ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ενίσχυση της Μεθοδολογίας Privacy Safeguard – PriS με βάση τον GDPR

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

Χατζηγιαννίδου Μαρίας

Επιβλέπουσα Καθηγήτρια: Καρύδα Μαρία

Μέλη εξεταστικής επιτροπής: Καρύδα Μαρία, Κοκολάκης Σπύρος, Λουκής Ευριπίδης

Σάμος, Οκτώβριος 2022

Η σελίδα αυτή είναι σκόπιμα λευκή

Ευχαριστίες

Επιθυμώ να αποδώσω τις ευχαριστίες μου στα πρόσωπα που με βοήθησαν και με υποστήριξαν καθ' όλη τη διάρκεια της συγγραφής αυτής της διπλωματικής εργασίας.

Αρχικά θα ήθελα να ευχαριστήσω θερμά την επιβλέπουσα καθηγήτριά μου, Κυρία Βασιλική Διαμαντοπούλου, για τον χρόνο που αφιέρωσε αλλά και για την εμπιστοσύνη που μου έδειξε εξαρχής αναθέτοντάς μου το συγκεκριμένο θέμα καθώς και για την επιστημονική καθοδήγηση που μου έδωσε μέσω των διορατικών της παρατηρήσεων σε όλη τη διάρκεια της συγγραφής, παρέχοντας μου όλα τα απαραίτητα εφόδια για την ολοκλήρωση αυτής της διατριβής.

Θα ήθελα επίσης να ευχαριστήσω τους καθηγητές μου, Καρύδα Μαρία, Κοκολάκη Σπύρο και Λουκή Ευριπίδη, που υπήρξαν μέλη της επιτροπής αξιολόγησης της διπλωματικής μου εργασίας.

Τέλος έχω την ανάγκη να εκφράσω την ευγνωμοσύνη μου στους γονείς μου και τα αδέρφια μου, για την υποστήριξη και την πίστη που έδειξαν σε εμένα καθ' όλη τη διάρκεια των σπουδών μου.

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Λίστα Σχημάτων

Λίστα Πινάκων

Ακρωνύμια

BPR4GDPR	Business Process Re-engineering and functional toolkit for GDPR compliance
CRUD	Create Read Use Delete
DPIA	Data Privacy Impact Assessment
DPO	Data Protection Officer
DS	Data Subject
EKD	Enterprise Knowledge Development
FIPs	Code of Fair Information Practices
GBRAM	Goal Based Requirement Analysis Method
GDPR	General Data Protection Regulation
LINDDUN	Linkability Identifiability Non-repudiation Detectability Disclosure Information Non-compliance
PA-DFD	Privacy-Aware Data Flow Diagrams
PbD	Privacy by Design
PRIPARE	Preparing Industry to Privacy by Design by supporting its Application in Research
PriS	Privacy Safeguard
PoSeID-on	Protection and control of Secured Information by means of a privacy enhanced Dashboard
SA	Supervisory Authority
SMaRT	Scenario Management and Requirements Tool
STRAP	Structured Analysis Framework for Privacy
ΑΦΜ	Αριθμός Φορολογικού Μητρώου
ΕΑ	Εποπτική Αρχή
ΕΕ	Ευρωπαϊκή Ένωση
ΕΟΧ	Ευρωπαϊκός Οικονομικός Χώρος
ΠΣ	Πληροφοριακό Σύστημα
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών

Περίληψη

Οι σύγχρονοι ρυθμοί ζωής και η ανάγκη χρήσης της τεχνολογίας για την πραγματοποίηση των καθημερινών εργασιών έχει γίνει πλέον τρόπος ζωής για τους περισσότερους ανθρώπους και οργανισμούς. Η χρήση της τεχνολογίας αυτής απαιτεί την παροχή κάποιου είδους προσωπικών πληροφοριών με σκοπό την ταυτοποίηση του ατόμου και την αλληλεπίδρασή του με το σχετιζόμενο σύστημα. Παρέχοντας πολλές προσωπικές πληροφορίες ένα άτομο μπορεί να γίνει ευάλωτο σε επιθέσεις που έχουν τη δυνατότητα να παραβιάσουν το απόρρητό του. Για τον λόγο αυτό η ΕΕ εισήγαγε τον GDPR, σύμφωνα με τις διατάξεις του οποίου πρέπει να συμμορφώνονται όλοι οι οργανισμοί ώστε να προστατεύονται τα δικαιώματα των ατόμων στην ιδιωτική ζωή.

Στα πλαίσια της εργασίας αυτής εξετάζεται ο τρόπος με τον οποίο μπορεί μια υπάρχουσα μεθοδολογία που σκοπό έχει την προστασία της ιδιωτικότητας να ενισχυθεί προκειμένου να ικανοποιεί ορισμένες από τις διατάξεις του GDPR. Πιο συγκεκριμένα αναλύεται η μεθοδολογία PriS, η οποία είναι μία μεθοδολογία προσανατολισμένη στους στόχους του συστήματος και σκοπό έχει την ενσωμάτωση απαιτήσεων απορρήτου εγκαίρως στη διαδικασία ανάπτυξης του συστήματος και κατ' επέκταση του οργανισμού. Περιγράφονται επομένως τα βήματα που ακολουθεί, οι ιδιότητες απορρήτου που ικανοποιεί καθώς και το πλαίσιο πάνω στο οποίο στηρίζεται η προαναφερθείσα μεθοδολογία. Παράλληλα γίνεται μια περιγραφή της έννοιας του GDPR και επιπλέον μια περιγραφή του μοντέλου που ενισχύει τη μεθοδολογία και την ενισχύει, ώστε εφόσον εφαρμοστεί για την ανάπτυξη ενός νέου ή υπάρχοντος ΠΣ, το εν λόγω σύστημα να ικανοποιεί τις αρχές του GDPR.

Προκειμένου να γίνει πιο κατανοητό το περιεχόμενο της εργασίας παρουσιάζονται αρχικά μεθοδολογίες που έχουν ως στόχο την προστασία της ιδιωτικότητας από τον σχεδιασμό και είναι προσανατολισμένες στους στόχους ενός συστήματος. Ο πρώτος λόγος που γίνεται η περιγραφή αυτή είναι διότι η μεθοδολογία PriS ανήκει σε αυτή την κατηγορία των μεθοδολογιών, μεθοδολογίες που είναι δηλαδή προσανατολισμένες στους στόχους του συστήματος. Ο δεύτερος λόγος είναι επειδή ανάμεσα σε αυτές τις μεθοδολογίες, η PriS είναι αυτή που ξεχωρίζει για λόγους που θα παρουσιαστούν παρακάτω και επιλέγεται ως η μεθοδολογία που θα ενισχυθεί με βάση τον GDPR. Πέρα από την περιγραφή γίνεται και η παρουσίαση έργων και μεθοδολογιών που συμμορφώνονται με τον GDPR.

Προσδιορίζονται κατόπιν έννοιες σχετικές με τον GDPR, όπως οι οντότητες του, οι απαιτήσεις του αλλά και αρχές του και παράλληλα αναλύεται η έννοια του απορρήτου καθώς και ιδιότητες αυτού όπως η Ταυτοποίηση, η Αυθεντικοποίηση, η Εξουσιοδότηση, η Προστασία Δεδομένων, η Ανωνυμία, η Ψευδωνυμία, η Μη συνδεσιμότητα και η Μη παρατηρησιμότητα.

Τέλος γίνεται αναλυτικά η περιγραφή του model 5W, ενός μοντέλου που μέσω των ερωτημάτων που θέτει δίνει τη δυνατότητα στο υποκείμενο των δεδομένων να δηλώσει τις προτιμήσεις του σχετικά με τη διάθεση, αποθήκευση και επεξεργασία των προσωπικών του δεδομένων. Το μοντέλο αυτό που χρησιμοποιείται για τον εμπλουτισμό της μεθοδολογίας PriS με βάση τις αρχές του GDPR περιγράφεται και γίνεται πιο κατανοητό με τη βοήθεια μιας μελέτης περίπτωσης.

Λέξεις Κλειδιά: *GDPR, PriS, Μεθοδολογία, Προστασία της Ιδιωτικότητας, Υποκείμενο Δεδομένων, Προσωπικά Δεδομένα, 5W model.*

Abstract

Modern lifestyles and the need to use technology to perform daily tasks has now become a way of life for most people and organizations. The use of this technology requires the provision of some kind of personal information in order to identify the individual and each one's interaction with the related system. By providing a lot of personal information a person can become vulnerable to attacks that have the potential to violate their privacy. For this reason the EU introduced the GDPR, according to the provisions of which all organizations must comply in order to protect the rights of individuals to privacy.

In the context of this work there is an analysis of an existing methodology that aims to protect privacy and has a purpose to be strengthened in order to satisfies some of the provisions of the GDPR. More specifically, the methodology which is analyzed is well-known as PriS, which is a methodology oriented to system goals and its purpose is being incorporated to privacy requirements early in its developmental process system and by extension its organization. The steps that follow therefore described, the privacy properties it satisfies as well as the framework on which the aforementioned methodology is depended on . At the same time, a description of GDPR meaning is mentioned and in addition a description of the model that reinforces the methodology as long as it is implemented for the development of a new or existing PS, the system that satisfies GDPR principles.

In order to make the content of the work more comprehensible, the methodologies are initially presented that aim to protect privacy by design and are oriented towards the goals of a system. The first reason why the description of PriS methodology is mentioned , because of the fact that it belongs to this category of methodologies, methodologies that are oriented towards the objectives of the system. The second reason is because among these methodologies, PriS is the one that stands out for reasons that will be presented below and is chosen as the methodology which will be enhanced based on the GDPR.

In addition to the description, projects and methodologies are also presented that are GDPR compliant. Concepts relevant to the GDPR are then identified, such as its entities, its requirements but also its principles and at the same time the concept of privacy is analyzed as well as its properties such as Identification, Authentication, Authorization, Protection Data, Anonymity, Pseudonymity, Non-Connectivity and Non-Observability.

Finally, the 5W model is described in detail, a model that, through the questions it inquires, enables the data subject to state his preferences regarding the disposal, storage and processing of his/her personal data. This model used to enrich the PriS methodology based on GDPR principles is described and made more comprehensible with the help of a case study.

Keywords: *GDPR, PriS, Methodology, Privacy Protection, Data Subject, Personal Data, 5W model.*

1 *Εισαγωγή*

1.1 Πλαίσιο Μεθοδολογιών Συμμορφωμένο με τον GDPR

Η τεχνολογία είναι πλέον αναγκαίο μέρος της σύγχρονης κοινωνίας και καθημερινότητας. Όλο και περισσότεροι άνθρωποι χρησιμοποιούν συστήματα και εργαλεία λογισμικού, όπως εφαρμογές κινητών και υπολογιστών, ιστοτόπους, καθώς και άλλα συστήματα σε περιβάλλον υπολογιστή για την πραγματοποίηση των καθημερινών εργασιών. Κάθε φορά που γίνεται χρήση αυτών των εφαρμογών καθώς και των συστημάτων πληροφοριών, απαιτείται η παροχή κάποιου είδους προσωπικών πληροφοριών, όπως όνομα, διεύθυνση email, ΑΦΜ ή άλλες πληροφορίες προκειμένου να μπορεί να γίνει η αναγνώριση άρα και πιστοποίηση της ταυτότητας του ατόμου που χρησιμοποιεί την εφαρμογή ή το πληροφοριακό σύστημα αντίστοιχα. Παρέχοντας πολλές προσωπικές πληροφορίες ένα άτομο μπορεί να γίνει ευάλωτο σε επιθέσεις που έχουν τη δυνατότητα να παραβιάσουν το απόρρητό του.

Η προστασία της ιδιωτικότητας ορίζεται ως το δικαίωμα του ατόμου να αποφασίσει ποιο είδος πληροφοριών πρόκειται να συλλεχθεί, να χρησιμοποιηθεί ή και να επεξεργαστεί, [24]. Λαμβάνοντας υπόψιν το απόρρητο των χρηστών και για να διασφαλίσει ένα υψηλότερο επίπεδο απορρήτου στα συστήματα λογισμικού, η Ευρωπαϊκή Ένωση (ΕΕ) εισήγαγε νέες διατάξεις στον GDPR (Γενικό Κανονισμό Προστασίας Δεδομένων - General Data Protection Regulation - GDPR), [18]. Βασικός στόχος του GDPR είναι η προστασία των δικαιωμάτων των ατόμων στην ιδιωτική ζωή, καθώς και η διασφάλιση της συμμόρφωσης των οργανισμών με τις προτεινόμενες αρχές απορρήτου και τα δικαιώματα των χρηστών. Οι οργανισμοί λοιπόν πλέον καλούνται να αντιμετωπίζουν το απόρρητο στα πρώτα στάδια του κύκλου ζωής του λογισμικού, μια πρακτική γνωστή ως Privacy by Design (PbD). Το PbD υιοθετεί προληπτικά μέτρα που προλαμβάνουν τις απειλές, που εντοπίζουν αδυναμίες των συστημάτων και σκοπεύουν στη μείωση των κινδύνων που εντοπίστηκαν, νωρίς και με τρόπο συνεπή, αντί να εφαρμόζονται διορθωτικά μέτρα αργότερα για την επίλυση των συμβάντων ασφαλείας μετά την επέλευσή τους.

Αναπτύχθηκαν πολλές μεθοδολογίες που εστιάζουν σε διαφορετικές απαιτήσεις ιδιωτικότητας ανάλογα με τη διαδικασία που έχουν να φέρουν εις πέρας μεταξύ των οποίων η PriS, η GBRAM, η STRAP, η PRIPARE και η Secure Tropos. Οι μεθοδολογίες αυτές έχουν ως βασικό στόχο τη διευκόλυνση και την υποστήριξη της πρακτικής που αναφέρθηκε, Privacy by Design, δηλαδή την αποτύπωση των απαιτήσεων ιδιωτικότητας, επομένως και την προστασία των προσωπικών δεδομένων του ατόμου, σε ένα σύστημα που αναπτύσσεται ή αναβαθμίζεται. Παρ' ότι η ανάπτυξη και η χρήση των μεθοδολογιών αυτών κρίθηκε ιδιαίτερα σημαντική και χρήσιμη, ύστερα από τις νέες διατάξεις που έφερε ο GDPR εντοπίστηκαν νέα ζητήματα σχεδιασμού σχετικά με τη συμμόρφωση των μεθοδολογιών βάσει των αρχών του GDPR.

1.2 Αντικείμενο διπλωματικής

Αντικείμενο της παρούσας διπλωματικής εργασίας, όπως προκύπτει και από τον τίτλο «Ενίσχυση της Μεθοδολογίας Privacy Safeguard -PriS με βάση τον GDPR» είναι να εμπλουτιστεί η μεθοδολογία PriS με σκοπό να γίνει GDPR compliant, δηλαδή να ενισχυθεί με τις αρχές του GDPR, στο γενικό πλαίσιο του Privacy Engineering που ανήκει. Οι προτεινόμενες αλλαγές στη μεθοδολογία που αφορά τις νέες κατευθυντήριες γραμμές GDPR, που ισχύουν από τον Μάιο του 2018, παρέχουν μια προσέγγιση βήμα προς βήμα για τη διασφάλιση του Privacy by Design.

Σκοπός με την ενίσχυση της μεθοδολογίας PriS, η οποία είναι μια μεθοδολογία ανάλυσης στόχων απορρήτου, που σκοπό έχει την ενσωμάτωση απαιτήσεων απορρήτου εγκαίρως στη διαδικασία ανάπτυξης του συστήματος και κατ' επέκταση του οργανισμού, είναι η επικύρωση της ενίσχυσης της με τις διατάξεις του GDPR προκειμένου να βοηθηθούν οι οργανισμοί να επιτύχουν το Privacy by Design αλλά και να καλύψουν παράλληλα τυχόν κενά σε σχέση με την ενίσχυσή τους με τον GDPR, από τα αρχικά στάδια της ανάπτυξής τους.

Η εισαγωγή ενός μοντέλου γνωστού ως 5W model στο τρίτο βήμα της μεθοδολογίας PriS είναι αυτό που θα χρησιμοποιηθεί για την ενίσχυση της μεθοδολογίας. Το μοντέλο μέσα από πέντε ερωτήματα θα δώσει τη δυνατότητα στο υποκείμενο δεδομένων, δηλαδή του χρήστη ενός πληροφοριακού συστήματος ή τον πελάτη αντίστοιχα ενός οργανισμού, να δηλώσει τις προτιμήσεις του σχετικά με τη διάθεση, χρήση και επεξεργασία των προσωπικών του δεδομένων.

1.3 Δομή της διπλωματικής εργασίας

Στο Κεφάλαιο 1 της παρούσας εργασίας, γίνεται μια εισαγωγή σχετικά με τις μεθοδολογίες και τη σχέση τους με βάσει τον GDPR καθώς και με το περιεχόμενο της διπλωματικής εργασίας. Στο Κεφάλαιο 2 πραγματοποιείται επισκόπηση των μεθοδολογιών. Πιο συγκεκριμένα περιγράφεται πως κατηγοριοποιούνται οι μεθοδολογίες που έχουν ως στόχο το Privacy by Design,

ανάλογα με το που είναι προσανατολισμένες και γίνεται μάλιστα εκτεταμένη παρουσίαση των μεθοδολογιών που στρέφονται στους στόχους ενός συστήματος (goal-oriented methodologies). Επιπλέον σε αυτό το κεφάλαιο εξηγείται ο λόγος που επιλέχθηκε η μεθοδολογία PriS για ενίσχυση με βάση τις αρχές του GDPR και παρουσιάζονται άλλες μεθοδολογίες και έργα που ενισχύονται ήδη με τον GDPR. Το Κεφάλαιο 3 περιγράφει τον GDPR. Στο κεφάλαιο 4 πραγματοποιείται ο σκοπός της διπλωματικής αυτής εργασίας με την ενίσχυση της μεθοδολογίας PriS στα πλαίσια των αρχών του GDPR ενώ παράλληλα περιγράφεται ένα παράδειγμα για την κατανόηση της ενισχυμένης μεθοδολογίας. Η εργασία ολοκληρώνεται με το Κεφάλαιο 5 το οποίο εμπεριέχει τα συμπεράσματα και τη σύνοψη της έρευνας που εκπονήθηκε, καθώς και ορισμένες προτάσεις για να εμπλουτιστεί αυτή η μελέτη.

2 *Επισκόπηση Μεθοδολογιών για Privacy By Design*

2.1 Μεθοδολογίες Προσανατολισμένες στην Προστασία της Ιδιωτικότητας από τον Σχεδιασμό (Privacy by Design)

Η συνεχής ανάπτυξη συστημάτων και εφαρμογών που χρησιμοποιούν ολοένα και περισσότερο προσωπικά δεδομένα, όπως το όνομα ενός ατόμου, τη διεύθυνσή του, τον αριθμό δελτίου ταυτότητας ή ακόμη και δεδομένα που αφορούν την υγεία του, έχει οδηγήσει στην ανάγκη διαφύλαξης αυτών των προσωπικών δεδομένων. Η προστασία επομένως της ιδιωτικότητας και των προσωπικών δεδομένων αποτελεί πλέον ένα από τα κύρια ζητήματα για τους σχεδιαστές των εν λόγω συστημάτων. Για τον λόγο αυτό και προκειμένου να ληφθούν υπόψιν οι απαιτήσεις ιδιωτικότητας, που στοχεύουν στην προστασία των προσωπικών δεδομένων του ατόμου, σε ένα σύστημα που αναπτύσσεται ή αναβαθμίζεται έχει αναπτυχθεί ένα σύνολο μεθοδολογιών, τεχνικών και εργαλείων που διευκολύνουν και υποστηρίζουν την διαδικασία αυτή.

Οι μεθοδολογίες που έχουν αναπτυχθεί για την αποτύπωση των απαιτήσεων ιδιωτικότητας δεν ακολουθούν την ίδια γραμμή, καθώς καθεμία από αυτές εστιάζει σε διαφορετικές απαιτήσεις ιδιωτικότητας ανάλογα με τη διαδικασία που έχει να φέρει εις πέρας. Υπάρχουν λοιπόν οι μεθοδολογίες που είναι προσανατολισμένες στου στόχους του συστήματος (goal-oriented methodologies), μεθοδολογίες προσανατολισμένες στους κινδύνους τους συστήματος (risk-based methodologies) ή στις απειλές που έχει να αντιμετωπίσει το σύστημα (threat-driven methodologies). Ακόμη υπάρχουν μεθοδολογίες που στηρίζονται στην ανάλυση και μοντελοποίηση των προς εξέταση συστημάτων (model-based methodologies) καθώς και μεθοδολογίες που αφορούν κατηγορίες χρηστών-πρακτόρων του συστήματος (agent-oriented methodologies).

Το κεφάλαιο αυτό παρουσιάζει μεθοδολογίες που είναι προσανατολισμένες στους στόχους ενός συστήματος (goal-oriented methodologies). Ο λόγος για την επιλογή της συγκεκριμένης κατηγορίας μεθοδολογιών είναι επειδή κομμάτι της αποτελεί η μεθοδολογία PriS (Privacy Safeguard), που αποτελεί το κύριο αντικείμενο της παρούσας εργασίας καθώς σκοπός της τελευταίας είναι η ενίσχυση της μεθοδολογίας PriS. Ο πρώτος λόγος που επιλέγεται η PriS ως μεθοδολογία για την ενίσχυση της με τον GDPR είναι πως η PriS πέρα από το πρώιμο στάδιο σχεδίασης εντοπίζεται και στο στάδιο εφαρμογής ενός συστήματος, καλύπτοντας με αυτόν τον τρόπο το κενό μεταξύ του σχεδιασμού και της υλοποίησης ενός συστήματος και διευκολύνοντας τη διαδικασία ανάπτυξης του εν λόγω συστήματος. Ο δεύτερος λόγος που επιλέγεται η PriS μεθοδολογία, για να ενισχυθεί με τις αρχές του GDPR, είναι πως στο τρίτο βήμα της μεθοδολογίας προτείνονται έτοιμα πρότυπα διαδικασιών ιδιωτικότητας, τα οποία εμπεριέχουν δραστηριότητες και ροές δεδομένων που συνδέουν τις διεργασίες του υπό ανάπτυξη συστήματος, παρουσιάζοντας με τον τρόπο αυτό πώς πρέπει να λειτουργεί μια επιχείρηση σε ένα τομέα. Ο τελευταίος λόγος είναι διότι η PriS είναι η πιο χρησιμοποιούμενη μεθοδολογία για να εξάγει κάποιος απαιτήσεις απορρήτου με βάση τη βιβλιογραφία.

2.1.1 PriS – Privacy Safeguard

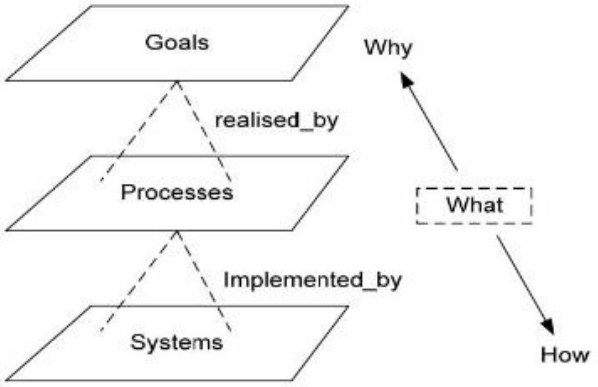
Η PriS – (Privacy Safeguard) [1], η πιο χρησιμοποιούμενη μεθοδολογία για να εξάγει κάποιος απαιτήσεις απορρήτου [7], είναι μια μεθοδολογία ανάλυσης στόχων απορρήτου που σκοπό έχει την ενσωμάτωση απαιτήσεων απορρήτου εγκαίρως στη διαδικασία ανάπτυξης του συστήματος και κατ' επέκταση του οργανισμού. Η μεθοδολογία αντιμετωπίζει τις απαιτήσεις απορρήτου ως στόχους που χρήζουν ικανοποίηση, παρέχοντας ένα φάσμα εννοιών για την μοντελοποίηση και τη μετάφραση αυτών των απαιτήσεων σε μοντέλα συστήματος. Η PriS χρησιμοποιεί πρότυπα διαδικασίας απορρήτου με σκοπό [2] :

1. Την περιγραφή της επιρροής των απαιτήσεων ιδιωτικότητας στις διαδικασίες που υποστηρίζονται από το πληροφοριακό σύστημα.
2. Τον ευκολότερο προσδιορισμό της αρχιτεκτονικής του συστήματος που ενισχύει πιο καλά τις επιχειρηματικές διεργασίες που συνδέονται με το απόρρητο.

Το μοντέλο εννοιών που χρησιμοποιεί η μεθοδολογία PriS στηρίζεται στο πλαίσιο Enterprise Knowledge Development (EKD) [1], το οποίο είναι μια συστηματική προσέγγιση που στόχο έχει να αναπτύξει και να τεκμηριώσει την οργανωσιακή γνώση. Ο συγκεκριμένος στόχος του πλαισίου (EKD) επιτυγχάνεται με τη μοντελοποίηση :

1. Των οργανωτικών στόχων που αποδίδουν τους σκόπιμους στόχους που ελέγχουν και διέπουν τη λειτουργία του
2. Των «φυσικών» διαδικασιών που λειτουργούν από κοινού με τους οργανωτικούς στόχους και

3. Των συστημάτων λογισμικού που υποστυλώνουν οι προαναφερθείσες διαδικασίες.



