Συλλογής» του ΒΗΜΑΤΟΣ 2 (PP-S2-1) παράλληλα με τους ελέγχους που αναφέρονται στον Πίνακας 3, ο ελεγκτής ιδιωτικότητας θα πρέπει, επίσης, να ελέγξει και όσα αναφέρονται στους Πίνακες (Πίνακας 7, Πίνακας 8, Πίνακας 9) που προκύπτουν από τις καθολικές αρχές παρακάτω).

- **Αρχή Ιδιωτικότητας**: Αρχή Διαφάνειας (**PP-G-1**)

- **Περιγραφή**: Η πρώτη καθολική αρχή είναι η «Αρχή Διαφάνειας» (Σχήμα 3). Όταν ένας οργανισμός επιθυμεί να υποστηρίξει τη διαφάνεια, πρέπει να θέτει στη διάθεση των χρηστών όλες τις πολιτικές, τις πρακτικές και τις διαδικασίες σχετικά με τα προσωπικά δεδομένα. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 7). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλα τα έγγραφα και τις πολιτικές, τα οποία ο οργανισμός χρησιμοποιεί προκειμένου να διατηρήσει τις υπηρεσίες του διαφανείς και να ενημερώσει τους χρήστες του. Εάν οι προαπαιτούμενες αρχές ιδιωτικότητας δεν ικανοποιούνται, ο έλεγχος της «Αρχής Διαφάνειας» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Διαφάνεια	Το έγγραφο που αναφέρει το σκοπό συλλογής των προσωπικών δεδομένων.				
	Το έγγραφο που αναφέρει σαφώς τις πολιτικές, τις πρακτικές και τις διαδικασίες για τη διαχείριση των προσωπικών πληροφοριών.				
	Τα τεχνικά ή άλλα μέσα που χρησιμοποιεί ο οργανισμός για να ενημερώσει τους χρήστες σχετικά με τη διαχείριση των προσωπικών δεδομένων τους. Ο ελεγκτής ιδιωτικότητας θα πρέπει να ελέγχει τα μέσα, στην πράξη.				
	Το έγγραφο που αναφέρει τον τρόπο με τον οποίο δημοσιοποιούνται οι πολιτικές, οι πρακτικές και οι διαδικασίες για τη διαχείριση των προσωπικών πληροφοριών. Ο ελεγκτής ιδιωτικότητας θα πρέπει να ελέγχει τους τρόπους δημοσιοποίησης, στην πράξη.				
	Το έγγραφο με τα βήματα που ενημερώνουν έναν χρήστη για όλες τις πολιτικές, τις πρακτικές και τις διαδικασίες για τη διαχείριση των προσωπικών δεδομένων (κατόπιν αιτήματος του χρήστη).				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής διαφάνειας και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 7: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Διαφάνειας"

- **Αρχή Ιδιωτικότητας**: Αρχή Ατομικής Συμμετοχής (**PP-G-2**)

- **Περιγραφή**: Η δεύτερη καθολική αρχή είναι η «Αρχή Ατομικής Συμμετοχής» (Σχήμα 3). Όταν ένας οργανισμός επιθυμεί να υποστηρίξει την ατομική συμμετοχή του χρήστη, θα πρέπει να επιτρέπει στους χρήστες να έχουν πρόσβαση και να τροποποιούν τα προσωπικά δεδομένα τους. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 8). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλες τις πολιτικές και τις διαδικασίες, τα οποία ο οργανισμός χρησιμοποιεί προκειμένου να βοηθήσει τους χρήστες να έχουν πρόσβαση στα προσωπικά δεδομένα τους. Εάν οι προαπαιτούμενες αρχές ιδιωτικότητας δεν ικανοποιούνται, ο έλεγχος της «Αρχής Ατομικής Συμμετοχής» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Ατομική Συμμετοχή	Το έγγραφο που αναφέρει την πολιτική που ενημερώνει τους χρήστες για τα προσωπικά δεδομένα που συλλέγει ο οργανισμός.				
	Το έγγραφο που αναφέρει τη συγκατάθεση του χρήστη.				
	Την πολιτική που αναφέρει το χρονικό διάστημα κατά το οποίο ο οργανισμός θα πρέπει να ανταποκρίνεται στα αιτήματα των χρηστών σχετικά με την πρόσβαση στις προσωπικές πληροφορίες που τους αφορούν.				
	Την πολιτική που αναφέρει τον τρόπο με τον οποίο τρίτες οντότητες διαχειρίζονται τα προσωπικά δεδομένα των χρηστών καθώς και τον τρόπο που οι χρήστες μπορούν να έχουν πρόσβαση σε αυτά.				
	Την πολιτική που αναφέρει όλες τις εξαιρέσεις, κατά τις οποίες απαγορεύεται η πρόσβαση στα προσωπικά δεδομένα των χρηστών.				
	Τις διαδικασίες παραπόνων.				
	Τις διαδικασίες ταυτοποίησης.				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής ατομικής συμμετοχής και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				

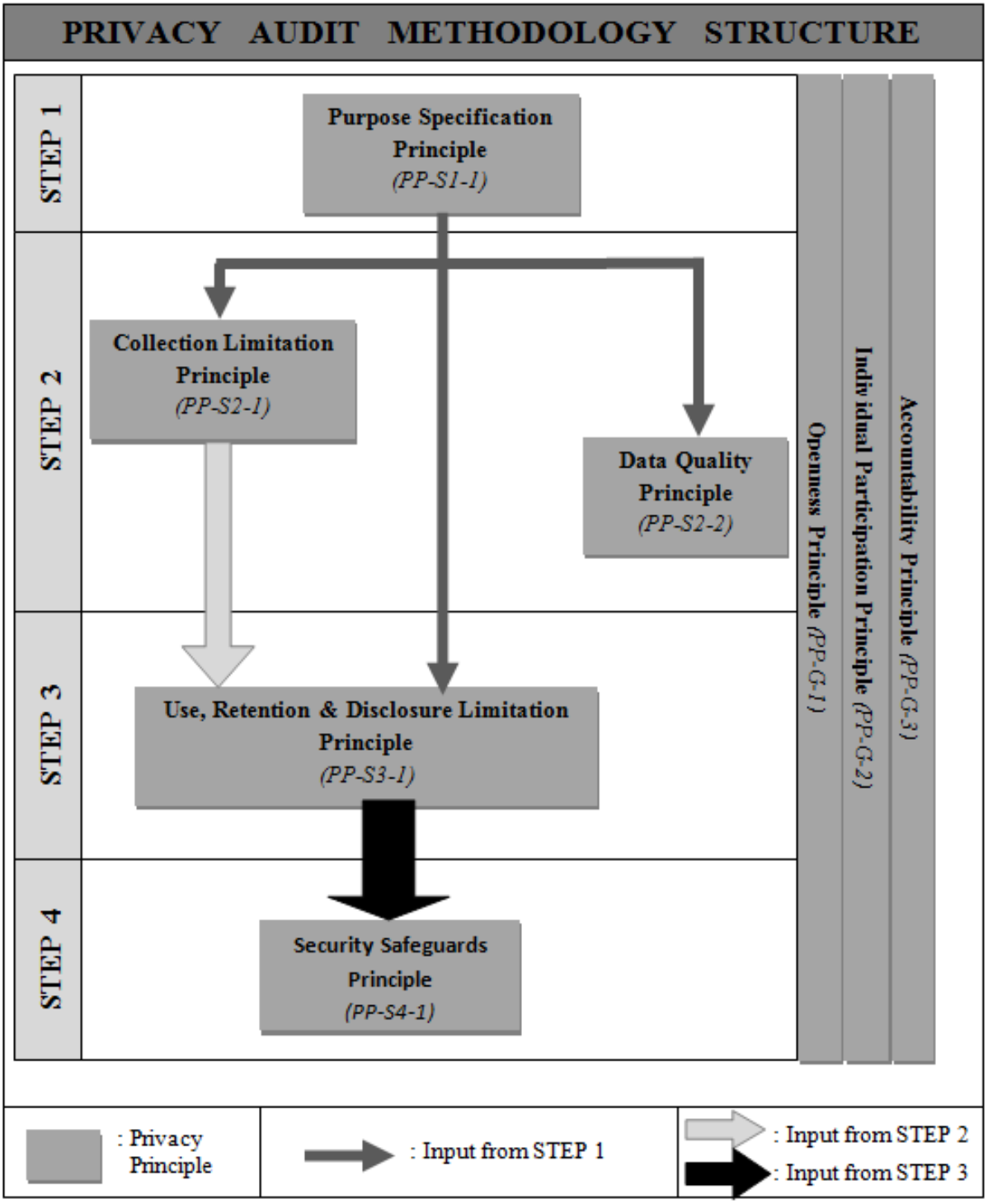
ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 8: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Ατομικής Συμμετοχής"

- **Αρχή Ιδιωτικότητας**: Αρχή Λογοδοσίας (**PP-G-3**)
- **Περιγραφή**: Η τελευταία καθολική αρχή είναι η «Αρχή Λογοδοσίας» (Σχήμα 3). Όταν ένας οργανισμός επιθυμεί να είναι αξιόπιστος, θα πρέπει να είναι υπεύθυνος ώστε να συμμορφώνεται με μέτρα, τα οποία ανταποκρίνονται και υλοποιούν τις αρχές ιδιωτικότητας που αναφέρθηκαν παραπάνω. Για να γίνει αυτό, μια σειρά από έγγραφα απαιτούνται να ελεγχθούν (Πίνακας 9). Συνεπώς, εάν ένας ελεγκτής ιδιωτικότητας θέλει να ελέγξει εάν ένας οργανισμός εφαρμόζει τη συγκεκριμένη αρχή ιδιωτικότητας, θα πρέπει να ζητήσει όλες τις πολιτικές και τις διαδικασίες, τα οποία ο οργανισμός χρησιμοποιεί προκειμένου να είναι αξιόπιστος ως προς τους χρήστες. Εάν οι προαπαιτούμενες αρχές ιδιωτικότητας δεν ικανοποιούνται, ο έλεγχος της «Αρχής Λογοδοσίας» δεν μπορεί να ολοκληρωθεί.

ΑΡΧΗ ΙΔΙΩΤΙΚΟΤΗΤΑΣ	ΑΠΟΔΕΙΚΤΙΚΟ ΣΤΟΙΧΕΙΟ	ΑΞΙΟΛΟΓΗΣΗ			ΕΝΕΡΓΕΙΕΣ
		Ι	ΔΙ	ΙΜ	
Λογοδοσία	Ο Υπεύθυνος Προστασίας Δεδομένων και οι εργαζόμενοι που είναι υπεύθυνοι για τη διαχείριση των προσωπικών δεδομένων των χρηστών.				
	Το πρόγραμμα εκπαίδευσης του Υπεύθυνου Προστασίας Δεδομένων και των εργαζομένων.				
	Την πολιτική σχετικά με τις ευθύνες του Υπεύθυνου Προστασίας Δεδομένων.				
	Τις συμπληρωματικές πολιτικές και τις διαδικασίες που έχει δημιουργήσει ο Υπεύθυνος Προστασίας Δεδομένων.				
	Την πολιτική ιδιωτικότητας του οργανισμού.				
	Την ύπαρξη εικονιδίων ιδιωτικότητας που ενημερώνουν τον χρήστη σχετικά με την τήρηση της αρχής λογοδοσίας και υποχρεώνουν τον οργανισμό να την ακολουθήσει.				
Ι: Ικανοποιούνται, ΔΙ: Δεν Ικανοποιούνται, ΙΜ: Ικανοποιούνται Μερικώς					

Πίνακας 9: Λίστα ελέγχου εγγράφων για τήρηση της "Αρχής Λογοδοσίας"



Σχήμα 3: Δομή Μεθοδολογίας Ελέγχου Ιδιωτικότητας

4.2.2 Οπτική από την πλευρά του χρήστη

Η προστασία των προσωπικών δεδομένων του χρήστη θα πρέπει πάντα να έχει κυρίαρχο ενδιαφέρον για τον οργανισμό. Ο χρήστης θα πρέπει, πάντα, να έχει το δικαίωμα να ενημερώνεται για τους μηχανισμούς προστασίας που υπάρχουν και υλοποιούνται, καθώς και για τα προσωπικά δεδομένα και τα έγγραφα που χρησιμοποιεί ο οργανισμός.

Πιο συγκεκριμένα, για να εμπιστευτεί ο χρήστης τον οργανισμό και τις προσφερόμενες υπηρεσίες, είναι απαραίτητο να του δοθεί το δικαίωμα να λάβει οποιαδήποτε πληροφορία χρειάζεται σχετικά με τη συλλογή, επεξεργασία και αποθήκευση των προσωπικών του δεδομένων, καθώς και τον τρόπο με τον οποίο ο οργανισμός συμμορφώνεται με τις βασικές αρχές ιδιωτικότητας. Ενδεικτικά, από την πλευρά του χρήστη οι ακόλουθες περιπτώσεις θα πρέπει να υποστηρίζονται από τον οργανισμό:

- Η πρώτη περίπτωση είναι όταν ο χρήστης επιθυμεί να ενημερωθεί για τη διαδικασία ελέγχου που ακολουθείται από τον οργανισμό. Σε αυτήν την περίπτωση, ο οργανισμός θα πρέπει να επιτρέψει στον χρήστη να λάβει πληροφορίες για όλα τα έγγραφα, τα μέσα και τις πολιτικές ή πρακτικές που χρησιμοποιούνται για τη συλλογή και επεξεργασία των προσωπικών δεδομένων του. Ο χρήστης θα πρέπει να έχει πρόσβαση σε όλα ή σε επιλεγμένα έγγραφα με τις πληροφορίες που προκύπτουν από τις αρχές ιδιωτικότητας. Αυτά τα έγγραφα θα πρέπει να προσφέρονται με τρόπο φιλικό προς τον χρήστη, έτσι ώστε οι χρήστες να έχουν εύκολη πρόσβαση σε αυτά οποιαδήποτε στιγμή.

- Η δεύτερη περίπτωση είναι όταν ο χρήστης επιθυμεί να επικοινωνήσει με τον οργανισμό προκειμένου να λάβει περισσότερες πληροφορίες. Ο οργανισμός θα πρέπει να παρέχει έναν κατάλληλο φιλικό προς τον χρήστη τρόπο ώστε να λαμβάνει αιτήματα χρηστών και να τους παρέχει τις απαραίτητες διευκρινίσεις. Η ιδέα πίσω από αυτή την αλληλεπίδραση, μεταξύ του οργανισμού και του χρήστη, είναι η υποστήριξη της απαραίτητης διαφάνειας που χρειάζεται ο χρήστης προκειμένου να αποφασίσει εάν θα συνεχίσει να χρησιμοποιεί τις υπηρεσίες που προσφέρει ο οργανισμός ή όχι.

- Η τρίτη περίπτωση είναι όταν ο χρήστης δεν ενδιαφέρεται για τις λεπτομέρειες της διαδικασίας ελέγχου αλλά χρειάζεται απλώς κάποια διαβεβαίωση ότι τα προσωπικά

του δεδομένα είναι ασφαλή. Για να το επιτύχει, ο οργανισμός θα μπορούσε να χρησιμοποιήσει τα ακόλουθα εικονίδια ελέγχου τήρησης κάποιας αρχής ιδιωτικότητας που θα τον ενημερώνουν οπτικά ότι ο οργανισμός έχει ελεγχθεί από έναν κατάλληλο φορέα.

Εικόνα 1: Εικονίδια ελέγχου τήρησης αρχών ιδιωτικότητας

4.3 Συμπεράσματα

Με γνώμονα τις πιο ευρέως χρησιμοποιούμενες αρχές ιδιωτικότητας, οι οποίες έχουν αναπτυχθεί είτε από χώρες είτε από δημόσιους / ιδιωτικούς φορείς, η προτεινόμενη μεθοδολογία είναι μια δομημένη μεθοδολογία ελέγχου ιδιωτικότητας που αποτελείται από διακριτά βήματα που μπορούν να ακολουθήσουν οι οργανισμοί για την προστασία ή/και τον έλεγχο της ιδιωτικότητας των χρηστών τους. Κάθε βήμα βασίζεται στη σημαντικότητα κάθε αρχής ιδιωτικότητας και στη σειρά της διαδικασίας ελέγχου. Η εφαρμογή της προτεινόμενης μεθοδολογίας ελέγχου ιδιωτικότητας σε πραγματικό περιβάλλον, αναδεικνύει τη σημασία της τόσο για τους οργανισμούς όσο και για τους χρήστες.

5 Κεφάλαιο 5: Μεθοδολογία αξιολόγησης του αντίκτυπου για την ιδιωτικότητα και την προστασία δεδομένων χρησιμοποιώντας μετρικές

5.1 Εισαγωγή

Καθώς οι εφαρμογές πληροφορικής αυξάνονται σταθερά, μέσω του Διαδικτύου, όλο και περισσότεροι άνθρωποι τις χρησιμοποιούν αποτυγχάνοντας να εκτιμήσουν τις θετικές ή ακόμα χειρότερα παραμελώντας τις πιθανές αρνητικές συνέπειες. Έτσι, το κύριο πρόβλημα που προκύπτει είναι πώς οι εταιρείες μπορούν να προστατεύσουν τα προσωπικά δεδομένα τόσο των πελατών όσο και των εργαζομένων, προκειμένου να αποφευχθούν οι παραβιάσεις της ιδιωτικότητας [3]. Αυτό είναι ένα ενδιαφέρον πεδίο μελέτης το οποίο θα πρέπει να ερευνηθεί διεξοδικά λόγω του γεγονότος ότι ένας τεράστιος όγκος προσωπικών πληροφοριών συλλέγεται, αποθηκεύεται, επεξεργάζεται, κοινοποιείται και δημοσιεύεται στο Διαδίκτυο [1] [2]. Πιο συγκεκριμένα, κατά τη χρήση εφαρμογών που βασίζονται στο Διαδίκτυο οι χρήστες διακινδυνεύουν την ιδιωτικότητά τους, καθώς τα προσωπικά τους δεδομένα ενδέχεται να εκτεθούν σε άλλους.

Προκειμένου να αποφευχθούν οι παραβιάσεις της ιδιωτικότητας, αρκετοί νόμοι, πρότυπα, κανονισμοί και οδηγίες/κατευθυντήριες γραμμές [4] έχουν εφαρμοστεί στις περισσότερες ανεπτυγμένες χώρες. Σκοπός είναι να υποχρεωθούν οι οργανισμοί να ενημερώσουν πλήρως τους χρήστες τους και να λάβουν την προηγούμενη συγκατάθεσή τους πριν συλλέξουν, αποθηκεύσουν ή επεξεργαστούν τα προσωπικά τους δεδομένα με οποιονδήποτε τρόπο. Ταυτόχρονα, οι αρχές ιδιωτικότητας [5], οι απαιτήσεις ιδιωτικότητας [6][7] και οι απαιτήσεις ασφάλειας [6][7] είναι επίσης χρήσιμες, καθώς βοηθούν στην ανάπτυξη ενός ολοκληρωμένου πλαισίου ασφάλειας και προστασίας της ιδιωτικότητας.

Είναι επομένως απαραίτητο να υπάρχουν μηχανισμοί που να διευκολύνουν την αξιολόγηση του αντίκτυπου των σύγχρονων συστημάτων και εφαρμογών πληροφορικής στην ιδιωτικότητα των πελατών. Αυτή η αξιολόγηση θα πρέπει να πραγματοποιείται κατά το στάδιο του σχεδιασμού ενός συστήματος ή μιας εφαρμογής πληροφορικής και οπωσδήποτε καθ' όλη τη διάρκεια του κύκλου ζωής του. Οι επιστήμονες εργάζονται προς αυτή την κατεύθυνση, προτείνοντας μεθοδολογίες που μπορούν να βοηθήσουν τους οργανισμούς να μετρήσουν τον αντίκτυπο των παραβιάσεων της ιδιωτικότητας. Ωστόσο,

εξακολουθεί να υπάρχει σαφής έλλειψη αξιόπιστων μετρικών συστημάτων (metric systems) που μπορούν να υιοθετήσουν οι οργανισμοί.

Λαμβάνοντας υπόψη ότι δεν υπάρχει ακόμη αποτελεσματική μεθοδολογία για την ποσοτικοποίηση των επιπτώσεων παραβίασης της ιδιωτικότητας, στις επόμενες ενότητες παρουσιάζεται μια προσέγγιση για την αξιολόγηση του επιπέδου ιδιωτικότητας ενός συστήματος. Εάν ποσοτικοποιηθεί ο αντίκτυπος από μια παραβίαση της ιδιωτικότητας, τα προσωπικά δεδομένα μπορούν να προστατευθούν αποτελεσματικά, υποστηρίζοντας έτσι τους χρήστες έναντι των προκλήσεων της ψηφιακής εποχής και βοηθώντας τους να ελαχιστοποιήσουν πιθανές εισβολές στην ιδιωτικότητα τους. Ένας επιπλέον στόχος είναι να διευκολυνθεί η ενιαία διαχείριση των απαιτήσεων ασφάλειας και ιδιωτικότητας με την έννοια ότι ειδικά αντίμετρα ασφαλείας μπορούν επίσης να βοηθήσουν στην ικανοποίηση των απαιτήσεων ιδιωτικότητας. Από αυτή την άποψη, η προτεινόμενη μεθοδολογία ενσωματώνει τα αποτελέσματα των μεθόδων ανάλυσης επικινδυνότητας (π.χ. CRAMM, Octave, VSRisk κτλ.) όσον αφορά την κρισιμότητα των αγαθών και τον πιθανό αντίκτυπό τους στον οργανισμό σε περίπτωση περιστατικού ασφάλειας (απώλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας).

Η υποενότητα 5.2, που ακολουθεί, παρέχει μια επισκόπηση της βιβλιογραφίας σχετικά με τις μεθοδολογίες εκτίμησης αντίκτυπου στην ιδιωτικότητα. Βασιζόμενοι στην επισκόπηση της βιβλιογραφίας, η υποενότητα 5.3 παρέχει μια επισκόπηση των διαφορετικών κατηγοριών δεδομένων που τηρούνται από οργανισμούς, μαζί με τις σχετικές αρχές και απαιτήσεις ιδιωτικότητας. Ακολουθεί περιγραφή της προτεινόμενης μεθοδολογίας αξιολόγησης αντίκτυπου της ιδιωτικότητας μαζί με τις παραγόμενες μετρικές για την ποσοτικοποίηση της κρισιμότητας των αρχών ιδιωτικότητας για έναν οργανισμό. Στην υποενότητα 5.4 εφαρμόζεται η προτεινόμενη μεθοδολογία σε δύο Πληροφοριακά Συστήματα Νοσοκομείων με διαφορετικά χαρακτηριστικά ως παραδείγματα. Η υποενότητα 5.5 εξάγει συμπεράσματα αναφέροντας παράλληλα μελλοντικές ενέργειες.

5.2 Εκτίμηση αντικτύπου της ιδιωτικότητας

Με την έλευση της τεχνολογικής εποχής, όλο και περισσότεροι άνθρωποι χρησιμοποιούν υπολογιστές σε καθημερινή βάση για να ικανοποιήσουν τις «ψηφιακές τους ανάγκες», όπως για παράδειγμα για να πραγματοποιούν ηλεκτρονικές συναλλαγές

μέσω του Διαδικτύου. Για να επιτευχθεί αυτό, δεν διστάζουν να παρέχουν προσωπικά δεδομένα που απαιτούνται για την πρόσβαση στις εφαρμογές. Ωστόσο, μπορούν να προστατευθούν πραγματικά όταν «προσφέρουν» τα προσωπικά τους δεδομένα τόσο πρόθυμα; Για να απαντηθεί αυτό το ερώτημα, είναι πρώτα απαραίτητο να εκτιμηθούν οι συνέπειες από μια πιθανή παραβίαση της ιδιωτικότητας, χρησιμοποιώντας μια μεθοδολογία Εκτίμησης Αντικτύπου της Ιδιωτικότητας (Privacy Impact Assessment - PIA). Έχοντας εκτιμήσει τον αντίκτυπο, τα εμπλεκόμενα μέρη μπορούν να υιοθετήσουν διορθωτικές ενέργειες για την εξάλειψη ή την ελαχιστοποίηση των συνεπειών [47]. Επιπλέον, η αποτυχία εφαρμογής μιας μεθοδολογίας PIA μπορεί να οδηγήσει σε παραβίαση των νόμων και των κανονισμών περί ιδιωτικότητας.

Η υιοθέτηση μιας μεθοδολογίας PIA μπορεί σίγουρα να ωφελήσει τόσο τους ίδιους τους χρήστες όσο και τους οργανισμούς [13] [47] [54]. Όσον αφορά τους χρήστες, το πρώτο και σημαντικότερο πλεονέκτημα είναι ότι μπορούν να διασφαλίσουν ότι οι εταιρείες που επεξεργάζονται τα προσωπικά δεδομένα τους, συμμορφώνονται με πρότυπα, νόμους και οδηγίες/κατευθυντήριες γραμμές. Επιπλέον, οι χρήστες μπορούν να καθορίσουν πώς οι πληροφορίες τους συλλέγονται, αποθηκεύονται και επεξεργάζονται, διασφαλίζοντας διαφάνεια. Από την άλλη πλευρά, υπάρχουν οφέλη και για τους οργανισμούς που εφαρμόζουν μια μεθοδολογία PIA, καθώς προστατεύουν τους πελάτες τους, μετριάζοντας τις παραβιάσεις της ιδιωτικότητας και διασφαλίζοντας συμμόρφωση με το νομικό πλαίσιο. Επιπρόσθετα, όταν οι οργανισμοί προσφέρουν υπηρεσίες συμβατές με ιδιωτικότητα (privacy-oriented services), εξασφαλίζουν τόσο την εμπιστοσύνη των πελατών όσο και των εργαζομένων τους. Τέλος, εξίσου σημαντικά είναι και τα οικονομικά οφέλη που προκύπτουν. Μειώνοντας το τρέχον κόστος ενός έργου μέσω της ελαχιστοποίησης του όγκου των πληροφοριών που συλλέγονται ή επεξεργάζονται, όπου είναι δυνατόν [54], ο οργανισμός μπορεί να γίνει πιο κερδοφόρος.

Παράλληλα με τα θετικά αποτελέσματα της εφαρμογής μιας μεθοδολογίας PIA, υπάρχουν και ορισμένα αρνητικά [13]. Η εφαρμογή και στη συνέχεια, η δημοσίευση των αποτελεσμάτων μιας μεθοδολογίας PIA μπορεί να βοηθήσει κακόβουλους να τα εκμεταλλευτούν, θέτοντας σε κίνδυνο την ιδιωτικότητα των χρηστών. Εξάλλου, μια μεθοδολογία PIA μπορεί να επιβάλλει καθυστερήσεις και πρόσθετο κόστος κατά την υλοποίηση ενός νέου έργου. Μια άλλη σημαντική ανησυχία είναι ο περιορισμός της

ευελιξίας των οργανισμών. Αυτό, πρακτικά, σημαίνει ότι οι οργανισμοί δεσμεύονται να λαμβάνουν ενέργειες με συγκεκριμένο τρόπο, βασιζόμενοι σε νόμους και κανονισμούς, χωρίς εναλλακτικές επιλογές, οι οποίες, για παράδειγμα, θα τους βοηθούσαν να ολοκληρώσουν συγκεκριμένες εργασίες πιο γρήγορα. Ωστόσο, τα πλεονεκτήματα υπερτερούν κατά πολύ των μειονεκτημάτων, καθώς μια μεθοδολογία PIA είναι οπωσδήποτε ένας πολύ καλός τρόπος για την προστασία της ιδιωτικότητας των χρηστών και τον μετριασμό των κινδύνων ιδιωτικότητας.

Λαμβάνοντας υπόψη τα προαναφερθέντα οφέλη από την εφαρμογή μια μεθοδολογίας PIA, μπορεί κάποιος να συμπεράνει ότι μέσω της εφαρμογής μιας μεθοδολογίας PIA οι πιο ευρέως γνωστές αρχές ιδιωτικότητας τηρούνται. Το 1980 [5] ο οργανισμός OECD πρότεινε οκτώ αρχές ιδιωτικότητας, οι οποίες έγιναν παγκοσμίως αποδεκτές, και συγκεκριμένα: αρχή καθορισμού του σκοπού (purpose specification principle), αρχή περιορισμού της συλλογής (collection limitation principle), αρχή διατήρησης ποιότητας των δεδομένων (data quality principle), αρχή περιορισμού της χρήσης (use limitation principle), αρχή διαφάνειας (openness principle), αρχή ατομικής συμμετοχής (individual participation principle), αρχή λογοδοσίας (accountability principle), αρχή εφαρμογής μέτρων προστασίας ασφάλειας (security safeguards principle). Στόχος τους ήταν να ελαχιστοποιήσουν τον κίνδυνο αποκάλυψης προσωπικών δεδομένων και να αποτελέσουν τη βάση της προστασίας της ιδιωτικότητας [40]. Η Ann Cavoukian [44] [55] [41] υποστηρίζει έντονα την έννοια της ιδιωτικότητας κατά το σχεδιασμό, σύμφωνα με την οποία η ιδιωτικότητα θα πρέπει να διατηρείται καθ' όλη τη διάρκεια του κύκλου ζωής ενός πληροφοριακού συστήματος, από τη σύλληψη της ιδέας ενός νέου συστήματος μέχρι και την υλοποίησή του. Σύμφωνα με τους Oetzel και Spiekermann [56] [57] η έννοια της ιδιωτικότητας κατά το σχεδιασμό είναι πολύ σημαντική σε μια μεθοδολογία PIA, καθώς οι μεθοδολογίες PIA προσπαθούν να ακολουθήσουν αυτές τις αρχές ιδιωτικότητας προκειμένου να επιτύχουν ιδιωτικότητα κατά το σχεδιασμό, η οποία είναι μια από τις πιο βασικές ανησυχίες σήμερα.

Προκειμένου ένας οργανισμός να προστατεύει τα προσωπικά δεδομένα ενός χρήστη, χρησιμοποιούνται οι Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας (Privacy Enhancing Technologies - PETs) για την ικανοποίηση των απαιτήσεων ιδιωτικότητας (προστασία δεδομένων, ανωνυμία / ψευδωνυμία, μη συνδεσιμότητα και μη παρατηρησιμότητα),

ταυτόχρονα με τις αρχές ιδιωτικότητας που αναφέρονται παραπάνω. Τα PETs είναι διάφορα τεχνικά και διαδικαστικά μέτρα που μπορούν να αποτρέψουν την μη απαραίτητη ή μη ηθελημένη επεξεργασία των προσωπικών δεδομένων των χρηστών και έτσι μπορούν να προστατεύσουν την ιδιωτικότητά τους [39][40].

Η ιδέα της εφαρμογής μιας μεθοδολογίας PIA είναι σχετικά νέα. Το Ηνωμένο Βασίλειο ήταν η πρώτη Ευρωπαϊκή χώρα που χρησιμοποίησε το εγχειρίδιο (handbook) της μεθοδολογίας PIA το οποίο αναπτύχθηκε και δημοσιεύτηκε από το Γραφείο Πληροφοριών ICO (Information Commissioner's Office - ICO) τον Δεκέμβριο του 2007, αναθεωρημένη έκδοση του οποίου κυκλοφόρησε τον Ιούνιο του 2009 [58] [47] [60]. Σε αυτό, τα βασικά στάδια μιας μεθοδολογίας PIA παρουσιάστηκαν με λεπτομέρεια. Τον Μάιο του ίδιου έτους, ακολούθησε η σύσταση της Ευρωπαϊκής Επιτροπής για τις ετικέτες αναγνώρισης ραδιοσυχνοτήτων (Radio Frequency Identification - RFID), όπου τα κράτη μέλη κλήθηκαν να διασφαλίσουν ότι η βιομηχανία, σε συνεργασία με τους εμπλεκόμενους φορείς της κοινωνίας, θα αναπτύξει ένα πλαίσιο για την εκτίμηση του αντίκτυπου της ιδιωτικότητας και της προστασίας δεδομένων, παρέχοντας στοιχεία για το Άρθρο 29 περί προστασίας δεδομένων [47] [59]. Τα παραπάνω, παρέχουν στοιχεία ότι η ανάγκη εφαρμογής μιας μεθοδολογίας PIA κέρδισε έδαφος πρόσφατα και ότι αποτελεί τη βάση για να ληφθεί υπόψη σοβαρά η ιδιωτικότητα στο μέλλον [61].

Πρόσφατα, η Ευρωπαϊκή Επιτροπή συγχρηματοδότησε το έργο PIAF (A Privacy Impact Assessment Framework για την προστασία των δεδομένων και τα δικαιώματα της ιδιωτικότητας), το οποίο στοχεύει να ενθαρρύνει την ΕΕ και τα κράτη μέλη της να υιοθετήσουν μια πολιτική PIA [62]. Το έργο διάρκειας 22 μηνών ολοκληρώθηκε τον Δεκέμβριο του 2012 και οδήγησε ως αποτέλεσμα σε έναν βήμα προς βήμα οδηγό για την εκτίμηση του αντίκτυπου της ιδιωτικότητας, έτσι ώστε τα ζητήματα ιδιωτικότητας να αντιμετωπίζονται καλύτερα και τα προσωπικά δεδομένα να προστατεύονται αποτελεσματικότερα από μη επιθυμητή επεξεργασία [63]. Αυτό το έργο υπογραμμίζει πόσο σημαντική είναι η εφαρμογή μιας μεθοδολογίας PIA στα πληροφοριακά συστήματα και ότι είναι υποχρεωτική σε όλα τα κράτη μέλη της ΕΕ.

Τον Μάιο του 2013, το Γραφείο Πληροφοριών ICO (Information Commissioner's Office - ICO) διεξήγαγε περαιτέρω έρευνα σχετικά με τις μεθοδολογίες PIA που οδήγησαν στη δημοσίευση της «Εκτίμησης αντικτύπου της ιδιωτικότητας και διαχείριση

επικινδυνότητας», στην οποία προτάθηκαν συγκεκριμένες βελτιώσεις, η σημαντικότερη από τις οποίες ήταν η καλύτερη ενσωμάτωση των μεθοδολογιών PIA με την υπάρχουσα διαχείριση έργων και τις διαδικασίες διαχείρισης επικινδυνότητας (risk management) [64]. Ένα χρόνο αργότερα, τον Φεβρουάριο του 2014 [54], το Γραφείο Πληροφοριών ICO (Information Commissioner's Office - ICO) δημοσίευσε τον Κώδικα Πρακτικής για την Εκτίμηση Αντικτύπου της Ιδιωτικότητας (PIA), ο οποίος ενημερώθηκε τον Ιανουάριο του 2017, προκειμένου να βοηθήσει τους οργανισμούς να συμμορφωθούν με τις υποχρεώσεις τους από τη νομοθεσία περί προστασίας δεδομένων όταν αλλάζουν τον τρόπο με τον οποίο χρησιμοποιούν τα προσωπικά δεδομένα [65].

Τον Μάιο του 2017, ο Διεθνής Οργανισμός Τυποποίησης (ISO) και η Διεθνής Ηλεκτροτεχνική Επιτροπή (IEC), που αποτελούν το εξειδικευμένο σύστημα για την παγκόσμια τυποποίηση, δημοσίευσαν ένα πρότυπο που σχετίζεται με την εκτίμηση αντικτύπου της ιδιωτικότητας (PIA) [66], το οποίο δεν διαφέρει σημαντικά από τον ορισμό των David Wright και Paul De Hert [47]. Συγκεκριμένα, υποστηρίζει ότι μια μεθοδολογία PIA είναι κάτι περισσότερο από ένα εργαλείο και ορίζεται ως μια διαδικασία που ξεκινά από τα αρχικά στάδια ενός συστήματος και συνεχίζεται σε όλο τον κύκλο ζωής και ανάπτυξής του, επιτυγχάνοντας έτσι ιδιωτικότητα κατά το σχεδιασμό [66]. Στόχος του Διεθνούς Προτύπου είναι να παρέχει οδηγίες/κατευθυντήριες γραμμές σχετικά με τη διαδικασία διεξαγωγής μιας μεθοδολογίας PIA και τη δομή και το περιεχόμενο μιας έκθεσης PIA. Σύμφωνα με το επίσημα δημοσιευμένο προσχέδιο [66] «θα αφορά όσους εμπλέκονται στο σχεδιασμό ή την υλοποίηση έργων, συμπεριλαμβανομένων όσων διαχειρίζονται συστήματα και υπηρεσίες επεξεργασίας δεδομένων». Επιπλέον, θα ισχύει για όλους τους δημόσιους και ιδιωτικούς φορείς.

Πριν από το επερχόμενο πρότυπο, ο οργανισμός ISO δημιούργησε ένα πρότυπο για διεξαγωγή μεθοδολογίας PIA στις χρηματοοικονομικές υπηρεσίες [67]. Στόχος του προτύπου ISO 22307:2008 ήταν να λειτουργήσει ως εργαλείο για την εσωτερική επεξεργασία προσωπικών δεδομένων κατά την ανάπτυξη ενός προτεινόμενου χρηματοοικονομικού συστήματος (Proposed Financial System - PFS). Το πρότυπο χρησιμοποιείται για τον μετριασμό των κινδύνων που εμφανίζονται όταν ένας οργανισμός επεξεργάζεται τα οικονομικά δεδομένα πελατών και καταναλωτών, επιχειρηματικών εταίρων καθώς και πολιτών.

Εκτός από οργανισμούς όπως ο ICO και ο ISO/IEC, διακεκριμένοι επιστήμονες έχουν κάνει έρευνα για τις μεθοδολογίες PIA. Έχουν προτείνει μεθοδολογίες PIA, οι οποίες μπορούν εύκολα να εφαρμοστούν από έναν οργανισμό, δίνοντας, ταυτόχρονα, ακριβή αποτελέσματα. Το 2012 [56] και το 2013 [57], οι Oetzel Marie Caroline και Spiekermann Sarah πρότειναν μια συστηματική μεθοδολογία για την εκτίμηση του αντίκτυπου της ιδιωτικότητας. Η μεθοδολογία PIA που πρότειναν και η οποία βασίζεται στη διαδικασία αξιολόγησης των κινδύνων ασφαλείας ενός οργανισμού του NIST (2002) [68] και στη διαδικασία PIA του Ηνωμένου Βασιλείου (ICO, 2009) [58], μειώνει την πολυπλοκότητα της νομοθεσίας περί ιδιωτικότητας για τους επαγγελματίες, βοηθώντας τους να λαμβάνουν αποφάσεις διαχείρισης ιδιωτικότητας για τις εφαρμογές τους. Επιπλέον, ορίζει στόχους ιδιωτικότητας, αξιολογεί το επίπεδο προστασίας που χρειάζονται, εντοπίζει απειλές και προτείνει μέτρα/ελέγχους.

Όσο περνούν τα χρόνια, η ταχεία βελτίωση των μεθοδολογιών PIA τονίζει τη σημαντικότητά τους για την ιδιωτικότητα και την προστασία των δεδομένων. Ωστόσο, δεν υπάρχει σαφής τρόπος να ποσοτικοποιηθεί ο αντίκτυπος της ιδιωτικότητας. Το 2011, ο David Wright [13] [15] τόνισε αυτή την ανάγκη, αναφέροντας ότι «*Το να γίνουν υποχρεωτικές οι μελέτες εκτίμησης αντικτύπου της ιδιωτικότητας δεν αρκεί. Απαιτούνται έλεγχοι και ορισμός μετρικών για να βεβαιωθούμε ότι οι μεθοδολογίες PIA πραγματοποιούνται σωστά και για να καθοριστεί εάν μπορούν να γίνουν βελτιώσεις στην ήδη υπάρχουσα διαδικασία*». Πιο πρόσφατα, το 2013, οι Kush Wadhwa και Rowena Rodrigues [14] συμφώνησαν με την αναφορά του David Wright, που πρακτικά σημαίνει ότι η συγκεκριμένη ανάγκη εξακολουθεί να υπάρχει.

Ένας από τους κύριους λόγους που οι οργανισμοί υιοθετούν μεθοδολογίες PIA είναι για να κερδίσουν την εμπιστοσύνη των χρηστών. Αρκετά εργαλεία, όπως το εργαλείο αξιολόγησης κινδύνων ιδιωτικότητας AIPCA/CICA, το εργαλείο SPIA (Security and Privacy Impact Assessment - SPIA) του Πανεπιστημίου της Πενσυλβάνια, το εργαλείο GS1 RFID Privacy Impact Assessment (PIA), το έξυπνο εργαλείο PIA του Πανεπιστημίου της Βιέννης για RFID εφαρμογές και το εργαλείο PIA για υπολογιστικό νέφος που προτάθηκε από τους Tancock, Pearson και Charlesworth (2010) [14], έχουν προταθεί για να βοηθήσουν τους οργανισμούς να αξιολογήσουν τους κινδύνους ιδιωτικότητας. Ωστόσο, κανένα από αυτά

δεν χρησιμοποιεί μετρικές για να ποσοτικοποιήσει τον αντίκτυπο μιας παραβίασης ιδιωτικότητας.

Τον Ιούλιο του 2016, ο Sushant Agarwal [69] τόνισε το γεγονός ότι παρόλο που υπάρχει μια σειρά από καλά δομημένα διαδικτυακά εργαλεία PIA (εργαλείο GS1, εργαλείο iPIA, εργαλείο SPIA, κτλ.), κανένα δεν επιτυγχάνει να παρέχει μια μετρική για την αξιολόγηση της προόδου στην εφαρμογή των ελέγχων ιδιωτικότητας. Στην έρευνά του, ανέπτυξε μια δομημένη μετρική για τη μέτρηση του κινδύνου ιδιωτικότητας. Πριν από τον Agarwal, οι Oetzel και Spiekermann [56] [57], είχαν ήδη προτείνει μια ποιοτική μετρική (χαμηλή, μεσαία, υψηλή) για τη μέτρηση των κινδύνων ιδιωτικότητας, αλλά η προσπάθειά τους ήταν αρκετά αδόμητη και δύσκολο να υπολογιστεί με σαφήνεια [69]. Προκειμένου να αξιολογήσει τον κίνδυνο ιδιωτικότητας, ο Agarwal τον όρισε ως το «προϊόν» του αντίκτυπου και της πιθανότητας. Πιο συγκεκριμένα, ο Agarwal αξιολόγησε τον αντίκτυπο, χρησιμοποιώντας την ταξινόμηση του Solove και την πιθανότητα, χρησιμοποιώντας τη δουλειά του Lipton. Για τον υπολογισμό του αντίκτυπου, χρησιμοποίησε τέσσερις διαφορετικές πτυχές της ιδιωτικότητας, χωρίζοντάς τις σε κατηγορίες και υποκατηγορίες. Για την πιθανότητα, χρησιμοποίησε ρόλους (εταιρείες, τρίτες οντότητες, άλλα) και χαρακτηριστικά δεδομένων (ποσότητα δεδομένων, ευαισθησία δεδομένων, αξία εμπλεκόμενων δεδομένων). Με αυτό τον τρόπο, πρότεινε μια δομημένη μετρική κινδύνου ιδιωτικότητας, αλλά απέτυχε να εμβαθύνει στα χαρακτηριστικά των οργανισμών που μπορεί να έχουν σημαντικό αρνητικό αντίκτυπο στην ιδιωτικότητα των χρηστών.

Τον Ιούνιο του 2015, η Commission Nationale de l'Informatique et des Libertés (CNIL) δημοσίευσε μια μεθοδολογία PIA, η οποία είναι σύμφωνη με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) της ΕΕ [4]. Σύμφωνα με την CNIL [70], η μεθοδολογία PIA βασίζεται σε δύο πυλώνες: πρώτον, τις θεμελιώδεις αρχές και τα δικαιώματα και, δεύτερον, τη διαχείριση των κινδύνων ιδιωτικότητας των υποκειμένων των δεδομένων. Πιο συγκεκριμένα, η μεθοδολογία αποτελείται από τέσσερα βήματα: τον ορισμό και την περιγραφή του πλαισίου της υπό εξέταση επεξεργασίας δεδομένων προσωπικού χαρακτήρα, τον προσδιορισμό των ήδη υπαρχόντων ή μελλοντικά προγραμματισμένων ελέγχων, την αξιολόγηση των κινδύνων ιδιωτικότητας και την απόφαση επικύρωσης του τρόπου με τον οποίο σχεδιάζεται να συμμορφώνεται με τις αρχές ιδιωτικότητας και να αντιμετωπίζει τους κινδύνους ή να επανεξετάζει τα προηγούμενα βήματα. Τον Δεκέμβριο

του 2017, η CNIL δημοσίευσε ένα δωρεάν και ανοιχτού κώδικα λογισμικό PIA [71] προκειμένου να βοηθήσει τους υπεύθυνους επεξεργασίας δεδομένων να ακολουθήσουν τη μεθοδολογία τους.

Τέλος, μπορούμε να συμπεράνουμε ότι ένας αποτελεσματικός τρόπος μέτρησης του αντίκτυπου της ιδιωτικότητας είναι η χρήση μετρικών. Οι μετρικές μπορούν να βοηθήσουν τους οργανισμούς να υπολογίσουν τη σημαντικότητα των απειλών και να τους οδηγήσουν στη λήψη μέτρων για τον μετριασμό των κινδύνων. Παρά τις αξιοσημείωτες προσπάθειες για τον καθορισμό των μετρικών από διάφορους ερευνητές [56] [57] [69], μέχρι στιγμής, δεν έχει υπάρξει λεπτομερής μεθοδολογία PIA που να χρησιμοποιεί μετρικές και, ταυτόχρονα, να λαμβάνει υπόψη τα χαρακτηριστικά του οργανισμού. Επιπλέον, δεν υπάρχει μεθοδολογία που να ενσωματώνει την αξιολόγηση της ασφάλειας και της ιδιωτικότητας.

5.3 Η προτεινόμενη μεθοδολογία ασφάλειας και αξιολόγησης αντίκτυπου της ιδιωτικότητας

5.3.1 Στόχος της προτεινόμενης μεθοδολογία

Η προτεινόμενη μεθοδολογία έχει σαν στόχο να βοηθήσει τους οργανισμούς να προστατεύσουν την ιδιωτικότητα των χρηστών τους και την ασφάλεια των δεδομένων που αποθηκεύουν και επεξεργάζονται. Πιθανοί χρήστες μπορεί να είναι οι πελάτες του οργανισμού (π.χ. άτομα που χρησιμοποιούν τις προσφερόμενες υπηρεσίες) ή οι εργαζόμενοι (π.χ. χρήστες που χειρίζονται τα συστήματα του οργανισμού).

Η καινοτομία της προτεινόμενης μεθοδολογίας είναι ότι μπορεί να χειριστεί ταυτόχρονα απαιτήσεις ασφάλειας και ιδιωτικότητας, καθώς χρησιμοποιεί τα αποτελέσματα της ανάλυσης επικινδυνότητας (risk analysis) μαζί με αυτά μιας μελέτης εκτίμησης αντικτύπου της ιδιωτικότητας (privacy impact assessment). Μια περαιτέρω καινοτομία της μεθοδολογίας είναι ότι εισάγει μετρικές για την ποσοτικοποίηση των απαιτήσεων και λαμβάνει υπόψη τα συγκεκριμένα χαρακτηριστικά του οργανισμού.

Θα πρέπει να τονιστεί ότι σκοπός δεν είναι η πρόταση μιας συγκεκριμένης μεθοδολογίας για την ασφάλεια των δεδομένων ή τη διαχείριση των κινδύνων κατά της ιδιωτικότητας (privacy risk management). Αντίθετα, σκοπός είναι να επιτραπεί σε έναν

οργανισμό να χρησιμοποιήσει μια υπάρχουσα μεθοδολογία για τη διαχείριση επικινδυνότητας (risk management) και την εκτίμηση του αντικτύπου της ιδιωτικότητας (privacy impact assessment), ενώ ταυτόχρονα, να διευκολύνει την ενσωμάτωση των απαιτήσεων ασφάλειας και ιδιωτικότητας με τις αρχές ιδιωτικότητας που υπαγορεύονται από το νομικό και κανονιστικό πλαίσιο. Όλα αυτά θα γίνονται στο πλαίσιο ενός συγκεκριμένου οργανισμού (π.χ. λαμβάνοντας υπόψη συγκεκριμένα χαρακτηριστικά, αντιλήψεις και προθέσεις του οργανισμού). Όπως φαίνεται στο Σχήμα 2, διαφορετικές μεθοδολογίες για την εξαγωγή των απαιτήσεων ασφάλειας και ιδιωτικότητας μπορούν να χρησιμοποιηθούν για να παράγουν τον συντελεστή κινδύνου (risk factor) για τα αγαθά του συστήματος (system assets). Ο συντελεστής κινδύνου «τροφοδοτεί» την προτεινόμενη μεθοδολογία (μέσω της αρχής εφαρμογής μέτρων προστασίας ασφάλειας (security safeguards principle)) προκειμένου να υπολογιστεί η συνολική κρισιμότητα για ένα συγκεκριμένο οργανισμό (λαμβάνοντας υπόψη τις αρχές ιδιωτικότητας και τα χαρακτηριστικά του οργανισμού).

Επομένως, η προσέγγισή της μεθοδολογίας είναι παρόμοια με αυτή του προτύπου ISO 27005 που δεν παρέχει καμία συγκεκριμένη μεθοδολογία για τη διαχείριση επικινδυνότητας ασφάλειας δεδομένων (information security risk management), αλλά επιτρέπει στον οργανισμό να υιοθετήσει οποιαδήποτε μεθοδολογία στο πλαίσιο του προτύπου.

5.3.2 Θεωρητικό υπόβαθρο

5.3.2.1 Ορισμοί συνόλων δεδομένων (Data Sets - DS)

Ένας τεράστιος όγκος δεδομένων αποθηκεύεται και υφίσταται επεξεργασία σε πληροφοριακά συστήματα (ΠΣ) ή/και φορητές συσκευές όπως κινητά τηλέφωνα ή tablet. Ωστόσο, η κρισιμότητα των δεδομένων δεν είναι πάντα η ίδια. Για παράδειγμα, ορισμένες εφαρμογές ενδέχεται να χρησιμοποιούν μόνο δεδομένα που είναι διαθέσιμα δημόσια, άλλες μπορεί να περιλαμβάνουν προσωπικά δεδομένα (όπως ονόματα, διευθύνσεις κτλ.) και άλλες μπορεί να επεξεργάζονται ευαίσθητα δεδομένα (όπως δεδομένα υγείας). Η κάθε περίπτωση παρουσιάζει διαφορετική κρισιμότητα και πρέπει να αντιμετωπίζεται διαφορετικά [3]. Για να αντιμετωπιστεί αυτή η διαφορετική κρισιμότητα, μέσω της προτεινόμενης μεθοδολογίας, τα δεδομένα που αποθηκεύει/επεξεργάζεται ένας

οργανισμός είτε εσωτερικά (π.χ. δεδομένα εργαζομένων) είτε εξωτερικά (π.χ. δεδομένα χρηστών) ταξινομούνται στις ακόλουθες κατηγορίες:

- **Προσωπικά Δεδομένα (Personal Data):** Υπάρχουν αρκετές προσεγγίσεις για τον ορισμό των προσωπικών δεδομένων. Ο Νόμος για την Προστασία Δεδομένων (Data Protection Act) [24] ορίζει τα προσωπικά δεδομένα ως δεδομένα που σχετίζονται με ένα άτομο το οποίο είναι ή μπορεί να αναγνωριστεί είτε άμεσα από τα δεδομένα είτε σε συνδυασμό με άλλες πληροφορίες που βρίσκονται ή είναι πιθανό να περιέλθουν στην κατοχή του υπεύθυνογ επεξεργασίας δεδομένων. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΕΕ) 2016/679 [4] ορίζει τα προσωπικά δεδομένα ως κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο 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. Για τις ανάγκες της προτεινόμενης μεθοδολογίας, αυτή η κατηγορία συνόλου δεδομένων θα περιλαμβάνει δεδομένα που ένας οργανισμός αποθηκεύει και επεξεργάζεται στα συστήματά του και σχετίζονται με ένα αναγνωρισμένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Μερικά ενδεικτικά παραδείγματα προσωπικών δεδομένων είναι: όνομα, επώνυμο, ηλικία, διεύθυνση, τηλέφωνο, email, εκπαίδευση.