Σχήμα 1. Πλαίσιο Enterprise Knowledge Development (EKD)

Το σχήμα του πλαισίου EKD παρουσιάζεται στο σχήμα 1, [1]. Όπως αποτυπώνεται στο σχήμα αυτό οι διαδικασίες (processes) αναφέρονται στο τι (what) πρέπει να γίνει, οι στόχοι (goals) αιτιολογούν γιατί (why) υπάρχουν οι σχετιζόμενες διαδικασίες (processes) ενώ τα συστήματα (systems) αναπαριστούν πως (how) μπορούν να υλοποιηθούν οι διαδικασίες (processes) χρησιμοποιώντας όρους κατάλληλων αρχιτεκτονικών συστημάτων.

Η PriS λαμβάνει υπόψη οκτώ διαφορετικές ιδιότητες απορρήτου για την περιγραφή της ιδιωτικότητας των χρηστών, που παρουσιάζονται στην ενότητα 3.2.1 , οι οποίες είναι : Ταυτοποίηση, Αυθεντικοποίηση, Εξουσιοδότηση, Προστασία Δεδομένων, Ανωνυμία, Ψευδωνυμία, Μη συνδεσιμότητα, Μη παρατηρησιμότητα. Η μεθοδολογία PriS περιέχει τέσσερα βήματα κατά την εφαρμογή της συνολικά. Τα τέσσερα βήματα που περιέχει η μεθοδολογία είναι :

1. Ανάδειξη των στόχων απορρήτου του συστήματος. Στο συγκεκριμένο βήμα προσδιορίζονται βασικά θέματα που αφορούν την προστασία της ιδιωτικής ζωής μέσω της επικοινωνίας με τους φορείς λήψης αποφάσεων και τα ενδιαφερόμενα μέρη. Επιπλέον επεξηγούνται γενικές απαιτήσεις απορρήτου σε σχέση με το πλαίσιο εφαρμογής και προσδιορίζονται οι απαιτήσεις απορρήτου που προϋπάρχουν και είναι ήδη κομμάτι των στόχων του οργανισμού.
2. Ανάλυση και εξέταση του αντικτύπου των στόχων απορρήτου, που προσδιορίστηκαν στο πρώτο βήμα της μεθοδολογίας, με την ανάλυση να γίνεται βάσει των διαδικασιών του συστήματος που υποστηρίζεται από τον οργανισμό και την εξέταση να πραγματοποιείται βάσει των διαδικασιών που αποσκοπούν στην επίτευξη αυτών των στόχων. Επίσης εντοπίζονται οι διαδικασίες που επιτυγχάνουν τους στόχους απορρήτου και επισημαίνονται ως διαδικασίες που σχετίζονται με το απόρρητο. Καινούργιοι στόχοι και αναθεώρηση των υφιστάμενων είναι πιθανό να υπάρξουν στη διάρκεια αυτού του βήματος.
3. Μοντελοποίηση των διαδικασιών απορρήτου με πρότυπο τα σχετικά μοτίβα διαδικασίας απορρήτου. Τα πρότυπα επιχειρηματικής διαδικασίας είναι

συνήθως γενικευμένα μοντέλα διαδικασιών, τα οποία περιλαμβάνουν δραστηριότητες και ροές που τα συνδέουν, παρουσιάζοντας πώς μια επιχείρηση πρέπει να λειτουργεί σε έναν συγκεκριμένο τομέα [3]. Μοντελοποίηση προτύπων διαδικασίας απορρήτου σε επιχειρησιακές διαδικασίες για τη μεθοδολογία PriS, έχουν γίνει από νεότερες μελέτες [4], συνεισφέροντας με αυτό τον τρόπο στη σχεδίαση της αρχιτεκτονικής του συστήματος η οποία μπορεί να υποστηρίξει όσο το δυνατόν καλύτερα τις σχετιζόμενες με την ιδιωτικότητα επιχειρησιακές διεργασίες (privacy-related business processes).

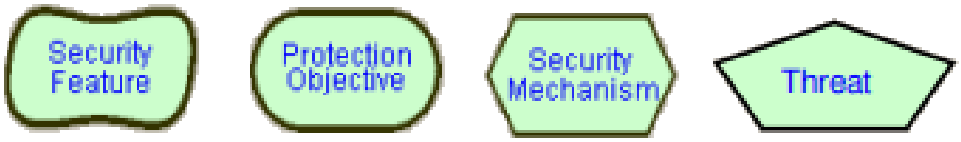
4. Ορισμός της αρχιτεκτονικής συστήματος που υποστυλώνει πιο καλά τη διαδικασία που σχετίζεται με το απόρρητο που καθορίστηκε νωρίτερα μέσω του βήματος τρία. Για τον ορισμό της αρχιτεκτονικής αυτής χρησιμοποιούνται επίσης πρότυπα.

2.1.2 Secure Tropos

Η μεθοδολογία Secure Tropos, η οποία είναι η πιο συχνά χρησιμοποιούμενη μεθοδολογία στις επιστημονικές μελέτες [7], αποτελεί επέκταση της μεθοδολογίας Tropos ως προς δύο κατευθύνσεις, τις έννοιες και τη διαδικασία, και αναπτύχθηκε με στόχο την ενσωμάτωση της ασφάλειας σε όλη τη διαδικασία ανάπτυξης ενός Πληροφοριακού Συστήματος [5],[6]. Η μεθοδολογία αυτή είναι επίσης προσανατολισμένη στους στόχους (goal oriented) του συστήματος όπως η μεθοδολογία PriS και περιλαμβάνει τέσσερις δραστηριότητες μοντελοποίησης [6]. Οι δραστηριότητες αυτές περιλαμβάνουν :

1. Τη μοντελοποίηση αναφοράς ασφαλείας. Σε αυτή τη δραστηριότητα μοντελοποίησης, η οποία έχει ως στόχο να επιτρέψει την ευελιξία κατά τα στάδια ανάπτυξης ενός συστήματος πολλαπλών πρακτόρων και επίσης να εξοικονομήσει χρόνο και προσπάθεια, προσδιορίζονται οι ανάγκες ασφαλείας που αφορούν το μελλοντικό σύστημα, τα πιθανά προβλήματα, όπως απειλές και ευάλωτα σημεία, που έχουν σχέση με την ασφάλεια του συστήματος καθώς και προτάσεις για την αντιμετώπιση των προβλημάτων. Μέσα από την ανάλυση αυτή προκύπτει το διάγραμμα αναφοράς ασφαλείας, το οποίο αν και δημιουργείται στα πρώτα στάδια ανάπτυξης του συστήματος λαμβάνεται υπόψιν και στην υπόλοιπη διαδικασία ανάπτυξης του, για τον εντοπισμό περιορισμών ασφαλείας και πιθανών μέσων που συντείνουν στην αντιμετώπιση αυτών των περιορισμών που αφορούν την ασφάλεια. Επίσης στη διάρκεια αυτής της δραστηριότητας εξετάζονται χαρακτηριστικά ασφαλείας, όπως το απόρρητο, η διαθεσιμότητα και η ακεραιότητα, στόχοι προστασίας όπως η εξουσιοδότηση, η κρυπτογραφία και η λογοδοσία, μηχανισμοί ασφαλείας που βοηθούν στην εκπλήρωση των στόχων προστασίας και απειλές όπως η κοινωνική μηχανική, η ανίχνευση κωδικού πρόσβασης και οι επιθέσεις υποκλοπής. Έννοιες που αφορούν το διάγραμμα που

δημιουργείται από τη μοντελοποίηση της αναφοράς ασφαλείας παρουσιάζεται στο σχήμα 2.



Σχήμα 2. Διάγραμμα από τη Μοντελοποίηση Αναφοράς Ασφάλειας

2. Τη μοντελοποίηση περιορισμών ασφαλείας, η οποία περιλαμβάνει μικρότερες δραστηριότητες μοντελοποίησης όπως την ανάθεση περιορισμών ασφαλείας, την εκχώρησή και την ανάλυσή – αποσύνθεσή τους. Η ανάθεση περιορισμών ασφαλείας επιτρέπει την ανάθεση ενός περιορισμού ασφαλείας από έναν παράγοντα σε άλλον. Η εκχώρηση ενός περιορισμού ασφαλείας σε έναν στόχο υποδεικνύεται με έναν σύνδεσμο συνεισφοράς που φέρει την ετικέτα "περιορίζει". Η αποσύνθεση – ανάλυση των περιορισμών ασφαλείας προσδιορίζει πιθανούς ασφαλείς στόχους που μπορεί να εισαγάγει ο περιορισμός στο σύστημα. Όλη αυτή η διαδικασία μοντελοποίησης των περιορισμών ασφαλείας έχει ως στόχο να βοηθήσει τους προγραμματιστές να μειώσουν όσον το δυνατόν περισσότερο τους περιορισμούς που στοχεύουν στην ασφάλεια του συστήματος.
3. Τη μοντελοποίηση ασφαλών οντοτήτων. Η δραστηριότητα αυτή η οποία είναι συμπληρωματικό στοιχείο της προηγούμενης δραστηριότητας (μοντελοποίηση περιορισμών ασφαλείας), περιέχει την ανάλυση στόχων ασφαλείας, εργασιών και πόρων που περιγράφονται σε ένα σύστημα πολλαπλών πρακτόρων.
4. Τη μοντελοποίηση ασφαλών δυνατοτήτων. Αυτή η τελευταία δραστηριότητα μοντελοποίησης της μεθοδολογίας Secure Tropos προσδιορίζει τις δυνατότητες ασφάλειας των πρακτόρων και των παραγόντων, λαμβάνοντας υπόψη τις εξαρτήσεις που περιλαμβάνουν οι ασφαλείς οντότητες στο εκτεταμένο διάγραμμα δρώντων, προκειμένου να εγγυηθεί την ικανοποίηση των περιορισμών ασφαλείας.

Η μεθοδολογία Secure Tropos υποστηρίζεται από την εφαρμογή SecTro Tool[5], που δημιουργήθηκε με Java[1], με στόχο να υποστηρίζει τους προγραμματιστές στις προαναφερθείσες δραστηριότητες μοντελοποίησης της μεθοδολογίας. Στη διάρκεια αναπαράστασης των τεσσάρων δραστηριοτήτων το εργαλείο διαθέτει μηχανισμό ελέγχου των κανόνων και των περιορισμών ώστε να ενημερώνει τον προγραμματιστή για οποιοδήποτε σφάλμα.

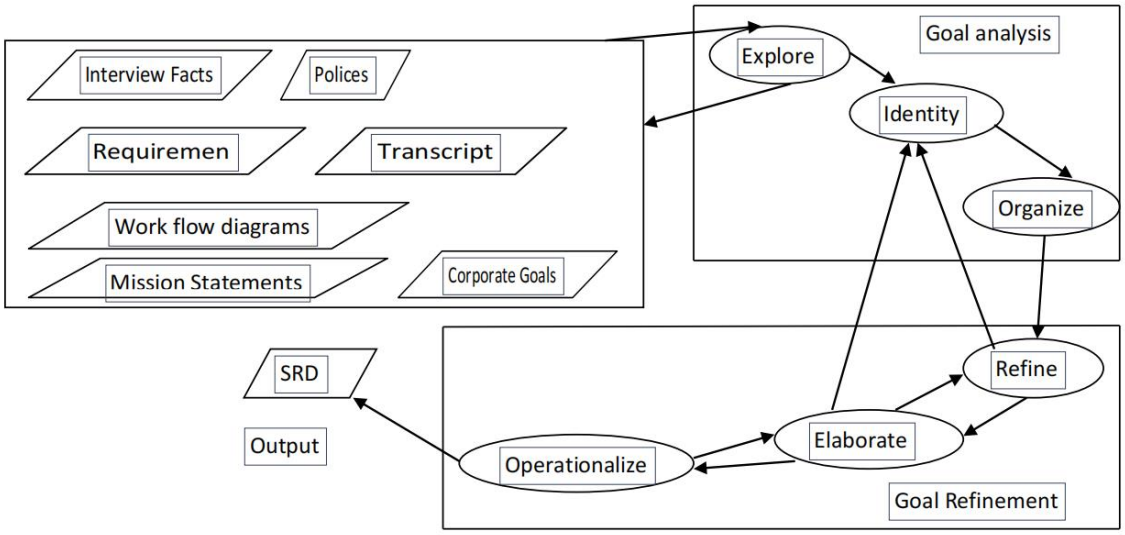
[1] Η **Java** είναι αντικειμενοστρεφής γλώσσα προγραμματισμού

2.1.3 GBRAM

Η μεθοδολογία GBRAM – Goal Based Requirement Analysis Method [8] έχει ως βασικό μέλημα να αναγνωρίσει και να αναλύσει τους μελλοντικούς οργανωτικούς στόχους του Πληροφοριακού Συστήματος για την ανάπτυξη συστημάτων λογισμικού. Η μεθοδολογία GBRAM επίσης προσανατολισμένη στους στόχους τους συστήματος όπως οι δύο προηγούμενες, ακολουθεί μια στρατηγική ανάλυσης καταστάσεων μέσω της οποίας προκύπτει υπό ποιες προϋποθέσεις ένας στόχος μπορεί να αποτύχει ή να μπλοκαριστεί, βρίσκοντας με αυτό τον τρόπο τις λύσεις που δημιουργούν αυτές τις αποτυχίες και τα μπλοκαρίσματα.

Η μεθοδολογία αποτελείται από δύο δραστηριότητες : την ανάλυση (goal analysis) και τη βελτίωση (goal refinement) στόχων. Η πρώτη δραστηριότητα (ανάλυση στόχων), αναγνωρίζει τις πηγές των στόχων και τις ταξινομεί σύμφωνα με τις σχέσεις εξάρτησης είτε ως στόχους ιδιωτικότητας είτε ως ευπάθειες. Οι πρώτοι (στόχοι ιδιωτικότητας) αντικατοπτρίζουν την προσπάθεια ενός οργανισμού να προστατεύσει την ιδιωτικότητα των πελατών του, ενώ οι ευπάθειες εκφράζουν απειλές που σχετίζονται με το απόρρητο του πελάτη. Η βελτίωση στόχων, δεύτερη δραστηριότητα της μεθοδολογίας GBRAM, πραγματοποιείται μέσα από επαναλαμβανόμενους τύπους ερωτήσεων. Το εργαλείο που χρησιμοποιείται για να υποστηρίζει τη μεθοδολογία λέγεται SMaRT (Scenario Management and Requirements Tool) [18] και η έξοδος του GBRAM είναι πάντα ένα έγγραφο απαιτήσεων λογισμικού (SRD). Το SRD περιλαμβάνει τις λειτουργικές και μη λειτουργικές απαιτήσεις του συστήματος.

Παρακάτω απεικονίζεται στο σχήμα οι δραστηριότητες της μεθοδολογίας GBRAM.



Σχήμα 3. Δραστηριότητες της μεθοδολογίας GBRAM

2.1.4 STRAP

Η μέθοδος STRAP (Structured Analysis Framework for Privacy) είναι και αυτή προσανατολισμένη στους στόχους του συστήματος (goal – oriented) [9]. Σκοπός της μεθόδου είναι η εξαγωγή και ο προσδιορισμός των απαιτήσεων απορρήτου στη διάρκεια του σχεδιασμού του συστήματος. Η μέθοδος STRAP μοντελοποιεί τους στόχους που αντιπροσωπεύουν τις λειτουργικές απαιτήσεις και τα ευάλωτα μέρη, δηλαδή τις απαιτήσεις απορρήτου, οι οποίες αν και αποτελούν εμπόδια για την εκπλήρωση των λειτουργικών απαιτήσεων οφείλουν να ικανοποιούνται από το σύστημα [9],[10]. Η συγκεκριμένη μέθοδος δεν υποστηρίζεται από κάποιο εργαλείο.

Το πλαίσιο STRAP εμπεριέχει τέσσερα βήματα κατά την διάρκεια της χρήσης του [10], τα οποία βήματα είναι :

1. Ανάλυση στόχων. Σε αυτό το βήμα αναλύονται οι στόχοι καθώς και οι υποστόχοι, οι ενεργές οντότητες και οι βασικές συνιστώσες του συστήματος. Ένα πρώτο σύνολο απαιτήσεων απορρήτου δημιουργείται μέσα από την καταγραφή πληροφοριών που σχετίζονται με το προς ανάπτυξη σύστημα. Η μέθοδος προκειμένου να ορίσει τους στόχους των προηγούμενων φάσεων κάνει χρήση ερωτηματολογίου. Μέσω του ερωτηματολογίου αυτού καταφέρνει να εντοπίσει διάφορες ευπάθειες του συστήματος σχετικά με την προστασία του απορρήτου, τις οποίες καταγράφει στο μοντέλο των στόχων ως τροχοπέδη μεταξύ των στόχων και των υποστόχων. Οι ευπάθειες που εντοπίστηκαν ελέγχονται προκειμένου να απαλειφθούν ομοιότητες, διπλότυπα που υπάρχουν, ξεκαθαρίζοντας με αυτό τον τρόπο όσες πλέον θεωρούνται αναγνωρισμένες και κατηγοριοποιώντας τες βάσει της λίστας καλών πρακτικών πληροφοριών (Code of Fair Information Practices – FIPs), διευκολύνοντας έτσι τη φάση στην οποία προτείνονται λύσεις.
2. Βελτιστοποίηση. Σε αυτό το στάδιο της μεθόδου διαγράφονται όσες ευπάθειες του συστήματος, που καταγράφηκαν στο προηγούμενο βήμα, έχουν λύση. Με αυτό τον τρόπο οι σχεδιαστές του συστήματος μειώνουν τις συνολικές ευπάθειες του συστήματος.
3. Αξιολόγηση. Αυτό το βήμα περιέχει τον έλεγχο και την αξιολόγηση των σεναρίων της σχεδίασης του προς ανάπτυξη συστήματος. Η αξιολόγηση γίνεται με ορισμένα κριτήρια και με στόχο να εξαλείψουν όσο τον δυνατόν περισσότερες ευπάθειες. Το σενάριο που αντιμετωπίζει τα περισσότερα ευάλωτα σημεία του συστήματος είναι αυτό που επιλέγεται γιατί εκτός του ότι περιορίζει τον κίνδυνο, εξασφαλίζει την προστασία της ιδιωτικότητας.
4. Επανάληψη. Η φάση αυτή περιλαμβάνει την επανάληψη των τριών προηγούμενων βημάτων με στόχο να λάβει υπόψιν όλες τις πιθανές αλλαγές που πραγματοποιήθηκαν στο σύστημα μετά την δημιουργία των νέων στόχων. Το βήμα της επανάληψης σταματά όταν δεν υπάρχουν αλλαγές στα βήματα που αναφέρθηκαν.

2.1.5 PRIPARE

Η μεθοδολογία PRIPARE (Preparing Industry to Privacy by Design by supporting its Application in Research) [20], είναι η τελευταία goal-oriented methodology που θα παρουσιαστεί στην εργασία. Σκοπός της παρούσας μεθοδολογίας είναι να καλύψει τους εμπλεκόμενους σε όλη την διάρκεια ανάπτυξης του συστήματος, μέσα από τις δύο φάσεις που την υποστηρίζουν, τη φάση της ανάλυσης και τη φάση του σχεδιασμού του συστήματος.. Η PRIPARE έχει σκοπό να καλύψει τις αρχές της ιδιωτικότητας από την φάση του σχεδιασμού και της υλοποίησης του συστήματος μέσω μιας διαδικασίας που εξηγεί με ακρίβεια τις διαδικασίες που απαιτούνται για τη σύνδεση από τις αφηρημένες αρχές και έννοιες της ιδιωτικότητας στις απαιτήσεις ιδιωτικότητας.

Η συγκεκριμένη μεθοδολογία κάνει χρήση δύο προσεγγίσεων για να προσδιορίσει τις απαιτήσεις ιδιωτικότητας στη φάση της ανάλυσης του συστήματος. Αυτές οι προσεγγίσεις συνοψίζονται ως εξής :

A. Η προσανατολισμένη στους στόχους προσέγγιση έχει ως σκοπό να μειώσει την αβεβαιότητα, από τα πρώτα στάδια της διαδικασίας ανάπτυξης ενός συστήματος καταγράφοντας ένα λεπτομερές σύνολο απαιτήσεων. Στόχος μέσα από αυτή την προσέγγιση είναι να καταγραφούν ιεραρχημένα και ταξινομημένα κατά προτεραιότητα οι απαιτήσεις ιδιωτικότητας. Επίσης η προσέγγιση αυτή επιτρέπει τη μετατροπή των πιο γενικών απαιτήσεων ιδιωτικότητας σε επιχειρησιακές απαιτήσεις. Η προσέγγιση αυτή έχει αντίστοιχα δυο βήματα από τα οποία αποτελείται :
    - Την ανάλυση, όπου οι αφηρημένες απαιτήσεις ιδιωτικότητας γίνονται σταδιακά ποιες συγκεκριμένες απαιτήσεις.
    - Το σχεδιασμό, μέσα από τον οποίο οι παραπάνω απαιτήσεις συσχετίζονται στα τεχνικά η οργανωτικά μέτρα που θα υλοποιηθούν.
B. Η προσανατολισμένη στην ανάλυση των κινδύνων προσέγγιση εμπεριέχει μέτρα για την αντιμετώπιση το κινδύνων που απειλούν το σύστημα, όπως το επίπεδο επικινδυνότητας. Η συγκεκριμένη προσέγγιση αποτελείται από τέσσερα βήματα :
    - Συμμόρφωση με το Νομικό Πλαίσιο : Χρησιμοποιούνται ερωτηματολόγια που βοηθούν στο να προσδιοριστεί η αποτίμηση αντίκτυπου ιδιωτικότητας (PIA).
    - Εκτίμηση Αντικτύπου : Προσφέρεται διπλή εκτίμηση του αντικτύπου, αφενός για τον οργανισμό, που συνήθως μεταφράζεται σε οικονομικές απώλειες, αφετέρου για τα υποκείμενα των δεδομένων, για την προστασία της ιδιωτικότητας τους.
    - Μέτρηση Κινδύνου : Γίνεται χρήση μιας συνάρτησης στην οποία λαμβάνεται υπόψη ο πιθανός αντίκτυπος και η πιθανότητα εμφάνισης του κινδύνου.
    - Αντιμετώπιση Ζητημάτων Ιδιωτικότητας : Ο περιορισμός της επικινδυνότητας δεν είναι πάντοτε εφικτός, για τον λόγο αυτό πρέπει να είναι σαφής η

εναπομείνασα επικινδυνότητα, η οποία πρέπει να καταγράφεται και να κοινοποιείται σε όλους τους εμπλεκόμενους.

Στην δεύτερη φάση της μεθοδολογίας που είναι ο σχεδιασμός του συστήματος, υπάρχουν τρία επιμέρους βήματα - προσεγγίσεις :

A. Top-Down Προσέγγιση: Από την ανάλυση των απαιτήσεων προκύπτει η αρχιτεκτονική του συστήματος, η οποία αρχιτεκτονική μπορεί να διαφέρει ανάλογα των παραδοχών εμπιστοσύνης μεταξύ των ενδιαφερομένων.
B. Down-Top Προσέγγιση: Σκοπός της συγκεκριμένης προσέγγισης είναι να προσδιορίσει τις ιδιότητες που αποδεικνύουν ότι ικανοποιούνται οι απαιτήσεις ιδιωτικότητας. Η συγκεκριμένη προσέγγιση εφαρμόζεται κυρίως όταν υπάρχει από πριν πηγαίος κώδικας.
C. Horizontal Προσέγγιση: Στόχος της παρούσας προσέγγισης η οποία έχει ήδη μια αρχιτεκτονική είναι η ενδυνάμωση της τελευταίας, που στοχεύει στην επίτευξη των στόχων ιδιωτικότητας ταυτόχρονα με τους επιχειρησιακούς στόχους, αποφεύγοντας κατ' αυτόν τον τρόπο κινδύνους που απειλούν την ιδιωτικότητα και διασφαλίζοντας πως υπάρχει ασφάλεια.

2.2 Επιλογή Μεθοδολογίας για συμμόρφωση με τον GDPR

Όπως αναλύθηκε στην προηγούμενη υποενότητα υπάρχουν διάφορες κατηγορίες μεθοδολογιών που στοχεύουν στο Privacy by Design. Οι κατηγορίες αυτές διαφέρουν ανάλογα με τον σκοπό που έχουν οι μεθοδολογίες που εμπεριέχονται σε αυτές. Έτσι για παράδειγμα στις goal-oriented methodologies περιλαμβάνονται μεθοδολογίες όπως η PriS, η Secure Tropos, η GBRAM, η STRAP, η PRIPARE. Οι μεθοδολογίες αυτές αν και ανήκουν στην ίδια κατηγορία μεθοδολογιών που στοχεύουν στο Privacy By Design, δεν ακολουθούν την ίδια διαδικασία. Υπάρχουν διαφορές ανάμεσα στα στάδια που εφαρμόζεται η κάθε μεθοδολογία, στις απαιτήσεις ιδωτικότητας που εξετάζει καθώς και στην τεχνική υλοποίηση.