- **Ευαίσθητα Δεδομένα (Sensitive Personal Data):** Τα ευαίσθητα προσωπικά δεδομένα μπορούν να θεωρηθούν υποκατηγορία προσωπικών δεδομένων. Τα ευαίσθητα προσωπικά δεδομένα, σύμφωνα με το νομικό πλαίσιο, χρήζουν υψηλής προστασίας. Ορίζονται στην ενότητα 2 του νόμου για την προστασία δεδομένων (Data Protection Act) [24] ως δεδομένα προσωπικού χαρακτήρα που αποτελούνται από πληροφορίες που σχετίζονται με το υποκείμενο των δεδομένων όσον αφορά τη φυλετική ή εθνική καταγωγή, πολιτικές απόψεις,

θρησκευτικές πεποιθήσεις ή άλλες πεποιθήσεις παρόμοιας φύσης, συμμετοχή σε συνδικάτα, σωματική ή ψυχική υγεία ή κατάσταση, σεξουαλική ζωή, διάπραξη ή υποτιθέμενη διάπραξη από το υποκείμενο των δεδομένων οποιουδήποτε αδικήματος, ή οποιαδήποτε διαδικασία για οποιοδήποτε αδίκημα που διαπράχθηκε ή φέρεται ότι έχει διαπραχθεί από το υποκείμενο των δεδομένων, η διάθεση τέτοιων διαδικασιών ή η ποινή οποιουδήποτε δικαστηρίου σε τέτοιες διαδικασίες. Για τις ανάγκες της προτεινόμενης μεθοδολογίας, αυτή η κατηγορία συνόλου δεδομένων θα περιλαμβάνει δεδομένα που ένας οργανισμός αποθηκεύει και επεξεργάζεται στα συστήματά του και σχετίζονται με ένα αναγνωρισμένο ή ταυτοποιήσιμο φυσικό πρόσωπο και ανήκουν σε οποιαδήποτε από τις προαναφερθείσες υποκατηγορίες.

- **Επιχειρησιακά Δεδομένα (Operational Data):** Επιχειρησιακά δεδομένα είναι τα δεδομένα που αποθηκεύει και επεξεργάζεται ένας οργανισμός, ως αποτέλεσμα της χρήσης των πληροφοριακών συστημάτων του. Πιο συγκεκριμένα, αυτή η κατηγορία περιλαμβάνει τα δεδομένα που δημιουργούνται από το ίδιο το πληροφοριακό σύστημα, όπως η καταγραφή των ενεργειών των χρηστών (logs). Για παράδειγμα, ένα αρχείο καταγραφής ενεργειών (log file) μπορεί να περιέχει λεπτομέρειες σχετικά με τις προσπάθειες σύνδεσης ενός χρήστη, για πόσο διάστημα ήταν συνδεδεμένος, το χρονικό πλαίσιο που χρησιμοποίησε μια συγκεκριμένη εφαρμογή κτλ.

- **Οικονομικά Δεδομένα (Financial Data):** Αυτό το σύνολο δεδομένων περιλαμβάνει όλα τα οικονομικά δεδομένα ενός οργανισμού (που σχετίζονται με τους υπαλλήλους ή/και τους χρήστες του). Ομοίως με τα επιχειρησιακά δεδομένα, δεν παρέχονται από χρήστες ή υπαλλήλους, αλλά «δημιουργούνται» από τον οργανισμό για λογαριασμό των χρηστών ή/και των υπαλλήλων του. Πιο συγκεκριμένα, τα οικονομικά δεδομένα ταξινομούνται σε δύο υποκατηγορίες: α) Δεδομένα που σχετίζονται με τη μισθοδοσία των υπαλλήλων του οργανισμού, β) Δεδομένα που σχετίζονται με πληρωμές από χρήστες του οργανισμού για τις παρεχόμενες υπηρεσίες. Θα πρέπει να

τονιστεί ότι τα οικονομικά δεδομένα και για τις δύο υποκατηγορίες παράγονται από τον οργανισμό.

- **Άλλα Δεδομένα (Others Data):** Οποιαδήποτε δεδομένα δεν μπορούν να ταξινομηθούν σε κάποια από τις παραπάνω κατηγορίες θα ληφθούν υπόψη σε αυτό το τελικό σύνολο δεδομένων. Ωστόσο, ο τύπος, η χρήση και η κρισιμότητα των δεδομένων θα πρέπει να ορίζονται ρητά.

5.3.2.2 Ο ρόλος των αρχών ιδιωτικότητας και των απαιτήσεων ασφάλειας και ιδιωτικότητας

Οι αρχές ιδιωτικότητας μαζί με όλες τις απαιτήσεις ιδιωτικότητας, πρέπει να ικανοποιούνται από τον οργανισμό προκειμένου να παρέχει υπηρεσίες συμβατές με την τήρηση της ιδιωτικότητας. Εξίσου σημαντική είναι και η ικανοποίηση των απαιτήσεων ασφαλείας. Στο [22], μια ολοκληρωμένη μεθοδολογία για τη διευκόλυνση των οργανισμών να προσδιορίσουν τα κατάλληλα μέτρα προστασίας ασφάλειας και ιδιωτικότητας για τα πληροφοριακά τους συστήματα, έχει προταθεί (Σχήμα 2). Πιο συγκεκριμένα, στο Σχήμα 2 προσδιορίζονται τα βήματα που πρέπει να κάνει ένας οργανισμός προκειμένου να προσδιορίσει τις απαιτήσεις ασφάλειας και ιδιωτικότητας, για το υπό μελέτη σύστημα, λαμβάνοντας υπόψη τις αρχές ιδιωτικότητας, καθώς και το στάδιο στο οποίο ο οργανισμός θα πρέπει να επιλέξει τα κατάλληλα μέτρα προστασίας για την ικανοποίηση των προαναφερόμενων απαιτήσεων. Η επιλογή των μέτρων προστασίας βασίζεται στις προσδιορισμένες απαιτήσεις ασφάλειας και ιδιωτικότητας και, στην πραγματικότητα, έρχεται να ικανοποιήσει την αρχή εφαρμογής μέτρων προστασίας ασφάλειας (security safeguards principle).

Επιπλέον, στο [23] μια ταξινόμηση τεσσάρων επιπέδων των υφιστάμενων αρχών ιδιωτικότητας, με βάση τη σημαντικότητά τους και τη σειρά που θα πρέπει να διενεργηθεί μια πιθανή διαδικασία ελέγχου, έχει προταθεί (Σχήμα 3). Όλα τα βήματα είναι αλληλεξαρτώμενα και θα πρέπει να ακολουθούνται με αυστηρή σειρά, καθώς η αποτυχία ελέγχου οποιουδήποτε βήματος συνεπάγεται ότι δεν έχει νόημα να συνεχιστεί η διαδικασία ελέγχου. Ταυτόχρονα, έχει εντοπιστεί ότι υπάρχει ανάγκη να τηρούνται ορισμένες αρχές ιδιωτικότητας καθ' όλη τη διάρκεια της διαδικασίας ελέγχου.

Πιο συγκεκριμένα, το πρώτο βήμα είναι το πιο σημαντικό αφού η «Αρχή Καθορισμού του Σκοπού (Purpose Specification Principle)» ορίζει το σκοπό της συλλογής και χρήσης δεδομένων. Εάν αυτή η αρχή ιδιωτικότητας δεν ικανοποιηθεί, οι άλλες αρχές ιδιωτικότητας δεν θα εφαρμοστούν με σωστό τρόπο, παραβιάζοντας την ιδιωτικότητα των δεδομένων. Το δεύτερο βήμα περιλαμβάνει την ικανοποίηση της «Αρχής Περιορισμού της Συλλογής (Collection Limitation Principle)» και της «Αρχής Διατήρησης Ποιότητας των Δεδομένων (Data Quality Principle)». Εάν έχει καθοριστεί ο σκοπός από το βήμα 1, η συλλογή και χρήση των δεδομένων πρέπει να είναι περιορισμένη και να σχετίζεται με το σκοπό. Επιπλέον, τα δεδομένα που συλλέγονται θα πρέπει να είναι ακριβή και ενημερωμένα. Εάν αυτές οι αρχές ιδιωτικότητας δεν ικανοποιηθούν, οι επερχόμενες αρχές ιδιωτικότητας δεν θα εφαρμοστούν με σωστό τρόπο, παραβιάζοντας την ιδιωτικότητα των δεδομένων. Το τρίτο βήμα περιλαμβάνει την ικανοποίηση της «Αρχής Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης (Use, Retention and Disclosure Limitation Principle)». Εάν πληρούνται οι αρχές ιδιωτικότητας από το βήμα 2, τα δεδομένα θα πρέπει να χρησιμοποιούνται περιορισμένα, να διατηρούνται και να αποκαλύπτονται σύμφωνα με τις πολιτικές των οργανισμών. Εάν η αρχή ιδιωτικότητας στο τρίτο βήμα δεν ικανοποιηθεί, οι επερχόμενες αρχές ιδιωτικότητας δεν θα εφαρμοστούν με σωστό τρόπο, παραβιάζοντας την ιδιωτικότητα των δεδομένων. Το τέταρτο και τελευταίο βήμα περιλαμβάνει την ικανοποίηση της «Αρχής Εφαρμογής Μέτρων Προστασίας Ασφάλειας (Security Safeguards Principle)».

Οι άλλες αρχές ιδιωτικότητας περιλαμβάνουν την ικανοποίηση της «Αρχής Διαφάνειας (Openness Principle)», της «Αρχής Ατομικής Συμμετοχής (Individual Participation Principle)» και της «Αρχής Λογοδοσίας (Accountability Principle)». Αυτές οι αρχές ιδιωτικότητας θα πρέπει να τηρούνται καθ' όλη τη διάρκεια εφαρμογής της μεθοδολογίας.

Βασιζόμενοι στην ιεραρχία των βημάτων (όπως απεικονίζεται στο Σχήμα 3), το Βήμα 1 είναι το πιο σημαντικό, το Βήμα 2 είναι πιο σημαντικό από το Βήμα 3 και το Βήμα 3 είναι πιο σημαντικό από το Βήμα 4. Οι άλλες αρχές ιδιωτικότητας θα πρέπει να εφαρμόζονται οριζόντια.

5.3.3 Ποσοτικοποίηση των απαιτήσεων ασφάλειας και ιδιωτικότητας

Προκειμένου να διευκολυνθούν οι ελεγκτές να «μετρήσουν» τον βαθμό στον οποίο οι απαιτήσεις ασφάλειας και ιδιωτικότητας έχουν ικανοποιηθεί από έναν οργανισμό, είναι απαραίτητο να εισαχθούν μετρικές που θα χρησιμοποιηθούν για την ποσοτικοποίηση των απαιτήσεων. Η προτεινόμενη μεθοδολογία εισάγει μετρικές που έχουν βασιστεί στον τύπο και τη σημαντικότητα των απαιτήσεων ασφάλειας και ιδιωτικότητας για ένα πληροφοριακό σύστημα, την κρισιμότητα των συνόλων δεδομένων που εμπλέκονται, τις ισχύουσες αρχές ιδιωτικότητας και τα χαρακτηριστικά του οργανισμού.

5.3.3.1 Απαιτήσεις ασφάλειας και σημαντικότητα των συνόλων δεδομένων

Το βασικό κριτήριο για τον προσδιορισμό της κρισιμότητας ενός περιστατικού ασφάλειας (security incident) και κατ' επέκταση των πιθανών συνεπειών για έναν οργανισμό, είναι ο βαθμός ευαισθησίας των δεδομένων που διατηρούνται σε αυτόν και υφίστανται επεξεργασία. Η βαρύτητα των απαιτήσεων ασφάλειας εξαρτάται από το βαθμό ευαισθησίας των συνόλων δεδομένων. Δηλαδή, όσο πιο ευαίσθητα χαρακτηριστούν τα δεδομένα τόσο πιο αυστηρές απαιτήσεις ασφαλείας θα πρέπει να υιοθετηθούν. Σε δεύτερο επίπεδο, για να αποφασιστεί ο βαθμός ευαισθησίας των δεδομένων είναι απαραίτητο να προσδιοριστούν όλα τα διαφορετικά υποσύνολα (υποκατηγορίες) δεδομένων και να αποτιμηθεί ανεξάρτητα το καθένα από αυτά. Ακολουθεί περιγραφή των μετρικών αποτίμησης των δεδομένων.

Μετρική 1.1: Ο βαθμός ευαισθησίας κάθε υποκατηγορίας δεδομένων

Περιγραφή Μετρικής: Ο βαθμός ευαισθησίας (severity) κάθε υποσυνόλου δεδομένων (data subcategory) θα εκτιμηθεί μέσω της χρήσης μιας μεθόδου ανάλυσης επικινδυνότητας (risk analysis method), όπως η CRAMM [25]. Το αποτέλεσμα της ανάλυσης επικινδυνότητας θα είναι μια αριθμητική τιμή γνωστή ως συντελεστής κινδύνου (risk factor). Η ταξινόμηση των δεδομένων σε διαφορετικές υποκατηγορίες θα βασίζεται στο γεγονός ότι όλα τα δεδομένα που ανήκουν σε ένα συγκεκριμένο υποσύνολο θα πρέπει να παρουσιάζουν παρόμοιο επίπεδο βαθμού ευαισθησίας για τον οργανισμό. Μερικές ενδεικτικές υποκατηγορίες δεδομένων είναι οι παρακάτω:

- Προσωπικά Δεδομένα (Δεδομένα που προσδιορίζουν μοναδικά ένα άτομο χρησιμοποιώντας ταυτότητες (IDs), προσωπική ή οικογενειακή κατάσταση, επιχειρηματικές δραστηριότητες κτλ.)
- Ευαίσθητα Προσωπικά Δεδομένα (Ιατρικά δεδομένα, καταδίκες κτλ.)
- Οικονομικά Δεδομένα (Δεδομένα που σχετίζονται με χρηματοοικονομικές συναλλαγές, ετήσιους φόρους κτλ.)
- Επιχειρησιακά Δεδομένα (Δεδομένα που δημιουργούνται κατά την εκτέλεση μιας υπηρεσίας, π.χ. cookies, ιδιωτικά αρχεία καταγραφής ενεργειών του οργανισμού κτλ.)
- Άλλα δεδομένα

Όπως ήδη αναφέρθηκε, η εκτίμηση του βαθμού ευαισθησίας των δεδομένων του οργανισμού, μέσω της ανάλυσης επικινδυνότητας, θα βασίζεται στον αντίκτυπο που θα μπορούσε να προκληθεί στον οργανισμό από ένα πιθανό περιστατικό ασφάλειας σε κάθε υποκατηγορία δεδομένων. Ο συνολικός αντίκτυπος για τον οργανισμό θα εξαρτηθεί από τον αντίκτυπο που προκαλείται από κάθε υποκατηγορία δεδομένων χωριστά, υιοθετώντας σε όλες τις περιπτώσεις το χειρότερο σενάριο.

Είσοδος στη Μετρική (Input): Το σύνολο δεδομένων (Data Set - DS) του οργανισμού, ταξινομημένο στις υποκατηγορίες δεδομένων DS1, DS2 … (DSn).

Τρόπος Υπολογισμού Μετρικής (Formulation): Μέσω της ανάλυσης επικινδυνότητας υπολογίζεται ο συντελεστής κινδύνου για κάθε υποκατηγορία δεδομένων, βασιζόμενο στον αντίκτυπο που θα μπορούσε να προκαλέσει στον οργανισμό ένα περιστατικό ασφάλειας.

Επίπεδο 1 – Πολύ χαμηλό : Ελάχιστος αντίκτυπος (Τιμή συντελεστή κινδύνου = 1)

Επίπεδο 2 – Χαμηλό : Μικρός αντίκτυπος (Τιμή συντελεστή κινδύνου = 2)

Επίπεδο 3 – Μεσαίο : Μέτριος αντίκτυπος (Τιμή συντελεστή κινδύνου = 3)

Επίπεδο 4 – Υψηλό : Σημαντικός αντίκτυπος (Τιμή συντελεστή κινδύνου = 4)

Επίπεδο 5 – Πολύ υψηλό : Η βιωσιμότητα του οργανισμού είναι σε κίνδυνο (Τιμή συντελεστή κινδύνου = 5)

Έξοδος της Μετρικής (Final Output): Παράγεται μια μετρική "SeveritySubCatDSx" για κάθε υποκατηγορία δεδομένων x (όπου x=1,2,…,n), που αντιπροσωπεύει τον αντίκτυπο που θα μπορούσε να προκληθεί στον οργανισμό από ένα περιστατικό ασφάλειας που επηρεάζει την υποκατηγορία δεδομένων DSx.

Μετρική 1.2: Ο βαθμός ευαισθησίας ολόκληρου του συνόλου δεδομένων

Περιγραφή Μετρικής: Ο συνολικός βαθμός ευαισθησίας (συντελεστής κινδύνου) των δεδομένων του οργανισμού υπολογίζεται μέσω των συντελεστών κινδύνου κάθε υποκατηγορίας δεδομένων χωριστά (Μετρική 1.1). Ο τρόπος υπολογισμού του συνολικού βαθμού ευαισθησίας είναι ο εξής:

- Εάν όλα τα δεδομένα του οργανισμού έχουν ταξινομηθεί σε μία κατηγορία, ο συνολικός βαθμός ευαισθησίας θα είναι ίσος με το βαθμό ευαισθησίας της συγκεκριμένης κατηγορίας δεδομένων.
- Εάν τα δεδομένα του οργανισμού έχουν ταξινομηθεί σε πολλές υποκατηγορίες δεδομένων, ο συνολικός βαθμός ευαισθησίας των δεδομένων του οργανισμού θα είναι ίση με το μέγιστο βαθμό ευαισθησίας των υποκατηγοριών δεδομένων. Αυτό συμβαίνει επειδή το μέγιστο επίπεδο ευαισθησίας καλύπτει όλες τις υποκατηγορίες δεδομένων.

Ο παραπάνω υπολογισμός απεικονίζεται στο Σχήμα 4.

Είσοδος στη Μετρική (Input): Ο βαθμός ευαισθησίας κάθε υποκατηγορίας δεδομένων (Μετρική 1.1).

Τρόπος Υπολογισμού Μετρικής (Formulation):

SeverityDS = max (SeveritySubCatDS1, … , SeveritySubCatDn)

<u>Περιπτώσεις</u>:

Εάν (n=1) τότε SeverityDS = SeveritySubCatDS

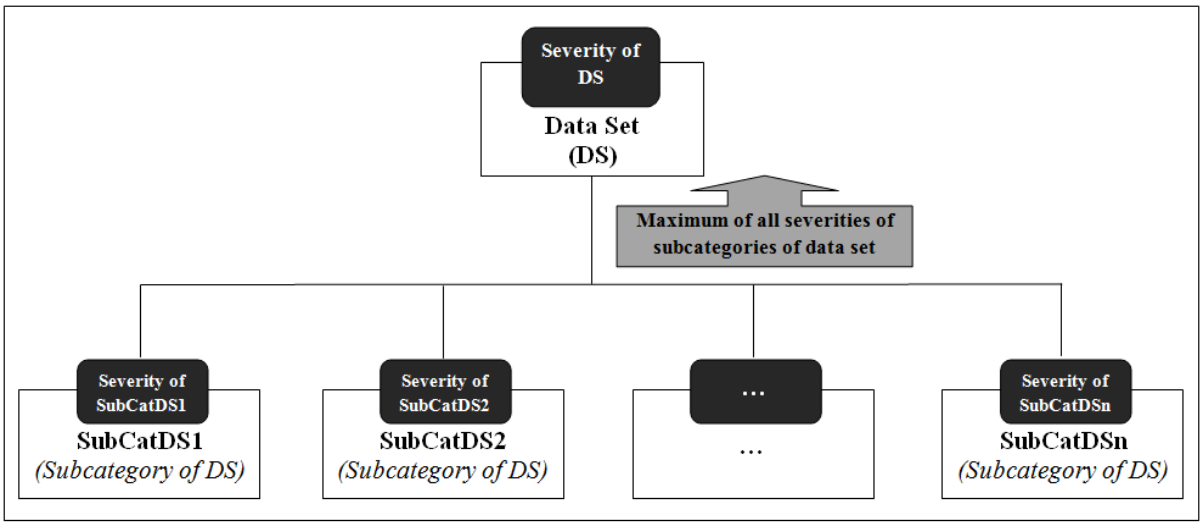
Εάν (n=2) τότε SeverityDS = max (SeveritySubCatDS1, SeveritySubCatDS2)

…

Εάν (n=n) τότε SeverityDS = max (SeveritySubCatDS1, … , SeveritySubCatDn)

Έξοδος της Μετρικής (Final Output): Παράγεται μια μετρική "SeverityDS", που αντιπροσωπεύει το συνολικό βαθμό ευαισθησίας των δεδομένων του οργανισμού.

Εάν ο οργανισμός έχει πολλά διαφορετικά σύνολα δεδομένων, το καθένα χωρισμένο σε διαφορετικές υποκατηγορίες δεδομένων, η παραπάνω μετρική "SeverityDS" θα υπολογιστεί ξεχωριστά για κάθε σύνολο δεδομένων. Η διαδικασία αντιμετώπισης επικινδυνότητας (risk treatment process) θα αρχίσει να εξετάζει πρώτα το σύνολο δεδομένων που παρουσιάζει το μεγαλύτερο βαθμό ευαισθησίας και μετά τα σύνολα δεδομένων με μικρότερο βαθμό ευαισθησίας.



Σχήμα 4: Ο υπολογισμός του συνολικού βαθμού ευαισθησίας ολόκληρου του συνόλου δεδομένων

5.3.3.2 Απαιτήσεις και αρχές ιδιωτικότητας

Εκτός από τις απαιτήσεις ασφάλειας, είναι σημαντικό να ληφθούν υπόψη και να ποσοτικοποιηθούν οι απαιτήσεις ιδιωτικότητας. Βασιζόμενοι στην υπόθεση ότι οι απαιτήσεις ιδιωτικότητας έχουν ληφθεί υπόψη μαζί με τις απαιτήσεις ασφάλειας, και επομένως καλύπτονται από τις ήδη καθορισμένες μετρικές, στην παρούσα ενότητα αξιολογούμε τις αρχές ιδιωτικότητας. Όπως εξηγείται στο [22] [23], οι αρχές ιδιωτικότητας ταξινομούνται σε μια ιεραρχία βημάτων (Σχήμα 3, Σχήμα 2). Παρακάτω, θα αναπτυχθούν μετρικές, που υπολογίζουν τον αντίκτυπο για τον οργανισμό, σε περιπτώσεις όπου ένα ή περισσότερα βήματα δεν ικανοποιούνται.

Ο ορισμός αυτών των μετρικών είναι πολύ πιο περίπλοκος, σε σύγκριση με αυτούς που χρησιμοποιούνται για τον υπολογισμό του βαθμού ευαισθησίας των συνόλων δεδομένων. Πιο συγκεκριμένα, οι μετρικές για τις αρχές ιδιωτικότητας εξαρτώνται από το ιεραρχικό επίπεδο (βήμα) της κάθε αρχής, που είναι σταθερή τιμή, και από τα χαρακτηριστικά του οργανισμού, που είναι μια μεταβλητή που εξαρτάται από τον τύπο και τις δραστηριότητες του οργανισμού.

Μετρική 2.1: Ιεραρχικό επίπεδο κάθε αρχής ιδιωτικότητας

Περιγραφή Μετρικής: Η μεθοδολογία ελέγχου ιδιωτικότητας που προτείνεται στο [23] έχει προκαθορισμένα βήματα. Η συγκεκριμένη μετρική αντικατοπτρίζει την κρισιμότητα του ιεραρχικού επιπέδου στο οποίο ανήκει μια αρχή ιδιωτικότητας, με το πιο κρίσιμο να είναι το Βήμα 1.

Είσοδος στη Μετρική (Input): Τα ιεραρχικά επίπεδα (βήματα) της μεθοδολογίας ελέγχου ιδιωτικότητας που προτείνεται στο [23].

Τρόπος Υπολογισμού Μετρικής (Formulation): Ανάλογα με το ιεραρχικό επίπεδο (βήμα) στο οποίο ανήκει μια αρχή ιδιωτικότητας, δίνεται στην κάθε αρχή ένας σταθερός συντελεστής βαρύτητας «app» (όπου pp = privacy principle (αρχή ιδιωτικότητας)). Η βαρύτητα αντανακλά τη σημαντικότητα του συγκεκριμένου βήματος, και συνεπώς των αρχών ιδιωτικότητας που σχετίζονται με αυτό το βήμα, για τον οργανισμό. Η ελάχιστη τιμή που μπορεί να λάβει ο συντελεστής βαρύτητας καθορίζεται ότι είναι 1. Επιπλέον, η βαρύτητα που σχετίζεται με κάθε βήμα τονίζει τη διαφορετική κρισιμότητα μεταξύ των διάφορων αρχών ιδιωτικότητας.

Πιο συγκεκριμένα:

Βήμα 1 – Αρχή/ές ιδιωτικότητας πολύ μεγάλης σημαντικότητας (Συντελεστής βαρύτητας = 3)

Βήμα 2 – Αρχή/ές ιδιωτικότητας υψηλής σημαντικότητας (Συντελεστής βαρύτητας = 2)

Βήμα 3 – Αρχή/ές ιδιωτικότητας μεσαίας σημαντικότητας (Συντελεστής βαρύτητας = 1)

Βήμα 4 – (Συντελεστής βαρύτητας = SeverityDS)

Ο συντελεστής βαρύτητας για την Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας (Security Safeguards Principle) (Βήμα 4) είναι ο μόνος που δεν είναι σταθερός και επομένως δεν "ευθυγραμμίζεται" με το ιεραρχικό επίπεδο με το οποίο συνδέεται η κάθε αρχή ιδιωτικότητας. Αυτό συμβαίνει γιατί η σημαντικότητα της συγκεκριμένης αρχής εξαρτάται σε μεγάλο βαθμό από το βαθμό ευαισθησίας του συνόλου δεδομένων που εξετάζεται, η οποία αντικατοπτρίζεται από την τιμή SeverityDS (Μετρική 1.2) που υπολογίζεται μέσω της ανάλυσης επικινδυνότητας/PIA.