Για παράδειγμα η GBRAM, η PRIPARE και η STRAP εφαρμόζονται στο πρώιμο στάδιο σχεδίασης του συστήματος. Η Secure Tropos εφαρμόζεται και στο αρχικό και στο τελικό στάδιο σχεδίασης Αντίθετα η PriS πέρα από το πρώιμο στάδιο σχεδίασης εντοπίζεται και στο στάδιο εφαρμογής ενός συστήματος, καλύπτοντας με αυτόν τον τρόπο το κενό μεταξύ του σχεδιασμού και της υλοποίησης ενός συστήματος και διευκολύνοντας τη διαδικασία ανάπτυξης του εν λόγω συστήματος. Αυτός είναι και ο πρώτος λόγος που επιλέγεται η PriS ως μεθοδολογία για την ενίσχυσή της με τον GDPR. Ένας ακόμη λόγος που επιλέγεται η μεθοδολογία PriS είναι γιατί είναι η πιο χρησιμοποιούμενη μεθοδολογία για να εξάγει κάποιος απαιτήσεις απορρήτου με βάση

το άρθρο «Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners».

Ο τρίτος λόγος που επιλέγεται η PriS μεθοδολογία, για να ενισχυθεί με τις αρχές του GDPR, είναι πως στο τρίτο βήμα της μεθοδολογίας προτείνονται έτοιμα πρότυπα διαδικασιών ιδιωτικότητας, τα οποία εμπεριέχουν δραστηριότητες και ροές δεδομένων που συνδέουν τις διεργασίες του υπό ανάπτυξη συστήματος, παρουσιάζοντας με τον τρόπο αυτό πώς πρέπει να λειτουργεί μια επιχείρηση σε ένα τομέα. Τα πρότυπα αυτά λοιπόν, τα οποία περιγράφονται σε δύο επίπεδα το καθένα καταφέρνουν να απλοποιήσουν την ικανοποίηση των στόχων – αρχών του GDPR, όπως παρουσιάζεται παρακάτω στο Κεφάλαιο 4.

2.3 Μεθοδολογίες και Έργα που συμμορφώνονται με τον GDPR

Υπάρχουν πάρα πολλά έργα που έχουν αναπτυχθεί με σκοπό να βοηθήσουν οργανισμούς σε διαφορετικούς τομείς να συμμορφωθούν με τον GDPR. Μεταξύ αυτών των έργων της Ευρωπαϊκής Ένωσης συμπεριλαμβάνονται το BPR4GDPR [13] - (Business Process Re-engineering and functional toolkit for GDPR compliance), το DEFeND [12], το SMOOTH [14], το PDP4E – (Privacy & Data Protection for Engineering) [15], το PAPAYA [16] καθώς και το PoSeID-on – (Protection and control of Secured Information by means of a privacy enhanced Dashboard [17]. Και τα έξι αυτά έργα στοχεύουν να αντιμετωπίσουν την έλλειψη ορισμένων λειτουργικών λύσεων που ανταποκρίνονται σε προκλήσεις νομικές που θέτει ο GDPR, παρέχοντας συστηματικές μεθόδους, λεπτομερείς τεχνικές και εργαλεία λογισμικού. Ο στόχος καθώς και το πεδίο εφαρμογής του κάθε έργου υλοποιείται διαφορετικά.

Μολονότι έχει δημιουργηθεί ένα πλήθος έργων που στοχεύει στην συνδρομή των οργανισμών με σκοπό την ενίσχυσή τους με τον GDPR, παρατηρείται πως οι μεθοδολογίες που ενισχύονται με τις αρχές του GDPR είναι ελάχιστες. Συγκεκριμένα μεθοδολογίες που έχουν ως σκοπό το Privacy by Design και ενισχύονται παράλληλα με τον GDPR δεν υπάρχουν στην έως τώρα βιβλιογραφία, με εξαίρεση την μεθοδολογία LINDDUN +, η οποία ενισχύθηκε πριν από λίγα χρόνια στα πλαίσια μιας εργασίας με σκοπό να καλύψει κενά σχεδιασμού που είχε η προηγούμενη μεθοδολογία (LINDDUN) βάσει του κανονισμού GDPR. Παρακάτω αναλύονται οι στόχοι των Ευρωπαϊκών Έργων υποενότητα (2.3.2), ενώ στην υποενότητα (2.3.1) γίνεται η παρουσίαση της μεθοδολογίας LINDDUN +.

2.3.1 Συνδυασμός LINDDUN με GDPR (LINDDUN +)

Η μεθοδολογία LINDDUN+ αποτελεί επέκταση της μεθοδολογίας LINDDUN, η οποία δεν ανήκει στις goal-oriented methodologies αλλά στις μεθοδολογίες που είναι προσανατολισμένες στις απειλές ενός συστήματος. Η επέκταση της μεθοδολογίας έγινε στα πλαίσια μιας εργασίας [11], με σκοπό να καλύψει κενά σχεδιασμού που είχε η μεθοδολογία LINDDUN βάσει του GDPR (Γενικού Κανονισμού Προστασίας Δεδομένων), επιτρέποντας παράλληλα στον σχεδιαστή του συστήματος να κατανοήσει καλύτερα σε ποιο σημείο της αρχιτεκτονικής υπάρχουν ευαίσθητες πληροφορίες που σχετίζονται με το απόρρητο υλοποιώντας κατ' αυτόν τον τρόπο ένα μέρος της διαδικασίας αυτοματοποίησης της αρχικής μεθοδολογίας LINDDUN.

Τα βήματα επέκτασης που ενισχύουν τη μεθοδολογία LINDDUN και δημιουργούν τη LINDDUN+ είναι στο σύνολο τρία [11] και προκύπτουν μετά από την αντιστοίχιση των αρχών που κάλυπτε η μεθοδολογία LINDDUN με τις οκτώ σε αριθμό αρχές προστασίας δεδομένων (data protection) που περιέχει ο GDPR και υπάρχουν αναλυτικά στο κεφάλαιο 3. Τα βήματα της ενισχυμένης μεθοδολογίας είναι :

1. Το PA-DFD. [2] Η εκτεταμένη αυτή έκδοση του DFD (Data Flow Diagram) στη LINDDUN+ υπάρχει για δύο λόγους. Ο πρώτος λόγος είναι για να διευκολύνει έναν επαγγελματία να προσδιορίσει ποια σημεία που σχετίζονται με το απόρρητο στην αρχιτεκτονική χρειάζονται περισσότερη προσοχή, διότι με ένα DFD αυτά τα σημεία πολλές φορές δεν γίνονται εύκολα αντιληπτά. Ο δεύτερος λόγος που εισάγεται ένα PA-DFD στη μεθοδολογία είναι για να την αυτοματοποιήσει., αφού σχετίζεται με την ανάπτυξη των κανόνων δέντρων απειλών που επιταχύνουν αυτή τη διαδικασία.
2. Επεκτάσεις των Δέντρων Απειλών (Threat Trees). Το βήμα αυτό στοχεύει στο να συμπεριληφθούν επιπλέον απειλές ώστε να καλυφθούν όσο το δυνατόν περισσότερο αρχές του GDPR, με την αναθεώρηση των ήδη υπαρχουσών κόμβων δύο δέντρων απειλών, του Content Unawareness και Policy Tree και του Non Compliance Tree.
3. Κανόνες LINDDUN+ Threat Tree. Με τους κανόνες του βήματος αυτού που στόχο έχουν να υλοποιήσουν ένα πρώτο βήμα στην ανάπτυξη ενός αυτοματοποιημένου εργαλείου αντιμετωπίζονται οι απειλές που εντοπίστηκαν στο προηγούμενο βήμα με τα δύο δέντρα.

[2] Το PA-DFD (Privacy-Aware Data Flow Diagrams), είναι μια επέκταση του DFD (Data Flow Diagram) καθώς προσθέτει επιπλέον ελέγχους απορρήτου στα ήδη υπάρχοντα DFD.

2.3.2 Στόχοι των Ευρωπαϊκών Έργων που συμμορφώνονται με τον GDPR

Σκοπός του BPR4GDPR [13] είναι η παροχή ενός ολιστικού πλαισίου ικανού να υποστηρίξει από άκρο σε άκρο συμβατές διεργασίες με τον GDPR, που υποστηρίζονται από Τεχνολογίες Πληροφορικής Επικοινωνιών (ΤΠΕ) σε διάφορες κλίμακες. Οι προτεινόμενες λύσεις είναι πολύ γενικές και στοχεύουν στην κάλυψη του πλήρους κύκλου ζωής της διεργασίας, από την αρχική αναγνώριση ή προδιαγραφή έως την εφαρμογή και την εκτέλεση της.

Το έργο DEFeND [12] είναι μια διεθνής συνεργασία που στόχο έχει να προσφέρει μια πλατφόρμα με σκοπό την εξουσιοδότηση ενός οργανισμού σε διαφορετικούς τομείς ώστε να αξιολογούν και να συμμορφώνονται με τον GDPR. Οι στόχοι του ευρωπαϊκού έργου DEFeND [12] είναι στο σύνολο δώδεκα. Σε αυτούς τους δώδεκα στόχους μεταξύ άλλων περιλαμβάνονται η ανάπτυξη σχεδίου απορρήτου GDPR, η διαχείριση καταγγελιών απορρήτου και ατομικών δικαιωμάτων, η εφαρμογή απόρρητο από σχεδιασμό, η συμπλήρωση κανονιστικών απαιτήσεων αναφοράς, η δημιουργία αποθετηρίου δεδομένων, η λήψη και η διαχείριση περιεχομένου χρήστη, η δημιουργία προγράμματος διαχείρισης τρίτων, η διαχείριση περιστατικών απορρήτου και οι ειδοποιήσεις παραβίασης, η ανωνυμοποίηση δεδομένων, η διεύθυνση διεθνών μεταβιβάσεων δεδομένων καθώς και η διεξαγωγή εκτιμήσεων κινδύνου απορρήτου (DPIA)[3] και η επιλογή κατάλληλων τεχνικών και οργανωτικών μέτρων ασφαλείας.

Το εργαλείο SMOOTH [14] βοηθά τις πολύ μικρές επιχειρήσεις να υιοθετήσουν και να συμμορφωθούν με τον GDPR σχεδιάζοντας και εφαρμόζοντας εύχρηστα και οικονομικά προσιτά εργαλεία. Αυτό το έργο έχει ως βασικό σκοπό την ευαισθητοποίηση των μικρών επιχειρήσεων σχετικά με τις υποχρεώσεις τους για τον GDPR και την ανάλυση του επιπέδου συμμόρφωσής τους με τον νέο κανονισμό προστασίας δεδομένων. Οι στόχοι του SMOOTH είναι συνολικά επτά. Ο πρώτος στόχος του έργου είναι να παραδώσει ένα διαδικτυακό διαδραστικό εγχειρίδιο GDPR για πολύ μικρές επιχειρήσεις. Ο δεύτερος στόχος είναι να εφαρμόσει σχέδιο διάδοσης και επικοινωνίας για την προσέγγιση μικροεπιχειρήσεων. Επιπλέον η ανάπτυξη προηγμένης τεχνολογίας για την αυτόματη αξιολόγηση της συμμόρφωσης των μικρομεσαίων επιχειρήσεων καθώς και η δημιουργία αναφορών συμμόρφωσης είναι δύο επιπλέον στόχοι του έργου. Τέλος η αξιολόγηση των λειτουργικών πτυχών της πλατφόρμας, η μεγιστοποίηση του πλήθους των επιχειρήσεων που χρησιμοποιούν το έργο και η επικύρωση της σκοπιμότητας της αγοράς της πλατφόρμας SMOOTH είναι οι τελευταίοι στόχοι που ολοκληρώνουν τον απώτερο σκοπό του έργου.

Το PDP4E [15] στοχεύει στην ευρεία δημιουργία προϊόντων, συστημάτων και υπηρεσιών που προστατεύουν καλύτερα το απόρρητο και τα προσωπικά δεδομένα των πολιτών της ΕΕ. Βοηθώντας τους μηχανικούς λογισμικού και συστημάτων με μεθόδους και εργαλεία λογισμικού σε εφαρμογές αρχών προστασίας δεδομένων το έργο στοχεύει στην ευρεία δημιουργία προϊόντων,

[3] DPIA – Μελέτη Εκτίμησης Αντικτύπου Προσωπικών Δεδομένων

συστημάτων και υπηρεσιών που προστατεύουν καλύτερα το απόρρητο και τα προσωπικά δεδομένα των πολιτών της ΕΕ.

Σκοπός του ευρωπαϊκού έργου PAPAYA [16] είναι η παροχή εργαλείων που επιτρέπουν τον υπολογισμό των Big Data Analytics για τη διατήρηση του απορρήτου, η παροχή πρωτοκόλλων επεξεργασίας δεδομένων πολλαπλών ρυθμίσεων, η διαχείριση κινδύνων μέσω πινάκων ελέγχου και ο καθορισμός ενός κοινού πλαισίου για τη διατήρηση του απορρήτου Big Data Analytics που δείχνει τη σχέση μεταξύ του απορρήτου, των πρωτοκόλλων και των αναλυτικών στοιχείων σε καθεμία από τις ρυθμίσεις που περιγράφονται και που ταιριάζει σε κάθε περίπτωση χρήσης. Τέλος η επικύρωση περίπτωσης χρήσης από άκρο σε άκρο είναι ο τελευταίος στόχος του έργου.

Το PoSeID-on [17], που είναι το τελευταίο έργο που συμμορφώνεται με τον GDPR και περιγράφεται στην εργασία, αποτελεί ένα ισχυρό εργαλείο για την υλοποίηση κάθε είδους ψηφιακής συνεργασίας μεταξύ δημόσιων και ιδιωτικών οργανισμών, καθώς φροντίζει να λύνει ή να μετριάζει τα περισσότερα από τα ζητήματα και τις ανησυχίες περί απορρήτου που αντιπροσωπεύουν τα κύρια εμπόδια στη δημιουργία πλατφόρμας οικοσυστήματος. Οι στόχοι του έργου είναι σε πλήθος έξι. Μεταξύ των στόχων είναι η ενδυνάμωση των υποκειμένων δεδομένων, η προστασία προσωπικών δεδομένων, η ελαχιστοποίηση και η ποιότητα των δεδομένων, η ανίχνευση απροσδόκητων και δυνητικά επιβλαβών συμπεριφορών, η επίδειξη συστήματος μέσω δοκιμών και επικύρωσης καθώς και το μοντέλο βιωσιμότητας PoSeID-on.

3 GDPR (Γενικός Κανονισμός Προστασίας Δεδομένων - ΓΚΠΔ)

3.1 Επισκόπηση του GDPR

Ο GDPR (Γενικός Κανονισμός για την Προστασία των Δεδομένων (ΕΕ) 2016/679 - ΓΚΠΔ) είναι ένας κανονισμός στην νομοθεσία της ΕΕ για την προστασία των δεδομένων και την ιδιωτικότητα στην Ευρωπαϊκή Ένωση και στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ) [18]. Βασικός σκοπός του GDPR είναι να βοηθήσει τα άτομα να ελέγχουν τις προσωπικές τους πληροφορίες - δεδομένα, κάνοντας απλούστερο το ρυθμιστικό περιβάλλον για τις διεθνείς επιχειρήσεις ενοποιώντας τον κανονισμό εντός της Ευρωπαϊκής Ένωσης.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων - (GDPR) [18], εισάγει νέες απαιτήσεις για την ασφάλεια και την προστασία δεδομένων μέσω 99 άρθρων και 173 αιτιολογικών σκέψεων. Ο Κανονισμός (GDPR) στοχεύει στην προστασία των δικαιωμάτων και της ελευθερίας των φυσικών προσώπων. Όλοι οι οργανισμοί και τα συστήματα που αλληλεπιδρούν με προσωπικά δεδομένα έχουν την υποχρέωση να συμμορφώνονται με τον GDPR με σκοπό να προστατεύσουν τα δεδομένα αυτά βελτιώνοντας παράλληλα τα επιχειρηματικά τους μοντέλα [19]. Η έκθεση των πεπραγμένων στοχεύει στην απόδειξη πως οι υπεύθυνοι επεξεργασίας συμμορφώνονται με τις αρχές του Κανονισμού. Κάθε οργανισμός επομένως πρέπει να απαντήσει σε ερωτήσεις που έχουν να κάνουν με το ποια δεδομένα επεξεργάζονται, πως και που αποθηκεύονται και για πόσο χρονικό διάστημα, ο σκοπός που επεξεργάζονται τα δεδομένα καθώς και ποιος έχει πρόσβαση σε αυτά και πως θα διαφυλαχθεί και επιτευχθεί η λογοδοσία.

Ο GDPR είναι ένα πολύπλοκος νόμος, όπως προκύπτει από την μελέτη, για τον λόγο αυτό είναι αρκετά περίπλοκο να κατανοηθεί και να εξεταστεί σε μεγαλύτερο βάθος από τους σχεδιαστές των συστημάτων. Παρακάτω στις υποενότητες της παρούσας ενότητας γίνεται η ανάλυση των αρχών και των οντοτήτων GDPR για την καλύτερη κατανόηση του κανονισμού καθώς και αντιστοίχιση των απαιτήσεων που προκύπτουν από τον GDPR από κάθε αρχή του.

3.1.1 Οντότητες GDPR

Οι οντότητες που περιέχονται στον GDPR είναι συνολικά έξι σε αριθμό [18]. Συγκεκριμένα είναι :

- **Υποκείμενο Δεδομένων (DS - Data Subject)** : είναι ένα φυσικό αναγνωρίσιμο πρόσωπο του οποίου η ταυτότητα έχει πιστοποιηθεί άμεσα ή έμμεσα, από δεδομένα που θα χρησιμοποιηθούν από τον υπεύθυνο επεξεργασίας ή από οποιοδήποτε άλλο νομικό ή φυσικό πρόσωπο. Υποκείμενο Δεδομένων ονομάζεται οποιοδήποτε πρόσωπο του οποίου τα δεδομένα συλλέγονται, διατηρούνται ή επεξεργάζονται.

- **Υπεύθυνος Επεξεργασίας (Controller)**: μπορεί να θεωρηθεί οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία και οποιοσδήποτε φορέας που ατομικά ή ομαδικά με άλλους φορείς ορίζει τους στόχους, τις προϋποθέσεις και τα μέσα επεξεργασίας προσωπικού χαρακτήρα. Ο υπεύθυνος επεξεργασίας διασφαλίζει πως η επεξεργασία των προσωπικών δεδομένων σωφρονίζεται με τις αρχές του GDPR (Accountability). Επίσης εφαρμόζει πολιτικές προστασίας δεδομένων και μέτρα ασφαλείας, κάνει εκτίμηση επιπτώσεων προστασίας δεδομένων - (DPIA , Data Protection Impact Assessment) για επεξεργασία υψηλού κινδύνου. Τέλος ενημερώνει τα DS για τα δικαιώματα που έχουν σε περίπτωση που παραβιαστούν τα προσωπικά τους δεδομένα και ενημερώνει την Εποπτική Αρχή (ΕΑ) εντός 72 ωρών, ενώ μπορεί να διαβιβάσει τα προσωπικά δεδομένα που επεξεργάζεται, σύμφωνα με ειδικές διατάξεις διασφάλισης.

- **Εκτελών Επεξεργασίας (Processor)**: ένας processor επεξεργάζεται προσωπικά δεδομένα για λογαριασμό του υπεύθυνου επεξεργασίας. Πιο αναλυτικά αυτό που κάνει ένας processor είναι να συγκεντρώνει προσωπικά δεδομένα διαδικτυακά ή και όχι, μέσα από εγγραφές, φόρμες επικοινωνίας, email, ψηφιακές πληρωμές και τιμολόγια. Επίσης χρησιμοποιεί, καταγράφει, αποθηκεύει, οργανώνει, ανακτά, αποκαλύπτει και φροντίζει για την διαγραφή των προσωπικών δεδομένων που έχουν συλλεχθεί. Τέλος δημιουργεί αποθέματα για όλες τις προαναφερόμενες κατηγορίες επεξεργασίας δεδομένων.

- **Υπεύθυνος Προστασίας Δεδομένων - (DPO, Data Protection Officer):** είναι ένα φυσικό ή νομικό πρόσωπο που διαχειρίζεται και εποπτεύει τις δραστηριότητες προστασίας δεδομένων, παρακολουθώντας εάν συμμορφώνεται η επεξεργασία των δεδομένων με τις διατάξεις προστασίας και ασφάλειας των προσωπικών δεδομένων GDPR. Συνεργάζεται με την ΕΑ.
- **Εποπτική Αρχή - (SA, Supervisory Authority)**: είναι υπεύθυνη για τον έλεγχο της εφαρμογής του Κανονισμού και για τη συνεισφορά στη συνεπή εφαρμογή του, βάσει του άρθρου 46.

- **Τρίτο Μέρος – (Third Part)**: αναφέρεται σε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέα εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και πρόσωπα που, υπό την άμεση εξουσία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται δεδομένα προσωπικού χαρακτήρα.

Οι αλληλεπιδράσεις των παραπάνω οντοτήτων ορίζονται από τα άρθρα του GDPR. Για παράδειγμα το υποκείμενο δεδομένων μπορεί να δηλώσει τη συγκατάθεσή του στον υπεύθυνο επεξεργασίας (άρθρο 4). Ο υπεύθυνος επεξεργασίας με τη σειρά του έχει την δυνατότητα να κατατοπίσει τα υποκείμενα δεδομένων σε περίπτωση που παραβιαστούν τα προσωπικά δεδομένα των τελευταίων (άρθρο 34).

3.1.2 Αρχές GDPR

Ο GDPR ορίζει επτά βασικές αρχές (άρθρο 5) [18], σύμφωνα με τις οποίες πρέπει να συμμορφώνεται κάθε είδους επεξεργασία που αφορά δεδομένα προσωπικού χαρακτήρα. Οι επτά αρχές του Κανονισμού παρουσιάζονται παρακάτω :

- **Νομιμότητα (Legality), Διαφάνεια (Transparency) και Αμεροληψία (Impartiality)** : Αυτή η αρχή εκφράζει πως τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία νόμιμα, δίκαια και με διαφάνεια σε σχέση με το υποκείμενο δεδομένων.

- **Περιορισμός Σκοπού (Purpose Limitation)** : Στόχος μέσα από αυτή την αρχή είναι οι υπεύθυνοι επεξεργασίας να φροντίζουν για τον καθορισμό και την τεκμηρίωση του σκοπού που χρησιμοποιούνται τα δεδομένα καθώς και για να παρέχουν την δυνατότητα ενημέρωσης των σκοπών και ελέγχου της συνοχής μεταξύ τους. Ουσιαστικά πρέπει να καταστεί σαφές πως τα προσωπικά δεδομένα δεν πρέπει να συλλέγονται και να επεξεργάζονται αόριστα αλλά συγκεκριμένα για νόμιμους και ξεκάθαρους σκοπούς.

- **Ελαχιστοποίηση Δεδομένων (Data Minimization)** : Αυτή η αρχή καθιστά σαφές ότι τα προσωπικά δεδομένα πρέπει να είναι επαρκή, σχετικά και να περιορίζονται σε ό,τι είναι απαραίτητο σε σχέση με τους σκοπούς για τους οποίους υφίστανται επεξεργασία.

- **Ακρίβεια (Accuracy)** : Μέσα από την αρχή αυτή του κανονισμού θα πρέπει να διασφαλίζεται η ακρίβεια οποιωνδήποτε προσωπικών δεδομένων που

δημιουργούνται ή ενημερώνονται με το δικαίωμα της διόρθωσης, επιτρέποντας στα υποκείμενα δεδομένων να διορθώσουν λανθασμένα προσωπικά δεδομένα.

- **Περιορισμός Αποθήκευσης (Storage Limitation)** : Μέσω αυτής της αρχής εξετάζεται ποια δεδομένα θα αποθηκευτούν γιατί και για πόσο χρονικό διάστημα. Αυτό γίνεται επειδή ο GDPR δεν θέτει συγκεκριμένα χρονικά όρια. Επομένως εφόσον δεν χρειάζονται πλέον τα δεδομένα θα πρέπει να διαγράφονται με ασφάλεια.

- **Ακεραιότητα (Integrity), Εμπιστευτικότητα (Confidentiality)** : Η λήψη κατάλληλων μέτρων ασφαλείας που έχουν ως σκοπό να προστατεύσουν τα προσωπικά δεδομένα είναι απαραίτητη για τη διατήρηση και τη διάθεση των αρχείων που εμπεριέχουν αυτά τα προσωπικά δεδομένα ώστε να αποδεικνύεται η συμμόρφωση της διαδικασίας με τον GDPR.

- **Υπευθυνότητα (Responsibility)** : Απαιτείται από τους υπεύθυνους επεξεργασίας να αναλαμβάνουν την ευθύνη για το τι κάνουν με τα προσωπικά δεδομένα και τον τρόπο με την οποία διαχειρίζονται τα δεδομένα και συμμορφώνονται με τις αρχές. Με αυτή την αρχή βεβαιώνεται πως υπάρχουν όλα τα κατάλληλα αρχεία τα οποία αποδεικνύουν τη συμμόρφωση της επεξεργασίας των δεδομένων με τον κανονισμό.