Οριζόντια/Παράλληλα βήματα – Αρχή/ές ιδιωτικότητας υψηλής σημαντικότητας (Συντελεστής βαρύτητας = 2)

Έξοδος της Μετρικής (Final Output): Παράγεται μια μετρική «app - Συντελεστής βαρύτητας» για κάθε αρχή ιδιωτικότητας, η οποία είναι:

- Συντελεστής βαρύτητας για την αρχή καθορισμού του σκοπού = 3
- Συντελεστής βαρύτητας για την αρχή περιορισμού της συλλογής = 2
- Συντελεστής βαρύτητας για την αρχή διατήρησης ποιότητας των δεδομένων = 2
- Συντελεστής βαρύτητας για την αρχή περιορισμού της χρήσης, διατήρησης και αποκάλυψης = 1
- Συντελεστής βαρύτητας για την αρχή εφαρμογής μέτρων προστασίας ασφάλειας = SeverityDS
- Συντελεστής βαρύτητας για την αρχή διαφάνειας = 2
- Συντελεστής βαρύτητας για την αρχή ατομικής συμμετοχής = 2
- Συντελεστής βαρύτητας για την αρχή λογοδοσίας = 2

Μετρική 2.2: Χαρακτηριστικά οργανισμού

Περιγραφή Μετρικής: Κάθε οργανισμός έχει τον δικό του τύπο, τις δικές του δραστηριότητες, τις δικές του ιδιαιτερότητες κτλ. Αυτά τα χαρακτηριστικά μπορεί να επηρεάσουν τον πιθανό αντίκτυπο ή/και πιθανές συνέπειες που μπορεί να έχει ένας οργανισμός σε περίπτωση περιστατικού παραβίασης ιδιωτικότητας.

Ένα "Διάνυσμα z1...N" χρησιμοποιείται για τη μοντελοποίηση των χαρακτηριστικών του οργανισμού. Κάθε χαρακτηριστικό έχει τη δική του κλίμακα, ανάλογα με το πώς επηρεάζει τον οργανισμό σε περίπτωση περιστατικού παραβίασης ασφάλειας ή ιδιωτικότητας. Για παράδειγμα, το χαρακτηριστικό «Όγκος Δεδομένων» έχει σημαντικότητα α εάν ο οργανισμός διαχειρίζεται πολύ μικρό όγκο προσωπικών δεδομένων, ενώ η σημαντικότητά του είναι β (όπου β > α) εάν ο οργανισμός διατηρεί και επεξεργάζεται σημαντικό όγκο ευαίσθητων δεδομένων.

Είσοδος στη Μετρική (Input): Τα χαρακτηριστικά του οργανισμού.

Τρόπος Υπολογισμού Μετρικής (Formulation): Ανάλογα με τα χαρακτηριστικά (characteristics - CH) του οργανισμού, θα χρησιμοποιηθεί ένα διάνυσμα για την αξιολόγηση του αντικτύπου τους σε ζητήματα ασφάλειας και ιδιωτικότητας.

z1...N = [αριθμητική τιμή για το CH1 από το εύρος: Τιμή1 Τιμή2 ... ΤιμήN]

[αριθμητική τιμή για το CH2 από το εύρος: Τιμή1 Τιμή2 ... ΤιμήN]

[…]

[αριθμητική τιμή για το CHN από το εύρος: Τιμή1 Τιμή2 ... ΤιμήN]

όπου: ενδεικτικά χαρακτηριστικά (CH) και τιμές παρουσιάζονται στον Πίνακα που ακολουθεί.

Α/Α	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΟΡΓΑΝΙΣΜΟΥ (CH 1, 2 … N)	ΕΥΡΟΣ ΤΙΜΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΟΡΓΑΝΙΣΜΟΥ
1.	Όγκος δεδομένων	1: Λίγα
		2: Πολλά
2.	Χρόνος ζωής δεδομένων	1: Δεν τηρούνται καθόλου δεδομένα
		2: Τα δεδομένα τηρούνται για συγκεκριμένο χρονικό διάστημα
		3: Τα δεδομένα τηρούνται για πάντα
3.	Τύπος δεδομένων	1: Δημόσια δεδομένα
		2: Ιδιωτικά Δεδομένα
		3: Ευαίσθητα Προσωπικά Δεδομένα

Α/Α	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΟΡΓΑΝΙΣΜΟΥ (CH 1, 2 … N)	ΕΥΡΟΣ ΤΙΜΩΝ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ ΟΡΓΑΝΙΣΜΟΥ
4.	Τρόπος συλλογής δεδομένων	1: Με γραπτή συγκατάθεση του υποκειμένου
		2: Με ηλεκτρονική συγκατάθεση (π.χ. αποδοχή «όρων και προϋποθέσεων»)
		3: Μέσω άλλης οντότητας (νόμιμης ή μη)
5.	Μέγεθος Οργανισμού	1: Μικρομεσαία Εταιρεία
		2: Μεγάλη Εταιρεία - Διεθνής
		3: Πολυεθνική Εταιρεία
6.	Αριθμός χρηστών	1: Κάτω από 100 χρήστες
		2: 100-1.000 χρήστες
		3: 1.000 χρήστες - …
7.	Νομικό Πλαίσιο της χώρας που έχει ιδρυθεί ο οργανισμός	1: Συμμόρφωση με τους νόμους
		2: Υπάρχουν αποκλίσεις από το Νομικό Πλαίσιο
8.	Νομικό Πλαίσιο της χώρας που λειτουργεί ο οργανισμός	1: Συμμόρφωση με τους νόμους
		2: Υπάρχουν αποκλίσεις από το Νομικό Πλαίσιο
9.	Ενημερότητα / Κουλτούρα Εργαζομένων	1: Είναι ενήμεροι
		2: Δεν είναι ενήμεροι
10.	Ιστορικό περιστατικών	1: Διατηρείται
		2: Δεν διατηρείται

Πίνακας 10: Ενδεικτικά χαρακτηριστικά ενός οργανισμού και αντίστοιχο εύρος τιμών

Έξοδος της Μετρικής (Final Output): Παράγεται μια μετρική "Διάνυσμα z1...N", που παρέχει τη σημαντικότητα κάθε χαρακτηριστικού του οργανισμού.

Μετρική 2.3: Καθορισμός χαρακτηριστικών οργανισμού

Περιγραφή Μετρικής: Η μετρική που παράγει το "Διάνυσμα z1...N" (Μετρική 2.2), το οποίο ορίζεται παραπάνω, παρέχει μια γενική αξιολόγηση του τρόπου με τον οποίο διάφορα χαρακτηριστικά του οργανισμού μπορούν να επηρεάσουν τον αντίκτυπο στον οργανισμό, σε περίπτωση περιστατικού παραβίασης ιδιωτικότητας. Ωστόσο, κάθε οργανισμός μπορεί, ανάλογα με τα δεδομένα που επεξεργάζεται και τον τύπο των δραστηριοτήτων του, να κρίνει τη σημαντικότητα κάθε χαρακτηριστικού διαφορετικά. Για να επιτρέπεται σε κάθε οργανισμό να καθορίσει τη σημαντικότητα των χαρακτηριστικών του, δίνεται ένα «ποσοστό προτεραιότητας (priority percentage)» σε κάθε χαρακτηριστικό.

Είσοδος στη Μετρική (Input): "Διάνυσμα z1...N" (Έξοδος Μετρικής 2.2).

Τρόπος Υπολογισμού Μετρικής (Formulation): Εφαρμόζοντας τα "ποσοστά προτεραιότητας" στο Διάνυσμα z1...N προκύπτει μια νέα μετρική:

*ki = Ποσοστά προτεραιότητας * Διάνυσμα z1...N*

Παράδειγμα:

*ki = (20% * CH1) + (18% * CH2) + (15% * CH3) + (12% * CH4) + (10% * CH5) + (8% * CH6) + (6% * CH7) + (5% * CH8) + (4% * CH9) + (2% * CH10)*

όπου: CH1,2,...,10: Χαρακτηριστικά 1,2,...,10 του οργανισμού (π.χ. όγκος δεδομένων, τύπος δεδομένων, κτλ.)

Έξοδος της Μετρικής (Final Output): Παράγεται μια μετρική «ki», που αντιπροσωπεύει την καθορισμένη (συγκεκριμένη για κάθε οργανισμό) κρισιμότητα των χαρακτηριστικών του σε ζητήματα ιδιωτικότητας.

Μετρική 2.4: Ο βαθμός ευαισθησίας των αρχών ιδιωτικότητας

Περιγραφή Μετρικής: Ο βαθμός ευαισθησίας κάθε αρχής ιδιωτικότητας (privacy principle - pp) εξαρτάται από δύο παράγοντες: τον «app - Συντελεστή βαρύτητας» για κάθε αρχή ιδιωτικότητας (ορίζεται στη Μετρική 2.1) και την σημαντικότητα των χαρακτηριστικών του οργανισμού («ki» που ορίζεται στη Μετρική 2.3).

Είσοδος στη Μετρική (Input): Ο συντελεστής βαρύτητας "app", η μετρική "ki".

Τρόπος Υπολογισμού Μετρικής (Formulation): Η τιμή της μετρικής "Severity PP" υπολογίζεται από τον συντελεστή βαρύτητας "app" και τη μετρική "ki".

*Severity PP = app * ki*

Έξοδος της Μετρικής (Final Output): Παράγεται μια μετρική "Severity PP", που αντιπροσωπεύει το συνολικό βαθμό ευαισθησίας κάθε αρχής ιδιωτικότητας.

5.3.4 Η προτεινόμενη μεθοδολογία αξιολόγησης αντίκτυπου της ιδιωτικότητας

Έχοντας ορίσει τις παραπάνω μετρικές, μπορούν να χρησιμοποιηθούν προκειμένου να καθοριστεί η σημαντικότητα κάθε αρχής ιδιωτικότητας για κάθε διαφορετικό σύνολο δεδομένων του οργανισμού. Η τιμή κάθε κελιού του πίνακα στον παρακάτω πίνακα (Πίνακας 11) υπολογίζεται σύμφωνα με τον ακόλουθο τύπο:

Κελί Πίνακα = Severity DS + Severity PP

Πρέπει να τονιστεί ότι η τιμή που προκύπτει στα κελιά του πίνακα για μια συγκεκριμένη αρχή ιδιωτικότητας και ένα συγκεκριμένο σύνολο δεδομένων, δεν θα είναι απαραίτητα ίδια για διαφορετικούς οργανισμούς, καθώς εξαρτάται από την τιμή της μετρικής «ki» που σχετίζεται με συγκεκριμένα χαρακτηριστικά του οργανισμού.

	Severity DS	[1…7]	[1…7]	…	[1…7]
Severity PP = a_{pp} *** ki =**	**Σύνολα Δεδομένων (Data Sets)** / **Αρχές Ιδιωτικότητας (Privacy Principles)**	**DATA SET 1** *SeverityDS1*	**DATA SET 2** *SeverityDS2*	**…**	**DATA SET N** *SeverityDSn*
[9] * k_1	**Αρχή Καθορισμού του Σκοπού (Purpose Specification Principle)** *SeverityPSP*	**ΕΠΙΠΕΔΟ ΣΗΜΑΝΤΙΚΟΤΗΤΑΣ ΑΣΦΑΛΕΙΑΣ & ΙΔΙΩΤΙΚΟΤΗΤΑΣ**			
[7] * k_2	**Αρχή Περιορισμού της Συλλογής (Collection Limitation Principle)** *SeverityCLP*				

[7] * k_3	**Αρχή Διατήρησης Ποιότητας των Δεδομένων (Data Quality Principle)** *SeverityDQP*	Εύρος τιμών για κάθε ***Κελί Πίνακα*** = [(Severity DSi) + (a_{pp}*ki_{min}) … (Severity DSi) + (a_{pp}*ki_{max})]
[5] * k_4	**Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης (Use, Retention and Disclosure Limitation Principle)** *SeverityURDLP*	
[3] * k_5	**Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας (Security Safeguards Principle)** *SeveritySSP*	
[7] * k_6	**Αρχή Διαφάνειας (Openness Principle)** *SeverityOP*	
[7] * k_7	**Αρχή Ατομικής Συμμετοχής (Individual Participation Principle)** *SeverityIPP*	
[7] * k_8	**Αρχή Λογοδοσίας (Accountability Principle)** *SeverityAP*	

όπου:

- Severity DS (συντελεστή κινδύνου για κάθε σύνολο δεδομένων)
- Severity PP (αρχές ιδιωτικότητας, απαιτήσεις ασφάλειας και ιδιωτικότητας, χαρακτηριστικά οργανισμού)
- Severity PP = a_{pp} * k_i
- a_{pp} = συντελεστής βαρύτητας κάθε αρχής ιδιωτικότητας
- ki = 100% * Vector zi (χαρακτηριστικά)
- z_i = χαρακτηριστικά οργανισμού

Πίνακας 11: Η προτεινόμενη μεθοδολογία αξιολόγησης αντίκτυπου της ιδιωτικότητας

Συνοψίζοντας, η τελική τιμή κάθε κελιού του πίνακα τονίζει την σημαντικότητα κάθε αρχής ιδιωτικότητας για κάθε σύνολο δεδομένων που διατηρεί ο οργανισμός. Η μεθοδολογία που χρησιμοποιείται για τον υπολογισμό αυτού του επιπέδου σημαντικότητας, όπως αναλύθηκε στις παραπάνω ενότητες, λαμβάνει υπόψη τις συνέπειες

που μπορεί να αντιμετωπίσει ο οργανισμός σε περίπτωση περιστατικού παραβίασης ασφάλειας ή ιδιωτικότητας σε ένα συγκεκριμένο σύνολο δεδομένων, τη βαρύτητα κάθε αρχής ιδιωτικότητας και τα μοναδικά χαρακτηριστικά κάθε οργανισμού (Πίνακας 10).

Οι τιμές του πίνακα που προκύπτουν προσφέρουν μια ισχυρή ένδειξη των μέτρων ασφάλειας και των μηχανισμών ιδιωτικότητας που θα πρέπει να υιοθετήσει ένας οργανισμός για την αποτελεσματική προστασία των δεδομένων του. Πιο συγκεκριμένα, η τιμή κάθε κελιού του πίνακα μπορεί να συγκριθεί με την ελάχιστη ή/και τη μέγιστη τιμή που μπορεί να λάβει το συγκεκριμένο κελί, ανάλογα με τα χαρακτηριστικά του οργανισμού (Πίνακας 10) και αν βρεθεί ότι είναι κοντά στη μέγιστη τιμή του κελιού, η σημαντικότητα της αρχής ιδιωτικότητας για το συγκεκριμένο σύνολο δεδομένων θεωρείται ότι είναι πολύ υψηλή.

5.4 Εφαρμογή της προτεινόμενης μεθοδολογίας αξιολόγησης αντίκτυπου της ιδιωτικότητας

Η προτεινόμενη μεθοδολογία αξιολόγησης αντίκτυπου της ιδιωτικότητας (Privacy Impact Assessment - PIA) είναι εφαρμόσιμη σε κάθε οργανισμό που συλλέγει, αποθηκεύει και επεξεργάζεται δεδομένα χρηστών. Σε αυτή την ενότητα, θα εφαρμοστεί, ως παράδειγμα, η παραπάνω μεθοδολογία σε δύο Πληροφοριακά Συστήματα Νοσοκομείων, με διαφορετικά χαρακτηριστικά. Τα αποτελέσματα παρουσιάζονται στις ακόλουθες υποενότητες.

5.4.1 Μελέτη περίπτωσης 1: Εγγραφή εθελοντή αιμοδότη (σε μεγάλο Νοσοκομείο)

5.4.1.1 Υπολογισμός μετρικών

Η προτεινόμενη μεθοδολογία έχει εφαρμοστεί σε ένα πληροφοριακό σύστημα (ΠΣ) που διατηρεί, σε Εθνικό επίπεδο, τους εθελοντές αιμοδότες. Το ΠΣ φιλοξενείται σε ένα μεγάλο Νοσοκομείο. Για την εφαρμογή της μεθοδολογίας συγκεντρώθηκαν οι απαραίτητες πληροφορίες μέσω του παρακάτω προτύπου.

ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

Όνομα νοσοκομείου	Γενικό Νοσοκομείο Χ
Υπεύθυνο άτομο	XXX *(το όνομα διαγράφηκε για λόγους ιδιωτικότητας)*
Στοιχεία επικοινωνίας υπεύθυνου ατόμου	XXX *(τα στοιχεία επικοινωνίας διαγράφηκαν για λόγους ιδιωτικότητας)*
Όνομα Πληροφοριακού Συστήματος	Εθνικό Μητρώο Εθελοντών Αιμοδοτών
Σκοπός Πληροφοριακού Συστήματος	Όταν ένας εθελοντής αιμοδότης επισκέπτεται ένα νοσοκομείο για να δώσει αίμα, για πρώτη φορά, πρέπει να εγγραφεί. Εκτός από τα προσωπικά του στοιχεία, ο αιμοδότης πρέπει να παρέχει ιατρικές πληροφορίες σύμφωνα με τις οποίες το Νοσοκομείο θα κρίνει αν είναι σε θέση ή όχι να γίνει αιμοδότης.
ΣΥΝΟΛΑ ΔΕΔΟΜΕΝΩΝ	
Προσωπικά Δεδομένα	Όνομα, Επώνυμο, Ημερομηνία Γέννησης, Ταυτότητα (προσωπική και αιμοδότη), Όνομα πατέρα, Όνομα μητέρας, Φύλο, Χώρα Γέννησης, Διεύθυνση, Στοιχεία επικοινωνίας, email, Σταθερό Τηλέφωνο, Κινητό Τηλέφωνο, ΑΜΚΑ
Ευαίσθητα Δεδομένα	Ιατρικό Ιστορικό: Παθήσεις - Χρόνια Νοσήματα, Συνήθειες (χόμπι, τατουάζ), Σεξουαλικές Προτιμήσεις, Ιατρικές Επεμβάσεις, Ιατρική Συμπεριφορά (Λήψη Φαρμάκων), Ιστορικό αιμοδοσίας. Αιμοληψία: Ημερομηνία αιμοληψίας, barcode. Λίστα ασθενών που χρησιμοποίησαν αίμα από τον συγκεκριμένο δότη (Επώνυμο Ασθενούς – Όνομα Ασθενούς – Όνομα Πατρός).
ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΝΟΣΟΚΟΜΕΙΟΥ	
Όγκος δεδομένων 1: Λίγα 2: Πολλά	Τιμή=2 Τεράστιος όγκος δεδομένων, λόγω του μεγάλου αριθμού των αιμοδοτών.
Χρόνος ζωής δεδομένων 1: Δεν τηρούνται καθόλου δεδομένα 2: Τα δεδομένα τηρούνται για συγκεκριμένο χρονικό διάστημα 3: Τα δεδομένα τηρούνται για πάντα	Τιμή=2 30 χρόνια διατήρησης δεδομένων.

Τύπος δεδομένων 1: Δημόσια δεδομένα 2: Ιδιωτικά Δεδομένα 3: Ευαίσθητα Προσωπικά Δεδομένα	Τιμή=3 Το νοσοκομείο επεξεργάζεται ευαίσθητα προσωπικά δεδομένα.
Τρόπος συλλογής δεδομένων 1: Με γραπτή συγκατάθεση του υποκειμένου 2: Με ηλεκτρονική συγκατάθεση (π.χ. αποδοχή «όρων και προϋποθέσεων») 3: Μέσω άλλης οντότητας	Τιμή=1 Η συγκατάθεση του χρήστη δίνεται μέσω ενός εγγράφου, το οποίο υπογράφει ο χρήστης.
Μέγεθος Οργανισμού 1: Μικρομεσαία Εταιρεία 2: Μεγάλη Εταιρεία - Διεθνής 3: Πολυεθνική Εταιρεία	Τιμή=2 Τεράστιο νοσοκομείο με μεγάλο πλήθος χρηστών.
Αριθμός χρηστών 1: Κάτω από 100 χρήστες 2: 100-1.000 χρήστες 3: 1.000 χρήστες - ...	Τιμή=3 512.882 εγγεγραμμένοι χρήστες
Νομικό Πλαίσιο της χώρας που έχει ιδρυθεί ο οργανισμός 1: Συμμόρφωση με τους νόμους 2: Υπάρχουν αποκλίσεις από το Νομικό Πλαίσιο	Τιμή=1 Το νοσοκομείο συμμορφώνεται με το Εθνικό νομικό πλαίσιο (νόμιμη βάση επεξεργασίας δεδομένων).
Νομικό Πλαίσιο της χώρας που λειτουργεί ο οργανισμός 1: Συμμόρφωση με τους νόμους 2: Υπάρχουν αποκλίσεις από το Νομικό Πλαίσιο	Τιμή=1 Δεν υπάρχει συνεργασία με άλλες χώρες. Δε γίνεται διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς.
Ενημερότητα / Κουλτούρα Εργαζομένων 1: Είναι ενήμεροι 2: Δεν είναι ενήμεροι	Τιμή=1 Το νοσοκομείο ενημερώνει τους υπαλλήλους του μέσω της πολιτικής ασφάλειας και

	ιδιωτικότητας.
Ιστορικό περιστατικών 1: Διατηρείται 2: Δεν διατηρείται	Τιμή=1 Το νοσοκομείο διατηρεί ιστορικό περιστατικών ασφάλειας και ιδιωτικότητας. Περιγράφεται στην πολιτική ασφάλειας και ιδιωτικότητας.

Πίνακας 12: Πρότυπο συλλογής δεδομένων από Νοσοκομείο

Έχοντας συγκεντρώσει όλες τις απαραίτητες πληροφορίες, έχει παρατηρηθεί ότι το συγκεκριμένο ΠΣ διατηρεί δύο σύνολα δεδομένων: προσωπικά δεδομένα και ευαίσθητα δεδομένα, μαζί με τις υποκατηγορίες τους. Σύμφωνα με την προτεινόμενη μεθοδολογία, θα πρέπει να υπολογιστούν οι ακόλουθες μετρικές:

Μετρική 1.1: Ο βαθμός ευαισθησίας κάθε υποκατηγορίας δεδομένων

Μετρική 1.2: Ο βαθμός ευαισθησίας ολόκληρου του συνόλου δεδομένων

Για το υπό μελέτη ΠΣ, πραγματοποιήθηκε ανάλυση επικινδυνότητας (χρησιμοποιώντας τη μέθοδο CRAMM, αν και θα μπορούσε να χρησιμοποιηθεί οποιαδήποτε άλλη μέθοδος ανάλυσης επικινδυνότητας) προκειμένου να εκτιμηθεί ο αντίκτυπος για τον οργανισμό σε περίπτωση που συμβεί ένα συμβάν ασφάλειας. Για να γίνει αυτό, εντοπίστηκαν οι πιθανές απειλές και οι ευπάθειες του συστήματος που μπορούν να εκμεταλλευτούν οι προαναφερθείσες απειλές. Ο συνδυασμός των:

- Αξία (για τον οργανισμό) των αγαθών (δεδομένων)
- Πιθανότητα εμφάνισης της απειλής
- Βαθμός ευαισθησίας των αναγνωρισμένων ευπαθειών

επέτρεψε να εκτιμηθεί ο συντελεστής κινδύνου για τις εμπλεκόμενες κατηγορίες δεδομένων. Πιο συγκεκριμένα:

Βαθμός ευαισθησίας προσωπικών δεδομένων (Severity PDS): Τιμή συντελεστή κινδύνου = 4 (μέγιστη τιμή όλων των βαθμών ευαισθησίας που εμφανίζονται παρακάτω)

- Όνομα - Επώνυμο, Τιμή συντελεστή κινδύνου = 3
- Ημερομηνία γέννησης, Τιμή συντελεστή κινδύνου = 2
- Δελτίο Ταυτότητας (προσωπική και αιμοδότη), Τιμή συντελεστή κινδύνου = 4

- Όνομα πατέρα - Όνομα μητέρας, Τιμή συντελεστή κινδύνου = 2
- Φύλο, Τιμή συντελεστή κινδύνου = 3
- Χώρα γέννησης, Τιμή συντελεστή κινδύνου = 3
- Διεύθυνση, Τιμή συντελεστή κινδύνου = 2
- Στοιχεία επικοινωνίας, Τιμή συντελεστή κινδύνου = 3
- email, Τιμή συντελεστή κινδύνου = 4
- Αριθμός σταθερού τηλεφώνου - Αριθμός κινητού τηλεφώνου, Τιμή συντελεστή κινδύνου = 2
- ΑΜΚΑ, Τιμή συντελεστή κινδύνου = 4

Βαθμός ευαισθησίας ευαίσθητων προσωπικών δεδομένων (Severity SPDS): Τιμή συντελεστή κινδύνου = 5 (μέγιστη τιμή των βαθμών ευαισθησίας των υποκατηγοριών δεδομένων που εμφανίζονται παρακάτω)

- **Ιατρικό ιστορικό: Τιμή συντελεστή κινδύνου = 5** (μέγιστη τιμή των βαθμών ευαισθησίας που εμφανίζονται παρακάτω)
    - Ασθένειες - Χρόνιες ασθένειες, Τιμή συντελεστή κινδύνου = 5
    - Συνήθειες (χόμπι, τατουάζ), Τιμή συντελεστή κινδύνου = 3
    - Σεξουαλικές Προτιμήσεις, Τιμή συντελεστή κινδύνου = 5
    - Ιατρικές χειρουργικές επεμβάσεις, Τιμή συντελεστή κινδύνου = 4
    - Ιατρική Συμπεριφορά (Λήψη φαρμάκων), Τιμή συντελεστή κινδύνου = 5
    - Ιστορικό αιμοδοσίας, Τιμή συντελεστή κινδύνου = 3
- **Αιμοληψία: Τιμή συντελεστή κινδύνου = 5** (μέγιστη τιμή των βαθμών ευαισθησίας που φαίνονται παρακάτω)
    - Ημερομηνία αιμοληψίας, Τιμή συντελεστή κινδύνου = 2

- Barcode, Τιμή συντελεστή κινδύνου = 5

- **Μια λίστα ασθενών που χρησιμοποίησαν το αίμα από τον συγκεκριμένο δότη: Τιμή συντελεστή κινδύνου = 3** (μέγιστη τιμή των βαθμών ευαισθησίας που φαίνονται παρακάτω)

  - Όνομα ασθενούς – Επώνυμο – Όνομα πατέρα, Τιμή συντελεστή κινδύνου = 3

Με βάση τις υπολογισμένες τιμές των μετρικών Severity PDS και Severity SPDS, αιτιολογείται, όπως αναμενόταν, ότι το σύνολο ευαίσθητων προσωπικών δεδομένων θα πρέπει να προστατεύεται με μεγαλύτερη προτεραιότητα από το σύνολο προσωπικών δεδομένων που διατηρεί το νοσοκομείο.

Μετρική 2.1: Ιεραρχικό επίπεδο κάθε αρχής ιδιωτικότητας

Σύμφωνα με την ενότητα 5.3.2.2, οι συντελεστές βαρύτητας (app) για κάθε αρχή ιδιωτικότητας (pp) είναι:

- Συντελεστής βαρύτητας για την αρχή καθορισμού του σκοπού = 3
- Συντελεστής βαρύτητας για την αρχή περιορισμού της συλλογής = 2
- Συντελεστής βαρύτητας για την αρχή διατήρησης ποιότητας των δεδομένων = 2
- Συντελεστής βαρύτητας για την αρχή περιορισμού της χρήσης, διατήρησης και αποκάλυψης = 1
- Συντελεστής βαρύτητας για την αρχή εφαρμογής μέτρων προστασίας ασφάλειας:
  - για ευαίσθητα προσωπικά δεδομένα: Severity SPDS = 5
  - για προσωπικά δεδομένα: Severity PDS = 4
- Συντελεστής βαρύτητας για την αρχή διαφάνειας = 2
- Συντελεστής βαρύτητας για την αρχή ατομικής συμμετοχής = 2
- Συντελεστής βαρύτητας για την αρχή λογοδοσίας = 2

Μετρική 2.2: Χαρακτηριστικά οργανισμού

Σύμφωνα με τον ορισμό της συγκεκριμένης μετρικής και λαμβάνοντας υπόψη τα χαρακτηριστικά και τις ιδιαιτερότητες του νοσοκομείου, το διάνυσμα z παίρνει τις ακόλουθες τιμές:

Z1-10: z1: [CH1=2] (Τεράστιος όγκος δεδομένων, λόγω του μεγάλου αριθμού των αιμοδοτών)

z2: [CH2=2] (30 χρόνια διατήρησης δεδομένων)

z3: [CH3=3] (Επεξεργασία ευαίσθητων προσωπικών δεδομένων)

z4: [CH4=1] (Τρόπος συλλογής: Η συγκατάθεση του χρήστη δίνεται μέσω ενός εγγράφου, το οποίο υπογράφει ο χρήστης)

z5: [CH5=2] (Τεράστιο Νοσοκομείο)

z6: [CH6=3] (512.882 εγγεγραμμένοι χρήστες)

z7: [CH7=1] (Το Νοσοκομείο συμμορφώνεται με το Εθνικό νομικό πλαίσιο)

z8: [CH8=1] (Δεν υπάρχει συνεργασία με άλλες χώρες. Δε γίνεται διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς.)

z9: [CH9=1] (Το Νοσοκομείο ενημερώνει τους υπαλλήλους του μέσω της πολιτικής ασφάλειας και ιδιωτικότητας)

z10: [CH10=1] (Το Νοσοκομείο διατηρεί ιστορικό περιστατικών ασφάλειας και ιδιωτικότητας. Περιγράφεται στην πολιτική ασφάλειας και ιδιωτικότητας.)

όπου CH1…10 = χαρακτηριστικά του νοσοκομείου

Μετρική 2.3: Καθορισμός χαρακτηριστικών οργανισμού

Σύμφωνα με τον ορισμό της συγκεκριμένης μετρικής, τα γενικά χαρακτηριστικά του νοσοκομείου από CH1 έως CH10 (διάνυσμα z, προηγούμενη μετρική 2.2), υπολογίζονται με

τέτοιο τρόπο ώστε να αντικατοπτρίζουν τη σημαντικότητα κάθε χαρακτηριστικού ανάλογα με τα συγκεκριμένα δεδομένα που επεξεργάζεται το νοσοκομείο και το συγκεκριμένο είδος δραστηριοτήτων που έχει:

- Για το CH1 (Όγκος δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 14%
- Για το CH2 (Χρόνος ζωής δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 10%
- Για το CH3 (Τύπος δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 20%
- Για το CH4 (Τρόπος συλλογής δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 10%
- Για το CH5 (Μέγεθος Οργανισμού) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 14%
- Για το CH6 (Αριθμός Χρηστών) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 14%
- Για το CH7 (Νομικό Πλαίσιο της χώρας που έχει ιδρυθεί ο οργανισμός) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 4%
- Για το CH8 (Νομικό Πλαίσιο της χώρας που λειτουργεί ο οργανισμός) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 4%
- Για το CH9 (Ενημερότητα / Κουλτούρα Εργαζομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 5%
- Για το CH10 (Ιστορικό περιστατικών) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 5%

k10 = (PCH1 * z1) + (PCH2 * z2) + + (PCH3 * z3) + (PCH4 * z4) + (PCH5 * z5) + (PCH6 * z6) + (PCH7 * z7) + (PCH8 * z8) + (PCH9 * z9) + (PCH10 * z10)

= (14% * 2) + (10% * 2) + (20% * 3) + (10% * 1) + (14% * 2) + (14% * 3) + (4% * 1) + (4% * 1) + (5% * 1) + (5% * 1)

= (0,28) + (0,2) + (0,6) + (0,1) + (0,28) + (0,42) + (0,04) + (0,04) + (0,05) + (0,05)

= 2,06

Η τιμή του k αντιπροσωπεύει την σημαντικότητα των διαφόρων χαρακτηριστικών του νοσοκομείου σε θέματα ιδιωτικότητας.

Μετρική 2.4: Ο βαθμός ευαισθησίας των αρχών ιδιωτικότητας

Η σημαντικότητα κάθε αρχής ιδιωτικότητας δίνεται από τον τύπο:

SeverityPP = app * k10

Τα αποτελέσματα είναι:

- SeverityPSP = 3 * 2,06 = 6,18
- SeverityCLP = 2 * 2,06 = 4,12
- SeverityDQP = 2 * 2,06 = 4,12
- SeverityURDP = 1 * 2,06 = 2,06
- SeveritySSP-SPD = 5 * 2,06 = 10,3 (Ευαίσθητα προσωπικά δεδομένα)
- SeveritySSP-PD = 4 * 2,06 = 8,24 (Προσωπικά δεδομένα)
- SeverityOP = 2 * 2,06 = 4,12
- SeverityIPP = 2 * 2,06 = 4,12
- SeverityAP = 2 * 2,06 = 4,12

5.4.1.2 Εφαρμογή μετρικών

Η τιμή κάθε κελιού του παρακάτω πίνακα έχει υπολογιστεί χρησιμοποιώντας τον ακόλουθο τύπο (βλ. ενότητα 5.3.4):

Κελί Πίνακα = Severity DS + Severity PP

και τις τιμές των ακόλουθων μετρικών:

- SeveritySPD = 5

- SeverityPD = 4
- SeverityPSP = 6,18
- SeverityCLP = 4,12
- SeverityDQP = 4,12
- SeverityURDP = 2,06
- SeveritySSP-SPD = 10,3 (Ευαίσθητα προσωπικά δεδομένα)
- SeveritySSP-PD = 8,24 (Προσωπικά δεδομένα)
- SeverityOP = 4,12
- SeverityIPP = 4,12
- SeverityAP = 4,12

Οι υπολογισμένες τιμές κελιών του πίνακα αντικατοπτρίζουν τη σημαντικότητα κάθε ζεύγους "αρχής ιδιωτικότητας – συνόλων δεδομένων" για το υπό εξέταση νοσοκομείο, λαμβάνοντας υπόψη τα συγκεκριμένα χαρακτηριστικά του. Ωστόσο, για να επιτραπεί στο νοσοκομείο να αποφασίσει για τις ενέργειες που θα πρέπει να γίνουν για την προστασία των δεδομένων, είναι απαραίτητο να συγκρίνει κάθε υπολογισμένη τιμή κελιού του πίνακα με τις πιθανές ελάχιστες, μέγιστες και μέσες τιμές του αντίστοιχου κελιού. Από αυτή την οπτική, αυτές οι τιμές έχουν υπολογιστεί για κάθε κελί του πίνακα και φαίνονται παρακάτω (Πίνακας 13).

	Severity DS	**5**	**4**
Severity PP = $a_{pp} * k_i$	**Σύνολα Δεδομένων (Data Sets)** / **Αρχές Ιδιωτικότητας (Privacy Principles)**	**Ευαίσθητα Προσωπικά Δεδομένα**	**Προσωπικά Δεδομένα**
6,18	**Αρχή Καθορισμού του Σκοπού (Purpose Specification Principle)** *SeverityPSP*	[min=8 ... max=13,04] 11,18 (avg=10,52)	[min=7 ... max=12,04] 10,18 (avg=9,52)

	Severity DS	**5**	**4**
Severity PP = $a_{pp} * k_i$	**Σύνολα Δεδομένων (Data Sets)** / **Αρχές Ιδιωτικότητας (Privacy Principles)**	**Ευαίσθητα Προσωπικά Δεδομένα**	**Προσωπικά Δεδομένα**
4,12	**Αρχή Περιορισμού της Συλλογής (Collection Limitation Principle)** *SeverityCLP*	[min=7 ... max=10,36] 9,12 (avg=8,68)	[min=6 ... max=9,36] 8,12 (avg=7,68)
4,12	**Αρχή Διατήρησης Ποιότητας των Δεδομένων (Data Quality Principle)** *SeverityDQP*	[min=7 ... max=10,36] 9,12 (avg=8,68)	[min=6 ... max=9,36] 8,12 (avg=7,68)
2,06	**Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης (Use, Retention and Disclosure Limitation Principle)** *SeverityURDLP*	[min=6 ... max=7,68] 7,06 (avg=6,84)	[min=5 ... max=6,68] 6,06 (avg=5,84)
SPD:10,3 PD:8,24	**Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας (Security Safeguards Principle)** *SeveritySSP*	[min=10 ... max=18,4] 15,3 (avg=14,2)	[min=8 ... max=14,72] 12,24 (avg=11,36)
4,12	**Αρχή Διαφάνειας (Openness Principle)** *SeverityOP*	[min=7 ... max=10,36] 9,12 (avg=8,68)	[min=6 ... max=9,36] 8,12 (avg=7,68)
4,12	**Αρχή Ατομικής Συμμετοχής (Individual Participation Principle)** *SeverityIPP*	[min=7 ... max=10,36] 9,12 (avg=8,68)	[min=6 ... max=9,36] 8,12 (avg=7,68)
4,12	**Αρχή Λογοδοσίας (Accountability Principle)** *SeverityAP*	[min=7 ... max=10,36] 9,12 (avg=8,68)	[min=6 ... max=9,36] 8,12 (avg=7,68)

Πίνακας 13: Η εφαρμογή της προτεινόμενης μεθοδολογίας αξιολόγησης αντίκτυπου της ιδιωτικότητας για το Νοσοκομείο

5.4.2 Μελέτη περίπτωσης 2: Εγγραφή ασθενή (σε Κέντρο Υγείας)

5.4.2.1 Υπολογισμός μετρικών

Ομοίως με το Παράδειγμα 1, η προτεινόμενη μεθοδολογία έχει επίσης εφαρμοστεί σε ένα πληροφοριακό σύστημα (ΠΣ) ενός τοπικού νοσοκομείου (Κέντρο Υγείας) σε μια μικρή πόλη. Το συγκεκριμένο ΠΣ χειρίζεται την εγγραφή των ασθενών προκειμένου το Κέντρο Υγείας να διατηρεί τα ιατρικά τους αρχεία. Για την εφαρμογή της μεθοδολογίας συγκεντρώθηκαν οι απαραίτητες πληροφορίες μέσω του παρακάτω προτύπου.

ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ	
Όνομα νοσοκομείου	Κέντρο Υγείας Υ
Υπεύθυνο άτομο	XXX *(το όνομα διαγράφηκε για λόγους ιδιωτικότητας)*
Στοιχεία επικοινωνίας υπεύθυνου ατόμου	XXX *(τα στοιχεία επικοινωνίας διαγράφηκαν για λόγους ιδιωτικότητας)*
Όνομα Πληροφοριακού Συστήματος	Εγγραφή ασθενούς στο πληροφοριακό σύστημα του Κέντρου Υγείας
Σκοπός Πληροφοριακού Συστήματος	Το Κέντρο Υγείας χρειάζεται να τηρεί ιατρικά αρχεία των ασθενών. Για να γίνει αυτό, ο ασθενής πρέπει πρώτα να εγγραφεί στο σύστημα.
ΣΥΝΟΛΑ ΔΕΔΟΜΕΝΩΝ	
Προσωπικά Δεδομένα	Όνομα, Επώνυμο, Ημερομηνία Γέννησης, Ταυτότητα, Όνομα πατέρα, Όνομα μητέρας, Φύλο, Χώρα Γέννησης, Διεύθυνση, Στοιχεία επικοινωνίας, email, Σταθερό Τηλέφωνο, Κινητό Τηλέφωνο, ΑΜΚΑ
Ευαίσθητα Δεδομένα	Ιατρικό Ιστορικό ασθενούς: Παθήσεις ασθενούς - Χρόνια Νοσήματα, Συνήθειες ασθενούς (χόμπι, τατουάζ), Σεξουαλικές Προτιμήσεις ασθενούς, Ιατρικές Επεμβάσεις ασθενούς, Ιατρική Συμπεριφορά ασθενούς (Λήψη Φαρμάκων). Ιατρικό Ιστορικό συγγενών: Νοσήματα συγγενών - Χρόνια Νοσήματα, κληρονομικότητα.
ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΕΝΤΡΟΥ ΥΓΕΙΑΣ	
Όγκος δεδομένων 1: Λίγα	Τιμή=1 Μικρός όγκος δεδομένων, λόγω του αριθμού των ασθενών.

2: Πολλά	
Χρόνος ζωής δεδομένων 1: Δεν τηρούνται καθόλου δεδομένα 2: Τα δεδομένα τηρούνται για συγκεκριμένο χρονικό διάστημα 3: Τα δεδομένα τηρούνται για πάντα	Τιμή=2 30 χρόνια διατήρησης δεδομένων.
Τύπος δεδομένων 1: Δημόσια δεδομένα 2: Ιδιωτικά Δεδομένα 3: Ευαίσθητα Προσωπικά Δεδομένα	Τιμή=3 Το κέντρο υγείας επεξεργάζεται ευαίσθητα προσωπικά δεδομένα.
Τρόπος συλλογής δεδομένων 1: Με γραπτή συγκατάθεση του υποκειμένου 2: Με ηλεκτρονική συγκατάθεση (π.χ. αποδοχή «όρων και προϋποθέσεων») 3: Μέσω άλλης οντότητας	Τιμή=1 Η συγκατάθεση του ασθενή δίνεται μέσω ενός εγγράφου, το οποίο υπογράφει ο ασθενής.
Μέγεθος Οργανισμού 1: Μικρομεσαία Εταιρεία 2: Μεγάλη Εταιρεία - Διεθνής 3: Πολυεθνική Εταιρεία	Τιμή=1 Τοπικό κέντρο υγείας με μικρό πλήθος ασθενών.
Αριθμός χρηστών 1: Κάτω από 100 χρήστες 2: 100-1.000 χρήστες 3: 1.000 χρήστες - ...	Τιμή=2 842 εγγεγραμμένοι ασθενείς στο πληροφοριακό σύστημα
Νομικό Πλαίσιο της χώρας που έχει ιδρυθεί ο οργανισμός 1: Συμμόρφωση με τους νόμους 2: Υπάρχουν αποκλίσεις από το Νομικό Πλαίσιο	Τιμή=1 Το κέντρο υγείας συμμορφώνεται με το Εθνικό νομικό πλαίσιο (νόμιμη βάση επεξεργασίας δεδομένων).
Νομικό Πλαίσιο της χώρας που	Τιμή=1

λειτουργεί ο οργανισμός 1: Συμμόρφωση με τους νόμους 2: Υπάρχουν αποκλίσεις από το Νομικό Πλαίσιο	Δεν υπάρχει συνεργασία με άλλες χώρες. Δε γίνεται διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς.
Ενημερότητα / Κουλτούρα Εργαζομένων 1: Είναι ενήμεροι 2: Δεν είναι ενήμεροι	Τιμή=1 Το κέντρο υγείας ενημερώνει τους υπαλλήλους του μέσω της πολιτικής ασφάλειας και ιδιωτικότητας.
Ιστορικό περιστατικών 1: Διατηρείται 2: Δεν διατηρείται	Τιμή=2 Το κέντρο υγείας δεν διατηρεί ιστορικό περιστατικών ασφάλειας και ιδιωτικότητας. Βρίσκεται σε μια μικρή πόλη χωρίς τις κατάλληλες υποδομές για την προστασία των δεδομένων τους.

Πίνακας 14: Πρότυπο συλλογής δεδομένων από Κέντρο Υγείας

Έχοντας συγκεντρώσει όλες τις απαραίτητες πληροφορίες, έχει παρατηρηθεί ότι το συγκεκριμένο ΠΣ διατηρεί δύο σύνολα δεδομένων: προσωπικά δεδομένα και ευαίσθητα δεδομένα, μαζί με τις υποκατηγορίες τους. Σύμφωνα με την προτεινόμενη μεθοδολογία, θα πρέπει να υπολογιστούν οι ακόλουθες μετρικές:

Μετρική 1.1: Ο βαθμός ευαισθησίας κάθε υποκατηγορίας δεδομένων

Μετρική 1.2: Ο βαθμός ευαισθησίας ολόκληρου του συνόλου δεδομένων

Ομοίως με το Παράδειγμα 1, οι συντελεστές κινδύνου για τις εμπλεκόμενες κατηγορίες δεδομένων έχουν υπολογιστεί όπως φαίνεται παρακάτω:

Βαθμός ευαισθησίας προσωπικών δεδομένων (Severity PDS): Τιμή συντελεστή κινδύνου = 3 (μέγιστη τιμή όλων των βαθμών ευαισθησίας που εμφανίζονται παρακάτω)

- Όνομα - Επώνυμο, Τιμή συντελεστή κινδύνου = 3
- Ημερομηνία γέννησης, Τιμή συντελεστή κινδύνου = 2
- Δελτίο Ταυτότητας, Τιμή συντελεστή κινδύνου = 3
- Όνομα πατέρα - Όνομα μητέρας, Τιμή συντελεστή κινδύνου = 2

- Φύλο, Τιμή συντελεστή κινδύνου = 3
- Χώρα γέννησης, Τιμή συντελεστή κινδύνου = 3
- Διεύθυνση, Τιμή συντελεστή κινδύνου = 2
- Στοιχεία επικοινωνίας, Τιμή συντελεστή κινδύνου = 2
- email, Τιμή συντελεστή κινδύνου = 3
- Αριθμός σταθερού τηλεφώνου - Αριθμός κινητού τηλεφώνου, Τιμή συντελεστή κινδύνου = 2
- ΑΜΚΑ, Τιμή συντελεστή κινδύνου = 3

Βαθμός ευαισθησίας ευαίσθητων προσωπικών δεδομένων (Severity SPDS): Τιμή συντελεστή κινδύνου = 4 (μέγιστη τιμή των βαθμών ευαισθησίας των υποκατηγοριών δεδομένων που εμφανίζονται παρακάτω)

- **Ιατρικό ιστορικό ασθενούς: Τιμή συντελεστή κινδύνου = 4** (μέγιστη τιμή των βαθμών ευαισθησίας που εμφανίζονται παρακάτω)
    - Ασθένειες - Χρόνιες ασθένειες ασθενούς, Τιμή συντελεστή κινδύνου = 4
    - Συνήθειες ασθενούς (χόμπι, τατουάζ), Τιμή συντελεστή κινδύνου = 3
    - Σεξουαλικές Προτιμήσεις ασθενούς, Τιμή συντελεστή κινδύνου = 3
    - Ιατρικές χειρουργικές επεμβάσεις ασθενούς, Τιμή συντελεστή κινδύνου = 4
    - Ιατρική Συμπεριφορά ασθενούς (Λήψη φαρμάκων), Τιμή συντελεστή κινδύνου = 3
- **Ιατρικό Ιστορικό συγγενών: Τιμή συντελεστή κινδύνου = 4** (μέγιστη τιμή των βαθμών ευαισθησίας που φαίνονται παρακάτω)
    - Ασθένειες - Χρόνιες ασθένειες συγγενών, Τιμή συντελεστή κινδύνου = 4
    - Κληρονομικότητα, Τιμή συντελεστή κινδύνου = 4

Με βάση τις υπολογισμένες τιμές των μετρικών Severity PDS και Severity SPDS, αιτιολογείται, όπως αναμενόταν, ότι το σύνολο ευαίσθητων προσωπικών δεδομένων θα

πρέπει να προστατεύεται με μεγαλύτερη προτεραιότητα από το σύνολο προσωπικών δεδομένων που διατηρεί το κέντρο υγείας.

Μετρική 2.1: Ιεραρχικό επίπεδο κάθε αρχής ιδιωτικότητας

Σύμφωνα με την ενότητα 5.3.2.2, οι συντελεστές βαρύτητας (app) για κάθε αρχή ιδιωτικότητας (pp) είναι:

- Συντελεστής βαρύτητας για την αρχή καθορισμού του σκοπού = 3
- Συντελεστής βαρύτητας για την αρχή περιορισμού της συλλογής = 2
- Συντελεστής βαρύτητας για την αρχή διατήρησης ποιότητας των δεδομένων = 2
- Συντελεστής βαρύτητας για την αρχή περιορισμού της χρήσης, διατήρησης και αποκάλυψης = 1
- Συντελεστής βαρύτητας για την αρχή εφαρμογής μέτρων προστασίας ασφάλειας:
    - για ευαίσθητα προσωπικά δεδομένα: Severity SPDS = 3
    - για προσωπικά δεδομένα: Severity PDS = 3
- Συντελεστής βαρύτητας για την αρχή διαφάνειας = 2
- Συντελεστής βαρύτητας για την αρχή ατομικής συμμετοχής = 2
- Συντελεστής βαρύτητας για την αρχή λογοδοσίας = 2

Μετρική 2.2: Χαρακτηριστικά οργανισμού

Σύμφωνα με τον ορισμό της συγκεκριμένης μετρικής και λαμβάνοντας υπόψη τα χαρακτηριστικά και τις ιδιαιτερότητες του κέντρου υγείας, το διάνυσμα z παίρνει τις ακόλουθες τιμές:

Z1-10: z1: [CH1=1] (Μικρός όγκος δεδομένων, λόγω του αριθμού των ασθενών)

z2: [CH2=2] (30 χρόνια διατήρησης δεδομένων)

z3: [CH3=3] (Επεξεργασία ευαίσθητων προσωπικών δεδομένων)

z4: [CH4=1] (Τρόπος συλλογής: Η συγκατάθεση του ασθενή δίνεται μέσω ενός εγγράφου, το οποίο υπογράφει ο ασθενής)

z5: [CH5=1] (Τοπικό κέντρο υγείας)

z6: [CH6=2] (842 εγγεγραμμένοι ασθενείς στο ΠΣ)

z7: [CH7=1] (Το κέντρο υγείας συμμορφώνεται με το Εθνικό νομικό πλαίσιο)

z8: [CH8=1] (Δεν υπάρχει συνεργασία με άλλες χώρες. Δε γίνεται διαβίβαση δεδομένων σε τρίτες χώρες ή διεθνείς οργανισμούς.)

z9: [CH9=1] (Το κέντρο υγείας ενημερώνει τους υπαλλήλους του μέσω της πολιτικής ασφάλειας και ιδιωτικότητας)

z10: [CH10=2] (Το κέντρο υγείας δεν διατηρεί ιστορικό περιστατικών ασφάλειας και ιδιωτικότητας. Βρίσκεται σε μια μικρή πόλη χωρίς τις κατάλληλες υποδομές για την προστασία των δεδομένων τους..)

όπου CH1…10 = χαρακτηριστικά του κέντρου υγείας

Μετρική 2.3: Καθορισμός χαρακτηριστικών οργανισμού

Ομοίως με το Παράδειγμα 1, ο υπολογισμός του διανύσματος z από το συγκεκριμένο τοπικό κέντρο υγείας έχει υπολογιστεί ως εξής:

- Για το CH1 (Όγκος δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 12%
- Για το CH2 (Χρόνος ζωής δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 8%
- Για το CH3 (Τύπος δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 24%
- Για το CH4 (Τρόπος συλλογής δεδομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 14%

- Για το CH5 (Μέγεθος Οργανισμού) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 10%
- Για το CH6 (Αριθμός Χρηστών) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 9%
- Για το CH7 (Νομικό Πλαίσιο της χώρας που έχει ιδρυθεί ο οργανισμός) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 7%
- Για το CH8 (Νομικό Πλαίσιο της χώρας που λειτουργεί ο οργανισμός) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 7%
- Για το CH9 (Ενημερότητα / Κουλτούρα Εργαζομένων) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 5%
- Για το CH10 (Ιστορικό περιστατικών) το ποσοστό βαρύτητας (PCH1) έχει οριστεί σε: 4%

k10 = (PCH1 * z1) + (PCH2 * z2) + + (PCH3 * z3) + (PCH4 * z4) + (PCH5 * z5) + (PCH6 * z6) + (PCH7 * z7) + (PCH8 * z8) + (PCH9 * z9) + (PCH10 * z10)

= (12% * 1) + (8% * 2) + (24% * 3) + (14% * 1) + (10% * 1) + (9% * 2) + (7% * 1) + (7% * 1) + (5% * 1) + (4% * 2)

= (0,12) + (0,16) + (0,72) + (0,14) + (0,1) + (0,18) + (0,07) + (0,07) + (0,05) + (0,08)

= 1,69

Η τιμή του k αντιπροσωπεύει την σημαντικότητα των διαφόρων χαρακτηριστικών του κέντρου υγείας σε θέματα ιδιωτικότητας.