3.1.3 Απαιτήσεις GDPR

Από τις παραπάνω αρχές οι οποίες είναι στο σύνολο επτά (7) προκύπτουν 12 απαιτήσεις. Από την πρώτη αρχή του κανονισμού προκύπτουν τέσσερις απαιτήσεις, για την δεύτερη αρχή δύο απαιτήσεις σχεδιασμού, για την τρίτη αρχή μια απαίτηση σχεδιασμού, για την τέταρτη αρχή του κανονισμού δύο απαιτήσεις σχεδιασμού, ενώ για κάθε μία από την πέμπτη, την έκτη, την έβδομη αρχή έχουμε μια απαίτηση. Παρακάτω (Πίνακας 1) παρουσιάζονται οι 7 αρχές του κανονισμού μαζί με τις απαιτήσεις που αντιστοιχίζονται σε κάθε αρχή, ενώ παράλληλα δίνεται μια μικρή περιγραφή για κάθε απαίτηση που προκύπτει από κάθε αρχή. Οι 12 αυτές απαιτήσεις είναι για να γίνουν καλύτερα κατανοητές οι αρχές του GDPR, ώστε να απλοποιηθεί και ο σχεδιασμός των συστημάτων που συμμορφώνονται με αυτόν.

Αρχές GDPR	**Απαιτήσεις GDPR**
1. Νομιμότητα, Δικαιοσύνη, Διαφάνεια	**Απαίτηση 1.** Διαχείριση Συναίνεσης DS **Απαίτηση 2.** Ειδοποίηση DS εάν παραβιαστούν τα δεδομένα **Απαίτηση 3.** Διασταύρωση Χρήσης Δεδομένων **Απαίτηση 4.** Συνεχής Έλεγχος της νόμιμης επεξεργασίας δεδομένων.
2. Περιορισμός Σκοπού	**Απαίτηση 5.** Ορισμός Σκοπού **Απαίτηση 6.** Ενημέρωση Σκοπού
3. Ελαχιστοποίηση Δεδομένων	**Απαίτηση 7.** Μείωση Συλλογής Δεδομένων ως προς τον σκοπό
4. Ακρίβεια	**Απαίτηση 8.** Έλεγχος της ακρίβειας των δεδομένων που χρησιμοποιήθηκαν για λάθη. **Απαίτηση 9.** Επαλήθευση της εφαρμογής Πολιτικής Δεδομένων
5. Περιορισμός Αποθήκευσης	**Απαίτηση 10.** Εξέταση του χώρου, του χρονικού διαστήματος και του λόγου αποθήκευσης των δεδομένων.
6. Ακεραιότητα, Εμπιστευτικότητα	**Απαίτηση 11.** Ορισμός Πολιτικών Ασφαλείας
7. Υπευθυνότητα	**Απαίτηση 12.** Απόδειξη Εφαρμογής Αρχών

Πίνακας 1 . Πίνακας αρχών και απαιτήσεων του GDPR

Απαίτηση 1. (Διαχείριση Συναίνεσης DS) : Το υποκείμενο δεδομένων μέσα από αυτή την απαίτηση μπορεί να εκφράσει τις προτιμήσεις απορρήτου του (ορισμός συναίνεσης, ανάκληση συγκατάθεσης, αποθήκευση συναίνεσης και συμμόρφωση με τη συναίνεση), μέσω ενός API[4]. Ουσιαστικά το υποκείμενο δεδομένων μέσω αυτής της απαίτησης μπορεί να περιγράψει και να ορίσει το είδος των δεδομένων που συλλέγονται, από πού συλλέγονται τα δεδομένα του, την αιτία που συλλέγονται τα δεδομένα του, ο χώρος που αποθηκεύονται τα δεδομένα που έχουν συλλεχθεί

[4] API - Διεπαφή Προγραμματισμού Εφαρμογών (application programming interface)

καθώς και το χρονικό διάστημα που κάποιος έχει πρόσβαση στα δεδομένα αλλά και το ποιος έχει πρόσβαση στα δεδομένα. Με αυτόν τον τρόπο το υποκείμενο δεδομένων δημιουργεί μια πολιτική συναίνεσης σύμφωνα με την οποία συμφωνεί σχετικά με τη διαχείριση και την επεξεργασία των δεδομένων.

Απαίτηση 2. (Ειδοποιήσεις DS σε περίπτωση παραβίασης δεδομένων) : Ο GDPR απαιτεί την υποστήριξη εντοπισμού παραβίασης δεδομένων σε σύντομο χρονικό διάστημα κάθε φορά που δεδομένα έχουν παραβιαστεί ή διαρρεύσει. Για τον λόγο αυτό είναι απαραίτητο να εφαρμόζεται η παρακολούθηση και η διαχείριση ειδοποιήσεων σε πραγματικό χρόνο, ώστε ένας ελεγκτής να μπορεί να ενημερώνει τα υποκείμενα δεδομένων σχετικά με το επίπεδο ασφαλείας που μπορεί να λειτουργήσει, ανάλογα με το είδος των ευαίσθητων δεδομένων που έχουν παραβιαστεί. Αυτή η διαδικασία γίνεται μέσω της συγκεκριμένης απαίτησης. Ο υπεύθυνος επεξεργασίας είναι αυτός που ευθύνεται για την κοινοποίηση των παρεμβολών και της παραβίασης πολιτικής σε περίπτωση που υπάρξει στο υποκείμενο δεδομένων καθώς και στον υπεύθυνο προστασίας των δεδομένων.

Απαίτηση 3. (Διασταύρωση Χρήσης Δεδομένων) : Σε αυτή τη φάση οι χρήστες μπορούν να εκχωρήσουν δικαιώματα πρόσβασης μόνο σε άλλα μέρη όπως εφαρμογές τρίτων, χώρους αποθήκευσης, στους χρήστες και τις συσκευές αυτών που έχουν εξουσιοδοτήσει. Με αυτό τον τρόπο είναι εξουσιοδοτημένοι μόνο οι κάτοχοι καθώς και όσοι χρήστες έχουν λάβει έγκριση να έχουν πρόσβαση στα δεδομένα.

Απαίτηση 4. (Συνεχής Έλεγχος της Νόμιμης Επεξεργασίας Δεδομένων) : Ένας υπεύθυνος επεξεργασίας οφείλει να εφαρμόσει μια αυτοματοποιημένη εύρεση σχετικών ή μερικών προσωπικών δεδομένων, επιτρέποντας με αυτό τον τρόπο την αναγνώριση δεδομένων καθώς και τη σύνδεση μεταξύ τους.

Απαίτηση 5. (Ορισμός Σκοπού) : Η πολιτική του ελέγχου πρόσβασης που έχει ως σκοπό τη χρήση δεδομένων για τον περιορισμό της πρόσβασης στην καθορισμένη πολιτική πρέπει να εμπλουτιστεί και να επεκταθεί από έναν υπεύθυνο επεξεργασίας.

Απαίτηση 6. (Ενημέρωση Σκοπού) : Μια ενημερωμένη διεπαφή χρήστη σχετικά με τις πολιτικές για τους σκοπούς που έχουν καθοριστεί σχετικά με την επεξεργασία των δεδομένων πρέπει να παρέχεται από έναν ελεγκτή. Σε περίπτωση που εκτελεσθεί κάποια μορφή επεξεργασίας διαφορετική από αυτή που ορίστηκε αρχικά, ο υπεύθυνος επεξεργασίας διασφαλίζει ότι αναλύεται, αιτιολογείται και τεκμηριώνεται ο σκοπός για τον οποίο θεωρείται συνεπής με τον παλιό.

Απαίτηση 7. (Μείωση της συλλογής δεδομένων ως προς τον σκοπό) : Με χρήση τεχνικών σχολιασμού ένας ελεγκτής μπορεί να φιλτράρει δεδομένα στο επίπεδο απορρόφησης σχετικά με τους συνδεδεμένους σκοπούς για κάθε χρήση δεδομένων. Τα δεδομένα που έχουν σχολιαστεί με κατάλληλους σκοπούς μπορούν να φιλτραριστούν ευκολότερα. Η ψευδωνυμοποίηση και η

ανωνυμοποίηση, πολλές φορές κρίνεται ιδιαίτερα χρήσιμη για την ελαχιστοποίηση συλλογής δεδομένων, όπως και οι απαιτήσεις περιορισμού αποθήκευσης. Ο λόγος είναι πως εάν δεν υπάρχουν χώροι αποθήκευσης των δεδομένων, δεν μπορούν να συλλεχθούν νέα δεδομένα, χωρίς ωστόσο αυτό να έχει σχέση με τον GDPR.

Απαίτηση 8. (Έλεγχος της ακρίβειας των δεδομένων που χρησιμοποιήθηκαν για λάθη) : Ένας υπεύθυνος επεξεργασίας πρέπει να ελέγχει τις πηγές δεδομένων σε σχέση με αυτές τις πηγές δεδομένων που ορίζονται στις πολιτικές συναίνεσης, με σκοπό να διασφαλίσει πως τα ανακριβή δεδομένα, λαμβανομένων υπόψη των σκοπών της επεξεργασίας, διαγράφονται ή διορθώνονται χωρίς καθυστέρηση. Σε αυτή την περίπτωση ο ελεγκτής μπορεί να χρησιμοποιήσει τη λειτουργία CRUD (Create, Read, Use, Delete), για τον πίνακα εργαλείων του υποκειμένου δεδομένων.

Απαίτηση 9. (Επαλήθευση της Εφαρμογής Πολιτικής Δεδομένων) : Η συγκεκριμένη απαίτηση ορίζει πως το υποκείμενο δεδομένων έχει δικαίωμα καθώς και τη δυνατότητα να δημιουργεί ή να ενημερώνει τις πολιτικές του δυναμικά, αποκτώντας πρόσβαση στον χώρο αποθήκευσης πολιτικών, ελέγχοντας προβλήματα που προκύπτουν από παρεμβολές. Με αυτόν τον τρόπο φαίνεται πως υπάρχει σεβασμός ως προς τα δικαιώματα του υποκειμένου δεδομένων.

Απαίτηση 10. (Εξέταση του χώρου, του χρονικού διαστήματος και του λόγου αποθήκευσης των δεδομένων) : Με αυτή την απαίτηση το υποκείμενο δεδομένων έχει τη δυνατότητα να εκφράσει για κάθε προσωπικό του δεδομένο που χρησιμοποιείται για επεξεργασία, τον σκοπό της συλλογής, το χρονικό διάστημα που θα είναι διαθέσιμο καθώς και τον χώρο αποθήκευσης του συγκεκριμένου δεδομένου. Με αυτόν τον τρόπο δημιουργείται μια πολιτική συναίνεσης η οποία αξιολογείται με μια μηχανή πολιτικής. Έχοντας γίνει αυτή η διαδικασία, ο υπεύθυνος επεξεργασίας μπορεί να περιγράψει πλέον ποια προσωπικά δεδομένα δεν απαιτούνται για επεξεργασία, προχωρώντας στην ανωνυμοποίηση αυτών των δεδομένων. Τα ανώνυμα δεδομένα αντικαθιστούν τα δεδομένα των χρηστών που είχαν συλλεχθεί αρχικά για επεξεργασία ή διαγράφονται ολικά από το σύστημα.

Απαίτηση 11. (Ορισμός Πολιτικών Ασφαλείας) : Τεχνικές ελέγχου ταυτότητας και εξουσιοδότησης καθώς και διαφορετικά πρωτόκολλα και τρόποι για τον έλεγχο ταυτότητας και της δημιουργίας ασφαλών συνδέσεων με πλατφόρμες ή συσκευές τρίτων είναι απαραίτητες για τη διασφάλιση της επεξεργασίας των δεδομένων του υποκειμένου δεδομένων.

Απαίτηση 12. (Απόδειξη Εφαρμογής Αρχών) : Ένας υπεύθυνος επεξεργασίας πρέπει να παρακολουθεί, να αποκλείει και να ελέγχει συλλέγοντας, ενοποιώντας, ασφαλίζοντας και αναλύοντας αρχεία καταγραφής ελέγχου. Η παρακολούθηση του ιστορικού αξιολόγησης κινδύνου υπογραμμίζει πόση πρόοδος έχει σημειωθεί με την πάροδο του χρόνου. Επίσης, τα αρχεία καταγραφής ελέγχου χρησιμοποιούνται για την απόδειξη της υπευθυνότητας συγκρίνοντας το εύρος επεξεργασίας με την πολιτική συναίνεσης που ορίζεται από το υποκείμενο δεδομένων. Ο

υπεύθυνος επεξεργασίας πρέπει να υποστηρίζει τον έλεγχο για κάθε υποκειμένου των δεδομένων, για να παρακολουθεί ποιος έχει πρόσβαση στα προσωπικά του δεδομένα. Ο χρήστης πρέπει να έχει πρόσβαση στα δεδομένα ελέγχου, λαμβάνοντας λεπτομέρειες σχετικά με τις προσβάσεις, όπως: πότε, πού, πώς και ποιος είχε πρόσβαση στα δεδομένα. Αυτή η δυνατότητα ζητείται ρητά από τον GDPR. Η επεξεργασία των προσωπικών δεδομένων θα πρέπει να τεκμηριώνεται και αυτή η τεκμηρίωση να έχει εκδοθεί και να διατηρείται ενημερωμένη.

3.2 Εισαγωγή στο Απόρρητο

Η σύλληψη και η εξήγηση ενός γενικού ορισμού της ιδιωτικής ζωής - απορρήτου μπορεί να είναι πολύ δύσκολη και η σημασία της έννοιας μπορεί να ποικίλλει μεταξύ διαφορετικών πλαισίων. Ένας από τους πιο αναφερόμενους ορισμούς για το απόρρητο δίνεται από τους Warren και Brandeis από το 1890 [26]. Περιγράφουν το απόρρητο ως «το δικαίωμα να μείνεις μόνος». Βέβαια το απόρρητο εκεί δεν αναφέρεται στο πλαίσιο της τεχνολογίας της πληροφορίας. Οι συγγραφείς συζητούν την παραβίαση του απορρήτου ως μια μορφή δυσφήμισης και έκθεσης. Πιο συγκεκριμένα, το παράδειγμα που χρησιμοποιούν είναι οι δημόσιοι αναγνώστες (πολίτες) μιας εφημερίδας να έχουν πρόσβαση σε προσωπικές πληροφορίες που αποκαλύπτουν οι δημοσιογράφοι, μέσω άρθρων που περιέχουν συκοφαντικές ειδήσεις σχετικά με αυτούς τους πολίτες.

Ένας άλλος τρόπος να σκεφτεί κανείς το απόρρητο είναι μέσω του «δικαιώματος να επιλέγει ποιες προσωπικές πληροφορίες για εκείνον είναι γνωστές σε ποιους ανθρώπους» [25]. Αυτός ο ορισμός ταιριάζει περισσότερο στο πλαίσιο των σημερινών περιβαλλόντων τεχνολογίας πληροφοριών, όπου τα δεδομένα συχνά αναφέρονται σε προσωπικές πληροφορίες με τη μορφή ψηφιακής φύσης. Σε αυτό το συγκεκριμένο πλαίσιο, το απόρρητο αναφέρεται σε ποιες προσωπικές πληροφορίες ένα άτομο είναι διατεθειμένο να μοιραστεί και να παρέχει σε οργανισμούς όταν χρησιμοποιεί τα προϊόντα ή τις υπηρεσίες του.

Προκειμένου να γίνει πιο κατανοητή η έννοια του απορρήτου, είναι απαραίτητο να γίνουν κατανοητές οι σχετικές ιδιότητές του. Οι Pfitzmann et al. [27] δημιούργησαν μια καθιερωμένη ορολογία για το απόρρητο. Καθορίζουν και εξηγούν ρητά τις βασικές ιδιότητες απορρήτου με σκοπό να διευκολύνουν το έργο των μηχανικών προστασίας προσωπικών δεδομένων. Έτσι, οι ορισμοί τους χρησιμοποιούνται στην ενότητα που ακολουθεί για να διευκρινιστούν οι ιδιότητες απορρήτου.

3.2.1 Ιδιότητες Απορρήτου

Οι πιο κοινές ιδιότητες του απορρήτου που χρησιμοποιούνται στις μεθοδολογίες του Κεφαλαίου 2, και είναι αυτές λαμβάνει υπόψιν η μεθοδολογία PriS για την περιγραφή της έννοιας του απορρήτου, είναι σε αριθμό οχτώ : Ταυτοποίηση, Αυθεντικοποίηση, Εξουσιοδότηση, Προστασία Δεδομένων, Ανωνυμία, Ψευδωνυμία, Μη συνδεσιμότητα, Μη παρατηρησιμότητα.

- **Ταυτοποίηση**: η διαδικασία εκείνη, κατά την οποία ένα άτομο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που απαιτούνται προκειμένου να συσχετιστεί με ένα από τα αντικείμενα που δικαιούνται προσπέλασης στους πόρους του.

- **Αυθεντικοποίηση**: η διαδικασία κατά την οποία ένα άτομο παρέχει σε ένα πληροφοριακό σύστημα τις πληροφορίες που απαιτούνται προκειμένου να ελεγχθεί η βασιμότητα της συσχέτισης που επιτεύχθηκε κατά τη διαδικασία της ταυτοποίησης.

- **Εξουσιοδότηση**: η διαδικασία που δίνει κάποιος την άδεια να κάνει ή να έχει κάτι.

- **Προστασία Δεδομένων**: η προστασία των προσωπικών πληροφοριών με στόχο το απόρρητο.

- **Ανωνυμία**: αναφέρεται στο πότε οι προσωπικές πληροφορίες ενός ατόμου παραμένουν κρυφές, δηλαδή μη αναγνωρίσιμες και επομένως ασφαλείς.

- **Ψευδωνυμία**: μια έννοια όπου σε ένα άτομο, συνηθέστερα χρήστη μιας υπηρεσίας λογισμικού, εκχωρείται ένα «ψεύτικο όνομα», όπως ένα ψευδώνυμο προκειμένου να μην είναι γνωστή η ταυτότητά του.

- **Μη συνδεσιμότητα**: Η αποσύνδεση δύο ή περισσότερων στοιχείων ενδιαφέροντος από την πλευρά του εισβολέα σημαίνει ότι εντός του συστήματος (που περιλαμβάνει αυτά και πιθανώς άλλα στοιχεία), ο εισβολέας δεν μπορεί να διακρίνει επαρκώς αν αυτά σχετίζονται ή όχι μεταξύ τους.

- **Μη παρατηρησιμότητα**: Η μη παρατηρησιμότητα είναι παρόμοια με τη μη ανιχνευσιμότητα, καθώς ο σκοπός είναι η πρόθεση απόκρυψης μιας οντότητας, μιας μονάδας επεξεργασίας, ενός ατόμου ή άλλης πληροφορίας από έναν αντίπαλο.

4 *Ενίσχυση της μεθοδολογίας PriS (Privacy Safeguard)*

4.1 Λόγοι επιλογής της PriS ως μεθοδολογία για ενίσχυση με βάση τον GDPR

Όπως προαναφέρθηκε σε προηγούμενο κεφάλαιο (Κεφάλαιο 2 – υποενότητα 2.1) υπάρχουν δύο συγκεκριμένοι λόγοι που έχει επιλεγεί η μεθοδολογία Privacy Safeguard (PriS), ως η μεθοδολογία για ενίσχυση με βάση τον κανονισμό του GDPR.

Ο πρώτος λόγος είναι πως η PriS πέρα από το πρώιμο στάδιο σχεδίασης εντοπίζεται και στο στάδιο εφαρμογής ενός συστήματος, καλύπτοντας με αυτόν τον τρόπο το κενό μεταξύ του σχεδιασμού και της υλοποίησης ενός συστήματος και διευκολύνοντας την διαδικασία ανάπτυξης του εν λόγω συστήματος. Η δεύτερη αιτία που επιλέχθηκε η PriS είναι ότι αποτελεί την πιο χρησιμοποιούμενη μεθοδολογία, σύμφωνα με έρευνα που έγινε σε επιστημονικό περιοδικό. Ο τρίτος λόγος που επιλέγεται η PriS μεθοδολογία, για να ενισχυθεί με τις αρχές του GDPR, είναι πως στο τρίτο βήμα της μεθοδολογίας προτείνονται έτοιμα πρότυπα διαδικασιών ιδιωτικότητας, τα οποία εμπεριέχουν δραστηριότητες και ροές δεδομένων που συνδέουν τις διεργασίες του υπό ανάπτυξη συστήματος, παρουσιάζοντας με τον τρόπο αυτό τη μέθοδο με την οποία πρέπει να λειτουργεί μια επιχείρηση σε ένα τομέα. Τα πρότυπα αυτά λοιπόν, τα οποία περιγράφονται σε δύο επίπεδα το καθένα καταφέρνουν να απλοποιήσουν την ικανοποίηση των στόχων – αρχών του GDPR, όπως παρουσιάζεται παρακάτω στο παρόν κεφάλαιο (υποενότητα 4.1.1).

Παρακάτω γίνεται αναφορά στην μεθοδολογία PriS, πριν από την ενίσχυση, ώστε να γίνουν αργότερα πιο κατανοητά τα βήματα που τη συμμορφώνουν με τις αρχές του GDPR. Παράλληλα παρουσιάζεται το παράδειγμα εφαρμογής της μεθοδολογίας PriS στο σύστημα e-voting από το

ερευνητικό άρθρο «Using Privacy Patterns for Incorporating Privacy Requirements». Η χρήση του συγκεκριμένου παραδείγματος είναι εσκεμμένη καθώς θα βοηθήσει αργότερα στην παράθεση του παραδείγματος που αφορά την ενισχυμένη μεθοδολογία PriS.

4.1.1 Μεθοδολογία πριν την Ενίσχυση

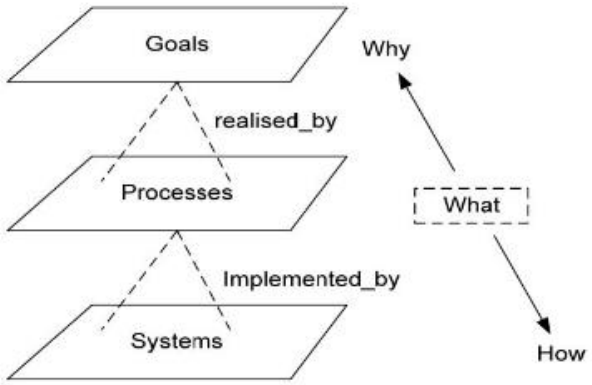
Η PriS – (Privacy Safeguard) [1], η πιο χρησιμοποιούμενη μεθοδολογία για να εξάγει κάποιος απαιτήσεις απορρήτου [7], είναι μια μεθοδολογία ανάλυσης στόχων απορρήτου που σκοπό έχει την ενσωμάτωση απαιτήσεων απορρήτου εγκαίρως στη διαδικασία ανάπτυξης του συστήματος και κατ' επέκταση του οργανισμού. Η μεθοδολογία αντιμετωπίζει τις απαιτήσεις απορρήτου ως οργανωτικούς στόχους που χρήζουν ικανοποίηση, παρέχοντας ένα φάσμα εννοιών για την μοντελοποίηση και τη μετάφραση αυτών των απαιτήσεων σε μοντέλα συστήματος. Η Pris χρησιμοποιεί πρότυπα διαδικασίας απορρήτου με σκοπό [2] :

1.Την περιγραφή της επιρροής των απαιτήσεων ιδιωτικότητας στις διαδικασίες που υποστηρίζονται από το πληροφοριακό σύστημα.

2.Τον ευκολότερο προσδιορισμό της αρχιτεκτονικής του συστήματος που ενισχύει πιο καλά τις επιχειρηματικές διεργασίες που συνδέονται με το απόρρητο.

Το μοντέλο εννοιών που χρησιμοποιεί η μεθοδολογία PriS στηρίζεται στο πλαίσιο Enterprise Knowledge Development (EKD) [1], το οποίο είναι μια συστηματική προσέγγιση που στόχο έχει να αναπτύξει και να τεκμηριώσει την οργανωσιακή γνώση. Ο συγκεκριμένος στόχος του πλαισίου (EKD) επιτυγχάνεται με τη μοντελοποίηση :

1. Των οργανωτικών στόχων που αποδίδουν τους σκόπιμους στόχους που ελέγχουν και διέπουν τη λειτουργία του
2. Των «φυσικών» διαδικασιών που λειτουργούν από κοινού με τους οργανωτικούς στόχους και
3. Των συστημάτων λογισμικού που υποστυλώνουν οι προαναφερθείσες διαδικασίες.



Σχήμα 1. Πλαίσιο Enterprise Knowledge Development (EKD)

Το σχήμα του πλαισίου EKD παρουσιάζεται στο σχήμα, [1]. Όπως αποτυπώνεται στο σχήμα αυτό οι διαδικασίες (processes) αναφέρονται στο τι πρέπει να γίνει, οι στόχοι (goals) αιτιολογούν γιατί υπάρχουν οι σχετιζόμενες διαδικασίες (processes) ενώ τα συστήματα (systems) αναπαριστούν πως μπορούν να υλοποιηθούν οι διαδικασίες (processes) χρησιμοποιώντας όρους κατάλληλων αρχιτεκτονικών συστημάτων.