Μετρική 2.4: Ο βαθμός ευαισθησίας των αρχών ιδιωτικότητας

Η σημαντικότητα κάθε αρχής ιδιωτικότητας δίνεται από τον τύπο:

SeverityPP = app * k10

Τα αποτελέσματα είναι:

- SeverityPSP = 3 * 1,69 = 5,07
- SeverityCLP = 2 * 1,69 = 3,38
- SeverityDQP = 2 * 1,69 = 3,38
- SeverityURDP = 1 * 1,69 = 1,69
- SeveritySSP-SPD = 4 * 1,69 = 6,76 (Ευαίσθητα προσωπικά δεδομένα)
- SeveritySSP-PD = 3 * 1,69 = 5,07 (Προσωπικά δεδομένα)
- SeverityOP = 2 * 1,69 = 3,38
- SeverityIPP = 2 * 1,69 = 3,38
- SeverityAP = 2 * 1,69 = 3,38

5.4.2.2 Εφαρμογή μετρικών

Η τιμή κάθε κελιού του παρακάτω πίνακα έχει υπολογιστεί χρησιμοποιώντας τον ακόλουθο τύπο (βλ. ενότητα 5.3.4):

Κελί Πίνακα = Severity DS + Severity PP

και τις τιμές των ακόλουθων μετρικών:

- SeveritySPD = 4
- SeverityPD = 3
- SeverityPSP = 5,07
- SeverityCLP = 3,38
- SeverityDQP = 3,38
- SeverityURDP = 1,69
- SeveritySSP-SPD = 6,76 (Ευαίσθητα προσωπικά δεδομένα)
- SeveritySSP-PD = 5,07 (Προσωπικά δεδομένα)

- SeverityOP = 3,38
- SeverityIPP = 3,38
- SeverityAP = 3,38

Για τους λόγους που περιγράφονται στο Παράδειγμα 1, τα κελιά του πίνακα παρακάτω (Πίνακας 15) περιλαμβάνουν τις ελάχιστες τιμές, τις μέγιστες τιμές και το μέσο όρο.

	Severity DS	**4**	**3**
Severity PP = $a_{pp} * k_i$	**Σύνολα Δεδομένων (Data Sets)** / **Αρχές Ιδιωτικότητας (Privacy Principles)**	**Ευαίσθητα Προσωπικά Δεδομένα**	**Προσωπικά Δεδομένα**
5,07	**Αρχή Καθορισμού του Σκοπού (Purpose Specification Principle)** *SeverityPSP*	[min=7 ... max=11,95] 9,07 (avg=9,475)	[min=6 ... max=10,95] 8,07 (avg=8,475)
3,38	**Αρχή Περιορισμού της Συλλογής (Collection Limitation Principle)** *SeverityCLP*	[min=6 ... max=9,3] 7,38 (avg=7,65)	[min=5 ... max=8,3] 6,38 (avg=6,65)
3,38	**Αρχή Διατήρησης Ποιότητας των Δεδομένων (Data Quality Principle)** *SeverityDQP*	[min=6 ... max=9,3] 7,38 (avg=7,65)	[min=5 ... max=8,3] 6,38 (avg=6,65)
1,69	**Αρχή Περιορισμού της Χρήσης, Διατήρησης και Αποκάλυψης (Use, Retention and Disclosure Limitation Principle)** *SeverityURDLP*	[min=5 ... max=6,65] 5,69 (avg=5,825)	[min=4 ... max=5,65] 4,69 (avg=4,825)
SPD:6,76 PD:5,07	**Αρχή Εφαρμογής Μέτρων Προστασίας Ασφάλειας (Security Safeguards Principle)** *SeveritySSP*	[min=8 ... max=14,6] 10,76 (avg=11,3)	[min=6 ... max=10,95] 8,07 (avg=8,475)
3,38	**Αρχή Διαφάνειας (Openness**	[min=6 ... max=9,3]	[min=5 ... max=8,3]

	Severity DS	**4**	**3**
Severity PP = $a_{pp} * k_i$	**Σύνολα Δεδομένων (Data Sets)** / **Αρχές Ιδιωτικότητας (Privacy Principles)**	**Ευαίσθητα Προσωπικά Δεδομένα**	**Προσωπικά Δεδομένα**
	Principle) *SeverityOP*	7,38 (avg=7,65)	6,38 (avg=6,65)
3,38	**Αρχή Ατομικής Συμμετοχής (Individual Participation Principle)** *SeverityIPP*	[min=6 ... max=9,3] 7,38 (avg=7,65)	[min=5 ... max=8,3] 6,38 (avg=6,65)
3,38	**Αρχή Λογοδοσίας (Accountability Principle)** *SeverityAP*	[min=6 ... max=9,3] 7,38 (avg=7,65)	[min=5 ... max=8,3] 6,38 (avg=6,65)

Πίνακας 15: Η εφαρμογή της προτεινόμενης μεθοδολογίας αξιολόγησης αντίκτυπου της ιδιωτικότητας για το Κέντρο Υγείας

5.4.3 Αιτιολόγηση της εφαρμογής της προτεινόμενης μεθοδολογίας και σύγκριση των αποτελεσμάτων της

Η εφαρμογή της προτεινόμενης μεθοδολογίας έχει επικυρωθεί μέσω των προαναφερθέντων μελετών περίπτωσης. Πιο συγκεκριμένα, έχει αποδειχθεί ότι η μεθοδολογία μπορεί να καλύψει όλες τις παραμέτρους που καλύπτουν άλλες υπάρχουσες μεθοδολογίες εκτίμησης αντικτύπου της ιδιωτικότητας και επιπλέον επιτυγχάνει να ποσοτικοποιήσει, μέσω των προτεινόμενων μετρικών, τον αντίκτυπο που μπορεί να προκαλέσει ένα πιθανό περιστατικό στον οργανισμό. Αυτή η ποσοτικοποίηση λαμβάνει υπόψη συγκεκριμένα χαρακτηριστικά του οργανισμού καθώς και την ιεράρχηση των αρχών ιδιωτικότητας για αυτόν τον οργανισμό.

Επιπλέον, λαμβάνοντας υπόψη τα αποτελέσματα που προέκυψαν από τις προηγούμενες μελέτες περίπτωσης, μπορεί να αιτιολογηθεί η εγκυρότητα της προτεινόμενης μεθοδολογίας από τα παρακάτω σημεία:

- Όλες οι τιμές των κελιών του πίνακα βρέθηκαν να είναι υψηλότερες από τη μέση τιμή (μέσο όρο) κάθε κελιού. Αυτό είναι αναμενόμενο, καθώς τα δεδομένα που συλλέγονται και από τους δύο οργανισμούς (Νοσοκομεία) είναι προσωπικά ή/και ευαίσθητα δεδομένα και όχι δημόσια/μη-κρίσιμα δεδομένα.

- Οι τιμές των κελιών του πίνακα που υπολογίζονται για το σύνολο ευαίσθητων δεδομένων είναι υψηλότερες από τις αντίστοιχες τιμές κελιών για το σύνολο προσωπικών δεδομένων. Αυτό είναι ορθό, καθώς η κρισιμότητα των ευαίσθητων δεδομένων είναι υψηλότερη σε σύγκριση με αυτή των προσωπικών δεδομένων.

- Οι τιμές των κελιών του πίνακα για τη μελέτη περίπτωσης 1 είναι υψηλότερες σε σύγκριση με τις αντίστοιχες τιμές κελιών για τη μελέτη περίπτωσης 2. Αυτό είναι επίσης αναμενόμενο, αφού το Νοσοκομείο της μελέτης περίπτωσης 1 είναι ένα γενικό νοσοκομείο με τεράστιο αριθμό ασθενών ενώ για τη μελέτη περίπτωσης 2 το νοσοκομείο είναι Κέντρο Υγείας με αρκετά μικρότερο αριθμό ασθενών. Οι προαναφερθείσες διαφορές τροφοδοτούν την προτεινόμενη μεθοδολογία με διαφορετικά χαρακτηριστικά και συντελεστές βαρύτητας για τους δύο οργανισμούς.

5.5 Συμπεράσματα

Στις παραπάνω ενότητες αναλύθηκε μια νέα μεθοδολογία Αξιολογησης Αντικτύπου της Ιδιωτικότητας (Privacy Impact Assessment - PIA) η οποία χρησιμοποιεί μετρικές και λαμβάνει υπόψη τις ιδιαιτερότητες και άλλα χαρακτηριστικά ενός οργανισμού. Στόχος είναι να βοηθηθούν οι οργανισμοί ώστε να μπορέσουν να εκτιμήσουν την σημαντικότητα πιθανών παραβιάσεων της ιδιωτικότητας και, ως εκ τούτου, να επιλέξουν τα κατάλληλα μέτρα ασφάλειας για την προστασία των δεδομένων που συλλέγουν, επεξεργάζονται και αποθηκεύουν.

Όσον αφορά τον εντοπισμό και την αξιολόγηση των κινδύνων, αυτό πραγματοποιείται μέσω της μεθοδολογίας διαχείρισης επικινδυνότητας ή/και μελέτης PIA που ο οργανισμός αποφασίζει να χρησιμοποιήσει, ενώ για την αντιμετώπιση των κινδύνων Θα μπορούσε να αναπτυχθεί μια νέα μεθοδολογία που θα βελτιώσει την προτεινόμενη μεθοδολογία με τρόπο που θα είναι σε θέση να υπολογίσει εκ νέου την σημαντικότητα

λαμβάνοντας υπόψη την καταλληλότητα/αποτελεσματικότητα των εφαρμοζόμενων τεχνικών αντιμετώπισης. Με αυτό τον τρόπο η νέα μεθοδολογία θα ακολουθεί τη λογική του μοντέλου Plan-Do-Check-Act (PDCA) του προτύπου ISO 27000. Επιπλέον, σε αυτή τη νέα μεθοδολογία θα μπορούσαν να ενσωματωθούν οι απαιτήσεις που θέτει ο νέος Κανονισμός Γενικής Προστασίας Δεδομένων (GDPR).

6 Κεφάλαιο 6: Ο ρόλος και οι απαιτήσεις του ΓΚΠΔ σε περιβάλλοντα υπολογιστικού νέφους

6.1 Εισαγωγή

Το υπολογιστικό νέφος (cloud computing) είναι μια τεχνολογία με τεράστια εξάπλωση σε πολλούς τομείς της Τεχνολογίας Πληροφοριών και Επικοινωνιών (ΤΠΕ). Πολλές έρευνες έχουν διεξαχθεί τα τελευταία χρόνια σχετικά με ζητήματα ασφάλειας, ιδιωτικότητας και εμπιστοσύνης (trust) σε περιβάλλοντα υπολογιστικού νέφους και ιδιαίτερα σε διαμοιραζόμενα περιβάλλοντα υπολογιστικού νέφους. Η έρευνα σε αυτόν τον τομέα είναι «ανοιχτή», επιβάλλοντας, ακόμη και σήμερα, εμπόδια στην υιοθέτηση του υπολογιστικού νέφους.

Από τον Μάιο του 2018 [4], οι πάροχοι υπολογιστικού νέφους θα πρέπει να συμμορφώνονται με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Ο ΓΚΠΔ έχει έναν πολύ βασικό στόχο: να εισαγάγει ένα υψηλότερο και πιο συνεπές επίπεδο προστασίας προσωπικών δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση (ΕΕ), το οποίο θα δώσει στους πολίτες τον έλεγχο των προσωπικών τους δεδομένων και θα απλοποιήσει το κανονιστικό/ρυθμιστικό περιβάλλον για τις επιχειρήσεις. Ο κανονισμός ισχύει για όλες τις εταιρείες που διατηρούν ή επεξεργάζονται δεδομένα πολιτών της ΕΕ, συμπεριλαμβανομένων των χρηστών υπολογιστικού νέφους, των παρόχων και των υπεργολάβων (sub-contractors) τους.

Το υπάρχον εθνικό νομικό πλαίσιο, που βασίζεται στην Οδηγία 95/46 της ΕΕ για την Προστασία Δεδομένων [49], δεν έχει επιτύχει εναρμόνιση των κανόνων προστασίας δεδομένων προσωπικού χαρακτήρα μεταξύ των κρατών μελών. Αυτές οι παραλλαγές, και μερικές φορές οι αντικρουόμενοι κανόνες, περιπλέκουν τις απαιτήσεις και τις διαδικασίες των επιχειρήσεων, ειδικά στη σημερινή ψηφιακή εποχή που τα δεδομένα ρέουν όλο και περισσότερο πέρα των συνόρων του κάθε κράτους μέλους. Εφαρμόζοντάς τον, ο ΓΚΠΔ στοχεύει να διασφαλίσει ότι οι ίδιοι κανόνες προστασίας δεδομένων θα ισχύουν ομοιόμορφα σε ολόκληρη την ΕΕ.

Ενώ πολλές από τις έννοιες και τις αρχές του ΓΚΠΔ έχουν βασιστεί στην Οδηγία 95/46 για την Προστασία Δεδομένων, ο κανονισμός εισάγει σημαντικούς νέους κανόνες και βελτιώσεις. Η έμφαση δίνεται στον τρόπο με τον οποίο χειρίζονται και προστατεύονται οι

προσωπικές πληροφορίες από οργανισμούς εντός της ΕΕ – και, σε ορισμένες περιπτώσεις, εκτός ΕΕ. Για τους παρόχους υπολογιστικού νέφους, οι νέες υποχρεώσεις είναι αρκετά εκτενείς και απαιτητικές. Οι παρακάτω ενότητες παρέχουν μια σύντομη καθοδήγηση σχετικά με το τι θα πρέπει να εξετάσει ένας πάροχος υπολογιστικού νέφους και ποιες περαιτέρω ενέργειες πρέπει να λάβει για να συμμορφωθεί με τον ΓΚΠΔ [72].

6.2 Απαιτήσεις του ΓΚΠΔ

Κατά τη διαδικασία συμμόρφωσης με τον ΓΚΠΔ σε περιβάλλοντα υπολογιστικού νέφους θα πρέπει να ληφθούν υπόψη αρκετές απαιτήσεις του κανονισμού, όπως παρουσιάζονται αναλυτικά στις παρακάτω υποενότητες.

6.2.1 Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope)

Ο ΓΚΠΔ ισχύει για τους «υπεύθυνους επεξεργασίας (controllers)» του υπολογιστικού νέφους (οι οποίοι αποφασίζουν πώς και γιατί γίνεται η επεξεργασία των προσωπικών δεδομένων) και τους «εκτελούντες την επεξεργασία (processors)» (οι οποίοι επεξεργάζονται προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας). Πιο συγκεκριμένα, ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία του υπολογιστικού νέφους που είναι εγκατεστημένος στην ΕΕ θα πρέπει να συμμορφώνεται με τις απαιτήσεις του ΓΚΠΔ. Τα υπολογιστικά νέφη που δεν έχουν έδρα στην ΕΕ αλλά προσφέρουν υπηρεσίες σε πολίτες της Ευρωπαϊκής Ένωσης ή περιλαμβάνουν ενέργειες παρακολούθησης που λαμβάνουν χώρα στην Ευρωπαϊκή Ένωση θα πρέπει επίσης, να συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ.

Ως έλεγχος, στο εάν ένα υπολογιστικό νέφος πρέπει να πληροί τις απαιτήσεις του ΓΚΠΔ ή όχι, κρίνεται απαραίτητη η εφαρμογή ενός μηχανισμού ελέγχου-ειδοποίησης που θα ελέγχει εάν ένας χρήστης υπολογιστικού νέφους (Software as a service) ή τα δεδομένα που ανεβαίνουν/επεξεργάζονται στο υπολογιστικό νέφος (Infrastructure as a Service) εμπίπτουν στον ΓΚΠΔ. Όταν ενεργοποιείται μια ειδοποίηση, θα πρέπει να γίνονται συγκεκριμένες αυτόματες ή/και μη αυτόματες ενέργειες λαμβάνοντας τεχνικά και οργανωτικά μέτρα, για να διασφαλιστεί η συμμόρφωση με τον ΓΚΠΔ.

6.2.2 Αρχές προστασίας δεδομένων (Data protection principles)

Οι πάροχοι υπολογιστικού νέφους θα πρέπει να διασφαλίζουν τις ακόλουθες αρχές προστασίας δεδομένων του ΓΚΠΔ:

- **Νομιμότητα, Αντικειμενικότητα και Διαφάνεια (Lawfulness, Fairness and Transparency)**: Τα προσωπικά δεδομένα του υποκειμένου των δεδομένων (data subject) πρέπει να υποβάλλονται σε επεξεργασία σύμφωνα με τις απαιτήσεις του νόμου, με σύννομο και θεμιτό τρόπο. Η συγκεκριμένη απαίτηση υπογραμμίζει την ανάγκη για τον υπεύθυνο επεξεργασίας δεδομένων να υιοθετεί πολιτικές ιδιωτικότητας που να είναι πιο φιλικές προς τα δεδομένα και, συνεπώς, σέβονται τα δικαιώματα ιδιωτικότητας.

- **Περιορισμός του Σκοπού (Purpose Limitation)**: Οι πάροχοι υπολογιστικού νέφους θα πρέπει να συλλέγουν, να αποθηκεύουν και να επεξεργάζονται προσωπικά δεδομένα για συγκεκριμένους και νόμιμους σκοπούς, απαγορεύοντας οποιαδήποτε επεξεργασία βρίσκεται εκτός του αρχικού πεδίου εφαρμογής. Το μόνο παράθυρο που αφήνει ανοιχτό ο ΓΚΠΔ για περαιτέρω επεξεργασία είναι στο πλαίσιο του δημοσίου συμφέροντος και της επιστημονικής έρευνας.

- **Ελαχιστοποίηση των Δεδομένων (Data Minimisation)**: Τα προσωπικά δεδομένα που αποθηκεύονται σε εγκαταστάσεις υπολογιστικού νέφους (cloud premises) θα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται σε ό,τι είναι απαραίτητο σε σχέση με τον σκοπό για τον οποίο έχουν συλλεχθεί.

- **Ακρίβεια (Accuracy)**: Ο υπεύθυνος επεξεργασίας του υπολογιστικού νέφους θα πρέπει να διατηρούν τα προσωπικά δεδομένα ακριβή και ενημερωμένα.

- **Περιορισμός της Περιόδου Αποθήκευσης (Storage Limitation)**: Όταν τα δεδομένα δεν απαιτούνται πλέον, σε σχέση με τον αρχικό σκοπό επεξεργασίας, θα πρέπει να διαγράφονται άμεσα.

- **Ακεραιότητα και Εμπιστευτικότητα (Integrity and Confidentiality)**: Η ακεραιότητα και η εμπιστευτικότητα θα πρέπει να διασφαλίζονται για την αποφυγή μη εξουσιοδοτημένης ή παράνομης επεξεργασίας ή/και τυχαίας απώλειας, καταστροφής ή ζημιάς.

- **Λογοδοσία (Accountability)**: Ο υπεύθυνος επεξεργασίας του υπολογιστικού νέφους φέρει την ευθύνη και είναι σε θέση να αποδείξει τη συμμόρφωση με τις αρχές προστασίας των δεδομένων.

Για να συμμορφωθούν με τα παραπάνω, οι πάροχοι υπολογιστικού νέφους θα πρέπει να διατηρούν πλήρη τεκμηρίωση των προσωπικών δεδομένων που τηρούν, από πού αυτά προέρχονται και με ποιον διαμοιράζονται, συμπεριλαμβανομένου του σκοπού/λόγου της επεξεργασίας. Η ελαχιστοποίηση των δεδομένων θα πρέπει να λαμβάνεται υπόψη σε έναν οργανισμό και ο σκοπός της συλλογής των πληροφοριών θα πρέπει να ορίζεται στην πολιτική ασφάλειας. Η προγραμματισμένη επαναξιολόγηση των δεδομένων θα πρέπει να πραγματοποιείται περιοδικά. Επιπλέον, για να διασφαλιστεί ο περιορισμός του σκοπού, είναι απαραίτητο να πραγματοποιούνται περιοδικοί έλεγχοι σε πελάτες και υπαλλήλους του υπολογιστικού νέφους. Επίσης, θα πρέπει να γίνονται περιοδικοί έλεγχοι συμμόρφωσης με την ακρίβεια των δεδομένων. Τέλος, ζωτικής σημασίας για τους παρόχους υπολογιστικού νέφους είναι η εφαρμογή μηχανισμών ελέγχου περιορισμού της αποθήκευσης και περιορισμού της μεταφοράς των δεδομένων. Για να διασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα, θα πρέπει να χρησιμοποιούνται μηχανισμοί όπως κρυπτογράφηση δεδομένων, κρυπτογραφημένα δίκτυα, τείχος προστασίας, κατακερματισμός δεδομένων και τεχνικές ανωνυμοποίησης. Η ψευδοανωνυμοποίηση, μια τεχνική ενίσχυσης της ιδιωτικότητας, θα πρέπει επίσης να εφαρμοστεί εάν είναι δυνατόν, αποφεύγοντας την άμεση συνδεσιμότητα των δεδομένων με τα υποκείμενα των δεδομένων. Όσον αφορά τη λογοδοσία και τη νομιμότητα της επεξεργασίας, κρίνεται απαραίτητη η εφαρμογή κατάλληλων μηχανισμών ελέγχου ως προς τα δεδομένα (πρόσβαση, επεξεργασία, διαγραφή, εξαγωγή κτλ.). Το έννομο συμφέρον θα πρέπει να τεκμηριώνεται και να περιλαμβάνεται με ακριβείς, σαφείς και συγκεκριμένους όρους στις συμβάσεις (Service Level Agreement – SLA).

6.2.3 Συγκατάθεση (Consent)

Οι πάροχοι υπολογιστικού νέφους που συλλέγουν/επεξεργάζονται οποιαδήποτε μορφή προσωπικών δεδομένων χρειάζονται πάντα νομική βάση για τη συλλογή/επεξεργασία. Σε ορισμένες περιπτώσεις, αυτή η νομική βάση μπορεί να είναι η συγκατάθεση του υποκειμένου των δεδομένων. Με άλλα λόγια, ο υπεύθυνος επεξεργασίας του υπολογιστικού νέφους θα πρέπει ανά πάσα στιγμή να είναι σε θέση να αποδείξει ότι το

υποκείμενο των δεδομένων έχει συναινέσει για την επεξεργασία των προσωπικών του δεδομένων. Εάν η συγκατάθεση του υποκειμένου των δεδομένων δίνεται στο πλαίσιο γραπτής δήλωσης που αφορά άλλα θέματα, η αίτηση απόκτησης συγκατάθεσης θα πρέπει να παρουσιάζεται με τρόπο που να διακρίνεται σαφώς από τα άλλα θέματα, σε κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή γλώσσα. Οποιοδήποτε μέρος μιας τέτοιας δήλωσης που συνιστά παράβαση του ΓΚΠΔ, δεν θα πρέπει να είναι δεσμευτικό. Το υποκείμενο των δεδομένων έχει το δικαίωμα να ανακαλέσει τη συγκατάθεσή του ανά πάσα στιγμή. Η ανάκληση της συγκατάθεσης δεν θα πρέπει να επηρεάζει τη νομιμότητα της επεξεργασίας που βασίζεται στη συγκατάθεση πριν από την ανάκλησή της. Πριν δώσει τη συγκατάθεσή του, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται σχετικά. Η ανάκληση θα πρέπει να είναι τόσο εύκολη όσο και η απόκτηση της συναίνεσης.

Οι μηχανισμοί διαχείρισης της συγκατάθεσης θα πρέπει να υποστηρίζονται μέσω κάποιας εφαρμογής λογισμικού η οποία θα υποστηρίζει την παροχή, την ενημέρωση, την ανάκληση και τη διατήρηση όλων των συγκαταθέσεων των χρηστών. Θα πρέπει να περιλαμβάνεται σαφή και απλή γλώσσα κατά την απόκτηση συναίνεσης προκειμένου να είναι κατανοητή και εύκολα προσβάσιμη από όλους (π.χ. μητρική γλώσσα του υποκειμένου των δεδομένων). Η ειδοποίηση για την ενημέρωση της συγκατάθεσης των χρηστών κρίνεται απαραίτητη όταν υπάρχει αλλαγή στον σκοπό ή τον τρόπο επεξεργασίας των προσωπικών δεδομένων.

6.2.4 Παιδιά και γονική συγκατάθεση (Children – parental consent)

Σε περίπτωση που μια υπηρεσία υπολογιστικού νέφους προσφέρεται απευθείας σε παιδί κάτω των 16 ετών, απαιτείται γονική συναίνεση (Άρθρο 8(1), ΓΚΠΔ). Η συγκεκριμένη συγκατάθεση θεωρείται νόμιμη μόνο εάν έχει δοθεί ή έχει εγκριθεί από τον κάτοχο της γονικής μέριμνας του παιδιού [73].

Οι πάροχοι υπολογιστικού νέφους που έχουν ως χρήστες παιδιά, θα πρέπει να επιβάλλουν μηχανισμούς για γονικό έλεγχο. Ο μηχανισμός ειδοποίησης που θα απαιτήσει περαιτέρω ενέργειες θα πρέπει να εφαρμόζεται όταν ένα παιδί προσπαθεί να χρησιμοποιήσει το υπολογιστικό νέφος ή όταν οι γονείς, του δίνουν δικαιώματα αποθήκευσης και επεξεργασίας των δεδομένων του. Αφού δημιουργηθεί ο μηχανισμός

ειδοποίησης, θα πρέπει να δημιουργηθεί και ένας μηχανισμός αυθεντικοποίησης για να εξασφαλιστεί ότι ο νόμιμος γονέας δίνει τη συγκατάθεσή του και ότι η γλώσσα συναίνεσης είναι φιλική προς τα παιδιά, προκειμένου τα παιδιά να κατανοήσουν ότι απαιτείται γονική έγκριση. Λογισμικό όπως αυτό που περιγράφεται στην υπο-ενότητα 6.2.3 θα πρέπει να χρησιμοποιείται και να έχει και τις παραπάνω λειτουργίες.

6.2.5 Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive data and lawful processing)

Σύμφωνα με τον ΓΚΠΔ ευαίσθητα δεδομένα είναι αυτά 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 τη σεξουαλική ζωή ή/και τον γενετήσιο προσανατολισμό ενός φυσικού προσώπου

Οι πάροχοι υπολογιστικού νέφους που συλλέγουν/επεξεργάζονται τέτοιες κατηγορίες δεδομένων θα πρέπει να λάβουν περαιτέρω μέτρα προκειμένου να ικανοποιήσουν τις απαιτήσεις του ΓΚΠΔ.

Στο πλαίσιο αυτό, οι τύποι ευαίσθητων δεδομένων που υποβάλλονται σε επεξεργασία θα πρέπει να ταυτοποιούνται και να περιγράφονται αναλυτικά στην πολιτική ασφάλειας του υπολογιστικού νέφους, παρέχοντας επίσης το λόγο για την αναγκαιότητά τους. Σε τεχνικό επίπεδο, θα είναι ζωτικής σημασίας να εφαρμοστεί ένας μηχανισμός προστασίας που θα εκτελεί σάρωση αρχείων και δεδομένων, ειδικά σε περιπτώσεις υλικού-ως-αρχιτεκτονική (hardware-as-a-service architecture) όπου η αποθήκευση δεδομένων προσφέρεται ως υπηρεσία [74].

6.2.6 Ενημερωτικές ειδοποιήσεις (Information notices)

Οι πάροχοι υπολογιστικού νέφους πρέπει να παρέχουν πληροφορίες μέσω της πολιτικής ιδιωτικότητάς τους ή/και κατόπιν αιτήματος των υποκειμένων των δεδομένων σχετικά με:

- την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας
- τα δεδομένα που εμπλέκονται, τον σκοπό επεξεργασίας και τη νομική βάση
- τον παραλήπτη ή τις κατηγορίες παραληπτών
- τα στοιχεία μεταφοράς δεδομένων εκτός ΕΕ
- την περίοδο διατήρησης δεδομένων
- τα δικαιώματα των ατόμων

Σημαντική θα ήταν η υιοθέτηση κάποιου εργαλείου για τη δημιουργία και τον αυτόματο διαμοιρασμό προτύπων εγγράφων για τις ενημερωτικές ειδοποιήσεις, τα αιτήματα των υποκειμένων των δεδομένων και τις απαντήσεις των παρόχων υπολογιστικού νέφους.

6.2.7 Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)

Οι πάροχοι υπολογιστικού νέφους θα πρέπει να παρέχουν στα Υποκείμενα των δεδομένων επιβεβαίωση εάν τα προσωπικά τους δεδομένα υποβάλλονται σε επεξεργασία, να τους δίνουν πρόσβαση στα δεδομένα και στις συμπληρωματικές πληροφορίες με δυνατότητα διόρθωσης ή διαγραφής τους («δικαίωμα στη λήθη»), να τους ενημερώνουν για την πηγή των δεδομένων και για το δικαίωμα στη φορητότητα.

Η ύπαρξη ολοκληρωμένων αναφορών και η χρήση πρότυπων εγγράφων είναι απαραίτητα. Θα πρέπει να χρησιμοποιούνται τεχνικές ειδοποιήσεων και διαγραφών ή μη διαθεσιμότητας δεδομένων που διατηρούνται στο υπολογιστικό νέφος. Οι πάροχοι υπολογιστικού νέφους θα πρέπει να μπορούν να εξάγουν δεδομένα με ασφαλή τρόπο και σε κοινή μορφή/τεχνολογία που μπορεί να υιοθετηθεί ευρέως για την υποστήριξη της φορητότητας (π.χ. xml, tab, csv). Επίσης, θα πρέπει να είναι σε θέση να παρέχουν μηχανισμούς για την εγκυρότητα του αιτήματος που υποβάλλουν τα Υποκείμενα των

δεδομένων καθώς και για την ανταπόκριση σε αιτήματα σχετικά με την πρόσβαση στα προσωπικά δεδομένα τους. Επιπλέον, θα πρέπει να μπορούν να ανιχνεύουν και να αναζητούν προσωπικά δεδομένα των Υποκειμένων όταν αυτό απαιτηθεί.

6.2.8 Δικαίωμα εναντίωσης (Right to object)

Οι πάροχοι υπολογιστικού νέφους θα πρέπει να παρέχουν στους ιδιοκτήτες των δεδομένων το δικαίωμα να εναντιωθούν σε μια επεξεργασία δεδομένων με εύκολο και ασφαλή τρόπο. Τεχνικά, αυτό μπορεί να γίνει μέσω μηχανισμού για την υποβολή ενστάσεων των Υποκειμένων των δεδομένων και πρόσθετες αυτοματοποιημένες ενέργειες.

6.2.9 Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της επεξεργασίας (Right to erasure and right to restriction of processing)

Η διαγραφή ή ο περιορισμός της επεξεργασίας θα πρέπει να εφαρμόζονται στο υπολογιστικό νέφος όταν ισχύει οποιοδήποτε από τα παρακάτω:

- Τα δεδομένα δεν είναι πλέον απαραίτητα για τον σκοπό για τον οποίο συλλέχθηκαν ή υποβλήθηκαν σε επεξεργασία
- Τα υποκείμενα των δεδομένων αποσύρουν τη συγκατάθεσή τους
- Οι υπεύθυνοι επεξεργασίας δεν μπορούν να αποδείξουν ότι υπάρχουν επιτακτικοί και νόμιμοι λόγοι για την επεξεργασία
- Μη νόμιμη επεξεργασία

Όταν τα δεδομένα δημοσιοποιούνται, ο πάροχος υπολογιστικού νέφους θα πρέπει να ειδοποιεί τους υπόλοιπους υπεύθυνους επεξεργασίας ότι ο ιδιοκτήτης των δεδομένων θέλει να περιορίσει την πρόσβαση ή ότι τα δεδομένα του πρέπει να διαγραφούν.

Οι πάροχοι υπολογιστικού νέφους θα πρέπει να διαθέτουν ειδικό λογισμικό διαγραφής για να διασφαλίζουν ότι δεν είναι δυνατή η ανάκτηση δεδομένων από τον αποθηκευτικό χώρο του σκληρού δίσκου. Επίσης, σε περιπτώσεις όπου οι πληροφορίες απαιτείται να διατηρηθούν για κάποιο χρονικό διάστημα, είναι απαραίτητο να υπάρχουν μηχανισμοί περιορισμού που δεν θα έχουν διαθέσιμες τις πληροφορίες αυτές, περιορίζοντας τα δεδομένα σε διαφορετικό σύστημα [75].

6.2.10Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and automated decision-taking)

Η κατάρτιση προφίλ αποτελείται από τρεις πτυχές: Αυτοματοποιημένη επεξεργασία (επεξεργασία με χρήση υπολογιστών) προσωπικών δεδομένων με σκοπό την αξιολόγηση προσωπικών πτυχών που σχετίζονται με ένα άτομο ή μια ομάδα ατόμων (συμπεριλαμβανομένης της ανάλυσης ή της πρόβλεψης). Οι οδηγίες/κατευθυντήριες γραμμές (guidelines) καθιστούν σαφές ότι ο ορισμός είναι πολύ ευρύς και ότι η επεξεργασία δεν χρειάζεται να οδηγεί σε συμπεράσματα – «η αξιολόγηση ή ταξινόμηση ατόμων που βασίζεται σε χαρακτηριστικά όπως η ηλικία, το φύλο και το ύψος τους θα μπορούσε να θεωρηθεί ως κατάρτιση προφίλ, ανεξάρτητα από οποιονδήποτε σκοπό» [76]. Οι οδηγίες/κατευθυντήριες γραμμές περιγράφουν την κατάρτιση προφίλ με τρία διαφορετικά στάδια, καθένα από τα οποία εμπίπτει στον ορισμό της κατάρτισης προφίλ σύμφωνα με τον ΓΚΠΔ: (1) συλλογή δεδομένων (2) αυτοματοποιημένη ανάλυση για τον εντοπισμό συσχετίσεων και (3) εφαρμογή της συσχέτισης σε ένα άτομο για προσδιορισμό των χαρακτηριστικών της παρούσας ή της μελλοντικής συμπεριφοράς του. Μια απόφαση που βασίζεται αποκλειστικά στην αυτοματοποιημένη επεξεργασία είναι μια απόφαση χωρίς ανθρώπινη συμμετοχή στη διαδικασία λήψης αποφάσεων. Οι οδηγίες/κατευθυντήριες γραμμές προειδοποιούν ότι η συμμετοχή ενός ατόμου στη διαδικασία παράκαμψης των κανόνων για αποκλειστικά αυτοματοποιημένη λήψη αποφάσεων δεν θα λειτουργούσε, καθώς η ανθρώπινη συμμετοχή θα πρέπει να είναι ουσιαστική και όχι απλώς να γίνεται συμβολικά. Το υποκείμενο των δεδομένων θα πρέπει να έχει την εξουσία να αλλάξει την απόφαση λαμβάνοντας υπόψη όλες τις διαθέσιμες πληροφορίες.

Τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται πότε έχει ληφθεί μια απόφαση χρησιμοποιώντας αποκλειστικά την αυτοματοποιημένη λήψη αποφάσεων και θα πρέπει να έχουν το δικαίωμα να ζητήσουν επανεξέταση της απόφασης. Η επανεξέταση θα πρέπει να γίνεται από άτομο με την κατάλληλη εξουσία και ικανότητα να αλλάξει την απόφαση και θα πρέπει να περιλαμβάνει ενδελεχή επανεξέταση όλων των σχετικών δεδομένων και τυχόν πρόσθετων πληροφοριών που παρέχονται από το υποκείμενο των δεδομένων. Οι οργανισμοί που χρησιμοποιούν αυτοματοποιημένη λήψη αποφάσεων θα

πρέπει επίσης να πραγματοποιούν τακτικές επιθεωρήσεις και να χρησιμοποιούν κατάλληλες διαδικασίες για την πρόληψη/αποφυγή σφαλμάτων.

6.2.11Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)

Το άρθρο 24 του ΓΚΠΔ κωδικοποιεί την υποχρέωση λογοδοσίας. Απαιτεί από τους υπεύθυνους επεξεργασίας να:

- Υλοποιήσουν κατάλληλα τεχνικά και οργανωτικά μέτρα (συμπεριλαμβανομένης της εισαγωγής της προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού, όπου χρειάζεται) για να διασφαλιστεί και να είναι σε θέση να αποδειχθεί ότι η επεξεργασία δεδομένων πραγματοποιείται σύμφωνα με τον ΓΚΠΔ
- Επανεξετάσουν και να επικαιροποιήσουν μέτρα, όπου είναι απαραίτητο, μέσω εσωτερικής και εξωτερικής αξιολόγησης, όπως οι σφραγίδες ιδιωτικότητας. Τα μέτρα αυτά θα πρέπει να λαμβάνουν υπόψη τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς επεξεργασίας και τον κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Σε περίπτωση παραβίασης προσωπικών δεδομένων, ο υπεύθυνος επεξεργασίας γνωστοποιεί, χωρίς αδικαιολόγητη καθυστέρηση και, όπου είναι εφικτό, το αργότερο 72 ώρες αφότου έλαβε γνώση της παραβίασης προσωπικών δεδομένων, στην εποπτική αρχή που είναι αρμόδια σύμφωνα με το άρθρο 55, εκτός εάν η παραβίαση προσωπικών δεδομένων είναι απίθανο να οδηγήσει σε κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Εάν η κοινοποίηση στην εποπτική αρχή δεν γίνει εντός 72 ωρών, θα πρέπει να συνοδεύεται από τους λόγους καθυστέρησης.

Έτσι, οι πάροχοι υπολογιστικού νέφους θα πρέπει να διαθέτουν μηχανισμούς για την προστασία του δικτύου, την κρυπτογράφηση και την κοινοποίηση προς τις εποπτικές αρχές και τα υποκείμενα των δεδομένων [77].

6.2.12Συγκεντρωτικά μέτρα ασφαλείας για τους παρόχους υπολογιστικού νέφους με βάση τις απαιτήσεις του ΓΚΠΔ

Στον παρακάτω Πίνακα, παρουσιάζονται συγκεντρωτικά τα μέτρα ασφάλειας που θα πρέπει να λάβει ένας πάροχος υπολογιστικού νέφους με βάση τις απαιτήσεις του ΓΚΠΔ που αναφέρθηκαν στις υπο-ενότητες 6.2.1 έως και 6.2.11.

ΓΚΠΔ – Παράμετροι υπολογιστικού νέφους	Μέτρα ασφάλειας
Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope): Πάροχος υπολογιστικού νέφους με παρουσία εκτός ΕΕ που στοχεύει σε άτομα εντός της ΕΕ. Οι χρήστες που εμπίπτουν στον ΓΚΠΔ θα πρέπει να αντιμετωπίζονται διαφορετικά από τους παρόχους υπολογιστικού νέφους, ώστε να συμμορφώνονται με τους κανόνες του.	• Μηχανισμός ελέγχου-ειδοποίησης για να ελέγχει εάν οι χρήστες εμπίπτουν στον ΓΚΠΔ και να εφαρμόζει αυτόματα τα τεχνικά και οργανωτικά μέτρα που έχουν σχεδιαστεί
Περιορισμός του Σκοπού (Purpose Limitation)	• Τεκμηρίωση προσωπικών δεδομένων που τηρούνται • Ελαχιστοποίηση δεδομένων • Μηχανισμός που θα ελέγχει με σάρωση αρχείων εάν έχουν παραβιαστεί οι κανόνες για την ελαχιστοποίηση δεδομένων • Επαναξιολόγηση δεδομένων • Εκπαίδευση και έλεγχος εργαζομένων για τήρηση του περιορισμού του σκοπού • Έλεγχοι συμμόρφωσης για την τήρηση της ακρίβειας των δεδομένων

ΓΚΠΔ – Παράμετροι υπολογιστικού νέφους	Μέτρα ασφάλειας
	• Μηχανισμοί σάρωσης για τήρηση του περιορισμού αποθήκευσης και του περιορισμού μεταφοράς δεδομένων • Ακεραιότητα και εμπιστευτικότητα: Κρυπτογράφηση δεδομένων και κρυπτογραφημένα δίκτυα • Τείχος προστασίας • Κατακερματισμός δεδομένων • Ανωνυμοποίηση • Λογοδοσία: Μηχανισμός ελέγχου και αναφορές πελατών
Νομιμότητα της επεξεργασίας και της περαιτέρω επεξεργασίας (Lawfulness of processing and further processing)	• Μηχανισμοί ελέγχου ως προς την πρόσβαση στα δεδομένα, την επεξεργασία τους, τη διαγραφή τους, την εξαγωγή τους
Έννομα συμφέροντα (Legitimate interests)	• Πλήρης τεκμηρίωση με ακριβείς, σαφείς και συγκεκριμένους όρους στις συμβάσεις (Service Level Agreement – SLA)
Συγκατάθεση (Consent)	• Λογισμικό που θα υποστηρίζει την παροχή, την ενημέρωση, την ανάκληση και τη διατήρηση της συγκατάθεσης
Παιδιά και γονική συγκατάθεση (Children – parental consent)	• Λογισμικό που θα υποστηρίζει την παροχή, την ενημέρωση, την ανάκληση και τη διατήρηση της συγκατάθεσης με ειδική λειτουργία

ΓΚΠΔ – Παράμετροι υπολογιστικού νέφους	Μέτρα ασφάλειας
	για γονική συναίνεση και μηχανισμό ελέγχου αυθεντικοποίησης
Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive data and lawful processing)	• Ορισμός ευαίσθητων δεδομένων στην πολιτική ασφάλειας • Λογισμικό για τη σάρωση αρχείων θα πρέπει να χρησιμοποιείται από παρόχους υπηρεσιών υπολογιστικού νέφους
Ενημερωτικές ειδοποιήσεις (Information notices)	• Ενημερωτικές ειδοποιήσεις με τα στοιχεία ταυτότητας και επικοινωνίας του υπεύθυνου επεξεργασίας, το σκοπό επεξεργασίας και τη νομική βάση, τις λεπτομέρειες μεταφοράς δεδομένων εκτός ΕΕ, την περίοδο διατήρησης δεδομένων και τα δικαιώματα των ατόμων
Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)	• Σκοπός επεξεργασίας και κατηγορίες δεδομένων που επεξεργάζονται • Απαιτούνται πλήρεις αναφορές και πρότυπα εγγράφων • Χρήση ειδοποιήσεων και αντίστοιχη διαγραφή ή μη διαθεσιμότητα δεδομένων που διατηρούνται • Εξαγωγή μηχανισμού δεδομένων με ασφαλή τρόπο και σε κοινή μορφή/τεχνολογία που μπορεί να υιοθετηθεί ευρέως για την υποστήριξη

ΓΚΠΔ – Παράμετροι υπολογιστικού νέφους	Μέτρα ασφάλειας
	της φορητότητας
Δικαίωμα εναντίωσης (Right to object)	• Λογισμικό για εύκολη εναντίωση και υποβολή ενστάσεων
Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της επεξεργασίας (Right to erasure and right to restriction of processing)	• Λογισμικό διαγραφής για να διασφαλιστεί ότι δεν είναι δυνατή η ανάκτηση δεδομένων από τον αποθηκευτικό χώρο του σκληρού δίσκου. • Μηχανισμοί περιορισμού, που δεν θα έχουν διαθέσιμες τις πληροφορίες, που απαιτείται να διατηρηθούν για κάποιο χρονικό διάστημα, εμποδίζοντας τα δεδομένα σε διαφορετικό σύστημα. • Ενημερωτικές ειδοποιήσεις άλλων υπεύθυνων επεξεργασίας που είναι μέλη του υπολογιστικού νέφους.
Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and automated decision-taking)	• Συγκατάθεση
Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)	• Τείχη προστασίας και προστασία δικτύου για την προστασία των δεδομένων • Κρυπτογράφηση δεδομένων και δικτύων

ΓΚΠΔ – Παράμετροι υπολογιστικού νέφους	Μέτρα ασφάλειας
	• Μηχανισμοί κοινοποίησης προς τις εποπτικές αρχές και το υποκείμενο των δεδομένων

Πίνακας 16: Μέτρα ασφάλειας που θα πρέπει να λάβει ένας πάροχος υπολογιστικού νέφους με βάση τις απαιτήσεις του ΓΚΠΔ

6.3 Μέτρα προστασίας ανά αρχιτεκτονική του υπολογιστικού νέφους

Το υπολογιστικό νέφος μπορεί να εμφανιστεί σε τρεις κύριες αρχιτεκτονικές/μοντέλα:

- *Υποδομή-ως-υπηρεσία (Infrastructure as a Service - IaaS):* Παρέχει πόρους υλικού όπως υπολογιστικές εγκαταστάσεις, αποθήκευση, μνήμη κτλ. Γνωστός πάροχος IaaS είναι η Amazon με το EC2 και το S3.
- *Πλατφόρμα-ως-υπηρεσία (Platform as a Service - PaaS):* Ο όρος πλατφόρμα σχετίζεται με συστήματα (π.χ. λειτουργικό σύστημα) που μπορούν να χρησιμοποιηθούν για την ανάπτυξη και τη δημιουργία παραμετροποιήσιμων εφαρμογών. Γνωστός πάροχος PaaS είναι το Microsoft Azure.
- *Λογισμικό-ως-υπηρεσία (Software as a Service - SaaS):* Παρέχει οποιοδήποτε είδος λογισμικού (εφαρμογή ή υπηρεσία) μέσω υπολογιστικού νέφους. Γνωστός πάροχος SaaS είναι η Salesforce.

Στους παρακάτω Πίνακες, παρουσιάζονται τα μέτρα προστασίας προσωπικών δεδομένων ανά αρχιτεκτονική του υπολογιστικού νέφους σύμφωνα με τις απαιτήσεις του ΓΚΠΔ.

INFRASTRUCTURE AS A SERVICE - IAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope)	Ο χώρος αποθήκευσης των προσωπικών δεδομένων θα πρέπει να είναι διαθέσιμος και να υποστηρίζει επιλογές για τον έλεγχο της γεωγραφικής ροής των πληροφοριών.

INFRASTRUCTURE AS A SERVICE - IAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
Αρχές προστασίας δεδομένων (Data protection principles)	Τα μέτρα προσδιορίζουν την αιτία της Παραβίασης Προσωπικών Δεδομένων, μετριάζουν τις αρνητικές επιπτώσεις και αποτρέπουν την επανάληψη.
Συγκατάθεση (Consent)	Δεν απαιτείται. Δεν υπάρχει άμεση σχέση με τα υποκείμενα των δεδομένων.
Παιδιά και γονική συγκατάθεση (Children – parental consent)	Δεν απαιτείται. Δεν υπάρχει άμεση σχέση με τα υποκείμενα των δεδομένων.
Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive data and lawful processing)	Μέτρα προστασίας δεδομένων και λογισμικό για σάρωση αρχείων δεδομένων.
Ενημερωτικές ειδοποιήσεις (Information notices)	Δεν απαιτείται.
Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)	Παροχή πληροφοριών σχετικά με τη μεταφορά δεδομένων και πληροφοριών σχετικά με τη διόρθωση και τη διαγραφή δεδομένων.
Δικαίωμα εναντίωσης (Right to object)	Δεν απαιτείται.
Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της επεξεργασίας (Right to erasure and right to restriction of processing)	Δεν απαιτείται.

INFRASTRUCTURE AS A SERVICE - IAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and automated decision-taking)	Δεν απαιτείται.
Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)	Δεν απαιτείται.

Πίνακας 17: Εφαρμοσιμότητα των απαιτήσεων του ΓΚΠΔ για την αρχιτεκτονική IaaS

PLATFORM AS A SERVICE - PAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope)	Αναλυτικές γεωγραφικές πληροφορίες θα πρέπει να είναι διαθέσιμες στο διαδίκτυο, με ειδοποίηση αλληλογραφίας και επίσημη τεκμηρίωση.
Αρχές προστασίας δεδομένων (Data protection principles)	Τα μέτρα προσδιορίζουν την αιτία της Παραβίασης Προσωπικών Δεδομένων, μετριάζουν τις αρνητικές επιπτώσεις και αποτρέπουν την επανάληψη.
Συγκατάθεση (Consent)	Δεν απαιτείται.
Παιδιά και γονική συγκατάθεση (Children – parental consent)	Δεν απαιτείται.
Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive	Πρέπει να χρησιμοποιούνται εργαλεία για την αναγνώριση των ευαίσθητων δεδομένων και σχετικά

PLATFORM AS A SERVICE - PAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
data and lawful processing)	μέτρα για την ταξινόμηση και την προστασία τους.
Ενημερωτικές ειδοποιήσεις (Information notices)	Διατήρηση πλήρους τεκμηρίωσης των πλατφορμών και των μηχανισμών ασφάλειας.
Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)	Όλες οι πληροφορίες που φιλοξενούνται πρέπει να είναι εξαγώγιμες και αναγνώσιμες.
Δικαίωμα εναντίωσης (Right to object)	Απαιτείται.
Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της επεξεργασίας (Right to erasure and right to restriction of processing)	Παροχή εργαλείων για περιορισμό της αποθήκευσης, της διατήρησης ή της διαγραφής των δεδομένων.
Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and automated decision-taking)	Δεν απαιτείται.
Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)	Συμπερίληψη τειχών προστασίας, εργαλείων προστασίας δικτύου και διαχείρισης συμβάντων.

Πίνακας 18: Εφαρμοσιμότητα των απαιτήσεων του ΓΚΠΔ για την αρχιτεκτονική PaaS

SOFTWARE AS A SERVICE - SAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope)	Ο χώρος αποθήκευσης των προσωπικών δεδομένων θα πρέπει να είναι διαθέσιμος και να υποστηρίζει επιλογές για τον έλεγχο της γεωγραφικής ροής των πληροφοριών.
Αρχές προστασίας δεδομένων (Data protection principles)	Τα μέτρα προσδιορίζουν την αιτία της Παραβίασης Προσωπικών Δεδομένων, μετριάζουν τις αρνητικές επιπτώσεις και αποτρέπουν την επανάληψη.
Συγκατάθεση (Consent)	Δεν απαιτείται. Δεν υπάρχει άμεση σχέση με τα υποκείμενα των δεδομένων.
Παιδιά και γονική συγκατάθεση (Children – parental consent)	Δεν απαιτείται. Δεν υπάρχει άμεση σχέση με τα υποκείμενα των δεδομένων.
Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive data and lawful processing)	Μέτρα προστασίας δεδομένων και λογισμικό για σάρωση αρχείων δεδομένων.
Ενημερωτικές ειδοποιήσεις (Information notices)	Δεν απαιτείται.
Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)	Παροχή πληροφοριών σχετικά με τη μεταφορά δεδομένων και πληροφοριών σχετικά με τη διόρθωση και τη διαγραφή δεδομένων.
Δικαίωμα εναντίωσης (Right to object)	Δεν απαιτείται.
Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της	Δεν απαιτείται.

SOFTWARE AS A SERVICE - SAAS	
Απαίτηση του ΓΚΠΔ	**Εφαρμοσιμότητα στον πάροχο υπολογιστικού νέφους**
επεξεργασίας (Right to erasure and right to restriction of processing)	
Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and automated decision-taking)	Δεν απαιτείται.
Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)	Δεν απαιτείται.

Πίνακας 19: Εφαρμοσιμότητα των απαιτήσεων του ΓΚΠΔ για την αρχιτεκτονική SaaS

Οι συμμετέχοντες στο υπολογιστικό νέφος, σε όρους ΓΚΠΔ, μπορούν να χωριστούν σε δύο κύριους ρόλους: τους εκτελούντες την επεξεργασία και τους υπεύθυνους επεξεργασίας δεδομένων. Τις περισσότερες φορές, οι πάροχοι υπολογιστικού νέφους ενεργούν ως εκτελούντες την επεξεργασία για λογαριασμό των πελατών/χρηστών τους που είναι οι υπεύθυνοι επεξεργασίας.

Στον παρακάτω πίνακα (Πίνακας 20), παρουσιάζονται τα συνιστώμενα και υποχρεωτικά μέτρα για τους παρόχους υπολογιστικού νέφους που δρουν ως εκτελούντες την επεξεργασία.