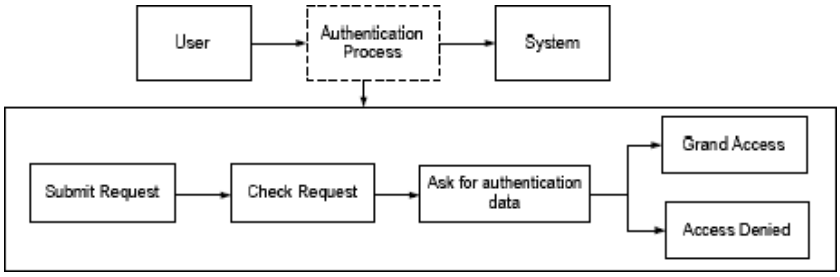
Η PriS λαμβάνει υπόψη οκτώ διαφορετικές ιδιότητες απορρήτου για την περιγραφή της ιδιωτικότητας των χρηστών, που παρουσιάζονται στην ενότητα 3.2.1, οι οποίες είναι : Ταυτοποίηση, Αυθεντικοποίηση, Εξουσιοδότηση, Προστασία Δεδομένων, Ανωνυμία, Ψευδωνυμία, Μη συνδεσιμότητα, Μη παρατηρησιμότητα. Η μεθοδολογία PriS περιέχει τέσσερα βήματα κατά την εφαρμογή της συνολικά. Τα τέσσερα βήματα που περιέχει η μεθοδολογία είναι :

1. Ανάδειξη των στόχων απορρήτου του συστήματος. Στο συγκεκριμένο βήμα προσδιορίζονται βασικά θέματα που αφορούν την προστασία της ιδιωτικής ζωής μέσω της επικοινωνίας με τους φορείς λήψης αποφάσεων και τα ενδιαφερόμενα μέρη. Επιπλέον επεξηγούνται γενικές απαιτήσεις απορρήτου σε σχέση με το πλαίσιο εφαρμογής και προσδιορίζονται οι απαιτήσεις απορρήτου που προϋπάρχουν και είναι ήδη κομμάτι των στόχων του οργανισμού.
2. Ανάλυση και εξέταση του αντικτύπου των στόχων απορρήτου, που προσδιορίστηκαν στο πρώτο βήμα της μεθοδολογίας, με την ανάλυση να γίνεται βάσει των διαδικασιών του συστήματος που υποστηρίζεται από τον οργανισμό και την εξέταση να πραγματοποιείται βάσει των διαδικασιών που αποσκοπούν στην επίτευξη αυτών των στόχων. Επίσης εντοπίζονται οι διαδικασίες που επιτυγχάνουν τους στόχους απορρήτου και επισημαίνονται ως διαδικασίες που σχετίζονται με το απόρρητο. Καινούργιοι στόχοι και αναθεώρηση των υφιστάμενων είναι πιθανό να υπάρξουν στη διάρκεια αυτού του βήματος.
3. Μοντελοποίηση των διαδικασιών απορρήτου με πρότυπο τα σχετικά μοτίβα διαδικασίας απορρήτου. Τα πρότυπα επιχειρηματικής διαδικασίας είναι συνήθως γενικευμένα μοντέλα διαδικασιών, τα οποία περιλαμβάνουν δραστηριότητες και ροές που τα συνδέουν, παρουσιάζοντας πώς μια επιχείρηση πρέπει να λειτουργεί σε έναν συγκεκριμένο τομέα [3]. Μοντελοποίηση προτύπων διαδικασίας απορρήτου σε επιχειρησιακές διαδικασίες για τη μεθοδολογία PriS, έχουν γίνει από νεότερες μελέτες [4], συνεισφέροντας με αυτό τον τρόπο στη σχεδίαση της αρχιτεκτονικής του συστήματος η οποία μπορεί να υποστηρίξει όσο το δυνατόν καλύτερα τις σχετιζόμενες με την ιδιωτικότητα επιχειρησιακές διεργασίες (privacy-related business processes).
4. Ορισμός της αρχιτεκτονικής συστήματος που υποστυλώνει πιο καλά τη διαδικασία που σχετίζεται με το απόρρητο που καθορίστηκε νωρίτερα μέσω του βήματος τρία. Για τον ορισμό της αρχιτεκτονικής αυτής χρησιμοποιούνται επίσης πρότυπα.

Τα πρότυπα επιχειρηματικής διαδικασίας που αφορούν την ιδιωτικότητα του βήματος τρία (3) όπως αναφέρθηκε προηγουμένως, αποτελούν μια από τις αιτίες επιλογής της μεθοδολογίας PriS. Καθένα από τα μοτίβα διαδικασίας απορρήτου που παρουσιάζονται πιο κάτω [21], περιγράφονται σε δύο επίπεδα. Το πρώτο επίπεδο, το οποίο φαίνεται στο σχήμα 4, είναι κοινό για όλα τα μοτίβα διαδικασίας απορρήτου, καθώς σε αυτό πραγματοποιείται η περιγραφή όπου ένας χρήστης σχετίζεται με το σύστημα, αυτό μπορεί να είναι είτε άτομο, είτε διαδικασία, είτε υπηρεσία, μέσω μιας ειδικής διαδικασίας, αυτής που σχετίζεται με το απόρρητο. Το δεύτερο επίπεδο είναι αυτό που ορίζει ποια απαίτηση ικανοποιείται, διαμορφώνοντας με αυτόν τον τρόπο τα διάφορα μοτίβα διαδικασίας απορρήτου. Γίνεται επομένως αντιστοίχιση της διαδικασίας απορρήτου με την απαίτηση απορρήτου που περιορίζει τη συγκεκριμένη διαδικασία.

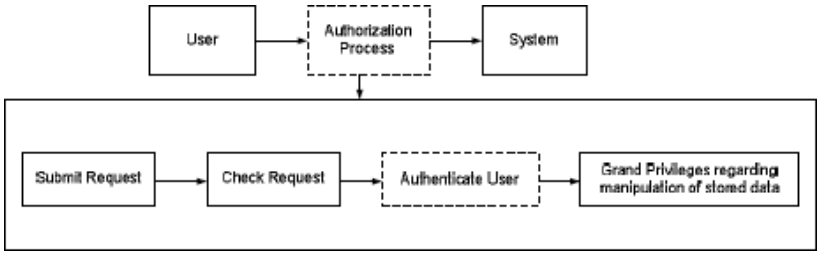
Σχήμα 4. Πρώτο (κοινό) Επίπεδο Μοτίβου

Τα διαφορετικά μοτίβα διαδικασίας απορρήτου προκύπτουν ανάλογα με τις απαιτήσεις που αντιμετωπίζουν. Για παράδειγμα υπάρχει το μοτίβο διαδικασίας που αντιμετωπίζει την απαίτηση πιστοποίηση της ταυτότητας του χρήστη και περιγράφει τις ανάλογες δραστηριότητες που χρειάζονται για να υλοποιηθεί η συγκεκριμένη διαδικασία (Σχήμα 5). Όπως φαίνεται όταν ο χρήστης θα υποβάλλει ένα αίτημα στο σύστημα, τότε το τελευταίο θα ελέγχει για την εγκυρότητα του αιτήματος. Σε περίπτωση που απαιτείται έλεγχος ταυτότητας τότε ο χρήστης θα παρέχει τα απαραίτητα δεδομένα για τον έλεγχο αλλιώς σε διαφορετική περίπτωση δεν θα του επιτρέπεται η πρόσβαση.



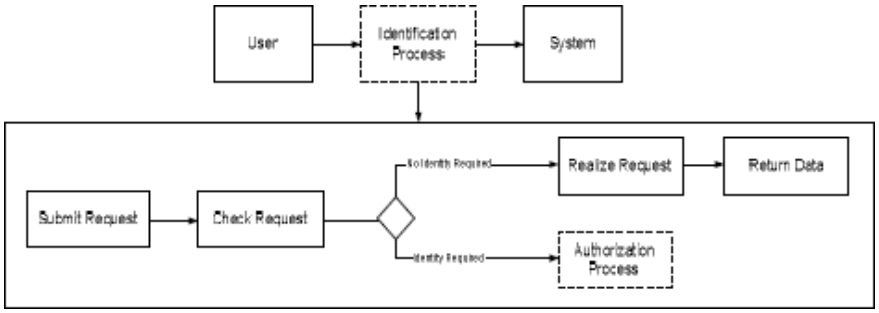
Σχήμα 5. Μοτίβο Ελέγχου Ταυτότητας

Πέρα από το μοτίβο ελέγχου ταυτότητας, υπάρχουν και άλλα μοτίβα. Υπάρχει το μοτίβο της διαδικασίας εξουσιοδότησης (Σχήμα 6), το μοτίβο που αντιστοιχεί στην απαίτηση αναγνώρισης (Σχήμα 7), το μοτίβο της διαδικασίας της προστασίας δεδομένων (Σχήμα 8), το μοτίβο που καταπολεμά απαιτήσεις ανωνυμίας και ψευδωνυμίας (Σχήμα 9), ενώ τέλος υπάρχουν και τα μοτίβα για τις απαιτήσεις αποσύνδεσης (Σχήμα 10) και μη παρατηρησιμότητας (Σχήμα 11).



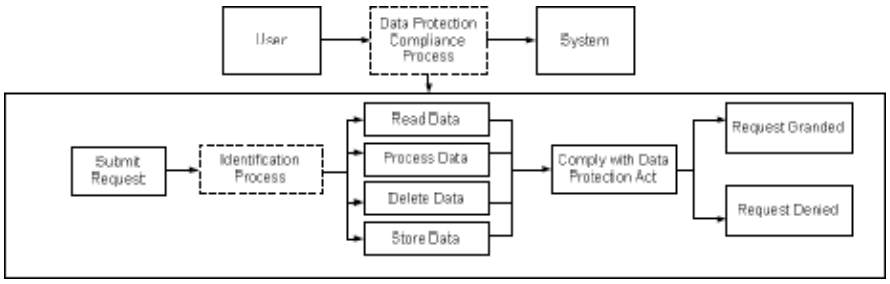
Σχήμα 6. Μοτίβο Εξουσιοδότησης

Το μοτίβο της εξουσιοδότησης (Σχήμα 6) περιγράφει πως τα προσωπικά δεδομένα του χρήστη, υποκειμένου δεδομένων, πρέπει να έχουν πρόσβαση μόνο από χρήστες που έχει εξουσιοδοτήσει ο πρώτος. Εάν για παράδειγμα ένας χρήστης υποβάλλει ένα αίτημα σε ένα πληροφοριακό σύστημα, θα πρέπει αρχικά να ελεγχθεί η φύση του αιτήματος και εφόσον γίνει και η διαδικασία ελέγχου ταυτότητας ανάλογα με τα δικαιώματα που έχει αυτός ο χρήστης τότε γίνεται να αποκτήσει πρόσβαση ή και όχι στη συγκεκριμένη υπηρεσία ή και δεδομένα για τα οποία υπέβαλλε αρχικά το αίτημα.



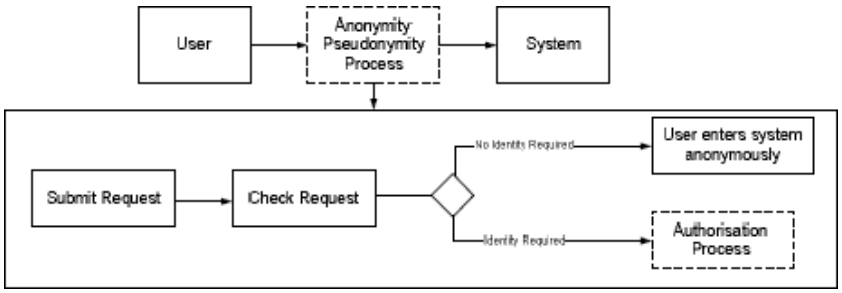
Σχήμα 7. Μοτίβο Αναγνώρισης

Το μοτίβο της αναγνώρισης (Σχήμα 7) αντίστοιχα ελέγχει εάν απαιτείται ή όχι η ταυτότητα ενός χρήστη όταν αυτός υποβάλλει αίτημα σε ένα σύστημα είτε για την απόκτηση πρόσβασης δεδομένων είτε για την διαχείριση αυτών. Εάν λοιπόν το αίτημα σχετίζεται με πρόσβαση σε προσωπικά δεδομένα ή σε εξατομικευμένες υπηρεσίες τότε ενεργοποιείται η διαδικασία εξουσιοδότησης όπως φαίνεται και στο σχήμα, ώστε να αποκτήσει ο χρήστης πρόσβαση στα δεδομένα.



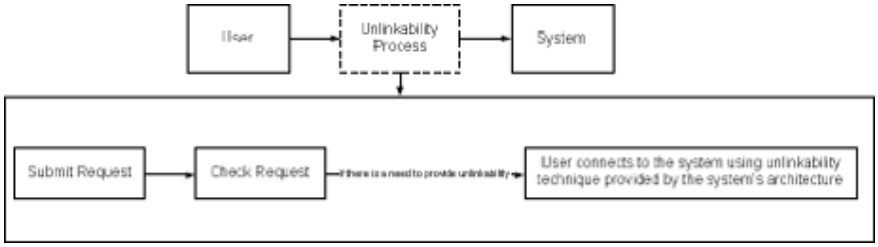
Σχήμα 8. Μοτίβο Προστασίας Δεδομένων

Το μοτίβο προστασίας δεδομένων (Σχήμα 8) έχει ως βασικό στόχο να διασφαλίσει ότι κάθε πρόσβαση, επεξεργασία κι διάθεση με τα προσωπικά δεδομένα, πραγματοποιείται σύμφωνα με τους κανονισμούς του απορρήτου του επιμέρους πληροφοριακού συστήματος και την οδηγία 95/46/ΕΚ [28] που αναφέρεται στην επεξεργασία και την ελεύθερη κυκλοφορία των προσωπικών δεδομένων. Όπως απεικονίζεται και στο σχήμα (Σχήμα 8) όταν ένας χρήστης προσπαθεί να αποκτήσει πρόσβαση σε προσωπικά δεδομένα, ενεργοποιείται μια διαδικασία αναγνώρισης για την ταυτοποίηση αυτού και για την παραχώρηση του δικαιώματος ανάγνωσης, επεξεργασίας, αποθήκευσης ή διαγραφής των προσωπικών του δεδομένων. Στη συνέχεια, εάν ο χρήστης ζητήσει να εκτελέσει οποιαδήποτε από τις παραπάνω εργασίες, το σύστημα ελέγχει εάν αυτό συμμορφώνεται με τους κανονισμούς απορρήτου και το αίτημα είτε εγκρίνεται είτε απορρίπτεται ανάλογα.



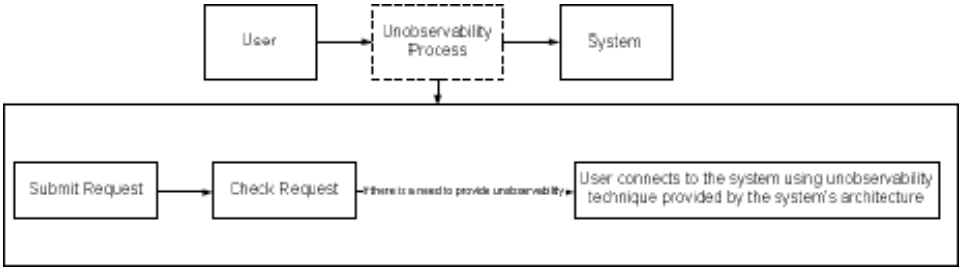
Σχήμα 9. Μοτίβο Ανωνυμίας και Ψευδωνυμίας

Όπως φαίνεται στο μοτίβο ανωνυμίας και ψευδωνυμίας (Σχήμα 6), πρώτον, ελέγχεται το αίτημα του χρήστη προκειμένου να αποφασιστεί εάν χρειάζεται ή όχι ταυτότητα. Εάν υπάρχει ανάγκη γνώσης της ταυτότητας του χρήστη, ενεργοποιείται η διαδικασία αναγνώρισης. Σε αντίθετη περίπτωση, ο χρήστης όχι μόνο λαμβάνει τις πληροφορίες του χωρίς να παρέχει προσωπικά δεδομένα, αλλά υλοποιούνται και συγκεκριμένες τεχνικές για την προστασία της ανωνυμίας του. Έτσι, η αναγνώριση μπορεί να αποτελεί υποτμήμα της ανωνυμίας ανάλογα με το εάν ζητούνται ή όχι συγκεκριμένα δεδομένα της ταυτότητας του χρήστη για επεξεργασία. Η ψευδωνυμία χρησιμοποιείται όταν δεν μπορεί να παρασχεθεί ανωνυμία, αλλά και πάλι με σκοπό την προστασία της ανωνυμίας του χρήστη.



Σχήμα 10. Μοτίβο Αποσύνδεσης

Τα δύο τελευταία μοτίβα της αποσύνδεσης (Σχήμα 10) και της μη παρατηρησιμότητας (Σχήμα 11) έχουν παρόμοια δομή. Ο χρήστης ζητά ένα αίτημα. Με βάση τις απαιτήσεις του συστήματος, και ανάλογα εάν πρέπει να πραγματοποιηθεί μία ή και οι δύο από αυτές τις απαιτήσεις, χρησιμοποιούνται κατάλληλες τεχνικές αποσύνδεσης ή μη παρατηρησιμότητας για τη σύνδεση του χρήστη με το σύστημα όπως το πρωτόκολλο Hordes[5], το σύστημα Tor[6] κ.τ.λ..



Σχήμα 11. Μοτίβο Μη Παρατηρησιμότητας

Αυτά τα επτά σε αριθμό μοτίβα διαδικασίας απορρήτου είναι που πλαισιώνουν τον σκοπό του τρίτου, σε σειρά, βήματος της μεθοδολογίας PriS καθώς και μία από τις αιτίες επιλογής της PriS, ως η μεθοδολογία που θα ενισχυθεί με βάση τον GDPR.

[5] Hordes : Πρωτόκολλο για την ανωνυμία βασισμένο σε πολλαπλές εκπομπές

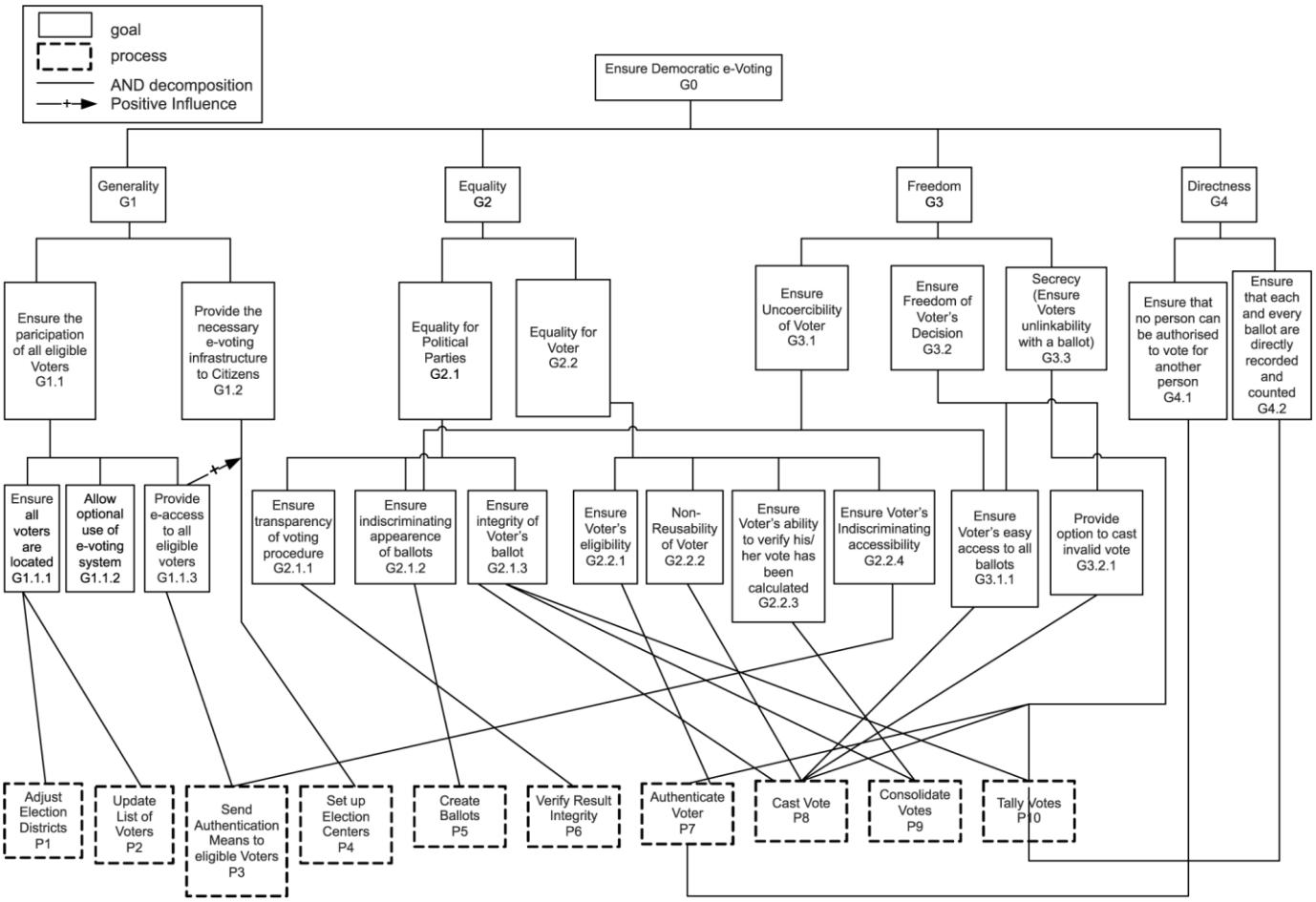
[6] Tor : Σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο

4.1.2 Μελέτη Περίπτωσης e-voting

Αντικείμενο αυτής της υποενότητας είναι εφαρμογή της μεθοδολογίας PriS σε ένα έργο ηλεκτρονικής ψηφοφορίας [21]. Η επιλογή του συγκεκριμένου έργου είναι σκόπιμη, όπως προαναφέρεται, καθώς υπάρχει στη βιβλιογραφία μέσα από το άρθρο «Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process», και επειδή διευκολύνει αργότερα την ενίσχυση της μεθοδολογίας PriS, εφόσον χρησιμοποιείται ως παράδειγμα και στην ανεπτυγμένη μεθοδολογία.

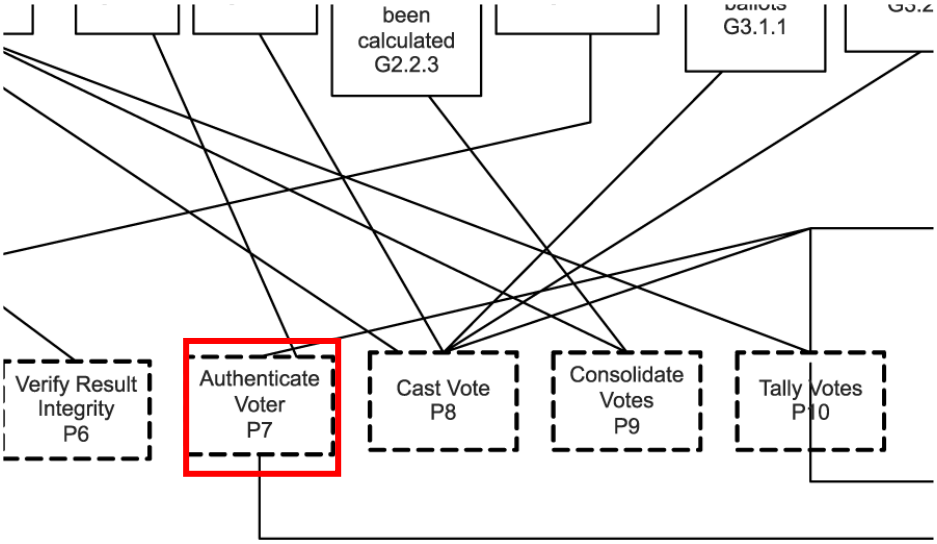
Βασικός στόχος ενός συστήματος ηλεκτρονικής ψηφοφορίας (e-voting) είναι η παραχώρηση του δικαιώματος ψήφου μέσω του διαδικτύου στους πολίτες, προκειμένου να απλοποιηθεί η εκλογική διαδικασία. Το συγκεκριμένο σύστημα (e-voting) έχει τέσσερις βασικές αρχές που διαμορφώνουν αυτό και θέτουν τους τέσσερις οργανωτικούς του στόχους. Οι στόχοι αυτοί : 1) Γενικότητα, 2) Ισότητα, 3) Ελευθερία και 4) Αμεσότητα συνεπάγονται διαφορετικά ζητήματα. Η γενικότητα λόγου χάρη δείχνει πως οι πολίτες που έχουν μια ηλικία και πάνω έχουν το δικαίωμα να συμμετέχουν στην εκλογική διαδικασία. Η ισότητα συνεπάγεται ότι και τα πολιτικά κόμματα αλλά και οι ψηφοφόροι έχουν ίσα δικαιώματα πριν, κατά τη διάρκεια και ύστερα από την εκλογική διαδικασία. Αντίστοιχα η ελευθερία υπαινίσσεται ότι δεν ασκείται καμία μορφή βίας, εξαναγκασμός, πίεση ή άλλες χειραγωγίες από το κράτος ή από άτομα κατά την εκλογική διαδικασία. Τέλος η αμεσότητα δείχνει πως δεν υπάρχει κανένας μεσάζων στη διαδικασία ψηφοφορίας και ότι κάθε ψηφοδέλτιο καταγράφεται και καταμετράται άμεσα.

Βάσει των τεσσάρων στόχων που αναλύθηκαν προηγουμένως (Γενικότητα, Ισότητα, Ελευθερία, Αμεσότητα) και με τη βοήθεια του πλαισίου, στο οποίο στηρίζεται το μοντέλο εννοιών που χρησιμοποιεί η μεθοδολογία PriS, Enterprise Knowledge Development (EKD) [1], κατασκευάζεται το μοντέλο στόχων του συστήματος e-voting και εντοπίζονται οι σχετικές διαδικασίες που υλοποιούν τους λειτουργικούς στόχους. Το μοντέλο αυτό παρουσιάζεται παρακάτω (Σχήμα 12).