Απαίτηση του ΓΚΠΔ	IaaS	PaaS	SaaS
Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope)	◪	◪	◪

Απαίτηση του ΓΚΠΔ	IaaS	PaaS	SaaS
Αρχές προστασίας δεδομένων (Data protection principles)			
Συγκατάθεση (Consent)			
Παιδιά και γονική συγκατάθεση (Children – parental consent)			
Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive data and lawful processing)			
Ενημερωτικές ειδοποιήσεις (Information notices)			
Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)			
Δικαίωμα εναντίωσης (Right to object)			
Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της επεξεργασίας (Right to erasure and right to restriction of processing)			
Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and			

Απαίτηση του ΓΚΠΔ	IaaS	PaaS	SaaS
automated decision-taking)			
Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)			

	**Υποχρεωτικά μέτρα**
	**Συνιστώμενα μέτρα**

Πίνακας 20: Συνιστώμενα και υποχρεωτικά μέτρα για τους παρόχους υπολογιστικού νέφους που δρουν ως εκτελούντες την επεξεργασία

Στον παρακάτω πίνακα (Πίνακας 21), παρουσιάζονται τα συνιστώμενα και υποχρεωτικά μέτρα για τους παρόχους υπολογιστικού νέφους που δρουν ως υπεύθυνοι επεξεργασίας.

Απαίτηση του ΓΚΠΔ	IaaS	PaaS	SaaS
Ουσιαστικό και εδαφικό πεδίο εφαρμογής (Material and territorial scope)			
Αρχές προστασίας δεδομένων (Data protection principles)			
Συγκατάθεση (Consent)			
Παιδιά και γονική συγκατάθεση (Children – parental consent)			

Απαίτηση του ΓΚΠΔ	IaaS	PaaS	SaaS
Ευαίσθητα δεδομένα και νόμιμη επεξεργασία (Sensitive data and lawful processing)			
Ενημερωτικές ειδοποιήσεις (Information notices)			
Πρόσβαση των Υποκειμένων στα δεδομένα, διόρθωση και φορητότητα (Subject access, rectification and portability)			
Δικαίωμα εναντίωσης (Right to object)			
Δικαίωμα διαγραφής («δικαίωμα στη λήθη») και Δικαίωμα περιορισμού της επεξεργασίας (Right to erasure and right to restriction of processing)			
Κατάρτιση προφίλ και αυτοματοποιημένη λήψη αποφάσεων (Profiling and automated decision-taking)			
Λογοδοσία, ασφάλεια και ειδοποίηση παραβίασης (Accountability, security and breach notification)			
	**Υποχρεωτικά μέτρα**		

Απαίτηση του ΓΚΠΔ		IaaS	PaaS	SaaS
[redacted]	**Συνιστώμενα μέτρα**			

Πίνακας 21: Συνιστώμενα και υποχρεωτικά μέτρα για τους παρόχους υπολογιστικού νέφους που δρουν ως υπεύθυνοι επεξεργασίας

Βασιζόμενοι στους παραπάνω Πίνακες, προκύπτει ότι η συμμόρφωση με τον ΓΚΠΔ ποικίλλει ανάλογα με τη φύση της παρεχόμενης υπηρεσίας υπολογιστικού νέφους (SaaS, PaaS, IaaS) και τον ρόλο που έχει ο πάροχος υπολογιστικού νέφους (υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία).

6.4 Συμπεράσματα

Στις παραπάνω ενότητες μελετήθηκε ο ΓΚΠΔ και συλλέχθηκαν όλες οι απαιτήσεις που θα πρέπει να τηρούν οι πάροχοι υπολογιστικού νέφους προκειμένου να είναι συμβατοί με τον Κανονισμό. Επίσης, παρουσιάστηκαν μέτρα ασφάλειας που θα πρέπει να λάβει ένας πάροχος υπολογιστικού νέφους με βάση τις συγκεκριμένες απαιτήσεις. Τέλος, παρουσιάστηκαν μέτρα προστασίας προσωπικών δεδομένων ανά αρχιτεκτονική του υπολογιστικού νέφους.

Μετά την εξαγωγή των παραπάνω απαιτήσεων του ΓΚΠΔ σε περιβάλλοντα υπολογιστικού νέφους προκύπτει ότι προκειμένου ένα Πληροφοριακό Σύστημα Υγείας, όπως αυτά που μελετήθηκαν στην Ενότητα 5.4, το οποίο χρησιμοποιεί περιβάλλον υπολογιστικού νέφους για τις υπηρεσίες που παρέχει, να είναι συμβατό ως προς την διαρκή ικανοποίηση των απαιτήσεων της ιδιωτικότητας εκτός από το είδος των δεδομένων που χρησιμοποιεί και τα χαρακτηριστικά του οργανισμού στον οποίο εφαρμόζεται, θα πρέπει να τηρεί και τις πρόσθετες απαιτήσεις που προέκυψαν από τις παραπάνω Ενότητες.

7 Κεφάλαιο 7: Συμπεράσματα και Μελλοντικές Ενέργειες

7.1 Συμπεράσματα

Στην εισαγωγή της παρούσας διδακτορικής διατριβής καταγράφηκαν οι στόχοι και η συνεισφορά κατά την επιστημονική έρευνα που πραγματοποιήθηκε. Πρώτος στόχος ήταν η καταγραφή των αρχών ιδιωτικότητας, των απαιτήσεων ιδιωτικότητας και των απαιτήσεων ασφάλειας μέσω δημόσιων και ιδιωτικών φορέων και του προτεινόμενου τρόπου εφαρμογής τους, για την οποία πραγματοποιήθηκε βιβλιογραφική επισκόπηση.

Το πρώτο συμπέρασμα, μέσω της παραπάνω ερευνητικής καταγραφής, οδήγησε στο γεγονός ότι δεν υπάρχει ένα ενιαίο πλαίσιο τήρησης των απαιτήσεων και αρχών ασφάλειας και ιδιωτικότητας που να μπορεί να ακολουθηθεί προκειμένου ένας οργανισμός να είναι συμμορφωμένος με αυτές. Ως αποτέλεσμα, προτάθηκε μια ενιαία μεθοδολογία εξαγωγής απαιτήσεων ασφάλειας και ιδιωτικότητας, η οποία ορίζει τον τρόπο με τον οποίο ένας οργανισμός μπορεί να λάβει αποτελεσματικά υπόψιν όλα τις παραπάνω απαιτήσεις ταυτόχρονα.

Το δεύτερο συμπέρασμα, μέσω της παραπάνω ερευνητικής καταγραφής, οδήγησε στο γεγονός ότι δεν υπάρχει μέχρι στιγμής καμία καταγεγραμμένη προσπάθεια για τον τρόπο που θα πρέπει να εφαρμοστούν οι υφιστάμενες αρχές ιδιωτικότητας (δηλαδή είναι ορισμένες αρχές πιο σημαντικές από άλλες; υπάρχει συγκεκριμένη σειρά που κάποιος πρέπει να προσπαθήσει να τις ικανοποιήσει και σε αυτή την περίπτωση ποια είναι αυτή η σειρά; κτλ.). Ως αποτέλεσμα, προτάθηκε μια δομημένη μεθοδολογία για τη διευκόλυνση του σχεδιασμού συστημάτων που «θέλουν» να είναι συνεπή με τις αρχές της ιδιωτικότητας.

Τέλος, από το Μάϊο του 2018 που η εφαρμογή και τήρηση του ΓΚΠΔ έχει γίνει απαραίτητη προϋπόθεση για όλους του δημόσιους και ιδιωτικούς φορείς που χειρίζονται προσωπικά δεδομένα και δεδομένα ειδικών κατηγοριών χρηστών, η εφαρμογή της Εκτίμησης Αντικτύπου Ιδιωτικότητας (Privacy Impact Assessment - PIA) κρίνεται καθοριστικής σημασίας. Σε αυτό το πλαίσιο, έγινε καταγραφή των ήδη υπαρχουσών μεθοδολογιών μελέτης εκτίμησης αντικτύπου προκειμένου να αξιολογηθούν οι πιθανές επιπτώσεις για ένα οργανισμό από περιστατικά παραβίασης ιδιωτικότητας των δεδομένων των χρηστών τους. Από αυτή την καταγραφή, προέκυψε το γεγονός ότι καμία μεθοδολογία

δεν λαμβάνει υπόψη, με μετρήσιμο τρόπο, τις κατηγορίες των δεδομένων και τα χαρακτηριστικά του οργανισμού. Ως αποτέλεσμα, προτάθηκε μια μεθοδολογία εκτίμησης αντικτύπου, η οποία συνδυάζει τις παραπάνω αρχές και απαιτήσεις ιδιωτικότητας με τον αντίκτυπο σε ένα υπό μελέτη οργανισμό από πιθανά περιστατικά παραβίασης ιδιωτικότητας καθώς και τα χαρακτηριστικά του οργανισμού, και καταλήγει στην ποσοτικοποίηση των τελικών αποτελεσμάτων σχετικά με τον έλεγχο της τήρησης της ιδιωτικότητας.

7.2 Μελλοντικές Ενέργειες

Η προτεινόμενη μεθοδολογία Εκτίμησης Αντικτύπου Ιδιωτικότητας (Privacy Impact Assessment - PIA) λαμβάνει υπόψη τα χαρακτηριστικά ενός οργανισμού και τις κατηγορίες των δεδομένων που χρησιμοποιεί προκειμένου να αξιολογήσει το επίπεδο της ιδιωτικότητας κάθε οργανισμού μέσω μετρικών.

Ένας από τους αρχικούς στόχους είναι η προσαρμογή της μεθοδολογίας στις απαιτήσεις του Γενικού Κανονισμού Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 2016/679 (ΓΚΠΔ) (General Data Protection Regulation - GDPR) [4], ο οποίος τέθηκε σε ισχύ τον Μάϊο του 2018. Το μοντέλο που θα αναπτυχθεί θα αποτελείται από πέντε στάδια συμμόρφωσης: Στάδιο 1 (Χαρτογράφηση Δεδομένων Οργανισμού), Στάδιο 2 (Ανάλυση Αποκλίσεων σε σχέση με τις απαιτήσεις του ΓΚΠΔ 2016/679), Στάδιο 3 (Εκτίμηση Αντικτύπου), Στάδιο 4 (Μέτρα Προστασίας Δεδομένων) και Στάδιο 5 (Πολιτικές και Διαδικασίες). Παράλληλα με τα Στάδια, θα αξιολογεί τα χαρακτηριστικά του οργανισμού και τον τύπο των δεδομένων των πληροφοριακών συστημάτων του και θα τον καθοδηγεί σχετικά με τα βήματα που πρέπει να ακολουθήσει σε κάθε στάδιο συμμόρφωσης.

Η επέκταση της μεθοδολογίας ανά περίπτωση οργανισμού και εξειδίκευση των συγκεκριμένων χαρακτηριστικών του, π.χ. συλλογή χαρακτηριστικών νοσοκομείου, παρόχου τηλεπικοινωνιών, εκπαιδευτικού ιδρύματος, τράπεζας, κτλ. αποτελεί έναν ακόμα μελλοντικό στόχο.

Επίσης, ένας τρίτος στόχος της προτεινόμενης μεθοδολογίας PIA είναι η επέκτασή της, ώστε για κάθε κατηγορία δεδομένων και συγκεκριμένα για κάθε αρχή ιδιωτικότητας που δεν τηρείται επαρκώς να προτείνει μέτρα και διορθωτικές ενέργειες ανά περίπτωση.

Τέλος, ένας τέταρτος μελλοντικός στόχος είναι η υλοποίηση εργαλείου της προτεινόμενης μεθοδολογίας PIA που να βοηθάει έναν οργανισμό να την εφαρμόσει άμεσα και αποτελεσματικά.

8 Αναφορές

1. W Hong, JYL Thong, Internet privacy concerns: An integrated conceptualization and four empirical studies, MIS Quarterly, Vol. 37, No. 1 (2013) pp. 275-298, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229627.
2. F Bélanger, RE Crossler, Privacy in the digital age: a review of information privacy research in information systems, Journal MIS Quarterly, Volume 35 Issue 4, December 2011, Pages 1017-1042, available at http://dl.acm.org/citation.cfm?id=2208951.
3. Sabrina De Capitani di Vimercati, Sara Foresti, Giovanni Livraga, Pierangela Samarati, Data Privacy: Definitions and Techniques, International Journal of Uncertainty, Fuzzi-ness and Knowledge-Based Systems 20(6): 793-818 (2012).
4. Regulation (EU) 2016/679 of the European Parliament and of the Council, The European Parliament and the Council of the European Union, April 27, 2016, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1485368166820&from=en.
5. OECD Privacy Principles, OECDprivacy.org, 1980, available at http://oecdprivacy.org/.
6. Makri E. L., Lambrinoudakis C., "Towards a Common Security and Privacy Requirements Elicitation Methodology", Proceedings of the 10th International Conference Global Security, Safety and Sustainability (ICGS3 2015), 151-160, Springer CCIS 534, London, UK, September 2015.
7. Makri E. L., Lambrinoudakis C., "Privacy Principles: Towards a Common Privacy Audit Methodology", Proceedings of the 12th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'15), pp. 219-234, Springer LNCS 9264, Valencia, Spain, September 2015.
8. Generally Accepted Privacy Principles (GAPP), 2010, available at www.cica.ca/privacy, www.aicpa.org/privacy, https://www.cippguide.org/2010/07/01/generally-accepted-privacy-principles-gapp/.
9. Σ. Ψωφίδης, Ε. Μάγκος, Ηλεκτρονικά Εργαλεία Ενίσχυσης της Ιδιωτικότητας στο Διαδίκτυο, Οκτώβριος 2016, https://apothesis.eap.gr/handle/repo/33048.

10. Kokolakis, S. (2017), Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & Security, Volume 64, January 2017, pp. 122-134.
11. Pew Research Center's (2019), Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
12. Sideri, Maria & Kitsiou, Angeliki & Tzortzaki, Eleni & Kalloniatis, Christos & Gritzalis, Stefanos. (2020). Προστασία της Ιδιωτικότητας σε Ψηφιακά Κοινωνικά Δίκτυα, Μια αναγκαία για τη διατήρηση της κοινωνικής συνοχής στην Κοινωνία της Πληροφορίας;, https://www.researchgate.net/publication/340272769_Prostasia_tes_Idiotikotetas_se_Psephiaka_Koinonika_Diktya_Mia_anankaia_gia_te_diaterese_tes_koinonikes_synoches_sten_Koinonia_tes_Plerophorias.
13. Wright, D.: Should privacy impact assessments be mandatory? Commun. ACM 54(8), 121–131 (2011). https://doi.org/10.1145/1978542.1978568. http://cacm.acm.org/magazines/2011/8
14. Kush Wadhwa & Rowena Rodrigues (2013) Evaluating privacy impact assessments, Innovation: The European Journal of Social Science Research, 26:1-2, 161-180, DOI: 10.1080/13511610.2013.761748, available at http://www.tandfonline.com/doi/abs/10.1080/13511610.2013.761748, http://www.tandfonline.com/doi/pdf/10.1080/13511610.2013.761748?needAccess=true
15. Wright, D.: Should privacy impact assessments be mandatory? Trilateral Research & Consulting, 17 September 2009. http://www.ics.forth.gr/nis09/presentations/18-wright.pdf
16. Kabouraki Konstantina, Gritzalis Stefanos, Moulinos Konstantinos, Towards a Privacy Audit Programmes Comparison Framework, Springer-Verlag Berlin Heidelberg 2004.
17. PrivacySense.net, The 10 Privacy Principles of PIPEDA, http://www.privacysense.net/10-privacy-principles-of-pipeda/.
18. Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, Utilizing a privacy impact assessment method using metrics in the healthcare sector, Information & Computer Security, 503-529, 2020.
19. Georgiopoulou Zafeiroula, Makri Eleni-Laskarina, Lambrinoudakis Costas, GDPR compliance: proposed technical and organizational measures for cloud provider, Information & Computer Security, 665-680, 2020.
20. Makri Eleni-Laskarina, Georgiopoulou Zafeiroula, Lambrinoudakis Costas, A proposed privacy impact assessment method using metrics based on organizational characteristics, Computer Security, ESORICS 2019, 122-139, 2019.
21. Georgiopoulou Zafeiroula, Makri Eleni-Laskarina, Lambrinoudakis Costas, GDPR Compliance: Proposed Technical and Organizational Measures for Cloud Providers, Information & Computer Security, ESORICS 2019, 181-194, 2019.

22. Makri Eleni-Laskarina, Lambrinoudakis Costas, Towards a Common Security and Privacy Requirements Elicitation Methodology, "Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security", ICGS3 2015, 151-159, Springer, 2015.
23. Makri Eleni-Laskarina, Lambrinoudakis Costas, Privacy Principles: Towards a Common Privacy Audit Methodology, "Trust, Privacy and Security in Digital Business", TrustBus 2015, 219-234, Springer, 2015.
24. Data Protection Act 1998, available at http://www.legislation.gov.uk/ukpga/1998/29/contents, http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf
25. European Union Agency for Network and Information Security (ENISA), CRAMM (CCTA Risk Analysis and Management Method), available at https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html
26. L. Barnard and R. von Solms, A formalized approach to the effective selection and evaluation of information security controls (2000), Computer & Security, Vol. 19, No. 2, pp. 185-194.
27. M.M. Eloff and S.H. von Solms, Information security management: A hierarchical framework for various approaches (2000), Computer & Security, Vol. 19, pp. 243-256.
28. Christos Kalloniatis, Evangelia Kavakli, Stefanos Gritzalis, Methods for Designing Privacy Aware Information Systems: A review, PCI, 2009.
29. PriS Methodology:Incorporating Privacy Requirements into the System Design Process, 3rd Symposium on Requirements Engineering for Information Sequrity (SREIS 2005)In conjunction with RE 05 - 13th IEEE International Requirements Engineering ConferenceParis, France, August 29, 2005, available at: http://www.academia.edu/2845236/PriS_Methodology_Incorporating_Privacy_Requirements_into_the_System_Design_Process.
30. C. Kalloniatis, E. Kavakli, E. Kontellis, (2010) "PRIS tool: A case tool for privacy-oriented Requirements Engineering", Journal of Information Systems Security, Vol. 6, No. 1, pp. 3-19, AIS.
31. C. Kalloniatis, E. Kavakli, E. Kontellis, “PriS Tool: A Case Tool for Privacy-Oriented RE”, Proceedings of the MCIS 2009 4th Mediterranean Conference on Information Systems, pp.913-925 (e-version), G. Doukidis et al. (Eds.), September 2009, Athens Greece.
32. C. Kalloniatis, E. Kavakli, S. Gritzalis, "PriS Methodology: Incorporating Privacy Requirements into the System Design Process", Proceedings of the 13th IEEE International Requirements Engineering Conference – SREIS 2005 Symposium on Requirements Engineering for Information Security, J. Mylopoulos, G. Spafford (Eds.) Paris, France, August 2005, IEEE CPS Conference Publishing Services.
33. C. Kalloniatis, E. Kavakli, S. Gritzalis, (2008) "Addressing Privacy Requirements in System Design: The PriS Method", Requirements Engineering (indexed in Thomson’s ISI Web of Knowledge), Vol.13, No.3, pp.241-255, Springer.
34. Directive of the European Parliament and of the Council, European Commission, Brussels, January 25, 2012, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0010&from=en.
35. The OECD Privacy Framework, OECD, 2013.
36. Information technology — Security techniques — Privacy framework, International Standard, ISO/IEC 29100:2011(E), 2011.

37. Privacy, Accountability and Trust – Challenges and Opportunities, ENISA, February 2, 2011, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/pat-study.
38. Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce, July 21, 2000, http://www.export.gov/safeharbor/eu/eg_main_018475.asp.
39. G.W. van Blarkom, J.J. Borking, J.G.E. Olk, "PET", Handbook of Privacy and Privacy-Enhancing Technologies, The Case of Intelligent Software Agents, 2003, ISBN 90-74087-33-7, available at http://www.andrewpatrick.ca/pisa/handbook/Handbook_Privacy_and_PET_final.pdf.
40. Yang Wang, Alfred Kobsa, Privacy-Enhancing Technologies, 2008, available at http://www.cs.cmu.edu/afs/cs/Web/People/yangwan1/papers/2008-Handbook-LiabSec-AuthorCopy.pdf.
41. Ann Cavoukian, Privacy by design – the 7 foundational principles, Technical report, Information and Privacy Commissioner of Ontario, January 2011. (revised version).
42. Jaap-Henk Hoepman, Privacy Design Strategies, May 7, 2013.
43. Jaap-Henk Hoepman, Privacy Design Strategies, October 25, 2012.
44. Ann Cavoukian, Creation of a Global Privacy Standard, November, 2006, available at http://www.ipc.on.ca/images/Resources/gps.pdf.
45. Directive of the European Parliament and of the Council, European Commission, Brussels, March 12, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.
46. Reform of data protection legislation, European Commission, 2012, available at http://ec.europa.eu/justice/data-protection/.
47. David Wright, Paul De Hert, Chapter 1: Introduction to Privacy Impact Assessment, Book Title: Privacy Impact Assessment, 2012, pp 3-32, available at http://link.springer.com/chapter/10.1007/978-94-007-2543-0_1#page-1.
48. Daniel Le Métayer, Chapter 20 - Privacy by Design: A Matter of Choice, Data protec-tion in a profiled world, Springer, 2010, available at http://link.springer.com/chapter/10.1007/978-90-481-8865-9_20.
49. Directive 95/46/EC of the European Parliament and of the Council, The European Parliament and the Council of the European Union, October 24, 1995, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
50. Canadian Standards Association, Model Code for the Protection of Personal Information, A National Standard of Canada, Canadian Standards Association, March, 1996, available at http://www.rogerclarke.com/DV/CanModel.html.
51. Günter Karjoth, Matthias Schunter, and Michael Waidner, Privacy-enabled Services for Enterprises, IBM Research, Zurich Research Laboratory, 2002, available at http://www.semper.org/sirene/publ/KaSW3_02.TrustBus-final-2002-05-01.pdf.
52. Tommie W. Singleton, IT and Privacy Audits, ISACA JOURNAL VOLUME 5, 2009.
53. Directive of the European Parliament and of the Council, European Commission, Brussels, March 12, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.
54. Information Commissioner's Office (ICO), Data Protection Act, Conducting privacy impact assessments code of practice, February 2014, available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.
55. Ann Cavoukian, Scott Taylor, Martin E. Abrams, Privacy by Design: essential for or-ganizational accountability and strong business practices, Identity in the Information

Society, Springer, 2010, available at http://link.springer.com/article/10.1007/s12394-010-0053-z.
56. Oetzel, Marie Caroline and Spiekermann, Sarah, "PRIVACY-BY-DESIGN THROUGH SYSTEMATIC PRIVACY IMPACT ASSESSMENT - A DESIGN SCIENCE APPROACH" (2012), ECIS 2012 Proceedings, paper 160, available at http://aisel.aisnet.org/ecis2012/160.
57. Oetzel, Marie Caroline and Spiekermann, Sarah, A systematic method for privacy im-pact assessments: a design science approach, European Journal of Information Systems (2013), 1–25.
58. Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Wilmslow, Cheshire, December 2007, Version 2.0, June 2009.
59. European Commission, Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C (2009) 3200 final, Brussels, 12 May 2009, available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009H0387&from=EN.
60. Information Commissioner's Office (ICO), Privacy Impact Assessment Handbook, Wilmslow, Cheshire, UK, Version 1.0, December 2007.
61. Sean Brooks, Ellen Nadeau, Privacy Risk Management for Federal Information Sys-tems, Information Technology Laboratory, NIST, Internal Report 8062, May 2015, available at http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.
62. European Commission, PIAF: A Privacy Impact Assessment Framework for data pro-tection and privacy rights, Duration: January 2011 - October 2012, available at http://www.piafproject.eu/Index.html.
63. David Wright, Kush Wadhwa, A step-by-step guide to privacy impact assessment, Sec-ond PIAF workshop, Sopot, Poland, 24 April 2012, available at http://www.piafproject.eu/ref/A_step-by-step_guide_to_privacy_impact_assessment-19Apr2012.pdf.
64. Information Commissioner's Office (ICO), Privacy impact assessment and risk man-agement, May 2013, available at https://ico.org.uk/media/1042196/trilateral-full-report.pdf.
65. Information Commissioner's Office (ICO), The Guide to Data Protection, January 2017, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-7.pdf.
66. ISO/IEC FDIS 29134, Information technology — Security techniques — Privacy impact assessment — Guidelines, Target publication date: 2017-05-30, available at http://www.iso.org/iso/catalogue_detail.htm?csnumber=62289, https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:dis:ed-1:v1:en.
67. John Martin Ferris, The ISO PIA Standard for Financial Services, Chapter 14: The ISO PIA Standard for Financial Services, Book Title: Privacy Impact Assessment, 2012, pp 307-321, available at http://link.springer.com/chapter/10.1007/978-94-007-2543-0_14.
68. NIST (National Institute of Standards and Technology). (2002) Risk management guide for information technology systems, NIST Special Publication 800-30.
69. Sushant Agarwal, Chapter: Developing a Structured Metric to Measure Privacy Risk in Privacy Impact Assessments, Book Title: Privacy and Identity Management. Time for a Revolution?, pp 141-155, 07 July 2016, available at: https://link.springer.com/chapter/10.1007%2F978-3-319-41763-9_10.

70. Commission Nationale de l'Informatique et des Libertés (CNIL), Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA), June 2015 Edition, available at: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf.
71. Commission Nationale de l'Informatique et des Libertés (CNIL), The open source PIA software helps to carry out data protection impact assesment, January 2018, available at: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.
72. Cloud security alliance, code of conduct for GDPR compliance, November 2017 available at https://downloads.cloudsecurityalliance.org/assets/research/gdpr/CSA_Code_of_Conduct_for_GDPR_Compliance.pdf
73. Information Commissioner's Office, Children and the GDPR , 22 March 2018, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulationgdpr/children-and-the-gdpr-1-0.pdf
74. Multistakeholder Expert Group, Contribution from the multistakeholder expert group to the stock-taking exercise of June 2019 on one year of GDPR application, 13 June 2019.
75. Norm Barber (2018), "The GDPR and its implications on cloud services", September 2017.
76. Deloitte (2018), "Data privacy in the cloud", September 2015.
77. Bird & Bird, Guide to the General Data Protection Regulation, January 2017.