Σχήμα 12. Goal Model του Συστήματος Ηλεκτρονικής Ψηφοφορίας (e-voting)

Όπως γίνεται αντιληπτό και από το παραπάνω σχήμα έχουν εφαρμοστεί τα δύο πρώτα βήματα της μεθοδολογίας PriS. Έχουν αναδειχθεί οι στόχοι και οι υποστόχοι αυτών του συστήματος, οι οποίοι περιγράφονται με πλαίσια (Βήμα 1 Μεθοδολογίας) ενώ έχει προσδιοριστεί και η σχέση και ο αντίκτυπος των στόχων αυτών μεταξύ τους μέσα από το Διάγραμμα Μοντέλου Στόχου (Goal Model Diagram) (Σχήμα 12), (Βήμα 2 Μεθοδολογίας). Στην τελευταία γραμμή του σχήματος με τα διακεκομμένα πλαίσια παρουσιάζονται οι αντίστοιχες διεργασίες που ικανοποιούν κάθε στόχο που βρίσκεται παραπάνω. Η μοντελοποίηση αυτών των διαδικασιών, που είναι και το τρίτο βήμα της PriS (Βήμα 3 Μεθοδολογίας), γίνεται με βάση τα μοτίβα διαδικασίας απορρήτου που παρουσιάστηκαν νωρίτερα στην υποενότητα 4.1.1. Για παράδειγμα η διαδικασία (P7) που αναφέρεται στην αυθεντικοποίηση του χρήστη (Σχήμα.13) κατά την εκλογική διαδικασία μπορεί να χρησιμοποιήσει το μοτίβο ελέγχου ταυτότητας, (Σχήμα.5). Το συγκεκριμένο μοτίβο, το Μοτίβο Ελέγχου Ταυτότητας, είναι η αιτία που εκκινεί την ιδέα για την ενίσχυση της μεθοδολογίας PriS παρακάτω στην ενότητα 4.2.



Σχήμα 13. Διαδικασία Αυθεντικοποίησης Χρήστη (P7)

4.2 Πλαίσιο Ενίσχυσης και Εφαρμογής

Στην παρούσα ενότητα της εργασίας παρουσιάζεται αρχικά το μοντέλο 5W, το οποίο χρησιμοποιείται για την ενίσχυση της μεθοδολογίας PriS με βάση τον GDPR ολοκληρώνοντας τον σκοπό της εργασίας. Επιπλέον παρατίθεται μια εφαρμογή του μοντέλου 5W στην ενισχυμένη μεθοδολογία PriS με τη χρήση του παραδείγματος του συστήματος ηλεκτρονικής ψηφοφορίας (e-voting) που χρησιμοποιείται στην υποενότητα 4.1.1.

4.2.1 Μοντέλο 5W

Στόχος μέσα από την εισαγωγή του μοντέλου αυτού (5W), είναι η επίτευξη των τεσσάρων από τις επτά αρχές του GDPR. Οι τέσσερις αυτές αρχές που είναι επιθυμητό να επιτευχθούν είναι:

a) Νομιμότητα, Δικαιοσύνη, Διαφάνεια (μέσα από τη Πολιτική Συναίνεσης που προκύπτει από το 5W),

b) Περιορισμός του Σκοπού (μέσα από το ερώτημα 2 του 5W model – προκύπτει επομένως από την επιλογή του DS, υποκείμενου δεδομένων, για το λόγο που θα υποβληθούν τα δεδομένα του σε επεξεργασία),

c) Περιορισμός Αποθήκευσης (μέσω του ερωτήματος 3 του μοντέλου – με την επιλογή του DS για το μέσο από το οποίο θα αντλούνται και τον χώρο στον οποίο θα

αποθηκεύονται τα δεδομένα του), (και του ερωτήματος 5 – με την επιλογή για το χρονικό διάστημα που θα είναι διαθέσιμα τα δεδομένα για επεξεργασία) και

d) Υπευθυνότητα (μέσα από τη Πολιτική Συναίνεσης που προκύπτει από το 5W).

Το κριτήριο επιλογής των παραπάνω αρχών έγινε λόγω των ερωτημάτων που θέτει το μοντέλο 5W. Απαντώντας δηλαδή ένας χρήστης στις πέντε ερωτήσεις του 5W model, καταφέρνει να ικανοποιήσει τις τέσσερις παραπάνω αρχές. Οι υπόλοιπες αρχές του GDPR, δηλαδή η αρχή της εμπιστευτικότητας, της ακρίβειας και της ελαχιστοποίησης των δεδομένων δεν ικανοποιούνται σε αυτή την εργασία.

Στο Μοντέλο 5W το DS (Data Subject – υποκείμενο δεδομένων), καλείται να δώσει απαντήσεις σε ερωτήσεις 5W's. Σύμφωνα με τη βιβλιογραφία από το ακρωνύμιο 5W προκύπτουν οι εξής πέντε (5) σε αριθμό ερωτήσεις, γι' αυτό και ο αριθμός 5 μπροστά :

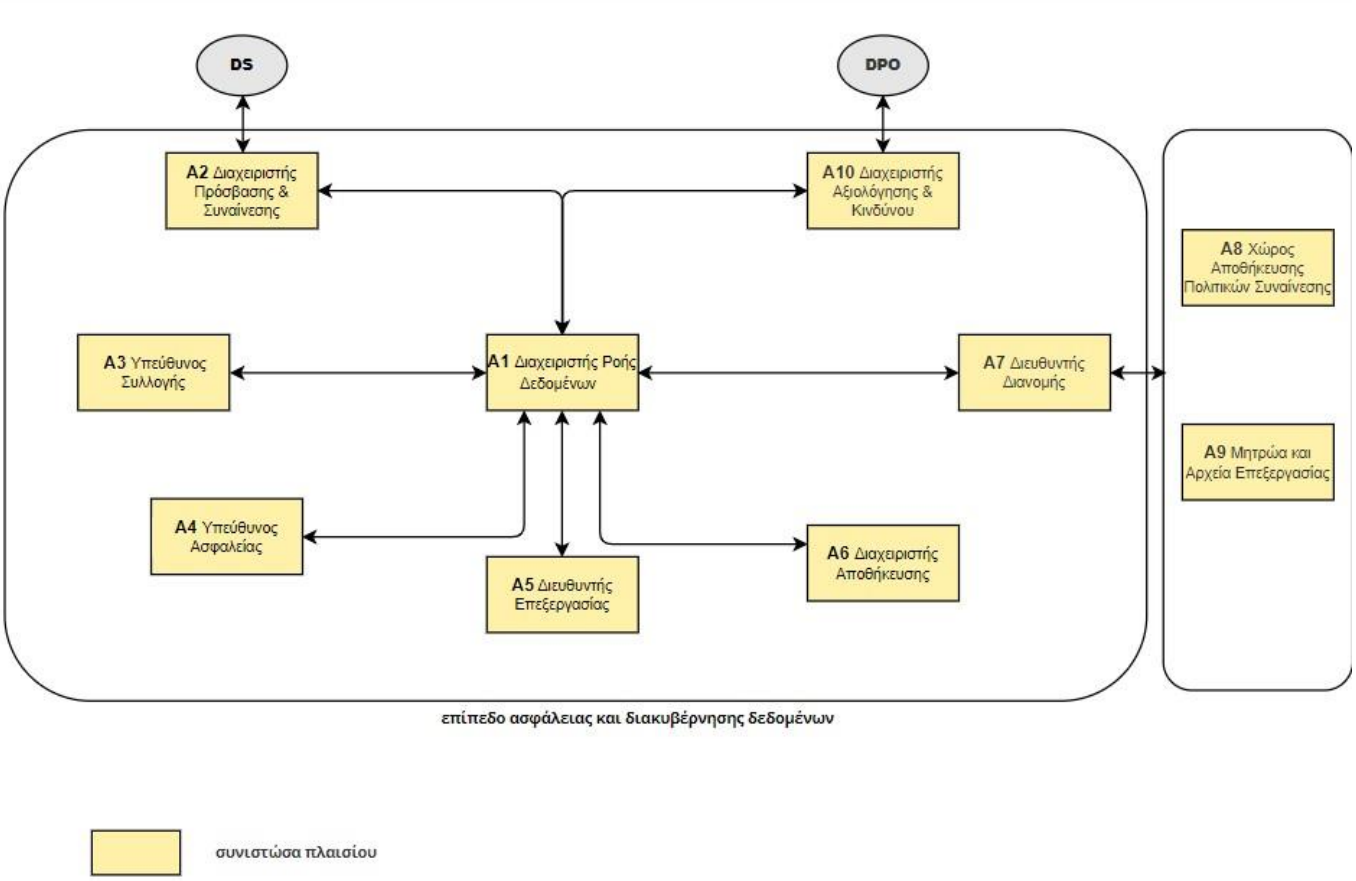
1. What (Σε ποια δεδομένα, data, θα υποβληθεί επεξεργασία),
2. Why (Ο λόγος για τον οποίο θα υποβληθούν τα δεδομένα σε επεξεργασία),
3. Where (Πως και που αποθηκεύονται τα δεδομένα του υποκειμένου),
4. Who (Ποιος μπορεί να έχει πρόσβαση στα δεδομένα του υποκειμένου) και
5. When (Για πόσο χρονικό διάστημα θα είναι διαθέσιμα τα δεδομένα).

Το μοντέλο 5W model περιέχει, όπως φαίνεται και παραπάνω, ερωτήσεις οι οποίες όταν απαντώνται βοηθούν στη συλλογή πληροφοριών. Είναι πολύ σημαντικό το ότι οι ερωτήσεις που θέτει το μοντέλο δεν απαντώνται με «ναι» ή «όχι» γιατί αυτό που επιθυμεί να δημιουργηθεί κάποιος που χρησιμοποιεί το μοντέλο είναι μια ολοκληρωμένη αναφορά που έχει στοιχεία και λεπτομέρειες. Το μοντέλο εντοπίζεται σε πολλά μέρη στη βιβλιογραφία όπως στον τομέα της δημοσιογραφίας, της έρευνας, σε τομείς διαχείρισης έργων καθώς και του marketing.

Ο λόγος λοιπόν για τον οποίο καλείται το υποκείμενο δεδομένων να απαντήσει τις παραπάνω ερωτήσεις είναι για να εκφράσει την συγκατάθεσή του σχετικά με την επεξεργασία των δεδομένων του, να δημιουργήσει επομένως μια πολιτική συναίνεσης. Απαντώντας στην πρώτη ερώτηση επομένως θα συμφωνεί ή όχι, εάν έχει το δικαίωμα επιλογής σε αποφάσεις που έχει λάβει ο υπεύθυνος επεξεργασίας, σχετικά με τα απαιτούμενα της κάθε διαδικασίας, ποια δεδομένα του θα υποβάλλονται σε επεξεργασία, με την δεύτερη ερώτηση τον λόγο για τον οποίο θα υποβάλλονται τα δεδομένα σε επεξεργασία ενώ με την τρίτη ερώτηση το μέσο από όπου θα αντλούνται καθώς και τον χώρο αποθήκευσης των δεδομένων. Παράλληλα με το τέταρτο ερώτημα το υποκείμενο δεδομένων, θα ορίζει ποιος μπορεί να έχει πρόσβαση στα δεδομένα του ενώ με το πέμπτο ερώτημα θα ορίζει το χρονικό διάστημα που θα διατίθενται τα δεδομένα.

Η διαδικασία που θα εφαρμόζεται για να ενισχυθεί η μεθοδολογία PriS με τον GDPR είναι συγκεκριμένη. Στην πρώτη φάση λοιπόν το υποκείμενο δεδομένων θα μπορεί να απαντήσει στις παραπάνω πέντε ερωτήσεις, μέσα από μια διεπαφή χρήστη. Εφόσον απαντήσει στα πέντε

ερωτήματα θα μπορεί να δηλώσει τις προτιμήσεις του, μέσα από κλειστού τύπου απαντήσεις που θα του δοθούν. Σκοπός είναι μέσω των ερωτημάτων το υποκείμενο να δηλώσει τις προτιμήσεις του σχετικά με τη συχνότητα συλλογής, τους "χώρους" αποθήκευσης των δεδομένων και το σύνολο των πληροφοριών που επιτρέπει να αποκαλύψει σε εφαρμογές τρίτων. Μόλις το υποκείμενο συμπληρώσει τις απαντήσεις, μέσα από τη διεπαφή, θα πραγματοποιείται ένας έλεγχος συμμόρφωσης με εργαλείο που παρέχεται για την αξιολόγηση και τη διαχείριση κινδύνων. Ο έλεγχος αυτός, ο οποίος θα γίνεται από τον διαχειριστή αξιολόγησης και κινδύνου τον οποίο θα ορίζει το εκάστοτε σύστημα, θα επαληθεύει ότι κάθε επιλογή του χρήστη σχετικά με την επεξεργασία των δεδομένων του θα λαμβάνεται υπόψιν και πως το κάθε επίπεδο επεξεργασίας και αποθήκευσης θα έχει δικαίωμα πρόσβασης μόνο στα εξουσιοδοτημένα δεδομένα. Αυτή η εργασία θα εκτελείται κάθε φορά που θα λαμβάνονται νέα δεδομένα. Το υποκείμενο των δεδομένων έπειτα θα ενημερώνεται, μετά από τον έλεγχο, σχετικά με το αν οι προτιμήσεις συμμορφώνονται ή όχι με τον GDPR ή και με άλλες νομοθεσίες για παράδειγμα με νομικές διατάξεις που αφορούν την υποχρέωση διατήρησης συγκεκριμένων δεδομένων ή οικονομικά δεδομένα που αφορούν ένα φυσικό πρόσωπο, μέσα από διαγράμματα ποσοστών τα όρια των οποίων θα δημιουργούν οι υπεύθυνοι του συστήματος. Στην περίπτωση που το ποσοστό που προκύπτει από τον έλεγχο βρίσκεται μέσα στα όρια των πολιτικών ελέγχων χρήσης, τότε το υποκείμενο μπορεί να αποθηκεύσει τις προτιμήσεις του και να ξεκινήσει η επεξεργασία των δεδομένων του σύμφωνα με αυτές. Στην αντίθετη περίπτωση, δηλαδή εάν το ποσοστό μετά τον έλεγχο που προκύπτει δεν είναι συμμορφωμένο με πολιτικές ελέγχου χρήσης, το υποκείμενο δεδομένων θα έχει το δικαίωμα να μην προχωρήσει στην αποθήκευση των επιλογών του αλλά να τις επεξεργαστεί ξανά. Παρακάτω παρουσιάζεται ένα διάγραμμα διάδοσης των δεδομένων της παραπάνω διαδικασίας.



Σχήμα 14. Διάγραμμα Διάδοσης Δεδομένων στο model 5W

Όπως περιγράφεται στο σχήμα υπάρχουν δέκα συνιστώσες πλαισίου του 5W model. Η κάθε συνιστώσα, στην περίπτωσή αυτή θα καλείται είτε διαχειριστής, είτε υπεύθυνος, είτε διευθυντής, υπάρχει και είναι υπεύθυνη για διαφορετικό σκοπό :

A1. Διαχειριστής Ροής Δεδομένων : Αυτή η συνιστώσα μπορεί να διαχειριστεί τον κύκλο ζωής των δεδομένων (από τη συλλογή έως τη διαγραφή) και να εντοπίσει παραβιάσεις ασφάλειας. Αναμεταδίδεται στις υπόλοιπες συνιστώσες (A2-A10) για συγκεκριμένες εργασίες, όπως η ειδοποίηση του χρήστη, σε περίπτωση παραβίασης δεδομένων και η ενημέρωση του υποκειμένου δεδομένων για τη χρήση των δεδομένων του.

A2. Διαχειριστής πρόσβασης και συναίνεσης : Εφαρμόζει και επιβάλλει τα δικαιώματα του χρήστη, με βάση τον GDPR, δηλαδή το δικαίωμα ενημέρωσης, πρόσβασης, διαγραφής, ενημέρωσης, το δικαίωμα στον περιορισμό επεξεργασίας και το δικαίωμα αντίρρησης.

Α3. Υπεύθυνος συλλογής : Είναι υπεύθυνος για τον σχολιασμό μη επεξεργασμένων δεδομένων με τα άκρα - όρια που ορίζονται στον διαχειριστή πρόσβασης και συναίνεσης. Η ελαχιστοποίηση δεδομένων επιβάλλεται σε αυτό το σημείο φιλτράροντας τα δεδομένα που συλλέγονται σε πολύ πρώιμο στάδιο.

Α4. Υπεύθυνος ασφαλείας : Με τη βοήθεια του υπευθύνου ασφαλείας κρυπτογραφούνται τα δεδομένα για τα οποία το υποκείμενο δεδομένων έχει δώσει συγκατάθεση για την επεξεργασία τους.

Α5. Διευθυντής επεξεργασίας : Βοηθά τους ελεγκτές να ελέγχουν το εύρος της διαδικασίας σε σχέση με τις πολιτικές συναίνεσης που ορίζονται στο στοιχείο διαχείρισης συναίνεσης από το υποκείμενο δεδομένων. Επίσης, κάθε δραστηριότητα επεξεργασίας αποθηκεύεται στο στοιχείο καταγραφής και εγγραφών επεξεργασίας Α9.

Α6. Διαχειριστής αποθήκευσης : Βοηθά τους ελεγκτές να διαχειρίζονται τα αποθηκευμένα δεδομένα (ακατέργαστα δεδομένα και επεξεργασμένα δεδομένα) και ελέγχει τη μεταφορά δεδομένων συγκρίνοντας τη θέση δεδομένων που ορίζεται στην πολιτική συναίνεσης και την τρέχουσα φυσική θέση των δεδομένων.

Α7. Διευθυντής διανομής : Εφαρμόζει τεχνικές ελέγχου ταυτότητας και εξουσιοδότησης για τον έλεγχο της πρόσβασης του χρήστη ή της υπηρεσίας σε προσωπικά δεδομένα.

Α8. Αποθήκευση Πολιτικών Συναίνεσης.

Α9. Μητρώα και αρχεία επεξεργασίας.

Α10. Διαχειριστής αξιολόγησης και κινδύνου : Αυτό το στοιχείο μπορεί να χρησιμοποιηθεί από τον υπεύθυνο προστασίας δεδομένων, ως υπηρεσία ελέγχου. Για παράδειγμα, παρέχει μια έξοδο για την κατάσταση της συμμόρφωσης με τον GDPR. Αυτό επιτυγχάνεται συγκρίνοντας το εύρος της πολιτικής συναίνεσης που συλλέγεται από τον χρήστη με την επιχειρηματική πολιτική που συνάπτεται από τη διαδικασία παροχής υπηρεσιών. Στη συνέχεια, αναφέρει μια κατάσταση συμμόρφωσης για κάθε υπηρεσία και καταδεικνύει τη συμμόρφωση ή τη μη συμμόρφωση για τους χρήστες.

Το ποσοστό υπολογισμού για το αν οι προτιμήσεις του υποκείμενου δεδομένων σχετικά με την επεξεργασία και τη διάθεση των δεδομένων του είναι GDPR Compliant, δηλαδή ενισχύονται με βάση τις αρχές του GDPR μπορεί να προκύψει από την συνθήκη :

S : P U E U D → L, όπου P σύνολο διεργασιών, E αποθηκευτικός χώρος, D δεδομένα και L προτιμήσεις υποκειμένου επεξεργασίας.

a. Μια διεργασία p είναι εξουσιοδοτημένη να επεξεργαστεί ένα δεδομένο d εάν : L(d) ⊆ L(p),
b. Ένας αποθηκευτικός χώρος είναι εξουσιοδοτημένος να αποθηκεύσει δεδομένα d εάν : L(d) ⊆ L(e).

Ουσιαστικά η παραπάνω συνθήκη περιγράφει για το (a) πως σε περίπτωση που οι προτιμήσεις (L) του υποκειμένου δεδομένων σχετικά με τα δεδομένα (d) που θα είναι διαθέσιμα, είναι υποσύνολο των προτιμήσεων (L) του συνόλου διεργασιών (p), δηλαδή των διεργασιών που έχουν οριστεί από πριν από το εκάστοτε σύστημα με βάση τον GDPR ως όριο, τότε η εκάστοτε διεργασία p είναι εξουσιοδοτημένη να επεξεργαστεί ένα δεδομένο d.

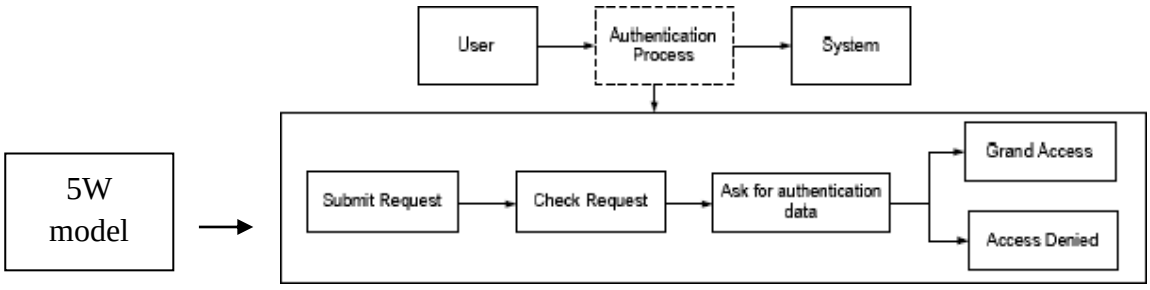
Η εισαγωγή του μοντέλου 5W προτείνεται να ενσωματωθεί στο τρίτο βήμα της μεθοδολογίας PriS (Βήμα 3 Μεθοδολογίας), όπου ορίζονται και τα μοτίβα διαδικασίας απορρήτου (μοτίβο διαδικασίας ελέγχου ταυτότητας, μοτίβο αποσύνδεσης, μοτίβο μη παρατηρησιμότητας κ.τ.λ.). Παρακάτω στην υποενότητα δίνεται ένα παράδειγμα σχετικά με την εφαρμογή του 5W model στο τρίτο βήμα της μεθοδολογίας PriS, κάνοντας χρήση του case-study με το e-voting της υποενότητας 4.1.2.

4.2.2 Μελέτη Περίπτωσης μετά την ενισχυμένη μεθοδολογία

Σε αυτή την υποενότητα γίνεται χρήση του case-study με θέμα το e-voting που αναφέρεται στην υποενότητα 4.1.2, για την εφαρμογή του 5W model στο τρίτο βήμα της μεθοδολογίας PriS. Η χρήση του συγκεκριμένου παραδείγματος είναι εσκεμμένη καθώς πέρα το ότι προϋπάρχει το μοντέλο στόχων του συστήματος και εντοπίζονται οι σχετικές διαδικασίες που υλοποιούν τους λειτουργικούς στόχους, σε προηγούμενη βιβλιογραφική εργασία [21], γίνεται πιο εύκολα κατανοητό η εισαγωγή του 5W model στη μεθοδολογία.

Οι στόχοι του e-Voting φαίνονται στο σχήμα (Σχήμα.12) το οποίο έχει παρθεί από το ερευνητικό άρθρο «Using Privacy Process Patterns for Incorporating Privacy Requirements». Όπως είναι λογικό ο χρήστης (υποκείμενο δεδομένων) DS πρέπει πριν από την ψηφοφορία να ταυτοποιήσει τον εαυτό του ώστε να διασφαλιστεί η ακεραιότητα της διαδικασίας (P7). Από την διεργασία P7, στην οποία πρέπει να γίνει η ταυτοποίηση του χρήστη (υποκειμένου δεδομένων), εξάγεται το μοτίβο ελέγχου ταυτότητας, (Σχήμα.5). Σε αυτό το σημείο προτείνεται η χρήση και η εισαγωγή της διεπαφής χρήστη για το μοντέλο 5W, με το οποίο το υποκείμενο δεδομένων θα

δηλώσει τις προτιμήσεις του σχετικά με την επεξεργασία των δεδομένων του, όπως φαίνεται πιο κάτω στο σχήμα (Σχήμα.15). Αυτό θα γίνει ένα βήμα πριν την επιβολή αιτήματος, με σκοπό να γίνει η μεθοδολογία PriS GDPR compliant. Ο λόγος που έχει επιλεχθεί το μοτίβο ελέγχου ταυτότητας είναι επειδή σε αυτό ο χρήστης, δηλαδή το υποκείμενο δεδομένων, παραχωρεί τα προσωπικά δεδομένα του, τα οποία είναι απαραίτητα για την αυθεντικοποίησή του επομένως για τον έλεγχο της ταυτότητάς του.



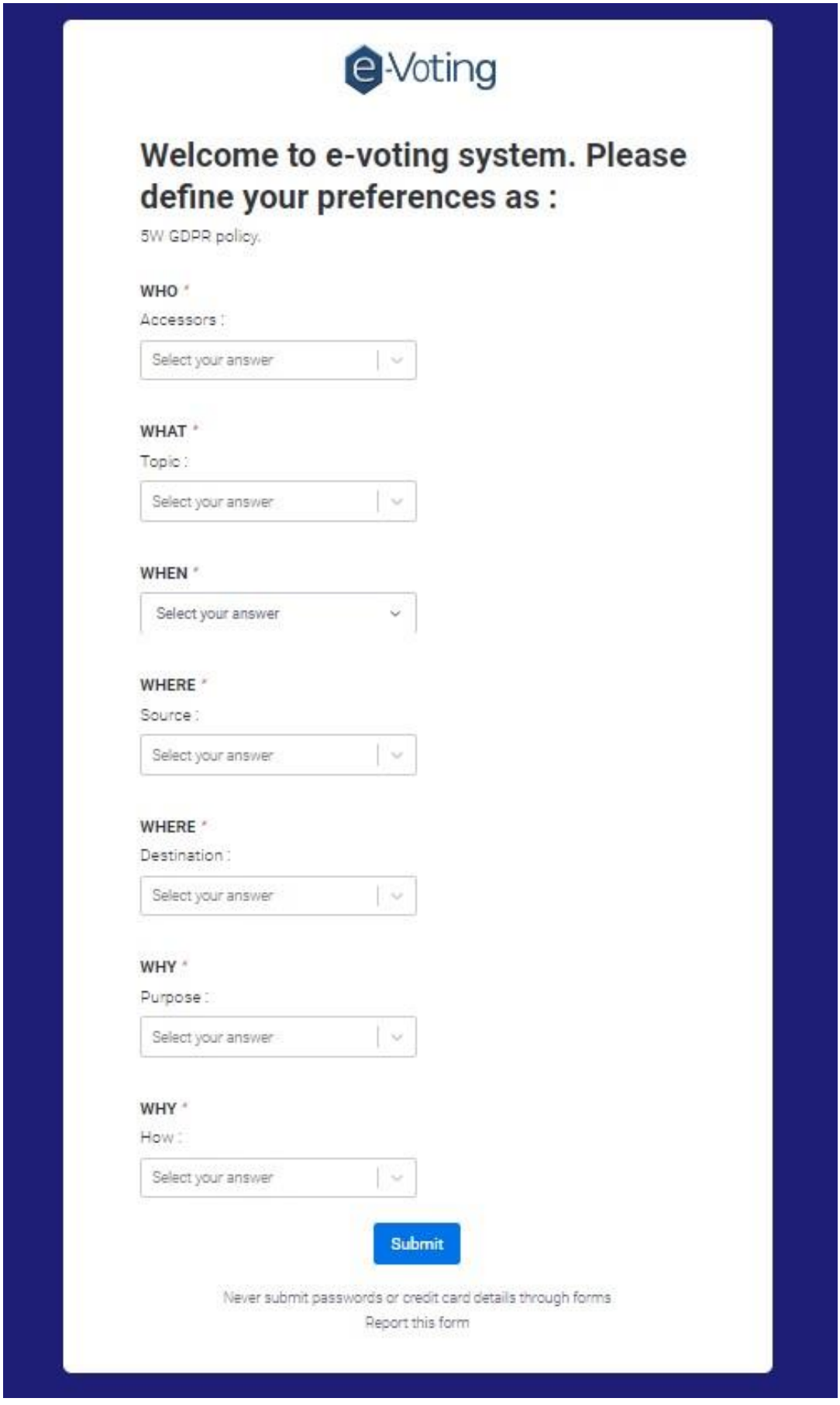
Σχήμα 15. Εισαγωγή του 5W model στο μοτίβο ελέγχου ταυτότητας

Παρακάτω παρουσιάζεται μια διεπαφή χρήστη καθώς και μερικά παραδείγματα γραφημάτων που αφορούν τη συγκατάθεση του χρήστη – ψηφοφόρου, δηλαδή του υποκείμενου δεδομένων, σχετικά με τις προτιμήσεις του για την επεξεργασία των δεδομένων του σε ένα σενάριο ηλεκτρονικής ψηφοφορίας. Η διεπαφή καθώς και τα γραφήματα αφορούν το σενάριο e-voting που περιεγράφηκε στην ενότητα 4.1.2.

Ένα σύστημα ηλεκτρονικής ψηφοφορίας (e-voting) έχει ως σκοπό, όπως αναφέρθηκε προηγουμένως στην ενότητα 4.1.2 να απλοποιήσει την εκλογική διαδικασία και να δώσει το δικαίωμα στους ψηφοφόρους να συμμετέχουν σε αυτή χωρίς να είναι αναγκαία η φυσική τους παρουσία σε κάποιο εκλογικό κέντρο. Στην περίπτωση αυτή ψηφοφόρος – χρήστης, άρα και υποκείμενο δεδομένων, θεωρείται η Alice. Η Alice λοιπόν ως υποκείμενο δεδομένων, DS, έχει το δικαίωμα να ορίσει και να τροποποιήσει τις προτιμήσεις της σχετικά με τη συλλογή και την επεξεργασία των προσωπικών της δεδομένων κατά τη διάρκεια της εκλογικής διαδικασίας, μέσα από την εισαγωγή του 5W model στο τρίτο βήμα της μεθοδολογίας PriS, (Σχήμα 15). Η συλλογή και η επεξεργασία των δεδομένων της Alice, αλλά και οποιουδήποτε χρήστη, είναι απαραίτητη για την αυθεντικοποίησή της/του όπως φαίνεται στο Σχήμα 13 όπου απεικονίζεται η διεργασία P7.

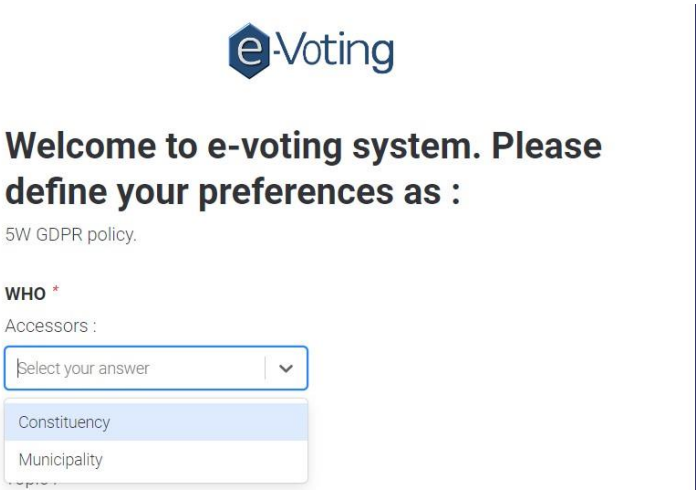
Η διαδικασία συγκατάθεσης της Alice για τη συλλογή και την επεξεργασία των προσωπικών της δεδομένων στην εκλογική διαδικασία ξεκινά με την εμφάνιση της διεπαφής που περιέχει τα ερωτήματα του 5W model, (Σχήμα 16).

Όπως φαίνεται και στη διεπαφή τα ερωτήματα που περιέχονται είναι πέντε : Who, What, When, Where και Why. Για καθένα από τα ερωτήματα, τα οποία είναι κλειστού τύπου, υπάρχουν συγκεκριμένες απαντήσεις τις οποίες η Alice μπορεί να επιλέξει για να δηλώσει τις προτιμήσεις της.



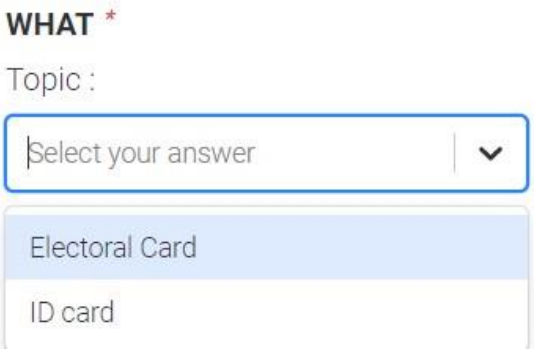
Σχήμα 16. 5W model για τη συναίνεση του DS (Alice)

Έτσι λοιπόν για το ερώτημα Who, η Alice μπορεί να επιλέξει ποιος μπορεί να έχει πρόσβαση στα δεδομένα της. Οι προτεινόμενες απαντήσεις για το ερώτημα αυτό είναι Constituency (Εκλογική Περιφέρεια) και Municipality (Δήμος), (Σχήμα 17).



Σχήμα 17. Επιλογή για το ποιος μπορεί να έχει πρόσβαση στα δεδομένα

Για το ερώτημα What η Alice μπορεί να επιλέξει ποια δεδομένα θα είναι διαθέσιμα για επεξεργασία. Στην περίπτωση αυτή ID card (Ταυτότητα) και Electoral card (Εκλογική κάρτα), (Σχήμα 18).

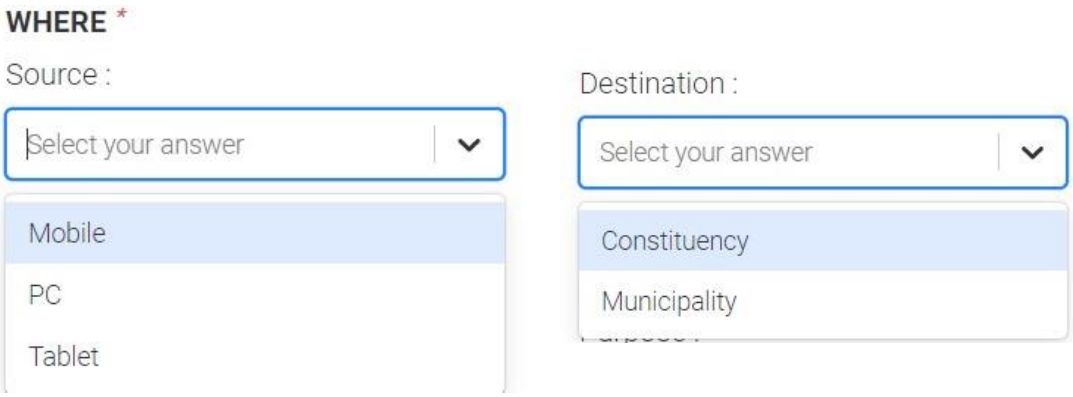


Σχήμα 18. Επιλογή για το ποια θα είναι τα δεδομένα που επιτρέπει το DS να επεξεργαστούν

Επίσης με την ερώτηση When η Alice επιλέγει το χρονικό διάστημα που επιτρέπει να είναι διαθέσιμα τα δεδομένα για επεξεργασία (1 year, 2 years, 4 years, 10 years), (Σχήμα 19).

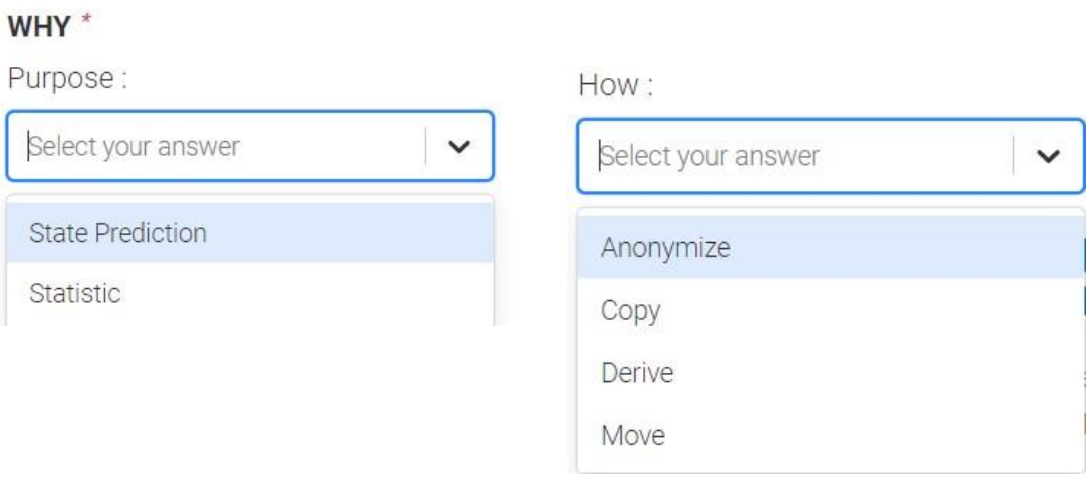
Σχήμα 19. Επιλογή για το χρονικό διάστημα που θα είναι διαθέσιμα τα δεδομένα

Με το ερώτημα Where το υποκείμενο δεδομένων, Alice, έχει το δικαίωμα να επιλέξει την πηγή λήψης των δεδομένων (source) που μπορεί να είναι το Mobile, το PC και το Tablet και τον χώρο αποθήκευσης - αποστολής αυτών (destination), δηλαδή Constituency (Εκλογική Περιφέρεια) και Municipality (Δήμος), (Σχήμα 20).



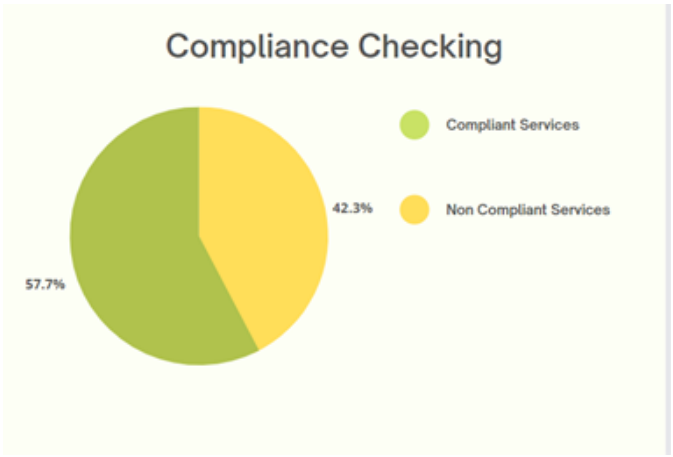
Σχήμα 20. Επιλογή της πηγής λήψης των δεδομένων και του χώρου αποθήκευσης

Τέλος με το ερώτημα Why η Alice έχει το δικαίωμα να επιλέξει τον λόγο (purpose) για τον οποίο διαθέτει τα δεδομένα που επέλεξε, State Prediction (Κατάσταση Πρόβλεψης) και Statistic (Στατιστικούς Λόγους), καθώς το είδος επεξεργασίας (how) που επιτρέπει για τα δεδομένα που διαθέτει : Anonymize, Copy, Derive, Move, (Σχήμα 21). Η Alice μπορεί να επιλέξει είτε μία είτε παραπάνω απαντήσεις για κάθε ερώτημα, εκτός του ερωτήματος When που θα πρέπει να επιλέξει μοναδική απάντηση.



Σχήμα 21. Επιλογή του σκοπού που διατίθενται τα δεδομένα και το είδος επεξεργασίας τους

Αφού η Alice συμπληρώσει τις προτιμήσεις της (δημιουργία πολιτικής συναίνεσης), και εφόσον έχει συλλέξει και διασφαλίσει τα δεδομένα της, ενδεικτικό παράδειγμα στο (Σχήμα 24), ο υπεύθυνος επεξεργασίας, πρέπει να αποδείξει ότι η συγκατάθεση της Alice εφαρμόζεται όπως επιθυμεί και έχει σχεδιαστεί τόσο για την Alice ως υποκείμενο δεδομένων, όσο και για τον υπεύθυνο προστασίας δεδομένων για λόγους διαφάνειας και συμμόρφωσης. Στη συνέχεια γίνεται έλεγχος της πολιτικής συναίνεσης που δημιούργησε η Alice με τον πίνακα ελέγχου που ικανοποιεί τις αρχές του GDPR. Στην περίπτωση που το ποσοστό που προκύπτει από τον έλεγχο που κάνει ο διαχειριστής αξιολόγησης και κινδύνων, συμφωνεί με την συνθήκη S : P U E U D -> L, η οποία ορίζεται από τον εκάστοτε φορέα και αντίστοιχα το πληροφοριακό σύστημα με βάση τις ανάγκες του, τότε η Alice μπορεί να αποθηκεύσει τις προτιμήσεις της και να ξεκινήσει η επεξεργασία των δεδομένων της σύμφωνα με αυτές, (Σχήμα 23). Στην αντίθετη περίπτωση, δηλαδή εάν το ποσοστό μετά τον έλεγχο που προκύπτει δεν είναι συμμορφωμένο με πολιτικές ελέγχου χρήσης, άρα και με την συνθήκη, η Alice θα έχει το δικαίωμα να μην προχωρήσει στην αποθήκευση των επιλογών της αλλά θα μπορεί να τις επεξεργαστεί ξανά. Η Alice, τέλος, θα μπορεί να ελέγξει μέσω γραφημάτων και ποσοστιαία τον σκοπό για τον οποίο επεξεργάζονται τα δεδομένα της, (Σχήμα 25), ενώ μέσα από φίλτρα θα μπορεί να δει τις επιλογές που έχει κάνει σχετικά με τα δεδομένα και τη διάθεσή τους, (Σχήμα 26) και (Σχήμα 27).

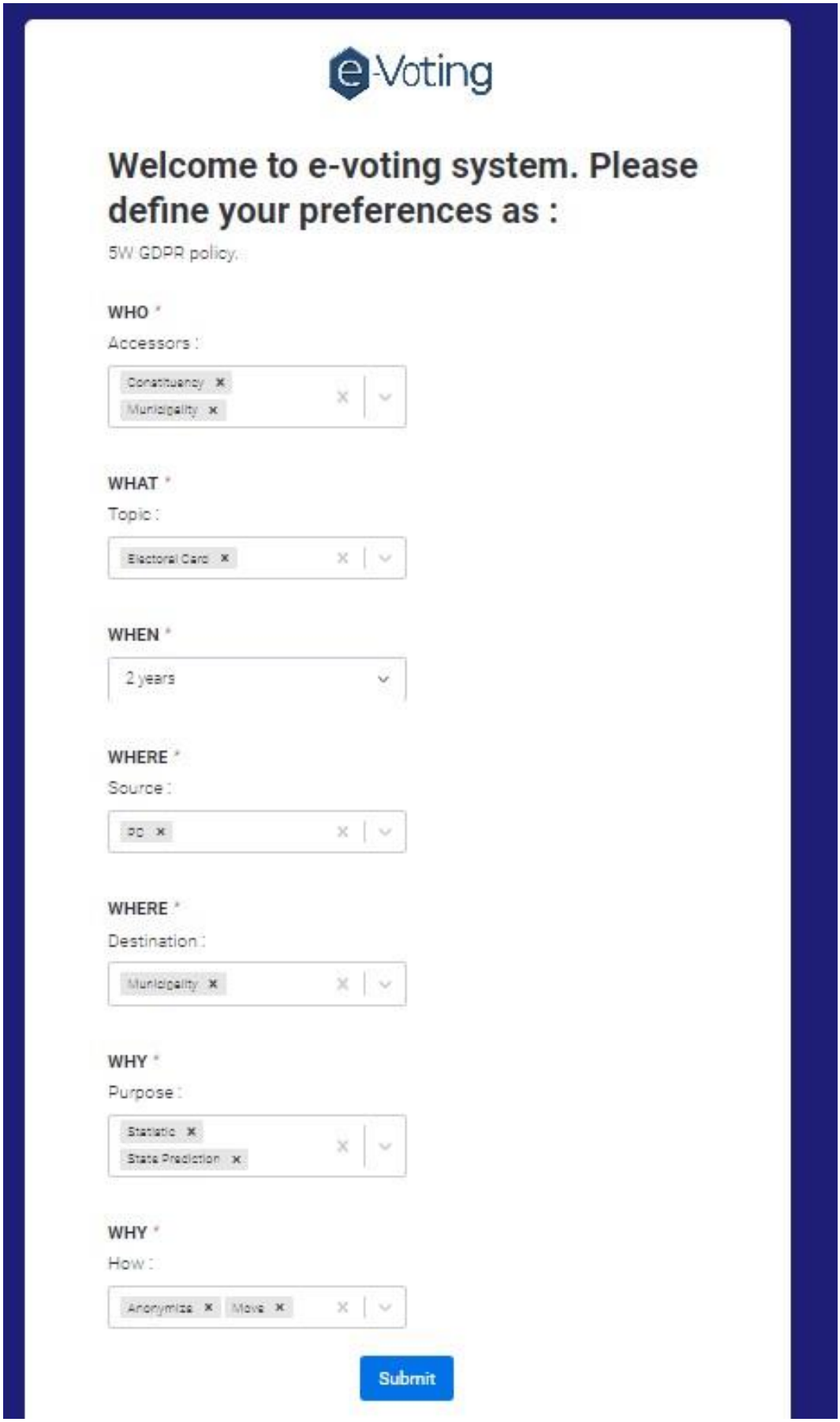


Σχήμα 22. Ποσοστό από τον έλεγχο συμμόρφωσης της πολιτικής συναίνεσης της Alice με τον GDPR

Παραπάνω στο γράφημα (Σχήμα 22) φαίνεται το ποσοστό μετά από έλεγχο με τη πολιτική συναίνεσης της Alice με τις συμβατές υπηρεσίες, δηλαδή τις προτιμήσεις της Alice καθώς και αυτές που δεν είναι συμβατές με τον GDPR. Όπως απεικονίζεται το ποσοστό συμβατότητας (57.7%) είναι μεγαλύτερο του ποσοστού που δεν συμβαδίζει (42.3%) επομένως η Alice θα μπορεί να αποθηκεύσει τις προτιμήσεις της σχετικά με τη διάθεση, την αποθήκευση και την επεξεργασία των δεδομένων της.

Εφόσον το ποσοστό συμβατότητας των επιλογών της Alice, μετά τον έλεγχο, είναι αυτό που υπερισχύει με βάση τον GDPR (Σχήμα 22), η Alice, άρα και οποιοσδήποτε χρήστης θα έχει τη δυνατότητα να αποθηκεύσει τις επιλογές του σε σχέση με τη διάθεση, την αποθήκευση, το είδος και την επεξεργασία των προσωπικών του δεδομένων. Όταν θα γίνεται η αποθήκευση αυτή μήνυμα οθόνης θα ενημερώνει τον χρήστη σχετικά με την αποθήκευση των επιλογών του (Σχήμα 23).

Σχήμα 23. Μήνυμα οθόνης μετά την αποθήκευση των επιλογών της Alice



Σχήμα 24. Ενδεικτική απάντηση της Alice

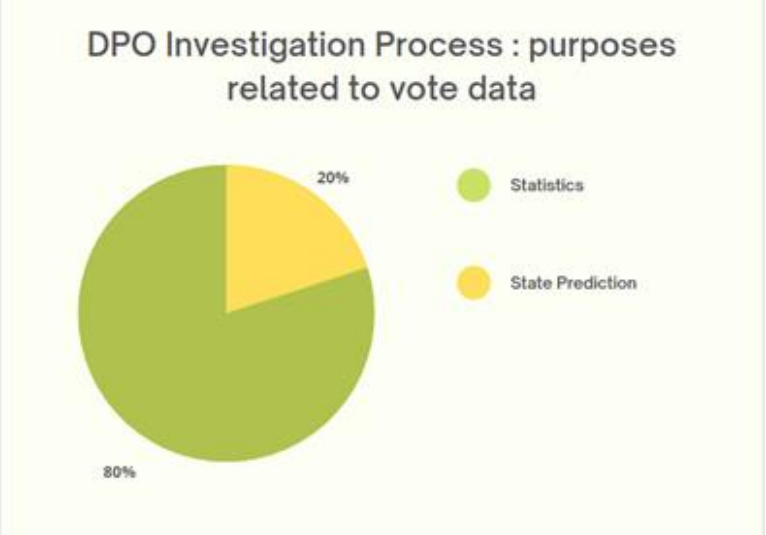
Παραπάνω δίνεται ένα παράδειγμα ενδεικτικών απαντήσεων της Alice. Όπως φαίνεται και από το στιγμιότυπο της διεπαφής (Σχήμα 24) η Alice έχει κάνει τις παρακάτω επιλογές :

- Για την ερώτηση Who, ποιος δηλαδή μπορεί να έχει πρόσβαση στα δεδομένα της, έχει εξουσιοδοτήσει άτομα που είναι αρμόδιοι της εκλογικής περιφέρειας (constituency) καθώς και τον Δήμο (municipality).
- Για την ερώτηση What, δηλαδή το είδος των δεδομένων που επιτρέπει να είναι διαθέσιμα η Alice έχει απαντήσει την εκλογική της κάρτα (electoral card).
- Στον χρόνο διάθεσης, ερώτηση When, που επιτρέπεται οποιαδήποτε επεξεργασία δεδομένων η Alice έχει επιλέξει τα δύο χρόνια (2 years).
- Για τον χώρο πηγής (Where source) από όπου μπορούν να είναι διαθέσιμα τα δεδομένα η Alice έχει επιλέξει τον υπολογιστή της (PC) ενώ για προορισμό και χώρο αποθήκευσης τον Δήμο (municipality).
- Τέλος για τον σκοπό που επιτρέπεται η διάθεση των προσωπικών δεδομένων της η Alice έχει επιλέξει και τον στατιστικό αλλά και την πρόβλεψη της κατάστασης της ψηφοφορίας, ενώ το είδος επεξεργασίας που επιτρέπει για τα προσωπικά της δεδομένα είναι η ανωνυμοποίησή τους αλλά η μετακίνηση τους.

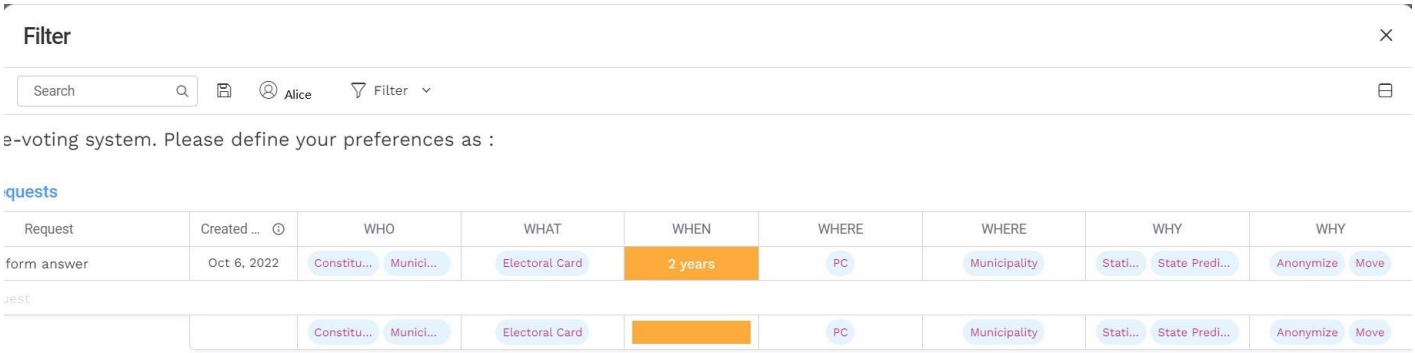
Από τα παραπάνω προκύπτει ότι οι προτιμήσεις της Alice περιγράφονται ως L{who: (constituency,municipality), what: (electoral card), when: (2 years), where.source: (PC), where.destination: (municipality), why.purpose: (statistic, state prediction), why.how: (anonymize,move)}. Επομένως στην περίπτωση που γίνει ένα αίτημα E1 για την επεξεργασία των δεδομένων της Alice, E1 για το οποίο ισχύει {who: (constituency), what: (electoral card), when: (1 year), where.source: (PC), where.destination: (municipality), why.purpose: (statistic, state prediction), why.how: (anonymize)}, τότε εφόσον ισχύει E1 $\subseteq$ L τότε το αίτημα εγκρίνεται και μπορεί να γίνει η επεξεργασία και η διάθεση των προσωπικών δεδομένων όπως έχει ορίσει η Alice με τις προτιμήσεις της. Στην αντίθετη περίπτωση όμως, δηλαδή σε ένα αίτημα E2 για το οποίο ισχύει who: (constituency), what: (electoral card), when: (4 years), where.source: (PC), where.destination: (municipality), why.purpose: (statistic, state prediction), why.how: (anonymize, move, derive, copy)}, δηλαδή E2 $\not\subseteq$ L, άρα δεν μπορεί να εγκριθεί το αίτημα για την χρήση και την επεξεργασία των δεδομένων βάσει των προτιμήσεων της Alice. Τα αιτήματα, E1 και E2 στην περίπτωση αυτή, γίνονται από την εκλογική περιφέρεια και το δήμο, δηλαδή από τα άτομα που έχει επιλέξει το υποκείμενο δεδομένων να έχουν δικαίωμα πρόσβασης στα δεδομένα του. Επομένως τα αιτήματα αυτά σχετικά με την επεξεργασία, χρήση και τη διάθεση των δεδομένων των υποκειμένων δεδομένων θα γίνεται από τους φορείς που έχει επιτρέψει και επιλέξει το υποκείμενο δεδομένων να έχουν δικαίωμα πρόσβασης.

Η Alice άρα και οποιοσδήποτε χρήστης, όπως προαναφέρθηκε, θα μπορεί να ελέγξει μέσω γραφημάτων και ποσοστιαία τον σκοπό για τον οποίο επεξεργάζονται τα δεδομένα της, (Σχήμα 25). Όπως φαίνεται στο συγκεκριμένο παράδειγμα το 20% είναι το ποσοστό για το οποίο γίνεται χρήση των δεδομένων της Alice, το οποίο αντιστοιχεί στην πρόβλεψη κατάστασης που θα

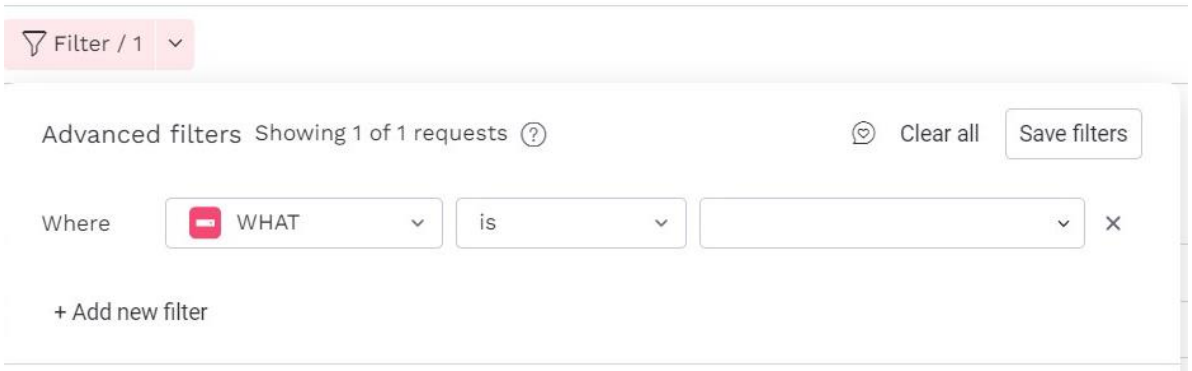
επικρατήσει σε μια ψηφοφορία, ενώ το 80% είναι το ποσοστό που αντιστοιχεί σε στατιστικούς σκοπούς χρήσης των δεδομένων.



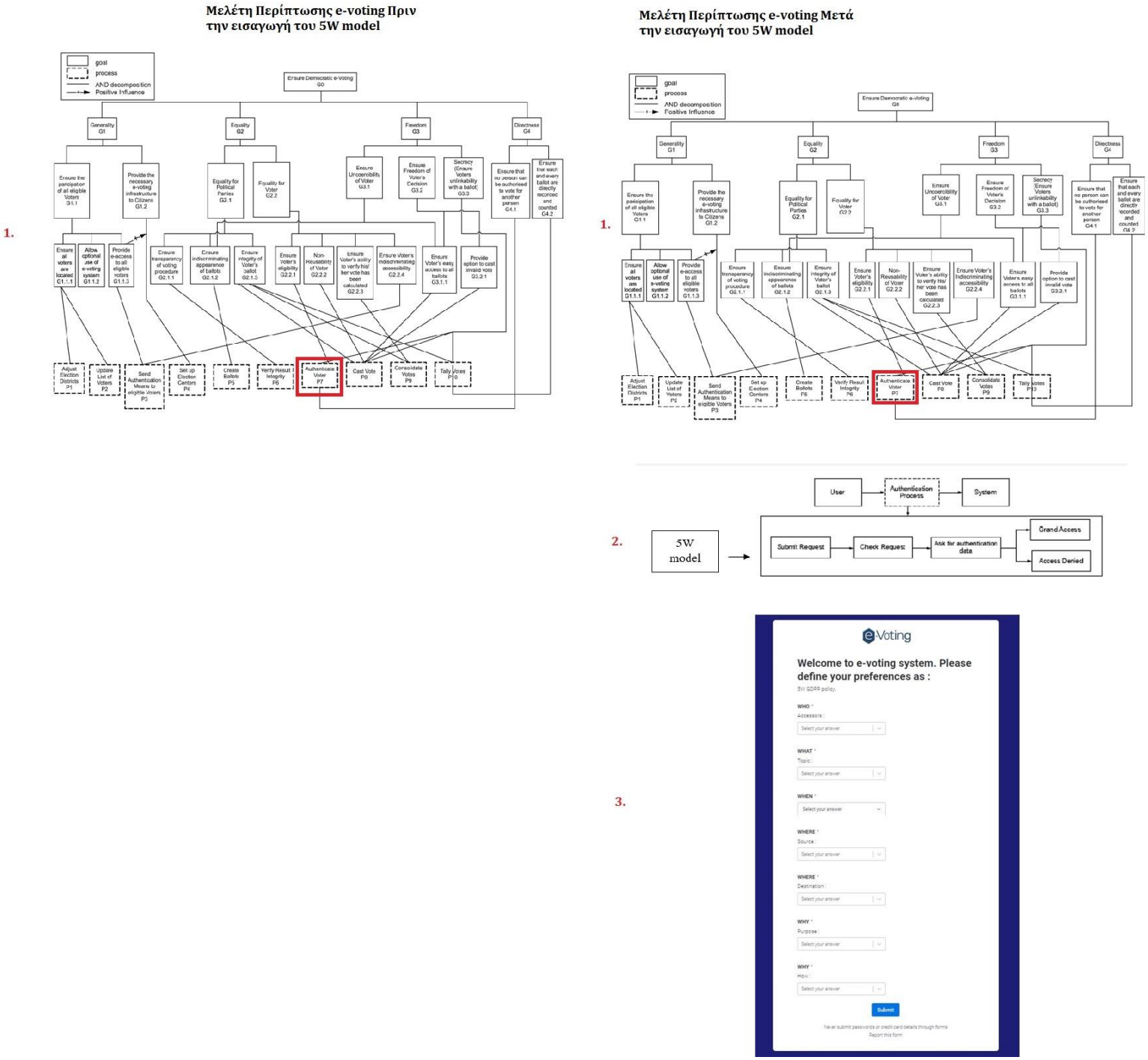
Σχήμα 25. Ποσοστιαία αναπαράσταση σκοπού χρήσης των δεδομένων της Alice



Σχήμα 26. Εμφάνιση επιλογών Alice



Σχήμα 27. Εμφάνιση επιλογών Alice βάσει του φίλτρου WHAT



Σχήμα 28. Μελέτη Περίπτωσης e-voting Πριν και Μετά την εισαγωγή του 5W model

4.3 Αποτελέσματα

Βασικός στόχος μέσα από την εισαγωγή του μοντέλου 5W ήταν η ενίσχυση της μεθοδολογίας Privacy Safeguard (PriS) βάσει του GDPR. Πιο αναλυτικά σκοπός ήταν η επίτευξη ορισμένων αρχών του GDPR μέσω του 5W model ώστε να γίνει η PriS GDPR compliant, δηλαδή να συμμορφώνεται με βάση τον GDPR. Οι αρχές του GDPR που επιτεύχθηκαν μέσω της εισαγωγής του 5W στο τρίτο βήμα της PriS είναι :

a) Η Νομιμότητα, Δικαιοσύνη, Διαφάνεια. Η συγκεκριμένη αρχή εκφράζει πως τα προσωπικά δεδομένα πρέπει να υποβάλλονται σε επεξεργασία νόμιμα, δίκαια και με διαφάνεια σε σχέση με το υποκείμενο δεδομένων. Αυτή η αρχή καλύπτεται μέσα από τη Πολιτική Συναίνεσης που προκύπτει από το 5W model.

b) Περιορισμός του Σκοπού. Στόχος μέσα από αυτή την αρχή είναι οι υπεύθυνοι επεξεργασίας να φροντίζουν για τον καθορισμό και την τεκμηρίωση του σκοπού που χρησιμοποιούνται τα δεδομένα καθώς και να παρέχουν την δυνατότητα ενημέρωσης των σκοπών και ελέγχου της συνοχής μεταξύ τους. Η αρχή αυτή ικανοποιείται μέσα από το ερώτημα 2 του 5W model, όπου προκύπτει από την επιλογή του DS, υποκείμενου δεδομένων, ο λόγος για τον οποίο θα υποβληθούν τα δεδομένα του σε επεξεργασία.

c) Περιορισμός Αποθήκευσης. Μέσω αυτής της αρχής εξετάζεται ποια δεδομένα θα αποθηκευτούν γιατί και για πόσο χρονικό διάστημα. Η ικανοποίηση της αρχής πραγματοποιείται μέσω του ερωτήματος 3 του μοντέλου, με την επιλογή του υποκειμένου δεδομένων για το που και το πως θα αποθηκεύονται τα δεδομένα του, καθώς και του ερωτήματος 5, με την επιλογή ξανά για το χρονικό διάστημα που θα είναι διαθέσιμα τα δεδομένα για επεξεργασία.

d) Υπευθυνότητα. Τέλος με αυτή την αρχή βεβαιώνεται πως υπάρχουν όλα τα κατάλληλα αρχεία τα οποία αποδεικνύουν την ενίσχυση της επεξεργασίας των δεδομένων με τον κανονισμό, συγκεκριμένα μέσα από τη Πολιτική Συναίνεσης που προκύπτει από το 5W που συμπληρώνει το υποκείμενο δεδομένων.

Σύμφωνα με τα παραπάνω φαίνεται πως ικανοποιούνται κάποιες από τις αρχές του GDPR, με την εισαγωγή του 5W model στο τρίτο βήμα της μεθοδολογίας PriS και συγκεκριμένα πριν από το μοτίβο ελέγχου ταυτότητας (Σχήμα 5). Επομένως εφόσον ικανοποιούνται ορισμένες από τις αρχές, η μεθοδολογία PriS με την εισαγωγή του 5W μπορεί να θεωρηθεί εν μέρει GDPR compliant, ότι ενισχύεται δηλαδή με τον GDPR (Πίνακας 2).

	Μεθοδολογία PriS πριν την εισαγωγή του 5W model	**Μεθοδολογία PriS μετά την εισαγωγή του 5W model**
Αρχές GDPR	1.Νομιμότητα, Δικαιοσύνη, Διαφάνεια	1.Νομιμότητα Δικαιοσύνη, Διαφάνεια ✓
	2.Περιορισμός Σκοπού	2.Περιορισμός Σκοπού ✓
	3.Ελαχιστοποίηση Δεδομένων	3.Ελαχιστοποίηση Δεδομένων
	4.Ακρίβεια	4.Ακρίβεια
	5.Περιορισμός Αποθήκευσης	5.Περιορισμός Αποθήκευσης ✓
	6.Ακεραιότητα, Εμπιστευτικότητα	6.Ακεραιότητα, Εμπιστευτικότητα
	7.Υπευθυνότητα	7.Υπευθυνότητα ✓

Πίνακας 2. Σύγκριση της μεθοδολογίας PriS σχετικά με την ενίσχυση με τις αρχές του GDPR πριν και ύστερα από την εισαγωγή του 5W model

5 *Συμπεράσματα και Σύνοψη*

Η παρούσα διπλωματική εργασία έχει ως βασικό στόχο την ενίσχυση μιας μεθοδολογίας PriS, με βάση τις διατάξεις του GDPR. Αιτία για τη συμμόρφωση της μεθοδολογίας με τον κανονισμό GDPR είναι η εισαγωγή νέων διατάξεων στον κανονισμό που σκοπό έχουν την προστασία των προσωπικών δεδομένων του ατόμου και τη συμμόρφωση κάθε οργανισμού και συστήματος με βάση αυτές από τα πρώτα στάδια της ανάπτυξης τους. Προκειμένου να εκπληρωθεί ο προαναφερθείς στόχος πραγματοποιήθηκε αρχικά ανάλυση των μεθοδολογιών που ανήκουν στην ίδια κατηγορία με τη PriS, ενώ έγινε και η περιγραφή της υπάρχουσας μεθοδολογίας. Επίσης παρουσιάστηκαν έργα καθώς και μια μεθοδολογία που συμμορφώνεται ήδη με τον κανονισμό GDPR. Έπειτα έγινε αναφορά στην έννοια του GDPR καθώς και στις οντότητες, αρχές και απαιτήσεις του ώστε να γίνει καλύτερη κατανόηση του μοντέλου που προτείνεται για την ενίσχυση της μεθοδολογίας με βάση τον κανονισμό.

Όπως παρατηρήθηκε από την ανάλυση των μεθοδολογιών που έγινε η μεθοδολογία PriS είναι αυτή που επιλέχθηκε για να γίνει GDPR compliant, να ενισχυθεί δηλαδή με βάση τον κανονισμό. Ο λόγος είναι αρχικά πως η PriS πέρα από το πρώιμο στάδιο σχεδίασης εντοπίζεται και στο στάδιο εφαρμογής ενός συστήματος, καλύπτοντας με αυτόν τον τρόπο το κενό μεταξύ του σχεδιασμού και της υλοποίησης ενός συστήματος και διευκολύνοντας την διαδικασία ανάπτυξης του εν λόγω συστήματος. Επίσης το γεγονός πως η συγκεκριμένη μεθοδολογία αποτελεί μια από τις πιο χρησιμοποιούμενες βάσει μιας επιστημονικής έρευνας αποτελεί το δεύτερο λόγο επιλογής της. Ο τρίτος λόγος που επιλέχθηκε η PriS μεθοδολογία, για να ενισχυθεί με τις αρχές του GDPR, είναι πως στο τρίτο βήμα της μεθοδολογίας προτείνονται έτοιμα πρότυπα διαδικασιών ιδιωτικότητας, τα οποία εμπεριέχουν δραστηριότητες και ροές δεδομένων που συνδέουν τις διεργασίες του υπό ανάπτυξη συστήματος, παρουσιάζοντας με τον τρόπο αυτό πως πρέπει να λειτουργεί μια επιχείρηση σε ένα τομέα. Τα πρότυπα αυτά λοιπόν, τα οποία περιγράφονται σε δύο επίπεδα το καθένα καταφέρνουν να απλοποιήσουν την ικανοποίηση των στόχων – αρχών του GDPR. Πράγματι όπως φαίνεται και από το παράδειγμα της ηλεκτρονικής ψηφοφορίας που χρησιμοποιείται στην εργασία, για τη καλύτερη κατανόηση της ενισχυμένης μεθοδολογίας, τα πρότυπα αποδεικνύονται πολύ χρήσιμα για την εφαρμογή του μοντέλου 5W που ενισχύει την PriS και την κάνει GDPR compliant.

Η ενίσχυση λοιπόν της PriS γίνεται με την εισαγωγή του 5W model στο τρίτο βήμα της μεθοδολογίας PriS και συγκεκριμένα πριν από το μοτίβο ελέγχου ταυτότητας. Το μοντέλο 5W μέσω των ερωτημάτων που θέτει δίνει τη δυνατότητα στο υποκείμενο των δεδομένων να δηλώσει τις προτιμήσεις του σχετικά με τη διάθεση, αποθήκευση και επεξεργασία των προσωπικών του δεδομένων, όπως φαίνεται και στο παράδειγμα της ηλεκτρονικής ψηφοφορίας, δημιουργώντας κατά αυτόν τον τρόπο μια πολιτική συναίνεσης σύμφωνη με τις επιλογές του υποκειμένου δεδομένων. Ως αποτέλεσμα επιτυγχάνεται η ενίσχυση της PriS με ορισμένες αρχές του GDPR. Η αρχή της νομιμότητας, του περιορισμού του σκοπού, του περιορισμού της αποθήκευσης αλλά και της υπευθυνότητας είναι αυτές που επιτυγχάνονται μέσω της εισαγωγής του 5W model στο τρίτο βήμα της μεθοδολογίας και όπως φαίνεται και από το παράδειγμα είναι πολύ σημαντικό να επιτυγχάνεται η ύπαρξή τους τόσο για τα υποκείμενα δεδομένων, δηλαδή τους χρήστες των συστημάτων ή τους πελάτες ενός οργανισμού, όσο και για τα ίδια τα συστήματα και τους οργανισμούς.

5.1 Προτάσεις για Μελλοντική Εργασία

Η εργασία αυτής της μελέτης περιλαμβάνει την ενίσχυση της μεθοδολογίας PriS με ορισμένες διατάξεις και αρχές του GDPR. Η ενίσχυση του τρίτου βήματος της μεθοδολογίας PriS που έγινε με την εισαγωγή του μοντέλου 5W κατάφερε να κάνει την μεθοδολογία, σε ένα μέρος της, GDPR compliant ικανοποιώντας τις αρχές της νομιμότητας, του περιορισμού της αποθήκευσης και του σκοπού καθώς και της υπευθυνότητας. Για το λόγο αυτό, θα ήταν ενδιαφέρον να διεξαχθεί μια άλλη μελέτη με σκοπό την ικανοποίηση των αρχών της εμπιστευτικότητας, της ακρίβειας και της ελαχιστοποίησης των δεδομένων με σκοπό να γίνει εξολοκλήρου η PriS μεθοδολογία ενισχυμένη με τον GDPR.

Επιπλέον θα ήταν ενδιαφέρον να διεξαχθεί μελέτη και για τον ορισμό του κατάλληλου threshold ανάλογα με τον φορέα, το είδος των δεδομένων καθώς και για το είδος των πολιτών που εφαρμόζεται κάθε φορά η ενισχυμένη μεθοδολογία PriS.

Τέλος η εφαρμογή του μοντέλου 5W σε μια διαφορετική μελέτη περίπτωσης, που αναπτύσσεται με τη μεθοδολογία PriS, θα ήταν ιδιαίτερα χρήσιμη, ώστε να γίνει έλεγχος εάν το μοντέλο μπορεί να ικανοποιήσει τις αρχές του GDPR και ανταποκριθεί με τον ίδιο τρόπο σε συστήματα που έχουν διαφορικές ανάγκες, δεδομένα και άτομα με τα οποία αλληλεπιδρούν

Βιβλιογραφία

[1] Kalloniatis C, Belsis P, Gritzalis S (2011), "A soft computing approach for privacy requirements engineering: The PriS framework", Applied Soft Computing, 2011 - Elsevier

[2] Kalloniatis C, Kavakli E and Kontellis, E, "Pris Tool: A Case Tool For Privacy Oriented Requirements Engineering" (2009). MCIS 2009 Proceedings. 71

[3] E. Kavakli, S. Gritzalis and C. Kalloniatis, "Protecting privacy in system design: the electronic voting case", Transforming Government: People, Process and Policy, 2007.

[4] V. Diamantopoulou, N. Argyropoulos, C. Kalloniatis and S. Gritzalis, "Supporting the design of privacy-aware business processes via privacy process patterns", in 11th International Conference on Research Challenges in Information Science (RCIS), IEEE, 2017, pp. 187-198.

[5] M. Pavlidis, S. Islam - CAiSE Forum, 2011 - researchgate.net "SecTro: A CASE Tool for Modelling Security in Requirements Engineering using Secure Tropos"

[6] H. Mouratidis, P. Giorgini International Journal of Software Engineering and Knowledge Engineering,Vol. 17, No. 02, pp. 285-309 (2007), "SECURE TROPOS: A SECURITY-ORIENTED EXTENSION OF THE TROPOS METHODOLOGY", 2007 - World Scientific

[7] ED. Canedo, IN. Bandeira, ATS. Calazans, PHT. Costa, ECR. Cançado & R. Bonifácio (2022), "Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners",2022 – Springer

[8] AI Antón, JB Earp - E-commerce security and privacy, "Strategies for developing policies and requirements for secure and private electronic commerce" 2001 – Springer

[9] A. Pattakou, AG. Mavroeidi, V. Diamantopoulou, C. Kalloniatis, S. Gritzalis (2018), "Towards the Design of Usable Privacy by Design Methodologies", 2018 - ieeexplore.ieee.org

[10] C. Kalloniatis, E. Kavakli, S. Gritzalis (2009), "Methods for designing privacy aware information systems: A review", 2009 - ieeexplore.ieee.org

[11] A. Ekdahl, L. Nyman (2019), "A Methodology to Validate Compliance to the GDPR" - 2019 - gupea.ub.gu.se

[12] Το έργο Defend (2021), https://www.defendproject.eu/

[13] Ο ανασχεδιασμός της επιχειρηματικής διαδικασίας και η λειτουργική εργαλειοθήκη για το έργο συμμόρφωσης με το GDPR (2021), https://www.bpr4gdpr.eu/

[14] Η πλατφόρμα Smooth (2021), https://smoothplatform.eu/

[15] Το έργο PDP4E (2021), https://www.pdp4e-project.eu/

[16] Το έργο PAPAYA (2021), https://www.papaya-project.eu/

[17] Το έργο PoSeID-on (2021), https://www.poseidon-h2020.eu/

[18] E (2020), General Data Protection Regulation - (GDPR), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[19] Pham P.l. The applicability of GDPR to the Internet of Things J Data Prot Priv , 2 (3) (2019), pp. 254 - 263 – Scopus

[20] N. Notario, A. Crespo, Y-S. Martín, J. M. d. Alamo, D. l. Métayer, T. Antignac, A. Kung, I. Kroener and D. Wright, "PRIPARE: integrating privacy best practices into a privacy engineering methodology", in IEEE Security and Privacy Workshops, IEEE, 2015

[21] Kalloniatis C, Kavakli E, Gritzalis S (2007), "Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process", 2007 - ieeexplore.ieee.org

[22] https://online.visual-paradigm.com/

[23] https://www.workforms.com/templates

[24]https://el.wikipedia.org/wiki/%CE%99%CE%B4%CE%B9%CF%89%CF%84%CE%B9%CE%BA%CF%8C_%CE%B1%CF%80%CF%8C%CF%81%CF%81%CE%B7%CF%84%CE%BF

[25] A. F. Westin. Privacy and Freedom. Washington and Lee Law Review, 1968

[26] S. D. Warren and L. D. Brandeis. The Right to Privacy. Harvard Law Review, 4(5):193–220, 1890

[27] A. Pfitzmann and M. Hansen. A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservabil ity, Pseudonymity, and Identity Management – 2010

[28] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο: Οδηγία 95/46/ΕΚ για την προστασία των ατόμων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας των δεδομένων αυτών - Οκτώβριος 1995

Υπεύθυνη Δήλωση Συγγραφέα

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον.