ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Προστασία Προσωπικών Δεδομένων σε Έξυπνα Περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Γεώργιος Β. Λιουδάκης

Αθήνα, Ιούλιος 2008

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Προστασία Προσωπικών Δεδομένων σε Έξυπνα Περιβάλλοντα

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Γεώργιος Β. Λιουδάκης

Συμβουλευτική Επιτροπή : Δήμητρα–Θεοδώρα Ι. Κακλαμάνη
Ιάκωβος Στ. Βενιέρης
Εμμανουήλ Ν. Πρωτονοτάριος

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή τη 17η Ιουλίου 2008.

.....	.....	.....
Δ.-Θ. Κακλαμάνη	Ι. Βενιέρης	Ν. Ουζούνογλου
Αναπλ. Καθηγήτρια Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.
.....	.....	.....
Μ. Θεολόγου	Γ. Στασινόπουλος	Κ. Κοντογιάννης
Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αναπλ. Καθηγητής Ε.Μ.Π.

.....
Χ. Δουληγέρης
Καθηγητής Παν. Πειραιώς

Αθήνα, Ιούλιος 2008

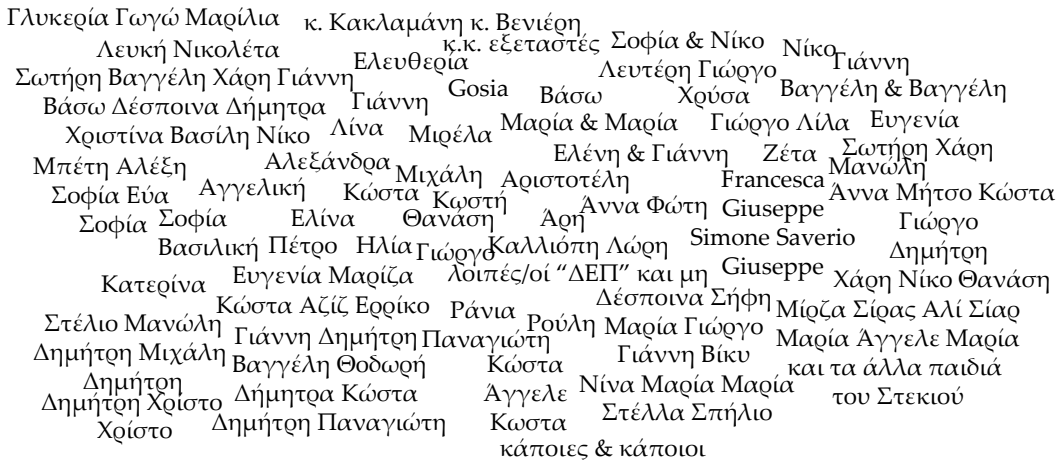
.....
Γεώργιος Β. Λιουδάκης

Διδάκτωρ Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Σε εκείνο το μάγκα,

που είχα την τύχη να είμαι γιος του.

Αντί Προλόγου



Για τα μικρά, για τα μεγάλα. Για κάθε συνενοχή.

Σας ευχαριστώ.

Περίληψη

Η πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνιών έχει δώσει ώθηση στην παροχή προηγμένων υπηρεσιών στους χρήστες. Ωστόσο, η παροχή των υπηρεσιών αυτών απαιτεί τη μετάδοση και επεξεργασία προσωπικών δεδομένων και, ως εκ τούτου, εγκυμονεί κινδύνους για την προσωπική ζωή. Η παρούσα Διατριβή έχει σαν αντικείμενο την προστασία των προσωπικών δεδομένων κατά την παροχή υπηρεσιών, μέσω της σχεδίασης και ανάπτυξης ενός πρωτότυπου συστήματος το οποίο παρεμβάλλεται μεταξύ χρηστών και παρόχων υπηρεσιών και μεριμνά για την ορθή χρήση των προσωπικών δεδομένων.

Στόχος του προτεινόμενου συστήματος είναι η εφαρμογή των απαιτήσεων της Νομοθεσίας αναφορικά με τη συλλογή και χρήση προσωπικών δεδομένων κατά την παροχή υπηρεσιών. Για το λόγο αυτό, πραγματοποιείται μία επισκόπηση του Νομικού Πλαισίου αναφορικά με την προστασία των προσωπικών δεδομένων, το οποίο αποτελεί την πηγή των απαιτήσεων για τη σχεδίαση του προτεινόμενου συστήματος.

Ως βάση της λειτουργίας του συστήματος, σχεδιάστηκε ένα σημασιολογικό πλαίσιο, βασισμένο σε μία οντολογία, το οποίο μοντελοποιεί τις θεμελιώδεις αρχές αναφορικά με την προστασία των προσωπικών δεδομένων, όπως αυτές πηγάζουν από τη Νομοθεσία. Η οντολογία αποτελεί ουσιαστικά το φορμαλιστικό ορισμό των σχετικών κανόνων πρόσβασης και εκτέλεσης συμπληρωματικών ενεργειών, ούτως ώστε οι αρχές της Νομοθεσίας να μπορούν να λειτουργήσουν ως είσοδος σε συστήματα λογισμικού και να ληφθούν υπόψη σε κάθε απόφαση.

Το προτεινόμενο σύστημα χρησιμοποιεί διάφορα πρωτότυπα μοντέλα και εργαλεία τα οποία προδιαγράφηκαν στο πλαίσιο της Διατριβής, όπως είναι η Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας, η οποία χρησιμοποιείται για το φορμαλιστικό προσδιορισμό των απαιτήσεων των χρηστών αναφορικά με την προστασία της ιδιωτικότητάς τους, και η Γλώσσα Προδιαγραφής Ροής Εργασιών Ιδιωτικότητας, η οποία χρησιμοποιείται για τον κατά περίπτωση προσδιορισμό των ενεργειών που πρέπει να πραγματοποιηθούν στο πλαίσιο της παροχής μίας υπηρεσίας, προκειμένου αυτή να είναι συμβατή τόσο με τις απαιτήσεις του Νομικού Πλαισίου όσο και με τις προτιμήσεις ιδιωτικότητας των χρηστών.

Για την εφαρμογή των ανωτέρω, προδιαγράφηκε ένα κατανεμημένο σύστημα λογισμικού το οποίο παρεμβάλλεται μεταξύ των χρηστών και των παρόχων υπηρεσιών και ελέγχεται από κάποια Αρχή Ιδιωτικότητας, μεριμνώντας για την εφαρμογή των νομικών κανόνων αναφορικά με την προστασία των προσωπικών δεδομένων αλλά και των αντίστοιχων προτιμήσεων των χρηστών. Το σύστημα τεκμηριώνεται επιπλέον με παραδείγματα της λειτουργίας του καθώς και με την αξιολόγησή του βάσει αναγνωρισμένων κριτηρίων.

Λέξεις κλειδιά: Ιδιωτικότητα, έξυπνα περιβάλλοντα, προστασία προσωπικών δεδομένων, Νομοθεσία προστασίας προσωπικών δεδομένων, έλεγχος πρόσβασης, σημασιολογικό μοντέλο, οντολογία, σύστημα μεσισμικού, κριτήρια ιδιωτικότητας.

Abstract

The advances of the Information and Communication Technologies have boosted the provision of advanced services to the users. However, the provision of these services demands the transmission and processing of personal data, thus, putting personal life into danger. The present Thesis targets the protection of personal data, through the design and development of a novel system that mediates between users and service providers and caters for the fair use of the personal data.

The goal of the proposed system is the enforcement of the Legal requirements concerning the collection and use of personal data in the context of services' provision. In that respect, a survey of the relevant Legal framework is performed, since this framework constitutes the source of the requirements for the design of the proposed system.

As the basis of the system's operation, a semantic model, based on an ontology, has been designed, which models the fundamental principles stemming form the Legislation regarding personal data protection. The ontology constitutes in essence the formal definition of the related rules that govern access control and the execution of the complementary tasks, so that to be feasible for the Legal provisions to constitute input to software systems and be taken under consideration in every decision.

The proposed system makes use of several innovative models and tools that have been specified in the context of the Thesis, such as the Privacy Rules Description Language, which is used for the formal specification of the users' preferences regarding the protection of their privacy, as well as the Privacy Workflow Specification Language, which is used for the ad hoc specification of the actions that must be executed in the context of a service's provision, in order for the service to be compliant with both the provisions of the Legal framework and the privacy preferences of the users.

For the enforcement of the concepts described above, a distributed software system has been specified, which mediates between the users and the service providers and is controlled by some Privacy Authority. The system caters for the enforcement of the legal rules regarding personal data protection, as well as of the corresponding users' preferences. The system is further documented with use cases of its operation, as well as its evaluation by means of well-appreciated criteria.

Keywords: Privacy, smart environments, personal data protection, personal data protection legislation, access control, semantic model, ontology, middleware system, privacy criteria.

Πίνακας Περιεχομένων

Αντί Προλόγου **7**

Περίληψη **9**

Abstract **11**

Πίνακας Περιεχομένων **13**

Πίνακας Σχημάτων **17**

Πίνακας Πινάκων **18**

1 Εισαγωγή **19**

1.1 Έξυπνα Περιβάλλοντα 19

1.2 Ιδιωτικότητα 22

1.3 Ορισμοί 23

1.4 Διάρθρωση της Διατριβής 24

2 Νομικό και Κανονιστικό Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων **27**

2.1 Εισαγωγή 27

2.2 Βασικές Αρχές Προστασίας Προσωπικών Δεδομένων 29

2.3 Ευρωπαϊκό Δίκαιο 31

2.3.1 Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ 31

2.3.2 Οι Ευρωπαϊκές Οδηγίες 2002/58/ΕΚ και 2006/24/ΕΚ 35

2.4 Ελληνικό Εθνικό Δίκαιο 39

3 Τεχνολογίες για την Προστασία των Προσωπικών Δεδομένων **43**

3.1 Τεχνολογίες για τη Διαχείριση της Ιδιωτικότητας 43

3.1.1 Η Πλατφόρμα για τις Προτιμήσεις Ιδιωτικότητας (P3P) 45

3.1.2 Ιπποκρατικές Βάσεις Δεδομένων 57

3.1.3 Έλεγχος Πρόσβασης Βάσει Σκοπού 62

3.1.4 Η Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML) ... 66

3.1.5 Η Γλώσσα Επιχειρησιακής Εξουσιοδότησης για Ιδιωτικότητα (EPAL) 72

3.2 Τεχνολογίες για την Προστασία της Ιδιωτικότητας 73

3.2.1 Κρυπτογραφικά Συστήματα 74

3.2.2 Συστήματα Ανωνυμίας και Ψευδωνυμίας 78

4 Γενική Περιγραφή της Προτεινόμενης Λύσης 81
4.1 Νομικές και Κανονιστικές Απαιτήσεις 81
4.2 Βασικές Αρχές της Προτεινόμενης Λύσης 84
4.3 Κατηγορίες Προσωπικών Δεδομένων 86
4.4 Τύποι Προσωπικών Δεδομένων, Υπηρεσιών και Ρόλων 87
4.5 Γενική Περιγραφή της Προτεινόμενης Αρχιτεκτονικής 89
4.6 Υπηρεσίες, Σύνοδοι και Συναλλαγές Ιδιωτικότητας 96
4.7 Πλαίσιο Επικοινωνίας 98
4.8 Κέλυφος Ιδιωτικότητας 100
5 Οντολογία Ιδιωτικότητας 103
5.1 Εισαγωγή 103
5.2 Σημασιολογικό Μοντέλο Πληροφοριών 105
5.3 Κανόνες Οντολογίας Ιδιωτικότητας 108
5.4 Βοηθητικές Κλάσεις 115
5.5 Σύνοψη Ιδιοτήτων OWL της Οντολογίας Ιδιωτικότητας 117
6 Οι Γλώσσες Περιγραφής Κανόνων Ιδιωτικότητας και Ροής Εργασιών Ιδιωτικότητας 119
6.1 Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας 119
6.2 Γλώσσα Περιγραφής Ροής Εργασιών Ιδιωτικότητας 126
7 Αρχιτεκτονική Μεσισμικού 133
7.1 Πληρεξούσιος Κόμβος Ιδιωτικότητας 133
7.1.1 Διαχειριστής Επικοινωνίας 133
7.1.2 Αποθετήριο Κανονισμών 135
7.1.3 Αποθετήριο Προσωπικών Δεδομένων 136
7.1.4 Μηχανή Πολιτικών 138
7.1.5 Διαχειριστής Συνόδων 139
7.1.6 Ενσωματωμένες Λειτουργικές Μονάδες 139
7.2 Διαχειριστής Ιδιωτικότητας Χρήστη 142
7.3 Κόμβος Υποδομής Ιδιωτικότητας 143
8 Παραδείγματα Χρήσης 145
8.1 Παράδειγμα Χρήσης Ενεργών Προσωπικών Δεδομένων 145
8.2 Παράδειγμα Χρήσης Ημιενεργών Προσωπικών Δεδομένων 151

8.3 Παράδειγμα Χρήσης Παθητικών Προσωπικών Δεδομένων 152
9 Αξιολόγηση της Προτεινόμενης Λύσης 157
9.1 Αξιολόγηση σε Σχέση με τις Νομικές και Κανονιστικές Απαιτήσεις.. 157
9.1.1 Νομιμότητα της Επεξεργασίας των Δεδομένων..... 157
9.1.2 Σκοπός της Επεξεργασίας των Δεδομένων 157
9.1.3 Αναγκαιότητα, Καταλληλότητα και Αναλογικότητα των Δεδομένων 158
9.1.4 Ποιότητα των Δεδομένων 158
9.1.5 Ταυτοποιήσιμα Δεδομένα 159
9.1.6 Πληροφόρηση των Υποκειμένων των Δεδομένων – Συγκατάθεση και Δικαιώματα Πρόσβασης των Υποκειμένων των Δεδομένων..... 159
9.1.7 Δεδομένα Θέσης και Κίνησης – Ειδικές Κατηγορίες Δεδομένων 160
9.1.8 Περιορισμός της Πρόσβασης 160
9.1.9 Ασφάλεια Δεδομένων και Εμπιστευτικότητα 161
9.1.10 Αποθήκευση Δεδομένων 161
9.1.11 Ειδοποιήσεις και λοιπές Αρμοδιότητες / Εξουσιοδοτήσεις των Αρμοδίων Αρχών..... 161
9.1.12 Εποπτεία και Επιβολή Προστίμων..... 162
9.1.13 Νόμιμη Παρακολούθηση και Συλλογή Δεδομένων..... 162
9.2 Αξιολόγηση με Βάση τα Κριτήρια του Ανεξάρτητου Κέντρου για την Προστασία της Ιδιωτικότητας 163
10 Συμπεράσματα – Μελλοντική Εργασία 173
Βιβλιογραφία 177
Παράρτημα Α′ – Δημοσιεύσεις 191
Διεθνή Περιοδικά 191
Πρακτικά Διεθνών Συνεδρίων 191

Πίνακας Σχημάτων

Σχήμα 1: Παράδειγμα Πολιτικής Ιδιωτικότητας Πλατφόρμας P3P. 51
Σχήμα 2: Παράδειγμα Προτιμήσεων Ιδιωτικότητας Χρήστη σε APPEL. 55
Σχήμα 3: Σχήμα Βάσης Δεδομένων 58
Σχήμα 4: Σχήμα Μεταδεδομένων Ιδιωτικότητας 58
Σχήμα 5: Πίνακας Πολιτικές-Ιδιωτικότητας 59
Σχήμα 6: Πίνακας Εξουσιοδοτήσεις-Ιδιωτικότητας 59
Σχήμα 7: Επισκόπηση Αρχιτεκτονικής Υλοποίησης Ιπποκρατικών Βάσεων Δεδομένων 60
Σχήμα 8: Παράδειγμα Μετασχηματισμού Ερωτήματος 62
Σχήμα 9: Δέντρο Σκοπών 63
Σχήμα 10: Διάγραμμα ροής πληροφορίας XACML 69
Σχήμα 11: Μοντέλο Πολιτικής Γλώσσας XACML 70
Σχήμα 12: Παράδειγμα Πολιτικής XACML 71
Σχήμα 13: Μοντέλο Πολιτικής Γλώσσας EPAL 73
Σχήμα 14: Μηχανισμός Λήψης Αποφάσεων του Πληρεξούσιου Κόμβου Ιδιωτικότητας. 92
Σχήμα 15: Αρχιτεκτονική Μεσισμικού Προστασίας Προσωπικών Δεδομένων. ... 93
Σχήμα 16: Κανάλια Επικοινωνίας 99
Σχήμα 17: Οντολογία Ιδιωτικότητας – Υπογράφος Προσωπικών Δεδομένων ... 107
Σχήμα 18: Οντολογία Ιδιωτικότητας – Υπογράφος Υπηρεσιών 108
Σχήμα 19: Οντολογία Ιδιωτικότητας – Παράδειγμα Κανόνα Δικαιώματος Πρόσβασης 113
Σχήμα 20: Οντολογία Ιδιωτικότητας – Παράδειγμα Κανόνα Δικαιώματος Εκτέλεσης 114
Σχήμα 21: Παράδειγμα Μετασχηματισμού Δεδομένων 116
Σχήμα 22: Πληρεξούσιος Κόμβος Ιδιωτικότητας 134
Σχήμα 23: Σχήμα Βάσης Προσωπικών Δεδομένων 137
Σχήμα 24: Οντολογία Ιδιωτικότητας – Υπηρεσία `JazzBarFinder` 146

Σχήμα 25: Κέλυφος Ιδιωτικότητας 147
Σχήμα 26: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `JazzBarFinder` 148
Σχήμα 27: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `Payment` 150
Σχήμα 28: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `RFIDElectronicTollCollection` 152
Σχήμα 29: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `ScrambledSurveillanceVideoCapture` 153
Σχήμα 30: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `ClearSurveillanceVideoCapture` 154

Πίνακας Πινάκων

Πίνακας 1: Σύνοψη Ιδιοτήτων OWL της Οντολογίας Ιδιωτικότητας 117
Πίνακας 2: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 1 – "Θεμελιώδης Τεχνικός Σχεδιασμός Προϊόντων Πληροφορικής" 165
Πίνακας 3: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 2 – "Νομιμότητα της Επεξεργασίας Δεδομένων" 166
Πίνακας 4: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 3 – "Τεχνικά – Οργανωτικά Μέτρα: Συμπληρωματικά Μέτρα για την Προστασία του Υποκειμένου των Δεδομένων" 168
Πίνακας 5: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 4 – "Δικαιώματα του Υποκειμένου των Δεδομένων" 170

1 Εισαγωγή

Η εποχή μας χαρακτηρίζεται από τεχνολογικές εξελίξεις οι οποίες μεταμορφώνουν δραστικά τον τρόπο που ζούμε και εργαζόμαστε. Η πρόοδος των Τεχνολογιών Πληροφορίας και Επικοινωνίας έχει δώσει την ώθηση για την ανάπτυξη και παροχή προηγμένων ηλεκτρονικών υπηρεσιών και τη δημιουργία έξυπνων περιβαλλόντων, με συνέπεια τα όρια μεταξύ του πραγματικού και του ψηφιακού κόσμου των ηλεκτρονικών υπολογιστών να γίνονται πολλές φορές δυσδιάκριτα.

Ωστόσο, η αξιοσημείωτη αυτή πρόοδος η οποία γενικά βελτιώνει την ποιότητα ζωής του σύγχρονου ανθρώπου, εγκυμονεί σοβαρούς κινδύνους για την ιδιωτική ζωή των πολιτών. Περισσότερο από έναν αιώνα από τη δημοσίευση της πρώτης πραγματείας αναφορικά με το γεγονός ότι η ιδιωτική ζωή των πολιτών τίθεται σε κίνδυνο από την τεχνολογική πρόοδο [1], ποτέ άλλοτε στην ιστορία οι πολίτες δεν ήταν τόσο ανήσυχοι σχετικά με το θέμα αυτό [2].

1.1 Έξυπνα Περιβάλλοντα

Τα έξυπνα περιβάλλοντα χαρακτηρίζονται από εκείνο που συνήθως αναφέρεται σαν "πανταχού παρούσα υπολογιστική" (ubiquitous computing). Ο όρος αυτός προέρχεται από ένα άρθρο – ορόσημο [3] του Mark Weiser το οποίο δημοσιεύτηκε πριν από περισσότερο από 15 χρόνια και αναφερόταν σε έναν ιδεατό κόσμο όπου τα υπολογιστικά στοιχεία βρίσκονται παντού, λειτουργούν στο παρασκήνιο με τρόπο διακριτικό και σχεδόν αόρατο, απαλλάσσοντας τον άνθρωπο από ένα μεγάλο μέρος των κουραστικών και τετριμμένων διαδικασιών, τόσο στην προσωπική όσο και στην επαγγελματική του ζωή.

Το 1999, η Συμβουλευτική Ομάδα για τις Τεχνολογίες της Κοινωνίας της Πληροφορίας (Information Society Technology Advisory Group – ISTAG) [4] της Ευρωπαϊκής Ένωσης χρησιμοποίησε τον όρο "περιβάλλουσα ευφυΐα" (ambient intelligence) με παρόμοιο τρόπο. Ο όρος χρησιμοποιήθηκε προκειμένου να περιγράψει έναν κόσμο όπου οι άνθρωποι θα περιβάλλονται από έξυπνες και διαισθητικές διεπαφές, ενσωματωμένες σε καθημερινά αντικείμενα και από ένα περιβάλλον το οποίο

θα αναγνωρίζει και θα ανταποκρίνεται αναλόγως στην παρουσία των ανθρώπων με τρόπο διακριτικό και αόρατο [5].

Η πανταχού παρούσα υπολογιστική και η περιβάλλουσα ευφυΐα σε συνδυασμό με τη ραγδαία ανάπτυξη και διάδοση των Διαδικτυακών υπηρεσιών και επικοινωνιών και των άλλων μορφών ηλεκτρονικής επικοινωνίας ορίζουν αυτό που στην παρούσα Διατριβή ονομάζεται "έξυπνα περιβάλλοντα".

Τα έξυπνα περιβάλλοντα, πέρα από τις προφανείς θετικές πλευρές τους, δημιουργούν σοβαρούς κινδύνους για την προσωπική ζωή. Αυτό οφείλεται κυρίως στους παρακάτω λόγους:

- *Η κλίμακα της συλλογής προσωπικών δεδομένων αυξάνεται ραγδαία*. Πράγματι, όσο τα υπολογιστικά συστήματα καθίστανται "αόρατα" και ενσωματώνονται στο περιβάλλον, η συλλογή όλο και περισσότερων δεδομένων λαμβάνει χώρα, δεδομένων μάλιστα που στο παρελθόν δεν ήταν δυνατό να αποτελέσουν αντικείμενο συλλογής. Χαρακτηριστικό παράδειγμα αποτελεί το ίχνος της γεωγραφικής θέσης σε συνεχή και πραγματικό χρόνο.

- Επιπλέον, οι προηγμένες υπηρεσίες που προσφέρονται κυρίως μέσω του Διαδικτύου, απαιτούν εγγενώς μεγάλη ποσότητα προσωπικών δεδομένων. Για παράδειγμα, η αγορά ενός προϊόντος σε κάποιο κατάστημα δεν απαιτεί – γενικά – την παροχή προσωπικών πληροφοριών. Αντίθετα, η αγορά του ίδιου προϊόντος από κάποιο Διαδικτυακό κατάστημα απαιτεί την παροχή δεδομένων προκειμένου να πραγματοποιηθεί π.χ. η χρέωση.

- *Ο τρόπος συλλογής προσωπικών δεδομένων είναι διαφορετικός*. Στα έξυπνα περιβάλλοντα, όχι μόνο τα υπολογιστικά συστήματα βρίσκονται παντού αλλά διαθέτουν προηγμένες δυνατότητες συλλογής προσωπικών δεδομένων. Χαρακτηριστικά παραδείγματα αποτελούν οι "έξυπνες" κάμερες παρακολούθησης [6] και οι διάφοροι αισθητήρες, όπως είναι οι συσκευές ραδιοσυχνότητας για προσδιορισμό ταυτότητας (Radio Frequency Identification – RFID) [7]. Σε πολλές μάλιστα περιπτώσεις, τα προσωπικά δεδομένα συλλέγονται χωρίς τη σχετική γνώση του ατόμου το οποίο αφορούν.

- *Συλλέγονται νέοι τύποι προσωπικών δεδομένων*. Η εξέλιξη της τεχνολογίας έχει δημιουργήσει τις προοπτικές για τη συλλογή δεδομένων που μέχρι πριν από λίγα

χρόνια περιοριζόταν από την ικανότητες της ανθρώπινης όρασης και ακοής. Η καταγραφή του ήχου από μεγάλη απόσταση, η παρακολούθηση των επικοινωνιών, ή η παρακολούθηση ολόκληρων γεωγραφικών περιοχών μέσω δορυφόρων που καταγράφουν εικόνες υψηλής ανάλυσης αποτελούν μερικά μόνο χαρακτηριστικά παραδείγματα. Οι προηγμένες υπηρεσίες συλλέγουν από καταναλωτικές συνήθειες και μέχρι ιατρικά δεδομένα και πολιτισμικές ή κοινωνικές συνήθειες και απόψεις. Ακόμα και τα συναισθήματα ενός ανθρώπου θα είναι δυνατό να καταγραφούν στο κοντινό μέλλον με εξαιρετική ακρίβεια μέσω ειδικών συστημάτων.

- *Η ευκολία πρόσβασης στα δεδομένα και οι πρωτοφανείς δυνατότητες που αυτή προσφέρει.* Στα έξυπνα περιβάλλοντα, τα προσωπικά δεδομένα όχι μόνο συλλέγονται αλλά και αποθηκεύονται για μεγάλα χρονικά διαστήματα, δυνητικά για πάντα. Επιπλέον, καθίσταται εύκολη η μετάδοσή τους αλλά και ο συνδυασμός τους προκειμένου να εξαχθούν συμπεράσματα. Τεράστια ποσότητα προσωπικών πληροφοριών εδράζει σε βάσεις δεδομένων σε ολόκληρο τον κόσμο. Μάλιστα, σε αρκετές περιπτώσεις η ίδια οντότητα συλλέγει ετερόκλητα προσωπικά δεδομένα τα οποία συλλέγονται από εντελώς διαφορετικές υπηρεσίες, όπως είναι το φαινόμενο της εταιρείας "google", η οποία έχει εξαγοράσει ένα μεγάλο αριθμό εταιρειών που αφορούν σε παροχή προηγμένων υπηρεσιών που συλλέγουν και αποθηκεύουν προσωπικά δεδομένα [8]. Καθίσταται λοιπόν σαφές ότι οι δυνατότητες εξαγωγής συμπερασμάτων που αφορούν στην προσωπική ζωή μέσω συνδυασμού ακόμα και εντελώς ετερόκλητων δεδομένων καθίσταται εύκολη, ιδιαιτέρως με τη χρήση τεχνολογιών όπως είναι οι Αποθήκες Δεδομένων (Data Warehouses) [9], η Εξόρυξη Δεδομένων (Data Mining) [10] και η Αναλυτική Επεξεργασία Δεδομένων (On Line Analytical Processing – OLAP) [11].

1.2 Ιδιωτικότητα

Η ιδιωτικότητα[1] χαρακτηρίζεται σαν ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, όπως έχει αναγνωριστεί από το Άρθρο 12 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα [12] των Ηνωμένων Εθνών. Αποτελεί αναμφίβολα ένα από τα πιο σημαντικά ζητήματα αναφορικά με τα δικαιώματα του ανθρώπου που επηρεάζονται από την εξελισσόμενη "Εποχή της Πληροφορίας".

Είναι μάλλον δύσκολο να δοθεί ένας ενιαίος ορισμός για την ιδιωτικότητα, καθώς αποτελεί σε μεγάλο βαθμό υποκειμενική έννοια ενώ διαφορετικές επιστήμες την εξετάζουν από διαφορετικές οπτικές γωνίες· στο πλαίσιο της παρούσας Διατριβής θα υιοθετηθεί ο ορισμός που διατυπώθηκε από τον Alan Westin το 1967 [13]:

Ιδιωτικότητα είναι η αξίωση των ατόμων, ομάδων και οργανισμών να καθορίζουν το χρόνο, τον τρόπο και την έκταση αναφορικά με τη συλλογή και επεξεργασία των προσωπικών τους δεδομένων.

Πολύ συχνά, η προστασία της ιδιωτικότητας θεωρείται – λανθασμένα – συνώνυμη της ασφάλειας των πληροφοριακών συστημάτων και των ηλεκτρονικών επικοινωνιών. Η αλήθεια είναι ότι οι μηχανισμοί ασφάλειας, όπως η χρήση κρυπτογραφίας και ο έλεγχος πρόσβασης (access control) σε συστήματα και δεδομένα, αποτελούν τη στοιχειώδη βάση για την προστασία της ιδιωτικότητας, χωρίς ωστόσο να αποτελούν πανάκεια. Για παράδειγμα, οι μηχανισμοί ασφάλειας δεν είναι σε θέση να αποτρέψουν μία επιχείρηση από το να πουλήσει τα προσωπικά δεδομένα των πελατών της σε κάποια άλλη επιχείρηση που θα προβεί σε κατάχρησή τους. Επιπλέον, μερικές φορές οι έννοιες της ασφάλειας και της ιδιωτικότητας είναι αντιθετικές. Ενδεικτικά, η αυτόματη παρακολούθηση των συμβάντων σε ένα σύστημα για σκοπούς διατήρησης της ασφάλειας (π.χ. για την ανίχνευση εισβολών) μπορεί να αποτελέσει απειλή για την ιδιωτικότητα των χρηστών του, όπως καταδεικνύεται στο άρθρο [14]. Το γεγονός αυτό είναι γνωστό σαν το *παράδοξο ασφάλειας – ιδιωτικότητας* [15].

Καθίσταται λοιπόν σαφές ότι οι μηχανισμοί της ασφάλειας των πληροφοριακών και επικοινωνιακών συστημάτων δεν επαρκούν για την προστασία τη ιδιωτικότητας. Για

[1] Ο όρος "Ιδιωτικότητα" αποτελεί μετάφραση του διεθνούς όρου "Privacy", σύμφωνα με τον Ελληνικό Οργανισμό Τυποποιήσεως.

το σκοπό αυτό, τα τελευταία χρόνια η ανάπτυξη νέων τεχνολογικών μηχανισμών αποτελεί ένα αναπτυσσόμενο ερευνητικό πεδίο. Ένας τέτοιος τεχνολογικός μηχανισμός αποτελεί το αντικείμενο της παρούσας Διατριβής. Η προτεινόμενη λύση βασίζεται στην αρχή της διαμεσολάβησης μεταξύ του χρήστη και του έξυπνου περιβάλλοντος ενός ολοκληρωμένου συστήματος, το οποίο μεριμνά για την απρόσκοπτη εφαρμογή της Νομοθεσίας περί προστασίας των προσωπικών δεδομένων.

1.3 Ορισμοί

Στη συνέχεια του κειμένου χρησιμοποιούνται διάφορες έννοιες, των οποίων το νόημα μπορεί να προκαλέσει σύγχυση. Για το λόγο αυτό, παρατίθενται οι παρακάτω ορισμοί:

- **Προσωπικά Δεδομένα** ή **Δεδομένα Προσωπικού Χαρακτήρα**: κάθε πληροφορία που αναφέρεται σε φυσικό πρόσωπο του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί "το πρόσωπο στο οποίο αναφέρονται τα δεδομένα"· ως πρόσωπο του οποίου η ταυτότητα μπορεί να εξακριβωθεί λογίζεται το πρόσωπο εκείνο που μπορεί να προσδιοριστεί, άμεσα ή έμμεσα, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός ή περισσοτέρων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από φυσική, βιολογική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική άποψη.
- **Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα** ή **Επεξεργασία**: κάθε εργασία ή σειρά εργασιών που πραγματοποιούνται με ή χωρίς τη βοήθεια αυτοματοποιημένων διαδικασιών και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώρηση, η οργάνωση, η αποθήκευση, η προσαρμογή ή η τροποποίηση, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η ανακοίνωση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η εναρμόνιση ή ο συνδυασμός, καθώς και το κλείδωμα, η διαγραφή ή η καταστροφή.
- **Αρχείο Δεδομένων Προσωπικού Χαρακτήρα** ή **Αρχείο**: κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα προσιτών με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση.

- **Υποκείμενο Δεδομένων**[1] ή **Χρήστης**: το πρόσωπο, φυσικό ή νομικό, στο οποίο αναφέρονται τα δεδομένα.
- **Πάροχος Υπηρεσίας** ή **Υπεύθυνος της Επεξεργασίας**: το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή οποιοσδήποτε άλλος φορέας που μόνος ή από κοινού με άλλους καθορίζει τους στόχους και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

1.4 Διάρθρωση της Διατριβής

Η Διατριβή αποτελείται από συνολικά δέκα Κεφάλαια. Πέρα από το παρόν εισαγωγικό Κεφάλαιο, το περιεχόμενο των υπολοίπων Κεφαλαίων συνοψίζεται ως ακολούθως.

Στο δεύτερο Κεφάλαιο συνοψίζεται το Νομικό και Κανονιστικό Πλαίσιο που διέπει την προστασία της ιδιωτικότητας και που ουσιαστικά αντανακλά τις απαιτήσεις που πρέπει να ικανοποιεί ένα τεχνολογικό σύστημα που στοχεύει στην προστασία των προσωπικών δεδομένων σε έξυπνα περιβάλλοντα. Έπειτα από μία σύντομη εισαγωγή και ιστορική αναδρομή, περιγράφονται οι βασικές αρχές προστασίας των προσωπικών δεδομένων όπως έχουν διαμορφωθεί και γίνει διεθνώς αποδεκτές. Στη συνέχεια, παρατίθεται η συνοπτική αλλά περιεκτική περιγραφή του Ευρωπαϊκού Δικαίου, το οποίο αποτελεί τη βάση για το Ελληνικό Εθνικό Δίκαιο, το οποίο επισκοπείται στο τέλος του Κεφαλαίου.

Στο τρίτο Κεφάλαιο παρουσιάζεται μία αναδρομή στις ερευνητικές προσπάθειες που πραγματοποιήθηκαν μέχρι σήμερα όσον αφορά την προστασία των προσωπικών δεδομένων. Καλύπτει τόσο τις λεγόμενες τεχνολογίες για την προστασία της ιδιωτικότητας όσο και αυτές για τη διαχείρισή της. Οι πρώτες αφορούν μεθόδους που εφαρμόζονται κυρίως από το χρήστη προκειμένου να προστατεύσει ενεργά (π.χ. με χρήση κρυπτογραφίας) ή να αποκρύψει (π.χ. με χρήση υπηρεσιών ψευδωνυμίας ή ανωνυμίας) τα προσωπικά του δεδομένα, κυρίως κατά το στάδιο της μετάδοσής τους. Οι δεύτερες αναφέρονται στην εφαρμογή μηχανισμών για τον έλεγχο της πρόσβασης σε προσωπικά δεδομένα και τη χρήση τεχνικών μέσων και συστημάτων που βασίζονται σε

[1] Ο όρος "Υποκείμενο Δεδομένων" αποτελεί απόδοση στην Ελληνική γλώσσα του όρου "Data Subject", ο οποίος χρησιμοποιείται στην Ευρωπαϊκή Οδηγία 95/46/ΕΚ [22].

πολιτικές και κανόνες για την εφαρμογή των απαιτήσεων της σχετικής Νομοθεσίας και των ίδιων των χρηστών, κυρίως σε επιχειρησιακά περιβάλλοντα.

Το τέταρτο Κεφάλαιο αποτελεί την εισαγωγή στην προτεινόμενη λύση, παρέχοντας μία γενική περιγραφή της. Πραγματοποιεί μία κωδικοποίηση / ανάλυση των Νομικών και Κανονιστικών απαιτήσεων όπως αυτές εξηγήθηκαν στο δεύτερο Κεφάλαιο, προκειμένου αυτές να χρησιμοποιηθούν για την προδιαγραφή της λύσης. Επιπλέον, εξηγεί βασικές έννοιες όπως είναι η Σύνοδος και η Συναλλαγή Ιδιωτικότητας και προβαίνει στην κατηγοριοποίηση των προσωπικών δεδομένων σε ενεργά, ημιενεργά και παθητικά, βάσει διαφόρων χαρακτηριστικών τους. Τέλος, δίνει μία συνοπτική αλλά συνολική περιγραφή της προτεινόμενης λύσης, με έμφαση στις ιδέες της Οντολογίας Ιδιωτικότητας και του Πληρεξούσιου Κόμβου Ιδιωτικότητας.

Το πέμπτο Κεφάλαιο παρουσιάζει αναλυτικά την Οντολογία Ιδιωτικότητας που αποτελεί μία από τις βασικές συνεισφορές της διατριβής. Η Οντολογία Ιδιωτικότητας αποτελεί το σημασιολογικό μοντέλο του συστήματος, καθώς και τη γνωσιακή βάση για την εξαγωγή συμπερασμάτων και τη λήψη αποφάσεων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας, αναφορικά με τη συλλογή, επεξεργασία και περαιτέρω μετάδοση των προσωπικών δεδομένων. Περιέχει, μεταξύ άλλων, σημασιολογικές αναφορές στους διάφορους τύπους προσωπικών δεδομένων, υπηρεσιών και ρόλων των οντοτήτων που συμμετέχουν στην αλυσίδα (χρήστης, πάροχος υπηρεσίας, Αρχή Ιδιωτικότητας) και τους κανόνες που διέπουν την παροχή των υπηρεσιών.

Στο έκτο Κεφάλαιο, παρουσιάζονται δύο πρωτότυπες γλώσσες, η προδιαγραφή των οποίων πραγματοποιήθηκε στο πλαίσιο της διατριβής. Η Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας χρησιμοποιείται για τον προσδιορισμό των προτιμήσεων των υποκειμένων των δεδομένων αναφορικά με την ιδιωτικότητα. Επιπλέον, στη γλώσσα αυτή εκφράζονται στην τελική τους μορφή οι κανόνες οι οποίοι προκύπτουν από την Οντολογία Ιδιωτικότητας, προκειμένου συνδυαστούν με τις προτιμήσεις του χρήστη. Από την άλλη πλευρά, η Γλώσσα Περιγραφής Ροής Εργασιών Ιδιωτικότητας χρησιμοποιείται από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας προκειμένου να περιγραφούν και συγχρονιστούν οι ενέργειες οι οποίες θα λάβουν χώρα για τη διασφάλιση της ιδιωτικότητας στο πλαίσιο της εξυπηρέτησης κάποιου αιτήματος για παροχή υπηρεσίας. Η εκάστοτε ροή εργασιών προκύπτει έπειτα από την επεξεργασία τόσο των κανόνων

που περιέχονται στην Οντολογία Ιδιωτικότητας, όσο και των προτιμήσεων του χρήστη, εφόσον υπάρχουν.

Το έβδομο Κεφάλαιο παρουσιάζει την αρχιτεκτονική μεσισμικού η οποία σχεδιάστηκε και υλοποιήθηκε στο πλαίσιο της διατριβής. Πέρα από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας, περιγράφονται τα υπόλοιπα βασικά δομικά στοιχεία της αρχιτεκτονικής, δηλαδή ο Διαχειριστής Ιδιωτικότητας Χρήστη και ο Κόμβος Υποδομής Ιδιωτικότητας. Αναλύεται η λειτουργία του κάθε δομικού στοιχείου, καθώς και ο τρόπος της μεταξύ τους διαλειτουργικότητας προκειμένου να επιτευχθεί ο στόχος της προστασίας των προσωπικών δεδομένων και να εφαρμοστούν οι απαιτήσεις της σχετικής Νομοθεσίας.

Το όγδοο Κεφάλαιο παρουσιάζει αντιπροσωπευτικά παραδείγματα χρήσης της προτεινόμενης λύσης. Τα παραδείγματα επιδεικνύουν τον τρόπο λειτουργίας της λύσης και αφορούν και τις τρεις κατηγορίες προσωπικών δεδομένων, όπως αυτές προσδιορίστηκαν στο πλαίσιο της διατριβής, δηλαδή τα ενεργά, ημιενεργά και παθητικά προσωπικά δεδομένα.

Στο ένατο Κεφάλαιο αξιολογείται η προτεινόμενη λύση. Η αξιολόγηση πραγματοποιείται με βάση δύο άξονες. Από τη μία πλευρά, χρησιμοποιούνται τα διεθνώς αναγνωρισμένα κριτήρια που έχουν προσδιοριστεί από το Ανεξάρτητο Κέντρο για την Προστασία της Ιδιωτικότητας, το οποίο αποτελεί την Αρχή Ιδιωτικότητας του Schleswig-Holstein της Γερμανίας. Από την άλλη πλευρά, αναλύεται ο τρόπος με τον οποίο η προτεινόμενη λύση ανταποκρίνεται στις απαιτήσεις της Νομοθεσίας σχετικά με την προστασία προσωπικών δεδομένων, όπως αυτές αναλύθηκαν στα προηγούμενα Κεφάλαια.

Τέλος, το δέκατο Κεφάλαιο αποτελεί τον επίλογο της διατριβής, υπογραμμίζοντας κάποια βασικά συμπεράσματα, αλλά και σκιαγραφόντας τις βασικές κατευθύνσεις που θα αποτελέσουν τους άξονες της συνέχισης της έρευνας έχοντας ως βάση τη λύση που προτείνεται από τη Διατριβή.

2 Νομικό και Κανονιστικό Πλαίσιο για την Προστασία των Προσωπικών Δεδομένων

Το Κεφάλαιο αυτό παρουσιάζει συνοπτικά τη Νομοθεσία που διέπει την προστασία των προσωπικών δεδομένων, η οποία ουσιαστικά αντανακλά τις απαιτήσεις που πρέπει να ικανοποιεί ένα τεχνολογικό σύστημα που στοχεύει στην προστασία των προσωπικών δεδομένων σε έξυπνα περιβάλλοντα.

Έπειτα από μία σύντομη εισαγωγή και ιστορική αναδρομή, περιγράφονται οι βασικές αρχές προστασίας των προσωπικών δεδομένων όπως έχουν διαμορφωθεί και γίνει αποδεκτές. Στη συνέχεια, παρατίθεται η συνοπτική αλλά περιεκτική περιγραφή του Ευρωπαϊκού Δικαίου, το οποίο αποτελεί τη βάση για το Ελληνικό Εθνικό Δίκαιο, το οποίο επισκοπείται στην Ενότητα 2.4.

2.1 Εισαγωγή

Όπως προαναφέρθηκε, η πρώτη πραγματεία αναφορικά με το γεγονός ότι η ιδιωτική ζωή των πολιτών τίθεται σε κίνδυνο από την τεχνολογική πρόοδο [1] δημοσιεύτηκε ήδη το 19ο αιώνα, όταν δύο νομικοί στην πολιτεία της Βοστόνης των Ηνωμένων Πολιτειών επισήμαναν τον κίνδυνο για την ιδιωτική ζωή που εγκυμονούσε η – σχετικά νέα τότε – τεχνολογία της λήψης φωτογραφιών. Τα Ηνωμένα Έθνη αναγνώρισαν την ιδιωτικότητα σαν ένα από τα θεμελιώδη δικαιώματα του ανθρώπου, με το Άρθρο 12 της Οικουμενικής Διακήρυξης για τα Ανθρώπινα Δικαιώματα [12]. Το ενδιαφέρον για την προστασία των προσωπικών δεδομένων αυξήθηκε ιδιαίτερα τις δεκαετίες του 1960 και 1970, με την έλευση των τεχνολογιών της πληροφορίας και τις προφανείς δυνατότητες παρακολούθησης και αρχειοθέτησης που αυτές έφερναν.

Το 1970, υιοθετήθηκε ο πρώτος σύγχρονος νόμος προστασίας προσωπικών δεδομένων από το Hesse, ένα από τα "κρατίδια" (Länder) της πρώην Δυτικής Γερμανίας. Ο νόμος αυτός [16] αποτέλεσε τη βάση για άλλες περιοχές της Δυτικής Γερμανίας, την ομοσπονδιακή της κυβέρνηση αλλά και χώρες πέρα από τη Γερμανία, όπως τη Σουηδία που το 1973 υιοθέτησε τον πρώτο παγκοσμίως εθνικό νόμο προστασίας προσωπικών

δεδομένων. Αρκετές Ευρωπαϊκές χώρες υιοθέτησαν παρόμοιους νόμους πριν από το τέλος της δεκαετίας του 1970.

Στις Ηνωμένες Πολιτείες της Αμερικής, το Κογκρέσο υιοθέτησε το "Νόμο περί Ιδιωτικότητας" (Privacy Act) το 1974 [17], εκτιμώντας ότι τα πολύπλοκα υπολογιστικά συστήματα δημιουργούσαν απειλές για την προσωπική ιδιωτικότητα. Ο νόμος αυτός δέχτηκε αρκετές τροποποιήσεις μέχρι σήμερα με σημαντικότερες εκείνη του 1988 [18], η οποία λάμβανε υπόψη τις τεχνολογικές εξελίξεις στο χώρο της πληροφορικής, καθώς και εκείνη του 2001, στο πλαίσιο του "Πατριωτικού Νόμου" (Patriot Act) [19], ο οποίος ενεργοποιεί τη δυνατότητα για αυξημένη παρακολούθηση προσώπων υπερβαίνοντας κατά πολύ τις μέχρι τότε επιτρεπόμενες εισβολές στην προσωπική ιδιωτικότητα. Στο πλαίσιο αυτό ορίζονται ενδυναμωμένες διαδικασίες παρακολούθησης και γίνονται πιο χαλαροί οι κανόνες για την άρση του απορρήτου των τηλεπικοινωνιών και τη συλλογή προσωπικών δεδομένων.

Στις αρχές της δεκαετίας του 1980, ο Οργανισμός Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development – OECD) [20], στον οποίο συμμετέχει και η Ελλάδα, εξέδωσε τις *Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων* (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) [21], οι οποίες αποτέλεσαν ορόσημο αναφορικά με την προστασία των προσωπικών δεδομένων. Οι κατευθυντήριες αυτές οδηγίες είχαν σαν σκοπό να βοηθήσουν στον εναρμονισμό των εθνικών νομοθεσιών των κρατών – μελών του Οργανισμού γύρω από μία κοινή βάση για την προστασία των προσωπικών δεδομένων. Παρόλο που οι κατευθυντήριες οδηγίες είχαν στη φύση τους συμβουλευτικό και όχι νομοθετικό χαρακτήρα, επέδρασαν σε πολύ μεγάλο βαθμό στη σχετική νομοθεσία που ακολούθησε σε παγκόσμιο επίπεδο, ενώ οι βασικές αρχές για την προστασία των προσωπικών δεδομένων που όρισαν αποτέλεσαν τη βάση των σύγχρονων νομοθετικών και κανονιστικών πλαισίων και παραμένουν διαχρονικές. Για το λόγο αυτό αναφέρονται σε αυτό το κεφάλαιο, ενώ οι βασικές αρχές παρουσιάζονται στην Ενότητα 2.2.

Τον Ιούλιο του 1990, η Ευρωπαϊκή Κοινότητα εξέδωσε την πρώτη πρόχειρη πρόταση για μία οδηγία περί της προστασίας των προσωπικών δεδομένων. Μετά από χρόνια διαβουλεύσεων, η τελική Οδηγία 95/46/ΕΚ [22] "για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την

ελεύθερη διακίνηση των δεδομένων αυτών" υιοθετήθηκε από το Ευρωπαϊκό Συμβούλιο το 1995 και τέθηκε σε εφαρμογή στα κράτη – μέλη από τον Οκτώβρη του 1998. Η Οδηγία αυτή αποτέλεσε ορόσημο και αποτέλεσε τη βάση για τη νομοθεσία όχι μόνο των κρατών – μελών της Ευρωπαϊκής Κοινότητας αλλά σε παγκόσμιο επίπεδο, αποτελώντας σήμερα το πιο επιδραστικό νομικό κείμενο περί της προστασίας των προσωπικών δεδομένων στον πλανήτη.

Το Δεκέμβριο του 1997, η Ευρωπαϊκή Κοινότητα εξέδωσε την Οδηγία 97/66/ΕΚ [23], περί της "επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα", με σκοπό τη διασφάλιση του απορρήτου των τηλεπικοινωνιών των πολιτών Η Οδηγία αυτή ουσιαστικά εξειδίκευσε και συμπλήρωσε την Οδηγία 95/46/ΕΚ σε ό,τι αφορά τον τηλεπικοινωνιακό τομέα και γρήγορα αντικαταστάθηκε από την Οδηγία 2002/58/ΕΚ [24] καθώς δεν ήταν σε θέση να διευθετήσει ζητήματα που αφορούσαν τις τελευταίες τεχνολογικές εξελίξεις. Η Οδηγία 2002/58/ΕΚ καλύπτει όλο το φάσμα των ηλεκτρονικών επικοινωνιακών και των υπηρεσιών που παρέχονται μέσω αυτών. Πολύ πρόσφατα εκδόθηκε μία νέα Οδηγία, η Οδηγία 2006/24/ΕΚ [25], η οποία τροποποιεί την Οδηγία 2002/58/ΕΚ σε ό,τι αφορά τη διατήρηση ορισμένων δεδομένων που παράγονται ή υφίστανται επεξεργασία από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, ώστε να διασφαλιστεί ότι τα δεδομένα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων.

2.2 Βασικές Αρχές Προστασίας Προσωπικών Δεδομένων

Οι βασικές αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων όπως ορίστηκαν από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης στις *Κατευθυντήριες Οδηγίες για την Προστασία της Ιδιωτικότητας και τη Διασυνοριακή Ροή των Προσωπικών Δεδομένων* [21] και που, περισσότερο ή λιγότερο, αντανακλώνται σε όλους τους σύγχρονους σχετικούς νόμους των δημοκρατικών κρατών παγκοσμίως, είναι οι παρακάτω:

- **Αρχή του περιορισμού της συλλογής** (collection limitation principle): Θα πρέπει να υπάρχουν όρια στη συλλογή προσωπικών δεδομένων, η συλλογή τους θα

πρέπει να πραγματοποιείται με χρήση θεμιτών και σύννομων μέσων και – όπου είναι δυνατό – με τη συναίνεση ή την ενημέρωση του χρήστη.

- **Αρχή της ποιότητας των δεδομένων** (data quality principle): Τα προσωπικά δεδομένα θα πρέπει να είναι σχετικά με το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν ενώ – στο βαθμό που είναι απαραίτητο για το σκοπό αυτό – θα πρέπει να είναι πλήρη, ακριβή και ενημερωμένα.
- **Αρχή προσδιορισμού του σκοπού** (purpose specification principle): Ο σκοπός για τον οποίο συλλέγονται προσωπικά δεδομένα θα πρέπει να προσδιορίζεται το αργότερο κατά τη χρονική στιγμή της συλλογής τους, ενώ η συνακόλουθη χρήση τους θα πρέπει να περιορίζεται στην εκπλήρωση του σκοπού αυτού ή κάποιου πλήρως συμβατού σκοπού.
- **Αρχή περιορισμού της χρήσης** (use limitation principle): Τα προσωπικά δεδομένα δε θα πρέπει να κοινοποιούνται σε τρίτες οντότητες ή να χρησιμοποιούνται για άλλο σκοπό εκτός από τον προσδιορισμένο σύμφωνα με την αρχή προσδιορισμού του σκοπού, εκτός εάν υπάρχει η σχετική συναίνεση του χρήστη ή η εξουσιοδότηση από το νόμο.
- **Αρχή της προστασίας της ασφάλειας** (security safeguards principle): Τα προσωπικά δεδομένα θα πρέπει να προστατεύονται με χρήση των κατάλληλων μηχανισμών απέναντι σε κινδύνους όπως η μη εξουσιοδοτημένη πρόσβαση, καταστροφή, χρήση, τροποποίηση ή κοινοποίηση σε τρίτες οντότητες.
- **Αρχή της διαφάνειας** (openness principle): Θα πρέπει να υπάρχει γενική διαφάνεια αναφορικά με τις πολιτικές και πρακτικές που σχετίζονται με τη συλλογή και επεξεργασία των προσωπικών δεδομένων καθώς και με την ταυτότητα του φορέα που διενεργεί τη συλλογή και επεξεργασία.
- **Αρχή της συμμετοχής του ατόμου** (individual participation principle): Το κάθε άτομο θα πρέπει να έχει το δικαίωμα:
  - Να αποκτά είτε απ' ευθείας από τον υπεύθυνο της επεξεργασίας είτε μέσω κάποιου άλλου τρόπου επιβεβαίωση αναφορικά με το αν ο υπεύθυνος της επεξεργασίας διαθέτει δεδομένα που σχετίζονται με το εν λόγω άτομο.

- Να του ανακοινώνονται δεδομένα που σχετίζονται με αυτό, μέσα σε εύλογο χρονικό διάστημα, με εύλογο τρόπο, σε μορφή εύκολα κατανοητή και εφόσον η ανακοίνωση προϋποθέτει κόστος, αυτό να μην είναι υπερβολικό.
- Να του παρέχονται οι λόγοι για τους οποίους απορρίπτονται αιτήσεις του που αναφέρονται στις δύο παραπάνω παραγράφους και να διατηρεί στην περίπτωση αυτή τη δυνατότητα της αμφισβήτησης της απόρριψης και της περαιτέρω διεκδίκησης.
- Να αμφισβητεί προσωπικά δεδομένα που σχετίζονται με αυτό και σε περίπτωση επιτυχημένης αμφισβήτησης να μπορεί να προχωρεί σε εξάλειψη, διόρθωση ή ολοκλήρωση των δεδομένων αυτών.

- **Αρχή της ευθύνης** (accountability principle): Κάθε υπεύθυνος της επεξεργασίας δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι υπόλογος αναφορικά με την εφαρμογή των μέτρων εκείνων που προάγουν τις παραπάνω αρχές που πρέπει να διέπουν την προστασία των προσωπικών δεδομένων.

Στις παραπάνω βασικές αρχές για την προστασία των προσωπικών δεδομένων βασίστηκε, μεταξύ άλλων, και η ανάπτυξη της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ [22], η οποία παρουσιάζεται παρακάτω.

2.3 Ευρωπαϊκό Δίκαιο

Η Ενότητα αυτή περιγράφει συνοπτικά την Ευρωπαϊκή νομοθεσία αναφορικά με την προστασία των προσωπικών δεδομένων, κυρίως μέσω των δύο βασικών σχετικών οδηγιών. Έτσι, η Ενότητα 2.3.1 περιγράφει την Οδηγία 95/46/ΕΚ [22], ενώ η Ενότητα 2.3.2 περιγράφει την Οδηγία 2002/58/ΕΚ [24], καθώς και την τροποποίησή της από την Οδηγία 2006/24/ΕΚ [25], με έμφαση στα θέματα εκείνα τα οποία μπορούν να ερμηνευτούν ως απαιτήσεις – τεχνικές ή διαχειριστικές – ενός συστήματος προστασίας προσωπικών δεδομένων.

2.3.1 Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ

Η Ευρωπαϊκή Οδηγία 95/46/ΕΚ [22] αποτελεί σήμερα το πιο επιδραστικό παγκοσμίως νομικό κείμενο αναφορικά με την προστασία των δεδομένων προσωπικού

χαρακτήρα, ορίζοντας ένα υψηλού επιπέδου πρότυπο. Υιοθετήθηκε επίσημα το Νοέμβριο του 1995 και τα κράτη – μέλη της Ευρωπαϊκής Ένωσης υποχρεώθηκαν να αναπροσαρμόσουν τις εθνικές τους νομοθεσίες τρία χρόνια αργότερα.

Ο βασικός στόχος της Οδηγίας είναι η προστασία της ιδιωτικότητας σαν θεμελιώδες δικαίωμα του ανθρώπου, αναφορικά προς τη συλλογή, επεξεργασία, αποθήκευση και μετάδοση των δεδομένων προσωπικού χαρακτήρα. Συμπληρωματικό στόχο της Οδηγίας αποτελεί η εφαρμογή ενός εναρμονισμένου νομικού πλαισίου σε όλα τα κράτη – μέλη της Ευρωπαϊκής Ένωσης, ούτως ώστε να προαχθεί η ελεύθερη διακίνηση προσωπικών δεδομένων μέσα στα σύνορα της Κοινότητας. Από την άλλη πλευρά, η Οδηγία εμποδίζει τη μετάδοση προσωπικών δεδομένων σε χώρες εκτός της Ευρωπαϊκής Ένωσης οι οποίες δεν έχουν την κατάλληλη νομοθεσία που να πληροί τα ελάχιστα πρότυπα προστασίας των δεδομένων προσωπικού χαρακτήρα. Η Οδηγία διαρθρώνεται σε επτά κεφάλαια, μία σύντομη περιγραφή των οποίων παρουσιάζεται στη συνέχεια.

Το Κεφάλαιο Ι της Οδηγίας (“Γενικές Διατάξεις”) παρέχει τους απαραίτητους ορισμούς και ορίζει τους σκοπούς και το πεδίο εφαρμογής της Οδηγίας. Σύμφωνα με το Άρθρο 3 (1), οι διατάξεις της Οδηγίας “εφαρμόζονται στην αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα καθώς και στη μη αυτοματοποιημένη επεξεργασία τέτοιων δεδομένων που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο”, όπου το ”αρχείο” ορίζεται σύμφωνα με τους ορισμούς του παρόντος (Ενότητα 1.3). Ωστόσο (Άρθρο 3 (2)), εξαιρείται η επεξεργασία όταν “πραγματοποιείται στο πλαίσιο δραστηριοτήτων που δεν εμπίπτουν στο πεδίο εφαρμογής του κοινοτικού δικαίου”, καθώς και όταν αφορά ”τη δημόσια ασφάλεια, την εθνική άμυνα, την ασφάλεια του κράτους (συμπεριλαμβανομένης και της οικονομικής ευημερίας του, εφόσον η επεξεργασία αυτή συνδέεται με θέματα ασφάλειας του κράτους) και τις δραστηριότητες του κράτους σε τομείς του ποινικού δικαίου” ή όταν “πραγματοποιείται από φυσικό πρόσωπο στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων”.

Το Κεφάλαιο ΙΙ της Οδηγίας (“Γενικές προϋποθέσεις σχετικά με τη θεμιτή επεξεργασία δεδομένων προσωπικού χαρακτήρα”) παρουσιάζει τις βασικές αρχές για την προστασία των προσωπικών δεδομένων, σε γενική συμφωνία με αυτές που ορίζονται από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (βλ. Ενότητα 2.2) και

αποτελεί τον κορμό της Οδηγίας. Οι "αρχές που πρέπει να τηρούνται ως προς την ποιότητα των δεδομένων" (Άρθρο 6) επιβάλλουν τη σύννομη και θεμιτή συλλογή και επεξεργασία των προσωπικών δεδομένων, την αρχή του αυστηρού προσδιορισμού του σκοπού για τον οποίο πραγματοποιούνται και το συμβιβασμό με το σκοπό αυτό κάθε περαιτέρω επεξεργασίας, καθώς και την αρχή της ακρίβειας. Υλοποιούν δηλαδή επί της ουσίας τις αρχές περιορισμού της συλλογής και της χρήσης, του προσδιορισμού του σκοπού και της ποιότητας των δεδομένων όπως ορίζονται στο [21]. Οι "βασικές αρχές της νόμιμης επεξεργασίας δεδομένων" (Άρθρο 7) αφορούν την αναγκαιότητα της επεξεργασίας των προσωπικών δεδομένων. Σύμφωνα με τις αρχές αυτές, τα προσωπικά δεδομένα μπορούν να υποστούν επεξεργασία μόνο εφόσον το πρόσωπο στο οποίο αναφέρονται έχει συναινέσει σχετικά ή εάν η επεξεργασία πραγματοποιείται στο πλαίσιο εκπλήρωσης ισχύοντος συμβολαίου στο οποίο εμπλέκεται το εν λόγω πρόσωπο ή είναι απαραίτητη για τη διασφάλιση ζωτικού συμφέροντός του, καθώς και για λόγους συμμόρφωσης με νομικές υποχρεώσεις ή εκπλήρωσης γενικού συμφέροντος. Σύμφωνα με τις "ειδικές κατηγορίες επεξεργασίας" (Άρθρο 8), η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων τα οποία "παρέχουν πληροφορίες για τη φυλετική ή εθνική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις, τη συμμετοχή σε συνδικαλιστικές οργανώσεις και την υγεία και τη σεξουαλική ζωή" απαγορεύεται. Ορίζονται ωστόσο και εξαιρέσεις. Τα Άρθρα 10 – 14 της Οδηγίας διατυπώνουν τα δικαιώματα του προσώπου στο οποίο αναφέρονται τα προσωπικά δεδομένα στην πρόσβασή του σε αυτά, καθώς και στην εκτενή ενημέρωσή του για τη συλλογή και την επεξεργασία τους συμπεριλαμβανομένων των σχετικών πληροφοριών, ορίζοντας παράλληλα και τις σχετικές εξαιρέσεις. Η εμπιστευτικότητα και η ασφάλεια της επεξεργασίας των προσωπικών δεδομένων υπογραμμίζονται από τα Άρθρα 16 και 17, ενώ τα Άρθρα 18 και 19 ορίζουν την υποχρέωση που έχει ο υπεύθυνος για την επεξεργασία να ενημερώνει την εθνική ελεγκτική αρχή καθώς και το περιεχόμενο αυτής της ενημέρωσης και τις προϋποθέσεις κάτω από τις οποίες η υποχρέωση αυτή απλουστεύεται ή δεν ισχύει. Το Άρθρο 20 προβλέπει τον εκ των προτέρων έλεγχο από την αρχή ελέγχου των επεξεργασιών εκείνων που ενέχουν ειδικούς κινδύνους για τα δικαιώματα και τις ελευθερίες των ενδιαφερομένων. Επιπλέον, το Άρθρο 21 ορίζει ότι πρέπει να λαμβάνονται μέτρα ούτως ώστε να διασφαλίζεται η δημοσιότητα των ως άνω περιγραφόμενων επεξεργασιών για τις οποίες έχει πραγματοποιηθεί ενημέρωση της αρχής ελέγχου με τη χρήση σχετικού μητρώου, το οποίο μπορεί να συμβουλεύεται ο

οποιοσδήποτε. Για εκείνες τις επεξεργασίες που δεν υπόκεινται σε κοινοποίηση στην αρχή ελέγχου, προβλέπεται η αντίστοιχη δημοσιοποίηση από τον υπεύθυνο τη επεξεργασίας ή άλλο οριζόμενο φορέα σε όποιο πρόσωπο το ζητήσει.

Το Κεφάλαιο ΙΙΙ της Οδηγίας ("Ένδικα μέσα, ευθύνη και κυρώσεις") προβλέπει ότι κάθε πρόσωπο έχει δικαίωμα να προσφύγει ενώπιον δικαστηρίου, εφόσον δεν μπορεί να επιληφθεί η ίδια η αρχή ελέγχου, σε περίπτωση παραβιάσεως δικαιωμάτων κατοχυρωμένων από την εθνική νομοθεσία που εφαρμόζεται στη σχετική επεξεργασία προσωπικών δεδομένων, ενώ προβλέπονται οι ευθύνες των υπευθύνων για την επεξεργασία και οι αντίστοιχες κυρώσεις.

Το ζήτημα της μεταφοράς προσωπικών δεδομένων σε χώρες εκτός Ευρωπαϊκής Ένωσης θίγεται από το Κεφάλαιο IV της Οδηγίας ("Διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες"). Σύμφωνα με το Άρθρο 25, η διαβίβαση προς τρίτη χώρα δεδομένων προσωπικού χαρακτήρα, τα οποία έχουν υποστεί επεξεργασία ή πρόκειται να υποστούν επεξεργασία μετά τη διαβίβασή τους, επιτρέπεται μόνον εάν η εν λόγω τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Ωστόσο, το Άρθρο 26 υπογραμμίζει διάφορες παρεκκλίσεις από την αρχή αυτή, όπως για την περίπτωση κατά την οποία το πρόσωπο στο οποίο αναφέρονται τα προσωπικά δεδομένα έχει συναινέσει σχετικά ή εάν η διαβίβαση πραγματοποιείται στο πλαίσιο εκπλήρωσης ισχύοντος συμβολαίου στο οποίο εμπλέκεται το εν λόγω πρόσωπο.

Στο Κεφάλαιο V της Οδηγίας ("Κώδικες δεοντολογίας") ενθαρρύνεται η εκπόνηση κωδίκων δεοντολογίας που αποσκοπούν στο να συμβάλουν, ανάλογα με τις κατά περίπτωση τομεακές ιδιομορφίες, στην ορθή εφαρμογή των εθνικών διατάξεων που θεσπίζουν τα κράτη μέλη κατ' εφαρμογή της Οδηγίας. Προβλέπεται επίσης ότι τα επαγγελματικά σωματεία και οι λοιπές οργανώσεις μπορούν να τους υποβάλουν προς εξέταση στην εθνική αρχή του κώδικες δεοντολογίας, προκειμένου να εξεταστεί η συμμόρφωσή τους με τη σχετική νομοθεσία.

Το Κεφάλαιο VI της Οδηγίας ("Αρχή ελέγχου και ομάδα για την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα") ορίζει δύο βασικούς θεσμικούς φορείς:

- Το Άρθρο 28 προβλέπει ότι, σε κάθε κράτος – μέλος, μία ή περισσότερες δημόσιες αρχές ελέγχου επιφορτίζονται, με πλήρη ανεξαρτησία, με τον έλεγχο της

εφαρμογής, στο έδαφός του, των εθνικών διατάξεων που έχουν θεσπισθεί από τα κράτη μέλη, κατ' εφαρμογή της Οδηγίας. Οι αρχές ελέγχου διαθέτουν μέσα για τη διεξαγωγή έρευνας (όπως το δικαίωμα πρόσβασης στα δεδομένα που αποτελούν αντικείμενο επεξεργασίας), αποτελεσματικές εξουσίες παρέμβασης, καθώς και την εξουσία παράστασης ενώπιον δικαστηρίου σε περίπτωση παράβασης των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της Οδηγίας, ή επισήμανσης των παραβάσεων αυτών στις δικαστικές αρχές. Κάθε πρόσωπο μπορεί να υποβάλει στην αρχή ελέγχου αίτηση σχετικά με την προστασία των δικαιωμάτων και ελευθεριών του έναντι της επεξεργασίας προσωπικών δεδομένων. Σημειώνεται ότι τα μέλη και οι υπάλληλοι των αρχών ελέγχου δεσμεύονται ακόμα και μετά την παύση των δραστηριοτήτων τους από το επαγγελματικό απόρρητο, όσον αφορά τις εμπιστευτικές πληροφορίες στις οποίες έχουν πρόσβαση.

- Τα Άρθρα 29 και 30 ορίζουν την "Ομάδα προστασίας των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα", η οποία έχει συμβουλευτικό χαρακτήρα, είναι ανεξάρτητη και απαρτίζεται από έναν αντιπρόσωπο της αρχής ή των αρχών ελέγχου που έχει ορίσει κάθε κράτος – μέλος, έναν αντιπρόσωπο της αρχής ή των αρχών που έχουν συσταθεί για τα όργανα και τους οργανισμούς της Ευρωπαϊκής Κοινότητας καθώς και έναν αντιπρόσωπο της Ευρωπαϊκής Επιτροπής. Στις αρμοδιότητές της περιλαμβάνονται η εξέταση οποιουδήποτε θέματος σχετικού με την εφαρμογή των εθνικών διατάξεων που έχουν θεσπισθεί κατ' εφαρμογή της Οδηγίας και η γνωμοδότηση προς την Ευρωπαϊκή Επιτροπή αναφορικά με σχέδια τροποποίησης της Οδηγίας και σχέδια συμπληρωματικών ή ειδικών μέτρων που πρέπει να ληφθούν για τη διασφάλιση των δικαιωμάτων και ελευθεριών των προσώπων έναντι της επεξεργασίας προσωπικών δεδομένων.

Τέλος, το Κεφάλαιο VII της Οδηγίας ("Κοινοτικά μέτρα εκτέλεσης") συμπληρώνει τα Κεφάλαια III, V και VI αναφορικά με τις μεθόδους μέσω των οποίων οι διατάξεις του Κεφαλαίου II τίθενται σε εφαρμογή σε εθνικό και Κοινοτικό επίπεδο.

2.3.2 Οι Ευρωπαϊκές Οδηγίες 2002/58/ΕΚ και 2006/24/ΕΚ

Η Ευρωπαϊκή Οδηγία 2002/58/ΕΚ [24] αναφερόμενη στην "επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα

των ηλεκτρονικών επικοινωνιών" αντικατέστησε την Οδηγία 97/66/ΕΚ [23]. Η τελευταία είχε επιληφθεί για πρώτη φορά τη μεταφορά των βασικών αρχών που όριζε η Οδηγία 95/46/ΕΚ [22] σε προβλέψεις και κανόνες που αφορούσαν συγκεκριμένα τον τομέα των τηλεπικοινωνιών. Ωστόσο, η ανάπτυξη των προηγμένων ψηφιακών τεχνολογιών και των Διαδικτυακών εφαρμογών και υπηρεσιών, καθώς και η ραγδαία εξάπλωση των κινητών ψηφιακών επικοινωνιών επέβαλλαν την αναθεώρηση της προηγούμενης Οδηγίας προκειμένου να καλυφθεί όλο το φάσμα των σύγχρονων ηλεκτρονικών επικοινωνιών.

Οι βασικές απαιτήσεις που θέτει η Οδηγία 2002/58/ΕΚ παρουσιάζονται στη συνέχεια. Στο Άρθρο 4 της Οδηγίας θίγεται το ζήτημα της ασφάλειας των προσωπικών δεδομένων, επιβάλλοντας την υποχρέωση του να λαμβάνονται από τους παρόχους υπηρεσιών και δικτύων όλα τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα προκειμένου να προστατεύεται η ασφάλεια των παρερχομένων υπηρεσιών.

Το Άρθρο 5 της Οδηγίας ασχολείται με το απόρρητο των επικοινωνιών, απαγορεύοντας "την ακρόαση, υποκλοπή, αποθήκευση ή άλλο είδος παρακολούθησης ή επιτήρησης των επικοινωνιών και των συναφών δεδομένων κίνησης από πρόσωπα πλην των χρηστών, χωρίς τη συγκατάθεση των ενδιαφερομένων χρηστών, εκτός αν υπάρχει σχετική νόμιμη άδεια". Το γεγονός αυτό ωστόσο δεν επηρεάζει, σύμφωνα με το ίδιο άρθρο, "οποιαδήποτε επιτρεπόμενη από το νόμο καταγραφή συνδιαλέξεων και των συναφών δεδομένων κίνησης όταν πραγματοποιούνται κατά τη διάρκεια νόμιμης επαγγελματικής πρακτικής με σκοπό την παροχή αποδεικτικών στοιχείων μιας εμπορικής συναλλαγής ή οποιασδήποτε άλλης επικοινωνίας επαγγελματικού χαρακτήρα".

Το Άρθρο 6 της Οδηγίας αναφέρεται εκτενώς στα δεδομένα κίνησης, δηλαδή τα δεδομένα εκείνα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μιας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Σύμφωνα με το Άρθρο αυτό, τα δεδομένα κίνησης τα οποία υποβάλλονται σε επεξεργασία και αποθηκεύονται από τον πάροχο του δικτύου ή κάποιας υπηρεσίας ηλεκτρονικών επικοινωνιών, πρέπει να απαλείφονται ή να καθίστανται ανώνυμα όταν δεν είναι πλέον απαραίτητα για το σκοπό της μετάδοσης μιας επικοινωνίας ή για την εκπλήρωση κάποιου άλλου θεμιτού σκοπού. Ο συνδρομητής ή ο χρήστης πρέπει να ενημερώνονται από τον πάροχο δικτύου ή κάποιας υπηρεσίας ηλεκτρονικών επικοινωνιών σχετικά με τον τύπο των δεδομένων κίνησης που υποβάλλονται σε επεξεργασία και τη διάρκεια της

επεξεργασίας αυτής, ενώ θα πρέπει να ζητείται και παρέχεται η συναίνεσή του για ορισμένους τύπους και σκοπούς επεξεργασίας (π.χ. για την εμπορική προώθηση των υπηρεσιών ηλεκτρονικών επικοινωνιών ή για την παροχή υπηρεσιών προστιθέμενης αξίας).

Αναφορικά με τα δεδομένα θέσης εκτός εκείνων της κίνησης, δηλαδή όλα εκείνα τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μιας υπηρεσίας ηλεκτρονικών επικοινωνιών, το Άρθρο 9 της Οδηγίας ορίζει ότι είναι δυνατό να υποστούν επεξεργασία, η επεξεργασία αυτή επιτρέπεται μόνον όταν αυτά καθίστανται ανώνυμα ή με τη ρητή συγκατάθεση των χρηστών ή συνδρομητών στην απαιτούμενη έκταση και για την απαιτούμενη διάρκεια για την παροχή μιας υπηρεσίας προστιθέμενης αξίας. Ο φορέας παροχής υπηρεσιών είναι υποχρεωμένος να ενημερώνει τους χρήστες ή συνδρομητές, προτού δώσουν τη συγκατάθεσή τους, σχετικά με τον τύπο των δεδομένων θέσης εκτός των δεδομένων κυκλοφορίας που υποβάλλονται σε επεξεργασία, τους σκοπούς και τη διάρκεια της εν λόγω επεξεργασίας, καθώς και το ενδεχόμενο μετάδοσής τους σε τρίτους για το σκοπό παροχής της υπηρεσίας προστιθέμενης αξίας. Στους χρήστες ή συνδρομητές πρέπει να δίνεται η δυνατότητα να ανακαλούν οποτεδήποτε τη συγκατάθεσή τους για την επεξεργασία των δεδομένων θέσης, εκτός των δεδομένων κίνησης. Επιπλέον, ορίζεται ότι όταν ο χρήστης έχει δώσει τη συγκατάθεσή του για την επεξεργασία δεδομένων θέσης εκτός των δεδομένων κίνησης, θα πρέπει να εξακολουθεί να έχει τη δυνατότητα, με απλά μέσα και ατελώς, να αρνείται προσωρινά την επεξεργασία των εν λόγω δεδομένων για κάθε σύνδεση με το δίκτυο ή για κάθε μετάδοση μιας επικοινωνίας.

Το Άρθρο 12 της Οδηγίας αναφέρεται στις συνθήκες εισαγωγής και περαιτέρω χρήσης των προσωπικών δεδομένων χρηστών ηλεκτρονικών επικοινωνιών σε τηλεφωνικούς καταλόγους συνδρομητών οι οποίοι είτε είναι ευθέως διαθέσιμοι στο κοινό είτε είναι δυνατή η εξαγωγή δεδομένων από αυτούς μέσω σχετικών ερωτήσεων. Σύμφωνα με το Άρθρο 12, οι συνδρομητές πρέπει να ενημερώνονται, ατελώς και πριν περιληφθούν στον κατάλογο, σχετικά με το σκοπό των καταλόγων στους οποίους μπορεί να περιλαμβάνονται τα προσωπικά τους δεδομένα, καθώς και σχετικά με τις περαιτέρω δυνατότητες χρήσης που βασίζονται σε λειτουργίες αναζήτησης. Επιπλέον, οι συνδρομητές πρέπει να έχουν την ευκαιρία να καθορίζουν εάν και ποια από τα

προσωπικά τους δεδομένα θα περιλαμβάνονται καταλόγους και να επαληθεύουν, να διορθώνουν ή να αποσύρουν τα εν λόγω δεδομένα.

Η Οδηγία δίνει ιδιαίτερη σημασία στις αυτόκλητες κλήσεις. Σύμφωνα με το Άρθρο 13, η χρησιμοποίηση οποιουδήποτε μέσου για σκοπούς απευθείας εμπορικής προώθησης επιτρέπεται μόνον στην περίπτωση συνδρομητών οι οποίοι έχουν δώσει εκ των προτέρων τη συγκατάθεσή τους. Έτσι, απαγορεύεται η πρακτική της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου με σκοπό την άμεση εμπορική προώθηση, τα οποία συγκαλύπτουν ή αποκρύπτουν την ταυτότητα του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα, ή δίχως έγκυρη διεύθυνση στην οποία ο αποδέκτης να μπορεί να ζητεί τον τερματισμό της επικοινωνίας αυτής.

Το Άρθρο 15 της Οδηγίας, τιτλοφορούμενο "Εφαρμογή ορισμένων διατάξεων της Οδηγίας 95/46/ΕΚ", θέτει περιορισμούς σχετικά με τα δικαιώματα και τις υποχρεώσεις που ορίζονται από την Οδηγία, για εκείνες τις περιπτώσεις που αφορούν τη διαφύλαξη της εθνικής ασφάλειας, της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων. Για τους λόγους αυτούς, η Οδηγία προβλέπει τη φύλαξη προσωπικών δεδομένων για ορισμένο χρονικό διάστημα.

Η απαίτηση για φύλαξη προσωπικών δεδομένων γίνεται πιο συγκεκριμένη από την Οδηγία 2006/24/ΕΚ [25], η οποία τροποποιεί την Οδηγία 2002/58/ΕΚ σε ό,τι αφορά το συγκεκριμένο ζήτημα. Η Οδηγία 2006/24/ΕΚ ορίζει συγκεκριμένου τύπους δεδομένων που αφορούν τηλεφωνικές (σταθερές και κινητές) και Διαδικτυακές υπηρεσίες, για τους οποίους προβλέπεται υποχρεωτική διατήρηση για συγκεκριμένα χρονικά διαστήματα, με σκοπό τη διασφάλιση ότι τα δεδομένα αυτά θα καθίστανται διαθέσιμα για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων. Σημειώνεται ότι η Οδηγία 2006/24/ΕΚ αναφέρει ρητά ότι δεν επιτρέπεται η διατήρηση δεδομένων που αποκαλύπτουν το περιεχόμενο των επικοινωνιών, ενώ πρόσβαση στα διατηρούμενα δεδομένα πρέπει να παρέχεται μόνο στις αρμόδιες εθνικές αρχές, σε ειδικές μόνο περιπτώσεις και σύμφωνα με τη νομοθεσία και τις απαιτήσεις της αναγκαιότητας και της αναλογικότητας.

2.4 Ελληνικό Εθνικό Δίκαιο

Η Ελλάδα κατοχυρώνει συνταγματικά ως ατομικά και κοινωνικά δικαιώματα το δικαίωμα στην προστασία προσωπικών δεδομένων και στο απόρρητο της επικοινωνίας. Συγκεκριμένα, το Άρθρο 9Α του Συντάγματος της Ελλάδας [26] αναφέρει ότι "καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων", ενώ προβλέπει ότι η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή. Επιπλέον, το Άρθρο 19 ορίζει ως απόλυτα απαραβίαστο το απόρρητο των επικοινωνιών, προβλέποντας ωστόσο το νομοθετικό ορισμό εγγυήσεων υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων. Προβλέπει επίσης το νομοθετικό ορισμό των σχετικών με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο.

Σε ό,τι αφορά την εναρμόνιση με το Κοινοτικό Δίκαιο, όπως είναι επόμενο η Ελλάδα έχει ενσωματώσει στο Εθνικό της Δίκαιο τις Κοινοτικές Οδηγίες που περιγράφονται παραπάνω. Στο πλαίσιο αυτό, η Οδηγία 95/46/ΕΚ τέθηκε σε ισχύ τον Απρίλιο του 1997 με το Νόμο 2472/1997 [27], αντικείμενο του οποίου είναι η "η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα προς προστασία των δικαιωμάτων και των θεμελιωδών ελευθεριών των φυσικών προσώπων και ιδίως της ιδιωτικής ζωής". Αναφορικά με την υλοποίηση του Άρθρου 28 της Οδηγίας καθώς και του Άρθρου 9Α του Συντάγματος, με το νόμο αυτό συγκροτήθηκε ως ανεξάρτητη δημόσια αρχή η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [28], με αποστολή την εποπτεία της εφαρμογής του νόμου και άλλων ρυθμίσεων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, καθώς και την ενάσκηση των κατά περίπτωση αρμοδιοτήτων που της ανατίθενται.

Πέρα από Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, ο Νόμος 3115/2003 [29] υλοποίησε το Άρθρο 19 του Συντάγματος συγκροτώντας μία δεύτερη ανεξάρτητη αρχή, την Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών [30]. Ο σκοπός της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών είναι "η προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και η ασφάλεια των δικτύων και πληροφοριών". Στην

έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου, που προβλέπονται από το νόμο.

Αναφορικά με την προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, η αρχική Ευρωπαϊκή Οδηγία 97/66/ΕΚ [23] είχε ενσωματωθεί στο Ελληνικό δίκαιο με το Νόμο 2474/1999 [31], ο οποίος από τον Ιούλιο του 2006 αντικαταστάθηκε από το Νόμο 3471/2006 [32] που αποτελεί προσαρμογή της νεότερης σχετικής Οδηγίας 2002/58/ΕΚ [24]. Σκοπός του Νόμου 3471/2006 είναι "η προστασία των θεμελιωδών δικαιωμάτων των ατόμων και ιδίως της ιδιωτικής ζωής και η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα και τη διασφάλιση του απορρήτου των επικοινωνιών στον τομέα των ηλεκτρονικών επικοινωνιών". Επιπλέον, ο Νόμος 3471/2006 τροποποιεί το Νόμο 2472/97 ως προς ορισμένες διατάξεις του, ενώ ορίζει τις αντίστοιχες αρμοδιότητες της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών και της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Η Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών εξέδωσε τον Ιανουάριο του 2005 ορισμένους Κανονισμούς που αφορούν άμεσα την προστασία των προσωπικών δεδομένων. Οι Κανονισμοί αυτοί αφορούν, από τη μία πλευρά, τη διασφάλιση του απορρήτου κατά την παροχή κινητών [33], σταθερών [34] και μέσω ασυρμάτων δικτύων [35] τηλεπικοινωνιακών υπηρεσιών, και από την άλλη, τη διασφάλιση του απορρήτου στις Διαδικτυακές υπηρεσίες και τις συναφείς υπηρεσίες και εφαρμογές [36], των διαδικτυακών υποδομών [37] και των εφαρμογών Διαδικτύου και των χρηστών τους [38].

Στις διατάξεις των Κανονισμών της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών οφείλουν να συμμορφώνονται όλοι οι τηλεπικοινωνιακοί πάροχοι οι οποίοι παρέχουν τηλεπικοινωνιακές υπηρεσίες κινητές, σταθερές ή μέσω ασυρμάτων δικτύων, καθώς και όλοι οι τηλεπικοινωνιακοί φορείς Διαδικτύου και οι Δημόσιοι Οργανισμοί και ιδιαίτερα οι πάροχοι πρόσβασης στο Διαδίκτυο, οι πάροχοι διαδικτυακών υπηρεσιών και οι πάροχοι διαδικτυακών υπηρεσιών προστιθέμενης αξίας. Αναφορικά με τους φορείς αυτούς, οι Κανονισμοί προδιαγράφουν τα απαραίτητα τεχνικά και οργανωτικά μέτρα τα οποία πρέπει να λαμβάνονται προκειμένου να διασφαλίζεται το απόρρητο των ηλεκτρονικών επικοινωνιών κάθε είδους και κατά συνέπεια των προσωπικών δεδομένων που μεταδίδονται στο πλαίσιο της διεξαγωγής των επικοινωνιών αυτών. Επιπλέον, οι

Κανονισμοί θεσπίζουν τις υποχρεώσεις των εν λόγω φορέων αναφορικά με την ασφάλεια και το απόρρητο των επικοινωνιών καθώς και απέναντι στην ανεξάρτητη αρχή, ενώ ορίζονται και τα σχετικά με τη διεξαγωγή ελέγχων στους φορείς αυτούς αναφορικά με τις υποχρεώσεις τους αυτές.

Σημειώνεται ότι οι Κανονισμοί της Αρχής Διασφάλισης Απορρήτου των Επικοινωνιών χαρακτηρίζονται από τέτοιο βαθμό πληρότητας που στην πράξη ωθούν τους φορείς που εμπίπτουν στις διατάξεις τους στην εφαρμογή των διεθνώς αναγνωρισμένων προτύπων ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων, όπως το ISO/IEC 17799 [39].

Τέλος, οι διαδικασίες καθώς και οι τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του ορίστηκαν με το Προεδρικό Διάταγμα 47/2005 [40] το Μάρτιο του 2005. Το Προεδρικό Διάταγμα 47/2005 ορίζει τα είδη της επικοινωνίας καθώς και τα στοιχεία εκείνα τα οποία, εφόσον τηρούνται οι νόμιμες προϋποθέσεις, είναι δυνατό να ζητούνται από τους παρόχους υπηρεσιών προστιθέμενης αξίας ή δικτύου. Από τις ειδικές περιπτώσεις που ορίζονται, ιδιαίτερο ενδιαφέρον παρουσιάζει η διάταξη που επιτρέπει στις αρμόδιες αρχές να αποκτούν πρόσβαση στα κλειδιά κρυπτογράφησης που εκδίδονται από Παρόχους Υπηρεσιών Πιστοποίησης (Certification Authorities), εφόσον φυσικά πληρούνται οι νόμιμες προϋποθέσεις και συντρέχουν οι νόμιμες αιτίες για αυτό. Επιπλέον, το Προεδρικό Διάταγμα 47/2005 ορίζει τα απαραίτητα μέσα και τον αναγκαίο εξοπλισμό για την άρση του απορρήτου, καθώς τη μέθοδο αλλά και τις αντίστοιχες υποχρεώσεις των παρόχων υπηρεσιών και δικτύων.

3 Τεχνολογίες για την Προστασία των Προσωπικών Δεδομένων

Το Κεφάλαιο αυτό παρουσιάζει συνοπτικά τις πιο σημαντικές τεχνολογίες που έχουν προταθεί ή εφαρμοστεί για την προστασία των προσωπικών δεδομένων. Μία μελέτη [41] που διεξήχθη το 2005 για λογαριασμό του Υπουργείου Επιστημών, Τεχνολογίας και Καινοτομίας της Δανίας από την εταιρεία META Group, διαχωρίζει τις τεχνολογίες αυτές σε δύο βασικές κατηγορίες:

- Τεχνολογίες για την Προστασία της Ιδιωτικότητας (Privacy Protection).
- Τεχνολογίες για τη Διαχείριση της Ιδιωτικότητας (Privacy Management).

Χωρίς ο διαχωρισμός αυτός να ακολουθείται στο παρόν κείμενο πλήρως ως προς το περιεχόμενο των κατηγοριών αυτών, θα χρησιμοποιηθούν οι όροι "Προστασία της Ιδιωτικότητας" και "Διαχείριση της Ιδιωτικότητας" καθώς ως έννοιες εκφράζουν σε μεγάλο βαθμό τις κυρίαρχες τάσεις για την προστασία των προσωπικών δεδομένων. Η πρώτη τάση ("Προστασία της Ιδιωτικότητας") αφορά μεθόδους που εφαρμόζονται κυρίως από το χρήστη προκειμένου να προστατεύσει ενεργά (π.χ. με χρήση κρυπτογραφίας) ή να αποκρύψει (π.χ. με χρήση υπηρεσιών ψευδωνυμίας ή ανωνυμίας) προσωπικά δεδομένα, κυρίως κατά το στάδιο της μετάδοσής τους. Η δεύτερη τάση ("Διαχείριση της Ιδιωτικότητας") αφορά την εφαρμογή μηχανισμών για τον έλεγχο της πρόσβασης σε προσωπικά δεδομένα και τη χρήση τεχνικών μέσων και ιδιαιτέρως συστημάτων που βασίζονται σε πολιτικές και κανόνες για την εφαρμογή των απαιτήσεων της σχετικής Νομοθεσίας και των ίδιων των χρηστών, κυρίως σε επιχειρησιακά περιβάλλοντα.

3.1 Τεχνολογίες για τη Διαχείριση της Ιδιωτικότητας

Οι τεχνολογίες για τη διαχείριση της ιδιωτικότητας αναφέρονται κυρίως σε μηχανισμούς για την αυτοματοποίηση της εφαρμογής πολιτικών ιδιωτικότητας και σε μηχανισμούς ελέγχου πρόσβασης. Οι πρώτοι αφορούν την κωδικοποίηση των πολιτικής ιδιωτικότητας σε κάποια γλώσσα που μπορεί να γίνει αντιληπτή από προγράμματα λογισμικού. Με τον τρόπο αυτό, κάποιος πράκτορας χρήστη (user agent) δύναται να

αποφασίσει εάν η πολιτική ιδιωτικότητας είναι συμβατή με τις προτιμήσεις που έχουν προκαθοριστεί από το χρήστη. Η πλέον δημοφιλής προσέγγιση προς την κατεύθυνση αυτή είναι η πλατφόρμα P3P, η οποία παρουσιάζεται στην Ενότητα 3.1.1.

Το βασικό πρόβλημα με τις τεχνολογίες αυτές είναι η έλλειψη μηχανισμών για την πραγματοποίηση των δεδηλωμένων από την πολιτική ιδιωτικότητας πρακτικών. Όπως έχει εύστοχα γραφτεί, οι τεχνολογίες αυτές προδιαγράφουν ουσιαστικά «υποσχέσεις ιδιωτικότητας»· από εκεί και πέρα όμως, απουσιάζουν τα μέσα που θα παράσχουν τις εγγυήσεις για την τήρηση των υποσχέσεων αυτών. Στο πνεύμα αυτό, στο [42] συνοψίζονται τέσσερις βασικές απαιτήσεις για τις δομημένες γλώσσες έκφρασης και εφαρμογής πολιτικών ιδιωτικότητας. Σύμφωνα με τις απαιτήσεις αυτές, μία τέτοια γλώσσα θα πρέπει:

- Να υποστηρίζει όχι μόνο περιορισμούς αναφορικά με το ποιος είναι επιτρεπτό να πραγματοποιεί κάποιες ενέργειες σε κάποιους πόρους, αλλά και να υποστηρίζει την αντιστοίχηση μεταξύ των σκοπών για τους οποίους πραγματοποιήθηκε η συλλογή των δεδομένων με τους σκοπούς για τους οποίους επιχειρείται η προσπέλαση των δεδομένων.
- Να υποστηρίζει την προδιαγραφή ευθέως εφαρμόσιμων πολιτικών, δηλαδή πολιτικών που περιγράφουν υποκείμενα, πόρους, ενέργειες και συνθήκες πρόσβασης με χρήση αναγνωριστικών τα οποία μπορούν να αντιστοιχηθούν αυτομάτως και απ' ευθείας σε πραγματικά αντικείμενα και λειτουργίες που χρησιμοποιούνται από εφαρμογές πληροφορικής.
- Να είναι δυνατό να λειτουργήσει σε οποιαδήποτε υπολογιστική πλατφόρμα, προκειμένου να μπορεί να χρησιμοποιηθεί ως πρότυπο.
- Να ταυτίζεται ή να είναι ολοκληρωμένη με τη γλώσσα προδιαγραφής πολιτικών ελέγχου πρόσβασης, καθώς και οι δύο τύποι πολιτικών αφορούν συνήθως τον έλεγχο της πρόσβασης στους ίδιους πόρους.

Οι απαιτήσεις αυτές αντικατοπτρίζουν ως ένα βαθμό τη λογική των τεχνολογιών ελέγχου πρόσβασης οι οποίες είναι προσανατολισμένες στην προστασία της ιδιωτικότητας και οι οποίες παρουσιάζονται στη συνέχεια. Οι υποκείμενοι μηχανισμοί ξεφεύγουν από τα καθιερωμένα μοντέλα ελέγχου πρόσβασης όπως είναι το μοντέλο Ελέγχου Πρόσβασης Βάσει Ρόλων (Role-Based Access Control – RBAC) [43], στοχεύοντας

ουσιαστικά στην ολοκλήρωση των πολιτικών ιδιωτικότητας και των μηχανισμών ελέγχου πρόσβασης.

3.1.1 Η Πλατφόρμα για τις Προτιμήσεις Ιδιωτικότητας (P3P)

Η Πλατφόρμα για τις Προτιμήσεις Ιδιωτικότητας (Platform for Privacy Preferences – P3P) [44] πρωτοπαρουσιάστηκε το 1997 από την Κοινοπραξία για τον Παγκόσμιο Ιστό (World Wide Web Consortium – W3C) [45]. Η πλατφόρμα P3P δίνει τη δυνατότητα σε Διαδικτυακές ιστοσελίδες να κωδικοποιούν και γνωστοποιούν τις πρακτικές τους αναφορικά με τη συλλογή και χρήση προσωπικών δεδομένων, με χρήση μίας πρότυπης γλώσσας, βασισμένης στο πρότυπο της γλώσσας XML (eXtensible Markup Language) [46]. Ως εκ τούτου, δίνεται η δυνατότητα στους πράκτορες των χρηστών (user agents) να αποκτήσουν και ερμηνεύσουν με αυτόματο τρόπο την πολιτική ιδιωτικότητας (privacy policy) της Διαδικτυακής ιστοσελίδας και να αποφασίσουν κατά πόσο αυτή βρίσκεται σε συμφωνία με τις αντίστοιχες προτιμήσεις και απαιτήσεις του χρήστη.

Τεχνικά, η πλατφόρμα P3P αποτελείται από ένα λεξιλόγιο διατυπωμένο σε XML, ένα σύνολο από βασικούς τύπους δεδομένων και από μία γλώσσα προδιαγραφής κανόνων αναφορικά με τις πρακτικές συλλογής και επεξεργασίας προσωπικών δεδομένων. Οι Διαδικτυακοί ιστότοποι συντάσσουν μία στατική πολιτική ιδιωτικότητας, την οποία κοινοποιούν στον πράκτορα χρήστη που επισκέπτεται το Διαδικτυακό ιστότοπο, ο οποίος στη συνέχεια πραγματοποιεί τη διερεύνηση της συμβατότητας της δεδηλωμένης πολιτικής ιδιωτικότητας με τις προτιμήσεις του χρήστη. Σε αυτή τη βάση, η πολιτική ιδιωτικότητας μπορεί να γίνει αποδεκτή ή να απορριφθεί, από τον πράκτορα χρήστη ή από τον ίδιο το χρήστη. Η πλατφόρμα P3P παρέχει επιπλέον το μηχανισμό των συμπαγών πολιτικών (compact policies), δηλαδή συνοπτικών πολιτικών που αφορούν τη χρήση των "cookies" και μόνο. Οι συμπαγείς πολιτικές είναι προαιρετικές και σκοπό έχουν την παροχή δυνατότητας βελτίωσης της επίδοσης τόσο για τον εξυπηρετητή όσο και για τον πράκτορα του χρήστη. Εφόσον οι πράκτορες χρήστη δεν είναι δυνατό να αντλήσουν το σύνολο της πληροφορίας που χρειάζονται αναφορικά με τις πρακτικές του Διαδικτυακού ιστότοπου, χρησιμοποιούν την πλήρη πολιτική ιδιωτικότητας.

Μία πολιτική ιδιωτικότητας η οποία εκφράζεται στο πλαίσιο της πλατφόρμας P3P αποτελείται από μία ακολουθία XML στοιχείων τύπου `STATEMENT`, τα οποία μπορεί να περιλαμβάνουν τα ακόλουθα υποστοιχεία:

- PURPOSE: Περιγράφει τους σκοπούς για τους οποίους πραγματοποιείται η συλλογή της πληροφορίας.
- RECIPIENT: Δηλώνει τους εν δυνάμει αποδέκτες της πληροφορίας η οποία συλλέγεται.
- RETENTION: Ορίζει τη διάρκεια που θα έχει η διατήρηση της πληροφορίας από το συλλέκτη της.
- DATA-GROUP: Παρέχει τον κατάλογο των τύπων δεδομένων που συλλέγονται για τους σκοπούς που δηλώνονται.
- CONSEQUENCE: Το περιεχόμενο του εν λόγω στοιχείου είναι αναγνώσιμο από ανθρώπους (human-readable) και σκοπό έχει την προβολή κατανοητών εξηγήσεων στους χρήστες αναφορικά με τις πρακτικές συλλογής και επεξεργασίας προσωπικών δεδομένων και τις επιπτώσεις τους.

Η πλατφόρμα P3P ορίζει διάφορους προκαθορισμένους τύπους τιμών για τα παραπάνω στοιχεία. Ενδεικτικά, κάποιες πιθανές προκαθορισμένες τιμές που μπορεί να λάβει το στοιχείο PURPOSE είναι:

- <current/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται θα χρησιμοποιηθούν μόνο για την εκπλήρωση της δραστηριότητας για την οποία παρέχονται από το χρήστη. Η δραστηριότητα αυτή μπορεί να αφορά είτε ένα μεμονωμένο γεγονός είτε μία επαναληπτική διαδικασία.
- <admin/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται θα χρησιμοποιηθούν ενδεχομένως για την τεχνική διαχείριση του Διαδικτυακού ιστότοπου.
- <tailoring/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την "υποκειμενική" διαμόρφωση (customization) για το χρήστη του περιεχομένου του Διαδικτυακού ιστότοπου, αλλά μόνο για τη συγκεκριμένη επίσκεψη.
- <pseudo-analysis/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την εξαγωγή συμπερασμάτων αναφορικά με τις συνήθειες,

ενδιαφέροντα ή άλλα χαρακτηριστικά του χρήστη, αλλά χωρίς τα συμπεράσματα αυτά να αντιστοιχίζονται με την ταυτότητα του συγκεκριμένου χρήστη.

- `<pseudo-decision/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την "υποκειμενική" διαμόρφωση (customization) για το χρήστη του περιεχομένου του Διαδικτυακού ιστότοπου, αλλά με χρήση ψευδωνύμων, ούτως ώστε η διαμόρφωση αυτή να μην αντιστοιχίζεται με στοιχεία που εκφράζουν την πραγματική ταυτότητα του χρήστη (π.χ. το όνομά του).
- `<individual-analysis/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την εξαγωγή συμπερασμάτων αναφορικά με τις συνήθειες, ενδιαφέροντα ή άλλα χαρακτηριστικά του χρήστη, σε συνδυασμό με δεδομένα τα οποία ταυτοποιούν το συγκεκριμένο χρήστη.
- `<individual-decision/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την "υποκειμενική" διαμόρφωση (customization) για το χρήστη του περιεχομένου του Διαδικτυακού ιστότοπου, σε συνδυασμό με δεδομένα τα οποία ταυτοποιούν το συγκεκριμένο χρήστη. Για παράδειγμα, στο πλαίσιο αυτό ένα Διαδικτυακό κατάστημα μπορεί να προτείνει στο χρήστη την αγορά συγκεκριμένων προϊόντων με βάση τι προηγούμενες αγορές που ο χρήστης έχει πραγματοποιήσει.
- `<contact/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την προώθηση προϊόντων ή υπηρεσιών μέσω της επικοινωνίας με το χρήστη με οποιοδήποτε μέσο εκτός από την τηλεφωνική επικοινωνία.
- `<telemarketing/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως για την πραγματοποίηση τηλεφωνικής επικοινωνίας με το χρήστη, με σκοπό την προώθηση προϊόντων ή υπηρεσιών.

Οι πιθανές προκαθορισμένες τιμές που μπορεί να λάβει το στοιχείο `RECIPIENT` περιλαμβάνουν:

- <ours/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν μόνο από τον εν λόγω οργανισμό ή/και από άλλους οργανισμούς οι οποίοι λειτουργούν εκ μέρους του οργανισμού για την εκπλήρωση των δεδηλωμένων σκοπών.
- <delivery/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως από τρίτο οργανισμό παροχής υπηρεσιών μεταφοράς προϊόντων, ο οποίος μπορεί να χρησιμοποιήσει τα δεδομένα για άγνωστους σκοπούς ή σκοπούς πέρα από εκείνους για τους οποίους ο χρήστης παρέχει τα δεδομένα.
- <same/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως από τρίτο οργανισμό, ο οποίος ακολουθεί τις ίδιες πρακτικές αναφορικά με τη χρήση των δεδομένων με τον οργανισμό ο οποίος συλλέγει τα δεδομένα.
- <other-recipient/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως από τρίτο οργανισμό, ο οποίος δεν ακολουθεί απαραιτήτως τις ίδιες πρακτικές αναφορικά με τη χρήση των δεδομένων με τον οργανισμό ο οποίος συλλέγει τα δεδομένα, αλλά είναι ελεγχόμενος από τον οργανισμό αυτό.
- <unrelated/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο θα χρησιμοποιηθούν ενδεχομένως από τρίτο οργανισμό, ο οποίος δεν ακολουθεί απαραιτήτως τις ίδιες πρακτικές αναφορικά με τη χρήση των δεδομένων με τον οργανισμό ο οποίος συλλέγει τα δεδομένα, ενώ οι πρακτικές αυτές είναι άγνωστες στον οργανισμό.
- <public/>: Δηλώνει το ενδεχόμενο πλήρους δημοσιοποίησης των δεδομένων τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο.

Οι πιθανές προκαθορισμένες τιμές που μπορεί να λάβει το στοιχείο RETENTION περιλαμβάνουν:

- <no-retention/>: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο δε θα διατηρηθούν με κανένα τρόπο μετά από την εκπλήρωση του σκοπού για τον οποίο παρέχονται και ο οποίος αφορά μία μεμονωμένη και σύντομη συνδιαλλαγή και ότι ακολούθως θα

καταστραφούν τόσο τα ίδια τα δεδομένα όσο και πιθανά ίχνη τους όπως σε αρχεία καταγραφής (log files).

- `<stated-purpose/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο δε θα διατηρηθούν με κανένα τρόπο μετά από την εκπλήρωση του σκοπού για τον οποίο παρέχονται.
- `<legal-requirement/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο ενδεχομένως θα διατηρηθούν πέρα από την εκπλήρωση του σκοπού για τον οποίο παρέχονται, προκειμένου να ικανοποιηθούν σχετικές Νομικές απαιτήσεις.
- `<business-practices/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο ενδεχομένως θα διατηρηθούν πέρα από την εκπλήρωση του σκοπού για τον οποίο παρέχονται, με σκοπό την πραγματοποίηση καθορισμένων επιχειρησιακών διαδικασιών του οργανισμού, ο οποίος στην περίπτωση αυτή θα πρέπει να διαθέτει καλώς ορισμένη πολιτική διατήρησης που να βασίζεται σε συγκεκριμένο χρονοδιάγραμμα καταστροφής των δεδομένων.
- `<indefinitely/>`: Δηλώνει ότι τα δεδομένα τα οποία συλλέγονται κατά την επίσκεψη ενός χρήστη στο Διαδικτυακό ιστότοπο ενδεχομένως θα διατηρηθούν πέρα από την εκπλήρωση του σκοπού για τον οποίο παρέχονται και για απροσδιόριστο χρονικό διάστημα.

Το στοιχείο `DATA-GROUP` παρέχει τον κατάλογο των διακριτών τύπων δεδομένων που συλλέγονται για τους σκοπούς που δηλώνονται. Ο κάθε τύπος προσδιορίζεται με XML υποστοιχεία `DATA`. Δηλαδή, κάθε `DATA-GROUP` περιέχει ένα ή περισσότερα υποστοιχεία `DATA`.

Το κάθε στοιχείο `DATA` περιλαμβάνει ένα υποχρεωτικό XML γνώρισμα (attribute), το `ref`, το οποίο δηλώνει το συγκεκριμένο τύπο δεδομένων που συλλέγεται. Το `ref` λαμβάνει ως τιμή ένα αναγνωριστικό τύπου Μοναδικού Αναγνωριστικού Πόρου (Unique Resource Identifier – URI) [47]. Το πρώτο μέρος του URI εκφράζει κάποιο σχήμα δεδομένων, ενώ το δεύτερο εκφράζει τον τύπο του δεδομένου με βάση το σχήμα εν χρήσει. Σημειώνεται ότι η πλατφόρμα P3P ορίζει κάποιο βασικό σχήμα δεδομένων το οποίο περιλαμβάνει αρκετούς τύπους δεδομένων, ταξινομημένους με ιεραρχικό τρόπο.

Το προαιρετικό γνώρισμα optional ενός στοιχείου DATA δηλώνει εάν ο Διαδικτυακός ιστότοπος ορίζει την υποβολή των συγκεκριμένων δεδομένων από το χρήστη σαν υποχρεωτική (τιμή "no") ή προαιρετική (τιμή "yes"). Επιπλέον, κάθε δεδομένο μπορεί να κατηγοριοποιηθεί με χρήση του XML στοιχείου CATEGORIES το οποίο περιγράφει τον τύπο της πληροφορίας που το εν λόγω δεδομένο εκφράζει. Η πλατφόρμα P3P ορίζει κάποιες προκαθορισμένες κατηγορίες οι οποίες αφορούν δημογραφικά δεδομένα, δεδομένα υγείας, ηλεκτρονικής και φυσικής επικοινωνίας, γεωγραφικής θέσης, συναλλαγών, κ.α.

Πρέπει να σημειωθεί ότι τα στοιχεία PURPOSE και RECIPIENT σε μία πολιτική ιδιωτικότητας μπορεί να χαρακτηρίζονται από XML γνωρίσματα τύπου required. Το γνώρισμα αυτό εκφράζει το κατά πόσο ο δεδηλωμένος σκοπός συλλογής ή ο εν δυνάμει παραλήπτης, αντίστοιχα, αποτελεί αναγκαίο μέρος της πρακτικής του Διαδικτυακού ιστότοπου. Οι τιμές τις οποίες μπορεί να λάβει το γνώρισμα required είναι:

- opt-in: Τα δεδομένα μπορούν να χρησιμοποιηθούν για το σκοπό αυτό ή να παραδοθούν σε επιπλέον παραλήπτες μόνο εφόσον ο χρήστης δώσει σχετική συγκατάθεση.
- opt-out: Τα δεδομένα μπορούν να χρησιμοποιηθούν για το σκοπό αυτό ή να παραδοθούν σε επιπλέον παραλήπτες εκτός και εάν ο χρήστης δηλώσει το αντίθετο με ρητό τρόπο. Ωστόσο, σημειώνεται ότι στην περίπτωση αυτή ο Διαδικτυακός ιστότοπος πρέπει να παρέχει σαφείς οδηγίες για τον τρόπο με τον οποίο ο χρήστης μπορεί να εναντιωθεί.
- always: Στην περίπτωση αυτή, θεωρείται απαραίτητη για το Διαδικτυακό ιστότοπο η χρήση δεδηλωμένων δεδομένων για τον εν λόγω σκοπό συλλογής ή η μεταβίβασή τους στους δεδηλωμένους παραλήπτες. Ο χρήστης δεν έχει επιλογή αποκλεισμού.

Το Σχήμα 1 παρουσιάζει, ως παράδειγμα, την πολιτική ιδιωτικότητας ενός υποθετικού Διαδικτυακού καταστήματος (π.χ. βιβλιοπωλείου). Το κατάστημα αυτό συλλέγει συγκεκριμένα προσωπικά δεδομένα τα οποία είναι αναγκαία για την πραγματοποίηση της συναλλαγής (όνομα, ταχυδρομική διεύθυνση και αριθμός πιστωτικής κάρτας), ενώ χρησιμοποιεί το ιστορικό αγορών των πελατών του, προκειμένου να πραγματοποιεί προσωποποιημένες προτάσεις αγορών. Για το σκοπό

αυτό, χρησιμοποιεί τις διευθύνσεις ηλεκτρονικού ταχυδρομείου των εγγεγραμμένων πελατών του.

```
<POLICY>
     .........
     <STATEMENT>
          <PURPOSE>
               <current/>
          </PURPOSE>
          <RECIPIENT>
               <ours/>
               <same/>
          </RECIPIENT>
          <RETENTION>
               <stated-purpose/>
          </RETENTION>
          <DATA-GROUP>
               <DATA ref="#user.name"/>
               <DATA ref="#user.home-info.postal"/>
               <DATA ref="#dynamic.miscdata">
                    <CATEGORIES>
                         <purchase/>
                    </CATEGORIES>
               </DATA>
          </DATA-GROUP>
     </STATEMENT>
     <STATEMENT>
          <PURPOSE>
               <individual-decision required="opt-in"/>
               <contact required="opt-in"/>
          </PURPOSE>
          <RECIPIENT>
               <ours/>
          </RECIPIENT>
          <RETENTION>
               <business-practices/>
          </RETENTION>
          <DATA-GROUP>
               <DATA ref="#user.home-info.online.email"/>
               <DATA ref="#dynamic.miscdata">
                    <CATEGORIES>
                         <purchase/>
                    </CATEGORIES>
               </DATA>
          </DATA-GROUP>
     </STATEMENT>
</POLICY>
```

Σχήμα 1: Παράδειγμα Πολιτικής Ιδιωτικότητας Πλατφόρμας P3P.

Σύμφωνα με την πολιτική ιδιωτικότητας που περιγράφεται στο Σχήμα 1, το πρώτο στοιχείο τύπου `STATEMENT` δηλώνει ότι το όνομα του χρήστη, η ταχυδρομική του διεύθυνση, καθώς και διάφορα άλλα δεδομένα της κατηγορίας `purchase` θα χρησιμοποιηθούν μόνο για την εκπλήρωση της δραστηριότητας για την οποία παρέχονται από το χρήστη, ενώ θα διατηρηθούν μόνο για το αναλόγως προβλεπόμενο

χρονικό διάστημα. Ο βαθμός διάδοσής τους αφορά μόνο οργανισμούς οι οποίοι ακολουθούν τις ίδιες πρακτικές αναφορικά με τη χρήση των δεδομένων με το εν λόγω Διαδικτυακό κατάστημα.

Το δεύτερο στοιχείο τύπου `STATEMENT` της πολιτικής ιδιωτικότητας που περιγράφεται στο Σχήμα 1 επιτρέπει στο Διαδικτυακό κατάστημα να χρησιμοποιήσει διάφορα δεδομένα της κατηγορίας `purchase`, καθώς και τη διεύθυνση ηλεκτρονικού ταχυδρομείου του χρήστη, προκειμένου αφενός να του παρέχονται προσωποποιημένες υπηρεσίες κατά τις επισκέψεις του στο Διαδικτυακό κατάστημα (π.χ. προτάσεις αγοράς βάσει του ιστορικού των συναλλαγών του) και αφετέρου προκειμένου το Διαδικτυακό κατάστημα να επικοινωνεί με το χρήστη και να τον ενημερώνει για προϊόντα τα οποία, κατά την κρίση του Διαδικτυακού καταστήματος, θα βρει ενδιαφέροντα. Η πολιτική δηλώνει ότι, ως εκ τούτου, τα δεδομένα αυτά θα διατηρηθούν για μεγαλύτερο χρονικό διάστημα από όσο απαιτείται για την παροχή της βασικής υπηρεσίας, ενώ τα δεδομένα αυτά δε θα παρασχεθούν σε τρίτους οργανισμούς. Ωστόσο, μέσω της τιμής `opt-in` του γνωρίσματος `required`, δηλώνεται ότι όλα αυτά θα λάβουν χώρα μόνο εφόσον ο χρήστης συναινέσει σχετικά με ρητό τρόπο.

Σημειώνεται ότι η πλατφόρμα P3P χρησιμοποιείται σήμερα από τα περισσότερα και πλέον διαδεδομένα συστήματα λογισμικού για πλοήγηση στο Διαδίκτυο (web browsers), όπως είναι ο Microsoft Internet Explorer και ο Mozilla Firefox. Στην ιστοσελίδα της Κοινοπραξίας για τον Παγκόσμιο Ιστό (W3C) διατηρείται ένας κατάλογος με τις διάφορες υλοποιήσεις της πλατφόρμας P3P [48]. Επιπλέον, ενδεικτικό στοιχείο αναφορικά με τη διάδοση της πλατφόρμας P3P είναι ότι ο οργανισμός Privacy Finder, είχε τον Οκτώβριο του 2006 καταγεγραμμένους περίπου 15.000 Διαδικτυακούς ιστότοπους που έκαναν χρήση αυτής [49].

Η πλατφόρμα P3P συμπληρώνεται από μία γλώσσα προδιαγραφής προτιμήσεων των χρηστών. Η Γλώσσα Διαπραγμάτευσης P3P Προτιμήσεων (A P3P Preference Exchange Language – APPEL) [50] δίνει τη δυνατότητα στους χρήστες να εκφράζουν τις προτιμήσεις τους αναφορικά με τα προσωπικά τους δεδομένα, χρησιμοποιώντας ένα σύνολο κανόνων προτιμήσεων. Ο τελικός στόχος είναι να διαθέτουν οι χρήστες τη δυνατότητα να ελέγχουν με αυτόματο τρόπο την πολιτική ιδιωτικότητας ενός Διαδικτυακού ιστότοπου και κατά πόσον αυτή συμφωνεί με τις αντίστοιχες προτιμήσεις τους, ούτως ώστε να αποφασίζουν εάν θα παράσχουν προσωπικά τους δεδομένα ή όχι.

Ένας πράκτορας χρήστη εφοδιασμένος με τις προτιμήσεις του χρήστη εκτελεί τις σχετικές εργασίες προς αυτήν την κατεύθυνση.

Ένας κανόνας εκφρασμένος σε APPEL αποτελείται από δύο μέρη, τα οποία εκφράζουν αντίστοιχα:

- Τη συμπεριφορά του κανόνα (rule behavior).
- Το σώμα του κανόνα (rule body).

Η συμπεριφορά ενός κανόνα όπως προδιαγράφεται στο στοιχείο – επικεφαλίδα του (της μορφής `<appel:RULE>`), καθορίζεται δύο παραμέτρους. Η πρώτη παράμετρος αφορά την ενέργεια που θα πραγματοποιηθεί εφόσον οι υφιστάμενες συνθήκες ενεργοποιήσουν τον κανόνα. Η ενέργεια εκφράζεται από το XML γνώρισμα `behavior`, το οποίο μπορεί να λάβει τρεις διαφορετικές τιμές:

- `request`: Στην περίπτωση αυτή δηλώνεται ότι η πρακτική η οποία περιγράφεται από το σώμα του κανόνα εκφράζει κάτι το αποδεκτό για το χρήστη.
- `block`: Δηλώνεται ότι το σώμα του κανόνα περιγράφει πρακτική απαράδεκτη για το χρήστη.
- `limited`: Δηλώνει την ενδιάμεση κατάσταση κατά την οποία η πρακτική η οποία περιγράφεται από το σώμα του κανόνα εκφράζει κάτι το αποδεκτό για το χρήστη, αλλά υπό περιορισμούς.

Η δεύτερη παράμετρος η οποία εκφράζεται από την επικεφαλίδα του κανόνα αφορά την άμεση αλληλεπίδραση με το χρήστη. Συγκεκριμένα, όταν το σχετικό XML γνώρισμα `prompt` έχει την τιμή "`no`", η ενέργεια η οποία εκφράζεται από το XML γνώρισμα `behavior`, εκτελείται απρόσκοπτα, χωρίς περαιτέρω επικοινωνία με το χρήστη. Αντίθετα, όταν το γνώρισμα `prompt` έχει την τιμή "`yes`", προτού εκτελεστεί η ενέργεια η οποία εκφράζεται από το XML γνώρισμα `behavior`, ζητείται η σχετική έγκριση από το χρήστη.

Το σώμα ενός APPEL κανόνα εκφράζει ένα υπόδειγμα (pattern) πολιτικής ιδιωτικότητας, το οποίο συγκρίνεται με την εκάστοτε πολιτική ιδιωτικότητας του Διαδικτυακού τόπου, προκειμένου να ληφθούν οι σχετικές αποφάσεις. Η μορφή του σώματος ακολουθεί τα πρότυπα τα οποία περιγράφηκαν παραπάνω για τη γλώσσα P3P.

Ένα ενδιαφέρον χαρακτηριστικό της γλώσσας APPEL είναι το XML γνώρισμα `connective`, το οποία λαμβάνει ως τιμές λογικούς τελεστές σύζευξης. Στις πιθανές τιμές περιλαμβάνονται: `or`, `and`, `non-or`, `non-and`, `or-exact` και `and-exact`. Οι δύο ασυνήθιστοι τελεστές `or-exact` και `and-exact` έχουν το εξής νόημα:

- `and-exact`: Προκειμένου να ικανοποιείται ο σχετικός κανόνας, πρέπει: (α) όλες οι περιεχόμενες εκφράσεις να περιέχονται στην εν λόγω πολιτική ιδιωτικότητας και (β) η πολιτική ιδιωτικότητας να περιέχει μόνο τις εκφράσεις αυτές. Στην περίπτωση του `and`, θα ήταν αρκετό να ικανοποιείται η απαίτηση (α).
- `or-exact`: Προκειμένου να ικανοποιείται ο σχετικός κανόνας, πρέπει: (α) μία τουλάχιστον ή περισσότερες από τις περιεχόμενες εκφράσεις να περιέχονται στην εν λόγω πολιτική ιδιωτικότητας και (β) η πολιτική ιδιωτικότητας να περιέχει μόνο εκφράσεις που περιέχονται στον κανόνα. Στην περίπτωση του `or`, θα ήταν αρκετό να ικανοποιείται η απαίτηση (α).

Το ακόλουθο Σχήμα 2 παρουσιάζει, ως παράδειγμα, τις προτιμήσεις ιδιωτικότητας κάποιου υποθετικού χρήστη, όπως έχουν προδιαγραφεί με χρήση της γλώσσας APPEL. Ο χρήστης αυτός είναι ευαίσθητος αναφορικά με θέματα ιδιωτικότητας, θέλοντας όμως ταυτόχρονα να απολαμβάνει κάποιες προσωποποιημένες υπηρεσίες. Για το σκοπό αυτό, επιτρέπει τη χρήση του ιστορικού αγορών, προκειμένου να απολαμβάνει προσωποποιημένες προτάσεις αγορών. Ωστόσο, θέλει να διατηρεί τη δυνατότητα να δίνει ή να αίρει τη συγκατάθεσή του σχετικά με τη χρήση του ιστορικού.

Οι κανόνες που παρουσιάζονται στο Σχήμα 2 είναι τρεις. Ο πρώτος κανόνας απαγορεύει (`behavior="block"`) όλους τους σκοπούς συλλογής δεδομένων πέρα από αυτόν της παροχής της υπηρεσίας όπως κάθε φορά ορίζεται. Ωστόσο, αφήνεται ανοιχτό το ενδεχόμενο παροχής ρητής συγκατάθεσης από το χρήστη για συλλογή δεδομένων με σκοπό την προσωποποιημένη διαμόρφωση για το χρήστη του περιεχομένου του Διαδικτυακού ιστότοπου, σε συνδυασμό με δεδομένα τα οποία ταυτοποιούν το χρήστη, καθώς και για τη χρήση των δεδομένων για την προώθηση προϊόντων ή υπηρεσιών μέσω της επικοινωνίας με το χρήστη με οποιοδήποτε μέσο εκτός από την τηλεφωνική επικοινωνία (αντίστοιχα: `<individual-decision required="always"/>` και `<contact required="always"/>`).

Ο δεύτερος APPEL κανόνας – προτίμηση ιδιωτικότητας που παρουσιάζεται στο Σχήμα 2 έχει σκοπό να διασφαλίσει ότι οι μόνοι παραλήπτες των προσωπικών δεδομένων του χρήστη θα είναι, εκτός από τον οργανισμό του Διαδικτυακού ιστότοπου, άλλοι οργανισμοί οι οποίοι ακολουθούν τις ίδιες πρακτικές αναφορικά με τη χρήση των δεδομένων. Στην πράξη, την επιθυμία αυτή ο χρήστης την εκφράζει αποκλείοντας όλα τα υπόλοιπα επίπεδα διασποράς των δεδομένων.

Τέλος, ο τρίτος APPEL κανόνας – προτίμηση ιδιωτικότητας του Σχήμα 2 ορίζει το τι θα εφαρμοστεί στην περίπτωση που οι εκάστοτε συνθήκες δεν υπαγορεύουν την ενεργοποίηση κανενός από τους δύο πρώτους κανόνες. Στην περίπτωση αυτή, η επιθυμία του χρήστη είναι να ελευθερωθούν τα δεδομένα προς το Διαδικτυακό ιστότοπο.

```
<appel:RULESET>
     <appel:RULE behavior="block">
          <POLICY>
               <STATEMENT>
                    <PURPOSE appel:connective="or">
                         <admin/>
                         <develop/>
                         <tailoring/>
                         <pseudo-analysis/>
                         <pseudo-decision/>
                         <individual-analysis/>
                         <individual-decision required="always"/>
                         <contact required="always"/>
                         <historical/>
                         <telemarketing/>
                         <other-purpose/>
                         <extension/>
                    </PURPOSE>
               </STATEMENT>
          </POLICY>
     </appel:RULE>
     <appel:RULE behavior="block">
          <POLICY>
               <STATEMENT>
                    <RECIPIENT appel:connective="or">
                         <delivery/>
                         <other-recipient/>
                         <unrelated/>
                         <public/>
                         <extension/>
                    </RECIPIENT>
               </STATEMENT>
          </POLICY>
     </appel:RULE>
     <appel:RULE behavior="request"/>
          <appel:OTHERWISE/>
     </appel:RULE>
</appel:RULESET>
```

Σχήμα 2: Παράδειγμα Προτιμήσεων Ιδιωτικότητας Χρήστη σε APPEL.

Αξίζει να σημειωθεί ότι οι προτιμήσεις ιδιωτικότητας του υποθετικού χρήστη όπως εκφράζονται στο Σχήμα 2 ικανοποιούνται από την πολιτική ιδιωτικότητας του υποθετικού Διαδικτυακού καταστήματος όπως παρουσιάζεται στο Σχήμα 1. Ο πρώτος κανόνας που τίθεται από το χρήστη αναφορικά με το σκοπό συλλογής και χρήση των δεδομένων δεν ενεργοποιείται καθώς ο σκοπός που δηλώνει το Διαδικτυακό κατάστημα στο πρώτο `STATEMENT` δεν περιλαμβάνεται μεταξύ των αυτών που αποκλείονται από το χρήστη, ενώ για τους σκοπούς του δεύτερου `STATEMENT` του Διαδικτυακού καταστήματος όπου έχουν δηλωθεί `opt-in`, η επιθυμία του χρήστη είναι `required="always"` οπότε και πάλι δεν υπάρχει ταίριασμα. Αντίστοιχα, ο δεύτερος κανόνας που έχει προδιαγραφεί από το χρήστη δεν ενεργοποιείται, καθώς οι πιθανοί αποδέκτες των προσωπικών δεδομένων που αποκλείονται από το χρήστη δεν περιλαμβάνονται στους πιθανούς αποδέκτες όπως προδιαγράφονται από το Διαδικτυακό κατάστημα.

Η πλατφόρμα P3P συμπεριλαμβανομένης και της γλώσσας APPEL έχουν δεχθεί γενικά αρκετή κριτική για την αποτελεσματικότητά τους. Διάφοροι ερευνητές εστιάζουν στην αναποτελεσματικότητα ορισμένων μηχανισμών και προτείνουν τροποποιήσεις ή συμπληρωματικούς μηχανισμούς για την κάλυψη των ελλείψεων. Για παράδειγμα, στο [51] επισημαίνονται διάφορα μειονεκτήματα της γλώσσας APPEL που αποτελούν σύμφωνα με τους συγγραφείς προϊόν λανθασμένων σχεδιαστικών επιλογών της γλώσσας και έχουν σαν αποτέλεσμα διάφορα προβλήματα, όπως την απόρριψη, σε κάποιες περιπτώσεις, συμβατών πολιτικών ιδιωτικότητας. Για το σκοπό αυτό, οι συγγραφείς προτείνουν μία εναλλακτική γλώσσα βασισμένη στο πρότυπο XPath [52], [53]. Ανάλογα, στο [54] επισημαίνονται προβλήματα τόσο της πλατφόρμας P3P όσο και της γλώσσας APPEL, με ιδιαίτερη έμφαση στις σημασιολογικές ανακολουθίες και αντιφάσεις. Για παράδειγμα, οι συγγραφείς δείχνουν ότι εάν η ίδια πολιτική ιδιωτικότητας συνταχθεί με διαφορετικό τρόπο, μπορεί στην πράξη να οδηγήσει σε εντελώς διαφορετικά αποτελέσματα. Σε παρόμοια συμπεράσματα έχουν καταλήξει και άλλοι ερευνητές, όπως, για παράδειγμα, στα [55] και [56].

Το μεγαλύτερο πρόβλημα της πλατφόρμας P3P, ωστόσο, είναι ότι δίνει απλώς τη δυνατότητα στους Διαδικτυακούς τόπους να εκφράσουν υποσχέσεις αναφορικά με την προστασία των προσωπικών δεδομένων. Δεν υπάρχει μηχανισμός που να διασφαλίζει το χρήστη ότι οι υποσχέσεις αυτές θα τηρηθούν. Επιπλέον, δε δίνεται η δυνατότητα στο

χρήστη να προκαθορίσει ο ίδιος τον τρόπο επεξεργασίας των προσωπικών του δεδομένων.

3.1.2 Ιπποκρατικές Βάσεις Δεδομένων

Μία από τις πρώτες και πλέον επιδραστικές προσεγγίσεις για την ενσωμάτωση των βασικών αρχών περί προστασίας της ιδιωτικότητας στις διαδικασίες ελέγχου πρόσβασης σε δεδομένα αποτελούν οι Ιπποκρατικές Βάσεις Δεδομένων (Hippocratic Databases), οι οποίες οφείλουν το όνομά τους στο ακόλουθο απόσπασμα από τον Όρκο του Ιπποκράτη: «*Και ό,τι δω ή ακούσω κατά την άσκηση του επαγγέλματός μου, ή κι εκτός, για τη ζωή των ανθρώπων, που δεν πρέπει ποτέ να κοινοποιηθεί, [ορκίζομαι] να σιωπήσω και να το τηρήσω μυστικό*»[1]. Η ιδέα των Ιπποκρατικών Βάσεων Δεδομένων παρουσιάστηκε το 2002 από ομάδα ερευνητών της εταιρείας IBM, η οποία θέλησε να καταστήσει τα Σχεσιακά Συστήματα Βάσεων Δεδομένων (Relational Database Systems) συμβατά με τις βασικές αρχές προστασίας της ιδιωτικότητας [57].

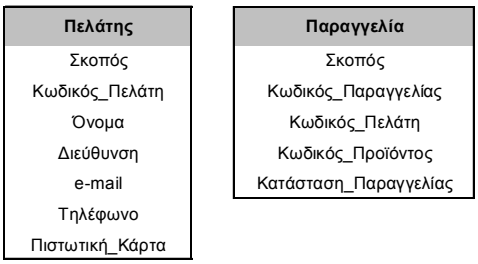
Οι έννοιες του σκοπού (purpose) και των μεταδεδομένων ιδιωτικότητας (privacy metadata) αποτελούν τους βασικούς άξονες των Ιπποκρατικών Βάσεων Δεδομένων. Ο σκοπός αντιπροσωπεύει την προτιθέμενη χρήση των πληροφοριών που αποθηκεύονται στη βάση δεδομένων, ενώ για κάθε σκοπό και για κάθε πληροφορία που συλλέγεται για το σκοπό αυτό τα μεταδεδομένα ιδιωτικότητας ορίζουν:

- τους εξωτερικούς-αποδέκτες (external-recipients), δηλαδή τις οντότητες στις οποίες θα κοινοποιηθεί η πληροφορία,
- την περίοδο-διατήρησης (retention-period), δηλαδή τη χρονική διάρκεια αποθήκευσης της πληροφορίας, και
- τους εξουδιοδοτημένους-χρήστες (authorized-users), δηλαδή το σύνολο των χρηστών (ανθρώπων ή διεργασιών του υποκείμενου συστήματος) που μπορούν να προσπελάσουν την πληροφορία.

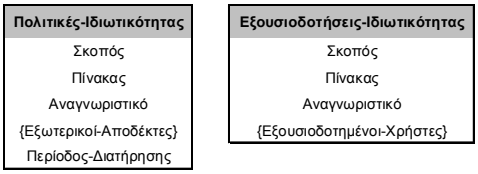
Στο πλαίσιο αυτό, σε κάθε πίνακα της βάσης δεδομένων προστίθεται το αναγνωριστικό (attribute) «Σκοπός». Έτσι, οι δύο πίνακες («Πελάτης» και «Παραγγελία»)

[1] Το απόσπασμα προέρχεται από τη μετάφραση του Όρκου στη νέα Ελληνική, όπως παρατίθεται στην ιστοσελίδα της Ιατρικής Σχολής του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών, http://www.med.uoa.gr/orkoi.php.

του υποθετικού σχήματος της βάσης δεδομένων ενός βιβλιοπωλείου υφίσταται το σχετικό μετασχηματισμό, όπως φαίνεται στο Σχήμα 3. Αναφορικά με τα μεταδεδομένα ιδιωτικότητας, αυτά καταχωρούνται στη βάση δεδομένων σε δύο επιπλέον πίνακες (Σχήμα 4): Πολιτικές-Ιδιωτικότητας (Privacy-Policies) και Εξουσιοδοτήσεις-Ιδιωτικότητας (Privacy-Authorizations). Ο πρώτος πίνακας εκφράζει ουσιαστικά για κάθε αναγνωριστικό ενός πίνακα της βάσης δεδομένων τους επιτρεπτούς σκοπούς, τους εξωτερικούς αποδέκτες και την περίοδο διατήρησης, ενώ ο δεύτερος εκφράζει τους σκοπούς για τους οποίους ο κάθε χρήστης είναι εξουσιοδοτημένος.



Σχήμα 3: Σχήμα Βάσης Δεδομένων



Σχήμα 4: Σχήμα Μεταδεδομένων Ιδιωτικότητας

Ένα παράδειγμα πίνακα πολιτικών ιδιωτικότητας για τη βάση δεδομένων του βιβλιοπωλείου παρουσιάζεται στο Σχήμα 5. Σύμφωνα με το παράδειγμα, για το σκοπό «Αγορά»:

- Για όλα τα αναγνωριστικά ορίζεται περίοδος διατήρησης ίση με ένα μήνα.
- Το όνομα του αγοραστή και η διεύθυνσή του διατίθενται στο φορέα που θα πραγματοποιήσει την παράδοση των προϊόντων («εταιρεία-παράδοσης»).
- Το όνομα του αγοραστή και οι πληροφορίες της πιστωτικής του κάρτας διατίθενται στο σχετικό πιστωτικό φορέα.

Από την άλλη, για διαφορετικούς σκοπούς ορίζονται μεγαλύτεροι χρόνοι διατήρησης, ενώ αποκλείονται τυχόν εξωτερικοί αποδέκτες.

Σκοπός	Πίνακας	Αναγνωριστικό	Εξωτερικοί-Αποδέκτες	Περίοδος-Διατήρησης
Αγορά	Πελάτης	Όνομα	{εταιρεία-παράδοσης, πιστωτικός-φορέας}	1 μήνας
Αγορά	Πελάτης	Διεύθυνση	{εταιρεία-παράδοσης}	1 μήνας
Αγορά	Πελάτης	e-mail	*κενό*	1 μήνας
Αγορά	Πελάτης	Πιστωτική_Κάρτα	{πιστωτικός-φορέας}	1 μήνας
Αγορά	Παραγγελία	Κωδικός_Προϊόντος	*κενό*	1 μήνας
Εγγραφή	Πελάτης	Όνομα	*κενό*	3 χρόνια
Εγγραφή	Πελάτης	Διεύθυνση	*κενό*	3 χρόνια
Εγγραφή	Πελάτης	e-mail	*κενό*	3 χρόνια
Προτάσεις-Αγοράς	Παραγγελία	Κωδικός_Προϊόντος	*κενό*	10 χρόνια

Σχήμα 5: Πίνακας Πολιτικές-Ιδιωτικότητας

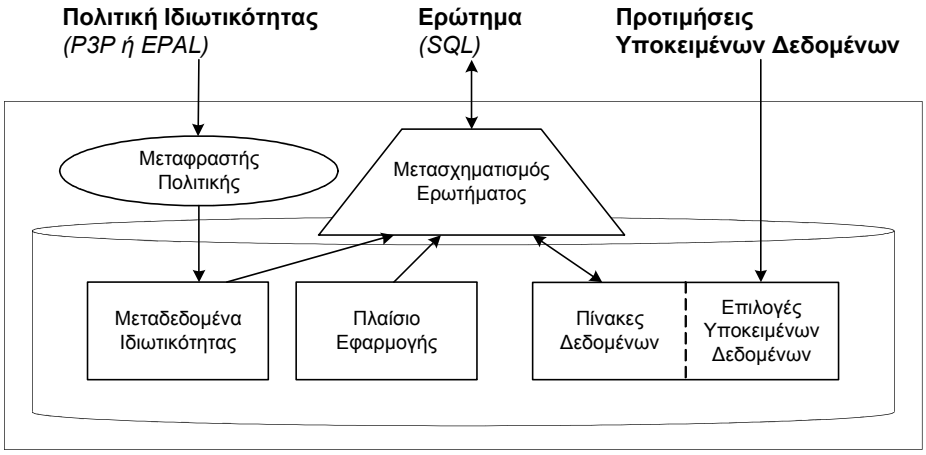
Σκοπός	Πίνακας	Αναγνωριστικό	Εξουσιοδοτημένοι-Χρήστες
Αγορά	Πελάτης	Κωδικός_Πελάτη	*όλοι*
Αγορά	Πελάτης	Όνομα	{εφαρμογή-παράδοσης, εφαρμογή-χρέωσης, εξυπηρέτηση-πελατών}
Αγορά	Πελάτης	Διεύθυνση	{εφαρμογή-παράδοσης}
Αγορά	Πελάτης	e-mail	{εφαρμογή-παράδοσης, εξυπηρέτηση-πελατών}
Αγορά	Πελάτης	Πιστωτική_Κάρτα	{εφαρμογή-χρέωσης}
Αγορά	Παραγγελία	Κωδικός_Παραγγελίας	*όλοι*
Αγορά	Παραγγελία	Κωδικός_Πελάτη	*όλοι*
Αγορά	Παραγγελία	Κωδικός_Προϊόντος	{εφαρμογή-παράδοσης}
Αγορά	Παραγγελία	Κατάσταση_Παραγγελίας	{εφαρμογή-παράδοσης, εξυπηρέτηση-πελατών}
Εγγραφή	Πελάτης	Κωδικός_Πελάτη	*όλοι*
Εγγραφή	Πελάτης	Όνομα	{εφαρμογή-εγγραφής, εξυπηρέτηση-πελατών}
Εγγραφή	Πελάτης	Διεύθυνση	{εφαρμογή-εγγραφής}
Εγγραφή	Πελάτης	e-mail	{εφαρμογή-εγγραφής, εξυπηρέτηση-πελατών}

Σχήμα 6: Πίνακας Εξουσιοδοτήσεις-Ιδιωτικότητας

Το Σχήμα 6 παρουσιάζει τον αντίστοιχο πίνακα των εξουσιοδοτήσεων ιδιωτικότητας. Σύμφωνα με το παράδειγμα, κάποιο λογισμικό σύστημα «εφαρμογή-παράδοσης» έχει δικαίωμα πρόσβασης στο όνομα, τη διεύθυνση και το e-mail του αγοραστή καθώς και στον κωδικό των προϊόντων που θα παραδοθούν, ενώ κάποια «εφαρμογή-χρέωσης» δικαιούται πρόσβαση στο όνομα και τις πληροφορίες της πιστωτικής κάρτας του αγοραστή.

Για την πρακτική εφαρμογή των αρχών των Ιπποκρατικών Βάσεων Δεδομένων, προτάθηκε από την ομάδα της IBM η αρχιτεκτονική που παρουσιάζεται στο Σχήμα 7 [58]. Η λειτουργική λογική της βασίζεται στην αρχή ότι όταν υποβάλλεται κάποιο ερώτημα (query) στη βάση δεδομένων, το ερώτημα αυτό μετασχηματίζεται από τη βάση δεδομένων ούτως ώστε το αποτέλεσμά του να συμμορφώνεται με τις πολιτικές ιδιωτικότητας αλλά και τις προτιμήσεις των υποκειμένων των δεδομένων. Λαμβάνεται επιπλέον υπόψη το εκάστοτε πλαίσιο εφαρμογής, το οποίο αποτελείται ουσιαστικά από το σκοπό με τον οποίο είναι συσχετισμένο το ερώτημα, καθώς και από τους αποδέκτες των αποτελεσμάτων. Η λειτουργία των Ιπποκρατικών Βάσεων Δεδομένων λαμβάνει

χώρα σε τρία στάδια: δημιουργία πολιτικής ιδιωτικότητας, διαπραγμάτευση προτιμήσεων και προσκόμιση δεδομένων, τα οποία συνοψίζονται στη συνέχεια.



Σχήμα 7: Επισκόπηση Αρχιτεκτονικής Υλοποίησης Ιπποκρατικών Βάσεων Δεδομένων

Κατά το στάδιο της δημιουργίας της πολιτικής ιδιωτικότητας, ο οργανισμός ο οποίος συλλέγει και επεξεργάζεται προσωπικά δεδομένα προδιαγράφει την πολιτική ιδιωτικότητας. Η πολιτική ορίζει τους κανόνες που καθορίζουν την πρόσβαση στα δεδομένα και την περαιτέρω διάθεσή τους με βάση τις εξουσιοδοτήσεις του χρήστη που υποβάλλει το ερώτημα, το δεδηλωμένο σκοπό του ερωτήματος και τους δυνητικούς αποδέκτες των αποτελεσμάτων. Επιπλέον, η πολιτική μπορεί να δίνει τη δυνατότητα επιλογής (opt-in) ή απαλλαγής (opt-out) στα υποκείμενα των δεδομένων αναφορικά με συγκεκριμένες ενέργειες επί των δεδομένων τους.

Η προδιαγραφή της πολιτικής ιδιωτικότητας μπορεί να πραγματοποιηθεί χρησιμοποιώντας κάποια σχετική γλώσσα περιγραφής, όπως την P3P (βλ. Ενότητα 3.1.1) ή την EPAL (βλ. Ενότητα 3.1.5). Από εκεί και πέρα, η πολιτική μετασχηματίζεται στην επιθυμητή μορφή των μεταδεδομένων ιδιωτικότητας τα οποία θα αποθηκευτούν τελικά στην Ιπποκρατική Βάση Δεδομένων.

Το στάδιο της διαπραγμάτευσης των προτιμήσεων αφορά ουσιαστικά δύο πράγματα: την προδιαγραφή προτιμήσεων ιδιωτικότητας από την πλευρά του υποκειμένου των δεδομένων και την αντιπαραβολή των προτιμήσεων αυτών με την πολιτική ιδιωτικότητας του οργανισμού. Ανάλογα με την υλοποίηση, το υποκείμενο των δεδομένων μπορεί να έχει τη δυνατότητα μέσω π.χ. κάποιας γραφικής διεπαφής να περιγράψει συνοπτικά ή λεπτομερώς τις προτιμήσεις του αναφορικά με την τύχη των

προσωπικών δεδομένων, ενώ μπορεί επίσης να προβλέπεται διαδραστικότητα ούτως ώστε οι ασυμβατότητες μεταξύ της πολιτικής ιδιωτικότητας και των προτιμήσεων να επιλύονται.

Το στάδιο της προσκόμισης των δεδομένων περιλαμβάνει την υποβολή, το μετασχηματισμό και την εκτέλεση του ερωτήματος στη βάση δεδομένων. Αποτελεί δηλαδή το στάδιο εκείνο κατά το οποίο εφαρμόζεται ο έλεγχος πρόσβασης στην πράξη, λαμβάνοντας υπόψη το εκάστοτε πλαίσιο της εφαρμογής, δηλαδή το σκοπό του ερωτήματος και τους αποδέκτες των αποτελεσμάτων.

Για την εφαρμογή της αρχής της περιορισμένης αποκάλυψης των δεδομένων, η ομάδα της IBM πρότεινε δύο διαφορετικά μοντέλα, το μοντέλο σημασιολογίας πίνακα (table semantics model) και το μοντέλο σημασιολογίας ερωτήματος (query semantics model). Εννοιολογικά, το πρώτο μοντέλο ορίζει μία όψη (view) του κάθε πίνακα της βάσης δεδομένων για κάθε συνδυασμό {σκοπός, αποδέκτες}, σύμφωνα με την πολιτική ιδιωτικότητας. Έτσι, οι όψεις αυτές ορίζουν μία νοητή βάση δεδομένων για κάθε συνδυασμό {σκοπός, αποδέκτες}, η οποία είναι ανεξάρτητη από το εκάστοτε ερώτημα· τα ερωτήματα υποβάλλονται και αποτιμώνται ως προς τη βάση δεδομένων αυτή. Από την άλλη, το μοντέλο σημασιολογίας ερωτήματος λαμβάνει υπόψη το εκάστοτε ερώτημα και αναλόγως πραγματοποιεί τη νοητή τροποποίηση των πινάκων. Και στα δύο μοντέλα, τα απαγορευμένα από την πολιτική ιδιωτικότητας κελιά λαμβάνουν την ειδική τιμή null της γλώσσας SQL η οποία έχει την έννοια «καμία τιμή».

Για παράδειγμα, έστω η βάση δεδομένων ενός νοσοκομείου και δύο πίνακες της βάσης, τον πίνακα «Ασθενείς» και τον πίνακα «Νοσοκόμοι». Σύμφωνα με την πολιτική ιδιωτικότητας του νοσοκομείου, προκειμένου κάποιος νοσοκόμος να αποκτήσει πρόσβαση στο ιστορικό ενός ασθενούς για κάποιο σκοπό «πραγματοποίηση φαρμακευτικής αγωγής», ο νοσοκόμος πρέπει να υπηρετεί στον όροφο όπου νοσηλεύεται ο ασθενής. Το Σχήμα 8 παρουσιάζει το σχετικό μετασχηματισμό. Κάποιος νοσοκόμος υποβάλλει στη βάση δεδομένων το απλό SQL ερώτημα που φαίνεται στο Σχήμα 8 (α) για τον παραπάνω σκοπό. Το ερώτημα επεκτείνεται με την αξιολόγηση της συνθήκης που ορίζεται από την πολιτική ιδιωτικότητας, όπως φαίνεται στο Σχήμα 8 (β) και επιστρέφει το ιστορικό του ασθενούς μόνο στην περίπτωση που η συνθήκη ικανοποιείται· διαφορετικά, επιστρέφει την τιμή `null`, αποκρύπτοντας την πληροφορία. Η παράμετρος

$USERID του Σχήματος αντιστοιχεί στη μεταβλητή του πλαισίου εφαρμογής που ταυτοποιεί το νοσοκόμο από τον οποίο υποβάλλεται το ερώτημα.

```
SELECT ιστορικό_ασθενούς
  FROM Ασθενείς
```

(α)

```
SELECT
       CASE WHEN EXIST
                (SELECT Κωδικός_Νοσοκόμου
                   FROM Νοσοκόμοι
                  WHERE Ασθενείς.όροφος_νοσηλείας = Νοσοκόμοι.όροφος_υπηρεσίας
                    AND $USERID = Νοσοκόμοι.Κωδικός_Νοσοκόμου)
          THEN ιστορικό_ασθενούς
          ELSE null
       END
  FROM Ασθενείς
```

(β)

Σχήμα 8: Παράδειγμα Μετασχηματισμού Ερωτήματος

3.1.3 Έλεγχος Πρόσβασης Βάσει Σκοπού

Οι Ιπποκρατικές Βάσεις Δεδομένων αποτέλεσαν το πρώτο βήμα για την προδιαγραφή συστημάτων βάσεων δεδομένων τα οποία λαμβάνουν υπόψη την προστασία της ιδιωτικότητας και ενέπνευσαν αρκετές αντίστοιχες ερευνητικές προσπάθειες (βλ. π.χ., [54]). Μία από τις πιο σημαντικές και αντιπροσωπευτικές προσεγγίσεις αποτελεί το μοντέλο Ελέγχου Πρόσβασης Βάσει Σκοπού (Purpose Based Access Control – PBAC), το οποίο πρωτοπαρουσιάστηκε το 2004 από ομάδα ερευνητών του Πανεπιστημίου Perdue των ΗΠΑ [59][60], ενώ στη συνέχεια εξελίχθηκε σε μεγάλο βαθμό [61]. Η βασική συνεισφορά του μοντέλου αυτού είναι ο αναλυτικός ορισμός της έννοιας του σκοπού, ο οποίος παρουσιάζεται στη συνέχεια της Ενότητας. Αναφορικά με το χαρακτηρισμό των δεδομένων (data labeling), δηλαδή τον τρόπο με τον οποίο τα δεδομένα συσχετίζονται με τους σκοπούς, το μοντέλο PBAC ορίζει ένα ευέλικτο σχήμα που πραγματοποιεί τις συσχετίσεις σε διαφορετικά επίπεδα, από μεμονωμένα κελιά ενός πίνακα μέχρι ολόκληρο πίνακα της βάσης δεδομένων. Για τη διαχείριση των ρόλων, το μοντέλο PBAC υιοθετεί μία προσέγγιση που βασίζεται στο μοντέλο RBAC ([43]), ενώ, όπως και στις Ιπποκρατικές Βάσεις Δεδομένων, τα ερωτήματα υφίστανται μετασχηματίζονται μετά την υποβολή τους.

Η έννοια του σκοπού παίζει τον κεντρικό ρόλο στο μοντέλο PBAC, καθώς αποτελεί την κύρια παράμετρο βάσει της οποίας λαμβάνονται οι αποφάσεις αναφορικά με την πρόσβαση στα δεδομένα. Το μοντέλο PBAC ορίζει μία ιεραρχική οργάνωση στο

σύνολο των σκοπών *P*, υπό μορφή δέντρου το οποίο καλείται *Δέντρο Σκοπών* (Purpose Tree – *PT*). Κάθε κόμβος του δέντρου αντιπροσωπεύει κάποιο σκοπό στο *P*, ενώ κάθε ακμή αντιπροσωπεύει μία ιεραρχική σχέση μεταξύ δύο σκοπών, εκφράζει δηλαδή κάποια σχέση γενίκευσης και ειδίκευσης μεταξύ δύο σκοπών. Στο Σχήμα 9 παρουσιάζεται ένα παράδειγμα Δέντρου Σκοπών.

Σχήμα 9: Δέντρο Σκοπών

Για κάθε σκοπό p_i ενός Δέντρου Σκοπών *PT* ορίζονται δύο σύνολα:

- Σύνολο Des(p_i), το οποίο περιλαμβάνει όλους τους απογόνους (descendants) του p_i, δηλαδή κάθε σκοπό $p_j \in P$ για τον οποίο υπάρχει ένα καθοδικό μονοπάτι από τον p_i στον p_j.
- Σύνολο Anc(p_i), το οποίο περιλαμβάνει τους προγόνους (ancestors) του p_i, δηλαδή κάθε σκοπό $p_j \in P$ για τον οποίο υπάρχει ένα ανοδικό μονοπάτι από τον p_i στον p_j.

Σημειώνεται ότι ο σκοπός p_i συμπεριλαμβάνεται και στα δύο αυτά σύνολα. Έτσι, αναφορικά με το σκοπό «μέσω-Συνεργάτη» ο οποίος εκφράζει την προώθηση προϊόντων μέσω κάποιου τρίτου φορέα-συνεργάτη (π.χ., κάποια εταιρεία προώθησης), ορίζονται τα σύνολα:

- Des(μέσω-Συνεργάτη) = {μέσω-Συνεργάτη, Σ-Email, Σ-Ταχυδρομικά}.
- Anc(μέσω-Συνεργάτη) = {μέσω-Συνεργάτη, Προώθηση, Γενικός-Σκοπός}.

Το μοντέλο PBAC διαχωρίζει τους Προτιθέμενους Σκοπούς (Intended Purposes) από τους Σκοπούς Πρόσβασης (Access Purposes). Οι πρώτοι αντιστοιχούν στους σκοπούς που έχουν συσχετιστεί με τα δεδομένα και ρυθμίζουν την πρόσβαση σε αυτά,

αποτελώντας ουσιαστικά την περίληψη της υποκείμενης πολιτικής ιδιωτικότητας. Από την άλλη, ένας Σκοπός Πρόσβασης αντιστοιχεί στον ιδιαίτερο σκοπό μίας συγκεκριμένης ενέργειας πρόσβασης στα δεδομένα. Η απόφαση αναφορικά με την πρόσβαση στα δεδομένα λαμβάνεται τελικά με βάση τη συσχέτιση μεταξύ των αντίστοιχων Σκοπών Πρόσβασης και Προτιθέμενων Σκοπών, όπως θα περιγραφεί στη συνέχεια.

Οι περισσότερες πολιτικές και προτιμήσεις ιδιωτικότητας είναι εκ φύσεως «θετικές», υπό την έννοια ότι οι εκάστοτε δεδηλωμένοι σκοποί είναι επιτρεπόμενοι, δηλαδή λειτουργούν ως επιλεκτικό κριτήριο για την παροχή πρόσβασης στα αντίστοιχα δεδομένα. Στο πλαίσιο αυτό, υπονοείται ότι η απουσία ενός σκοπού από το σύνολο των επιτρεπόμενων σκοπών συνεπάγεται ότι η πρόσβαση για το σκοπό αυτό δεν είναι επιτρεπτή. Η προσέγγιση αυτή έχει υιοθετηθεί και από τα περισσότερα μοντέλα, όπως το P3P. Αντίθετα, το μοντέλο PBAC εισάγει ένα διαχωρισμό μεταξύ των θετικών και των αρνητικών πολιτικών ιδιωτικότητας. Έτσι, το μοντέλο ορίζει τους Επιτρεπόμενους Προτιθέμενους Σκοπούς (Allowed Intended Purposes – AIP) και τους Απαγορευμένους Προτιθέμενους Σκοπούς (Prohibited Intended Purposes – PIP). Η δομή αυτή παρέχει μεγαλύτερη ευελιξία στην άσκηση ελέγχου πρόσβασης, ενώ η χρήση των PIP διασφαλίζει ότι δε θα επιτραπεί ποτέ η πρόσβαση σε δεδομένα για κάποιους συγκεκριμένους σκοπούς. Σε περίπτωση που υπάρχει αντίθεση μεταξύ των επιτρεπόμενων και απαγορευμένων σκοπών σε κάποια δεδομένα, υπερισχύει ο απαγορευμένος σκοπός.

Το μοντέλο PBAC ορίζει τελικά ως έναν Προτιθέμενο Σκοπό IP, σχετιζόμενο με κάποια δεδομένα, την πλειάδα ⟨AIP, PIP⟩, δηλαδή μία δομή η οποία περιλαμβάνει το σύνολο των δεδηλωμένων επιτρεπόμενων σκοπών AIP, καθώς και το σύνολο των απαγορευμένων σκοπών PIP.

Σύμφωνα με το μοντέλο PBAC, όταν κάποιος σκοπός p_j δηλώνεται ως Επιτρεπόμενος Προτιθέμενος Σκοπός (δηλαδή $p_j \in$ AIP), τότε και οι απόγονοί του θεωρούνται ως επιτρεπόμενοι. Από την άλλη, όταν κάποιος σκοπός p_k δηλώνεται ως Απαγορευμένος Προτιθέμενος Σκοπός (δηλαδή $p_k \in$ PIP), τότε τόσο οι απόγονοί του όσο και οι πρόγονοί του θεωρούνται ως απαγορευμένοι. Έτσι, ορίζονται τα εξής σύνολα:

- Σύνολο Συνεπαγόμενων Επιτρεπόμενων Προτιθέμενων Σκοπών $AIP^{\uparrow}$, το οποίο περιλαμβάνει όλους τους απογόνους όλων των σκοπών aip_j του AIP, δηλαδή:

$$\text{AIP}^{\uparrow} = \bigcup_{aip_j \in AIP} \text{Des}(aip_j)$$

- Σύνολο Συνεπαγόμενων Απαγορευμένων Προτιθέμενων Σκοπών $\text{PIP}^{\uparrow\downarrow}$, το οποίο περιλαμβάνει όλους τους προγόνους και απογόνους όλων των σκοπών pip_k του PIP, δηλαδή:

$$\text{PIP}^{\uparrow\downarrow} = (\bigcup_{pip_k \in PIP} \text{Anc}(pip_k)) \bigcup (\bigcup_{pip_k \in PIP} \text{Des}(pip_k))$$

Είναι προφανές ότι η διαφορά των δύο αυτών συνόλων εκφράζει το σύνολο (IP^*) όλων των προτιθέμενων σκοπών για τους οποίους τελικά θα επιτραπεί η πρόσβαση, δηλαδή $IP^* = \text{AIP}^{\uparrow} - \text{PIP}^{\uparrow\downarrow}$.

Για παράδειγμα, θεωρώντας το Δέντρο Σκοπών *PT* που παρουσιάζεται στο Σχήμα 9 και ότι ένας Προτιθέμενος Σκοπός *IP* ορίζεται στο δέντρο αυτό ως εξής: *IP* = ⟨{Διαχείριση, Απευθείας}, {A-Email}⟩. Τότε, τα σύνολα $\text{AIP}^{\uparrow}$, $\text{PIP}^{\uparrow\downarrow}$ και IP^* προκύπτουν αντίστοιχα:

- $\text{AIP}^{\uparrow} = \text{Des}(\text{Διαχείριση}) \bigcup \text{Des}(\text{Απευθείας}) \Rightarrow$

  $\text{AIP}^{\uparrow}$ = {Διαχείριση, Ανάλυση, Διαχείριση-Προφίλ} ⋃ {Απευθείας, A-Email, A-Τηλέφωνο, Ειδικές-Προσφορές, Αναβάθμιση-Υπηρεσιών} ⇒

  $\text{AIP}^{\uparrow}$ = {Διαχείριση, Ανάλυση, Διαχείριση-Προφίλ, Απευθείας, A-Email, A-Τηλέφωνο, Ειδικές-Προσφορές, Αναβάθμιση-Υπηρεσιών}.

- $\text{PIP}^{\uparrow\downarrow} = \text{Anc}(\text{A-Email}) \bigcup \text{Des}(\text{A-Email}) \Rightarrow$

  $\text{PIP}^{\uparrow\downarrow}$ = {A-Email, Απευθείας, Προώθηση, Γενικός-Σκοπός} ⋃ {A-Email, Ειδικές-Προσφορές, Αναβάθμιση-Υπηρεσιών} ⇒

  $\text{PIP}^{\uparrow\downarrow}$ = {A-Email, Απευθείας, Προώθηση, Γενικός-Σκοπός, Ειδικές-Προσφορές, Αναβάθμιση-Υπηρεσιών}.

- $IP^* = \text{AIP}^{\uparrow} - \text{PIP}^{\uparrow\downarrow} \Rightarrow$

  IP^* = {Διαχείριση, Ανάλυση, Διαχείριση-Προφίλ, Απευθείας, A-Email, A-Τηλέφωνο, Ειδικές-Προσφορές, Αναβάθμιση-Υπηρεσιών} – {A-Email, Απευθείας, Προώθηση, Γενικός-Σκοπός, Ειδικές-Προσφορές, Αναβάθμιση-Υπηρεσιών} ⇒

  IP^* = {Διαχείριση, Ανάλυση, Διαχείριση-Προφίλ, A-Τηλέφωνο}.

Όπως προαναφέρθηκε, ένας Σκοπός Πρόσβασης εκφράζει τον ιδιαίτερο σκοπό μίας συγκεκριμένης ενέργειας πρόσβασης σε δεδομένα. Προκειμένου να παρθεί μία

απόφαση πρόσβασης, εξετάζεται η σχέση μεταξύ του Σκοπού Πρόσβασης *AP* και του Προτιθέμενου Σκοπού *IP* που έχει συσχετιστεί με τα αντίστοιχα δεδομένα. Συγκεκριμένα, προκειμένου να επιτραπεί η ζητούμενη πρόσβαση, ο σκοπός *AP* πρέπει να περιλαμβάνεται μεταξύ των Συνεπαγόμενων Επιτρεπόμενων Προτιθέμενων Σκοπών $\text{AIP}^{\uparrow}$, αλλά να μην ανήκει στο σύνολο των Συνεπαγόμενων Απαγορευμένων Προτιθέμενων Σκοπών $\text{PIP}^{\uparrow\downarrow}$. Την κατάσταση αυτή, το μοντέλο PBAC την ορίζει ως Συμμόρφωση του Σκοπού Πρόσβασης (Access Purpose Compliance) και ισχύει όταν και μόνο όταν ικανοποιούνται οι σχέσεις $AP \in \text{AIP}^{\uparrow}$ και $AP \notin \text{PIP}^{\uparrow\downarrow}$, δηλαδή όταν $AP \in IP^{*}$.

3.1.4 Η Επεκτάσιμη Γλώσσα Σήμανσης Ελέγχου Πρόσβασης (XACML)

Μία πολύ αξιόλογη προσπάθεια προδιαγραφής μίας δομημένης γλώσσας για την προδιαγραφή πολιτικών ιδιωτικότητας και κανόνων που θα μπορούν να είναι ευθέως εφαρμόσιμοι από τα αντίστοιχα συστήματα έχει πραγματοποιηθεί από τον οργανισμό Organization for the Advancement of Structured Information Standards (OASIS) [62], με την προδιαγραφή της Επεκτάσιμης Γλώσσας Σήμανσης Ελέγχου Πρόσβασης (eXtensible Access Control Markup Language – XACML) καθώς και της αρχιτεκτονικής για την εφαρμογή της [63]. Η γλώσσα XACML επιτυγχάνει να ικανοποιεί τις τέσσερις βασικές απαιτήσεις για τις δομημένες γλώσσες έκφρασης και εφαρμογής πολιτικών ιδιωτικότητας όπως αυτές συνοψίζονται στο [42]. Η γλώσσα XACML βασίστηκε σε μεγάλο βαθμό στην προγενέστερη γλώσσα XML Γλώσσα για Έλεγχο Πρόσβασης (XML Access Control Language – XACL) [64]. Η XACML είναι μία γλώσσα γενικού σκοπού για την άσκηση ελέγχου πρόσβασης, ενώ είναι ανεξάρτητη των υποκείμενων συστημάτων. Η βασική της προδιαγραφή επεκτείνεται μέσω των λεγόμενων προφίλ (profiles) τα οποία την καθιστούν ένα πολύ δυνατό εργαλείο περιγραφής πολιτικών. Στο πλαίσιο αυτό, ορίζεται και το προφίλ πολιτικής ιδιωτικότητας (privacy policy profile), το οποίο δίνει τη δυνατότητα διαχείρισης της έννοιας του σκοπού στο πλαίσιο μίας πολιτικής.

Η γλώσσα XACML ακολουθεί το αφαιρετικό μοντέλο για την εφαρμογή πολιτικών το οποίο έχει οριστεί από τον οργανισμό Internet Engineering Task Force (IETF) [65] και το Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization – ISO) [66]. Σύμφωνα με το μοντέλο αυτό [67][68][69], όλες οι αιτήσεις για πρόσβαση σε κάποιο προστατευμένο πόρο περνούν από κάποιο αφαιρετικό δομικό στοιχείο, το Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point – PEP), το οποίο

διαμορφώνει ένα αίτημα αναφορικά με σχετική απόφαση εξουσιοδότησης, το οποίο περιλαμβάνει μία περιγραφή τη αίτησης πρόσβασης: ποιος πραγματοποιεί την αίτηση πρόσβασης, ποιος πόρος αποτελεί το αντικείμενό της, τι λειτουργία ή ενέργεια πρόκειται να πραγματοποιηθεί, ποιος είναι ο σκοπός της, καθώς και κάθε άλλη σχετική πληροφορία.

Το αίτημα για απόφαση εξουσιοδότησης αποστέλλεται σε κάποιο άλλο αφαιρετικό δομικό στοιχείο, το Σημείο Απόφασης Πολιτικής (Policy Decision Point – PDP). Το σημείο PDP ανακτά τις πολιτικές που βρίσκουν εφαρμογή στο εν λόγω αίτημα μαζί με οποιαδήποτε άλλη πληροφορία μπορεί να απαιτείται αναφορικά με την αποτίμηση του αιτήματος και προβαίνει στην αποτίμηση του αιτήματος. Το αποτέλεσμα της αποτίμησης διαβιβάζεται στο σημείο PEP, το οποίο με τη σειρά του το εφαρμόζει, επιτρέποντας ή απαγορεύοντας την πρόσβαση στον εν λόγω προστατευμένο πόρο.

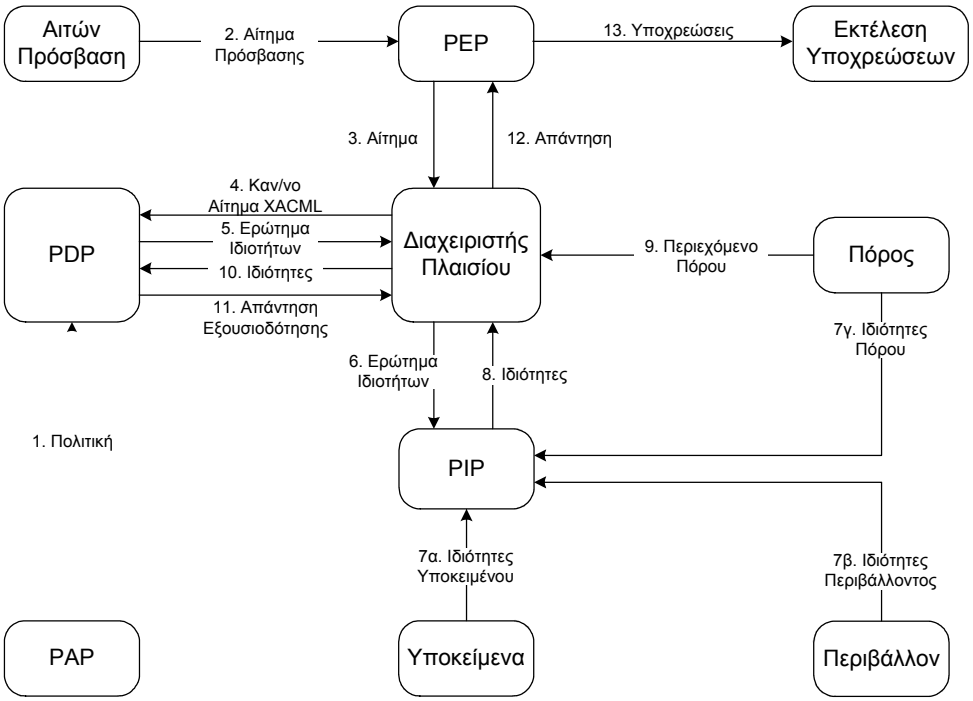
Η γλώσσα XACML έχει δομηθεί γύρω από τις ακόλουθες βασικές έννοιες:

- **Πόρος (Resource)**: Προσωπικά δεδομένα, υπηρεσίες, συστήματα ή οτιδήποτε άλλο μπορεί να αποτελέσει αντικείμενο κάποιου αιτήματος για πρόσβαση.
- **Ενέργεια (Action)**: Οποιαδήποτε λειτουργία πάνω σε έναν πόρο που καλύπτεται από την πολιτική.
- **Υποκείμενο (Subject)**: Εκείνη η οντότητα που αιτείται να πραγματοποιήσει κάποια ενέργεια σε κάποιο πόρο.
- **Απόφαση Εξουσιοδότησης (Authorization Decision)**: Το αποτέλεσμα της αποτίμησης κάποιας πολιτικής. Το αποτέλεσμα μπορεί να λάβει τις τιμές: Έγκριση (permit), Απαγόρευση (deny) Απροσδιοριστία (indeterminate) και Ανεφάρμοστο (not applicable). Προαιρετικά, η απόφαση εξουσιοδότησης μπορεί να προσδιορίζει και ένα σύνολο από υποχρεώσεις.
- **Ιδιότητα (Attribute)**: Τα διάφορα χαρακτηριστικά που αφορούν σε υποκείμενα, πόρους, ενέργειες, περιβάλλοντα. Για παράδειγμα, το όνομα ενός χρήστη, το αρχείο που θέλει να προσπελάσει, κλπ. αποτελούν τιμές ιδιοτήτων.
- **Περιβάλλον (Environment)**: Το σύνολο των πιθανών ιδιοτήτων που σχετίζονται με μία απόφαση εξουσιοδότησης αλλά είναι ανεξάρτητες του υποκειμένου, του πόρου ή της ενέργειας.

- **Υποχρέωση (Obligation)**: Κάποια λειτουργία η οποία πρέπει να πραγματοποιηθεί κατά την εφαρμογή της απόφασης εξουσιοδότησης.
- **Σημείο Απόφασης Πολιτικής (Policy Decision Point – PDP)**: Η οντότητα του συστήματος που πραγματοποιεί την αποτίμηση της πολιτικής και καταλήγει σε μία απόφαση εξουσιοδότησης.
- **Σημείο Εφαρμογής Πολιτικής (Policy Enforcement Point – PEP)**: Η οντότητα του συστήματος που πραγματοποιεί τον έλεγχο της πρόσβασης, εφαρμόζοντας τις αποφάσεις του σημείου PDP, στο οποίο απευθύνεται με τα αντίστοιχα αιτήματα αποτίμησης.
- **Σημείο Διαχείρισης Πολιτικής (Policy Administration Point – PAP)**: Η οντότητα του συστήματος στο οποίο συγγράφονται οι πολιτικές.
- **Σημείο Πληροφόρησης Πολιτικής (Policy Information Point – PIP)**: Η οντότητα του συστήματος που λειτουργεί ως πηγή των τιμών των ιδιοτήτων.
- **Διαχειριστής Πλαισίου (Context Handler)**: Η οντότητα του συστήματος που πραγματοποιεί τη μετατροπή των αιτήσεων εξουσιοδότησης από την εγγενή τους μορφή σε κανονική XACML μορφή (canonical XACML form), καθώς και τη μετατροπή των αποφάσεων εξουσιοδότησης από την κανονική XACML μορφή στη μορφή εκείνη που αντιλαμβάνεται το σχετικό σύστημα.

Ο τρόπος λειτουργίας της γλώσσας και του γενικότερου πλαισίου της XACML συνοψίζεται στο διάγραμμα ροής πληροφορίας που παρουσιάζεται στο Σχήμα 10. Σύμφωνα με αυτό, η λειτουργία του μοντέλου XACML αποτελείται από τα παρακάτω βήματα:

1. Οι πολιτικές ιδιωτικότητας συγγράφονται στο σημείο PAP και καθίστανται διαθέσιμες στο σημείο PDP.
2. Ο αιτών πρόσβαση σε κάποιο πόρο αποστέλλει το σχετικό αίτημα στο σημείο PEP.
3. Το σημείο PEP αποστέλλει το αίτημα για πρόσβαση στο διαχειριστή πλαισίου, στην πρωταρχική του μορφή.
4. Ο διαχειριστής πλαισίου δημιουργεί ένα κανονικοποιημένο αίτημα XACML και το αποστέλλει στο σημείο PDP.



Σχήμα 10: Διάγραμμα ροής πληροφορίας XACML

5. Το σημείο PDP αιτείται από το διαχειριστή πλαισίου οποιαδήποτε επιπλέον ιδιότητα του υποκειμένου, πόρου ή περιβάλλοντος.

6. Ο διαχειριστής πλαισίου αιτείται τις ιδιότητες από το σημείο PIP.

7. Το σημείο PIP αποκτά τις ιδιότητες που αφορούν το σχετικό αίτημα.

8. Το σημείο PIP αποστέλλει στο διαχειριστή τις ιδιότητες που αφορούν το σχετικό αίτημα.

9. Προαιρετικά, ο διαχειριστής πλαισίου ενσωματώνει τον πόρο στο σχετικό αίτημα.

10. Ο διαχειριστής πλαισίου αποστέλλει τις ιδιότητες που ζητήθηκαν και (προαιρετικά) τον πόρο στο σημείο PDP.

    Το σημείο PDP πραγματοποιεί την αποτίμηση του αιτήματος.

11. Το σημείο PDP τροφοδοτεί το διαχειριστή πλαισίου με την απάντηση – αποτέλεσμα της αποτίμησης για την απόφαση εξουσιοδότησης.

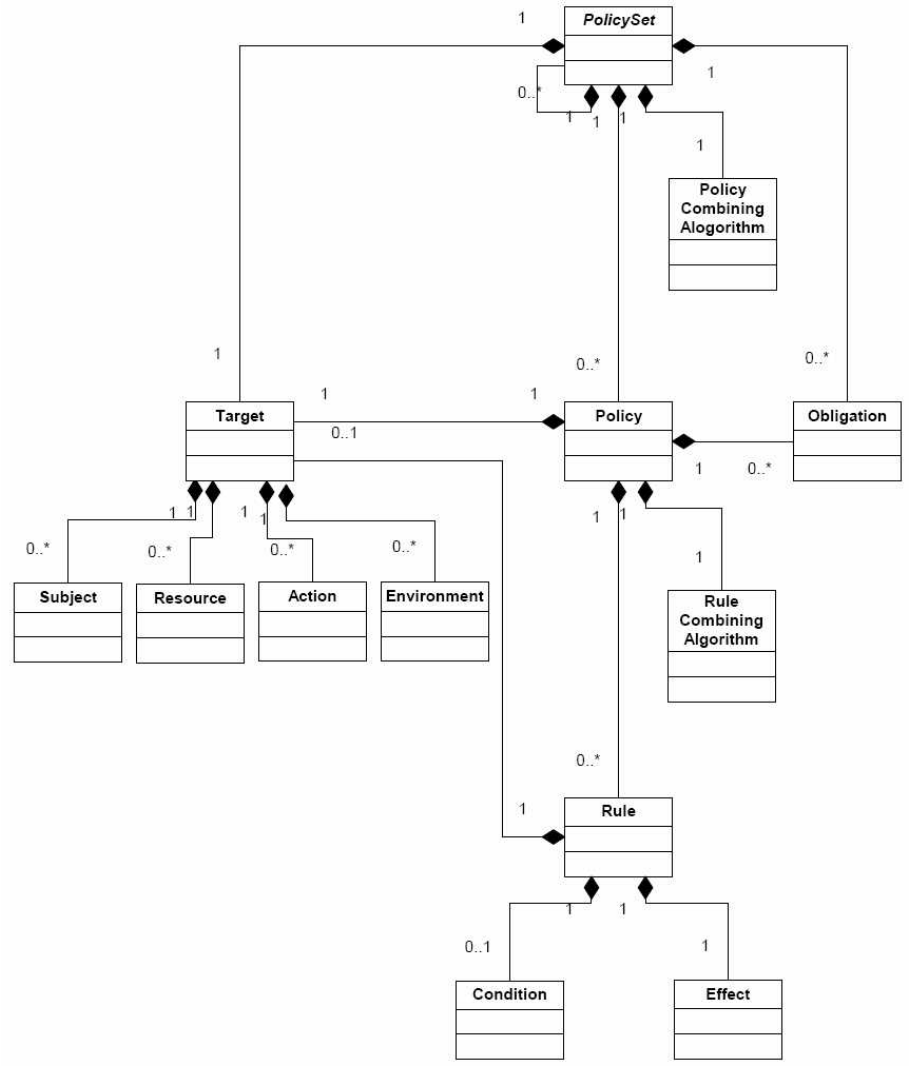
12. Ο διαχειριστής πλαισίου μεταφράζει την απάντηση στην εγγενή μορφή που αντιλαμβάνεται το σημείο PEP.

Ο διαχειριστής πλαισίου προωθεί την απάντηση στο σημείο PEP.

13. Το σημείο PEP εκτελεί τις υποχρεώσεις που προκύπτουν.

    Εφόσον σύμφωνα με την απόφαση εξουσιοδότησης η πρόσβαση επιτρέπεται, το σημείο PEP επιτρέπει την πρόσβαση στον αιτηθέντα προστατευμένο πόρο. Σε διαφορετική περίπτωση, το σημείο PEP προβαίνει σε άρνηση της πρόσβασης.

Αναφορικά με τη δομή μίας XACML πολιτικής, το σχετικό UML μοντέλο παρουσιάζεται στο παρακάτω Σχήμα 11, το οποίο προέρχεται από τη βασική προδιαγραφή της XACML [70].



Σχήμα 11: Μοντέλο Πολιτικής Γλώσσας XACML

```
<Policy PolicyId="SamplePolicy"
            RuleCombiningAlgId="rule-combining-algorithm:permit-overrides">
   <Target>
      <Subjects>
         <AnySubject/>
      </Subjects>
      <Resources>
         <ResourceMatch MatchId="function:string-equal">
            <AttributeValue DataType="string">SampleServer</AttributeValue>
            <ResourceAttributeDesignator DataType="string"
                        AttributeId="resource:resource-id"/>
         </ResourceMatch>
      </Resources>
      <Actions>
         <AnyAction/>
      </Actions>
   </Target>
   <Rule RuleId="LoginRule" Effect="Permit">
      <Target>
         <Subjects>
            <AnySubject/>
         </Subjects>
         <Resources>
            <AnyResource/>
         </Resources>
         <Actions>
            <ActionMatch MatchId="function:string-equal">
               <AttributeValue DataType="string">login</AttributeValue>
               <ActionAttributeDesignator DataType="string"
                           AttributeId="ServerAction"/>
            </ActionMatch>
         </Actions>
      </Target>
      <Condition FunctionId="function:and">
         <Apply FunctionId="function:time-greater-than-or-equal"
            <Apply FunctionId="function:time-one-and-only">
               <EnvironmentAttributeSelector DataType="time"
                           AttributeId="environment:current-time"/>
            </Apply>
            <AttributeValue DataType="time">09:00:00</AttributeValue>
         </Apply>
         <Apply FunctionId="function:time-less-than-or-equal"
            <Apply FunctionId="function:time-one-and-only">
               <EnvironmentAttributeSelector DataType="time"
                           AttributeId="environment:current-time"/>
            </Apply>
            <AttributeValue DataType="time">17:00:00</AttributeValue>
         </Apply>
      </Condition>
   </Rule>
   <Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
```

Σχήμα 12: Παράδειγμα Πολιτικής XACML

Όπως παρουσιάζεται στο Σχήμα 11, ένα Σύνολο Πολιτικών (Policy Set) αποτελεί τη ρίζα και περιλαμβάνει Πολιτικές (Policies), οι οποίες με τη σειρά τους απαρτίζονται από κανόνες (rules). Ο Στόχος (target) αποτελεί το πεδίο ορισμού του Κανόνα, Πολιτικής ή Συνόλου Πολιτικών, δηλαδή το σύνολο από υποκείμενα, πόρους, ενέργειες και περιβάλλοντα στα οποία εφαρμόζεται ο εν λόγω Κανόνας, Πολιτική ή Σύνολο Πολιτικών. Όπως προαναφέρθηκε, η Υποχρέωση (Obligation) ορίζει κάποια λειτουργία η οποία πρέπει να πραγματοποιηθεί κατά την εφαρμογή της απόφασης εξουσιοδότησης. Η

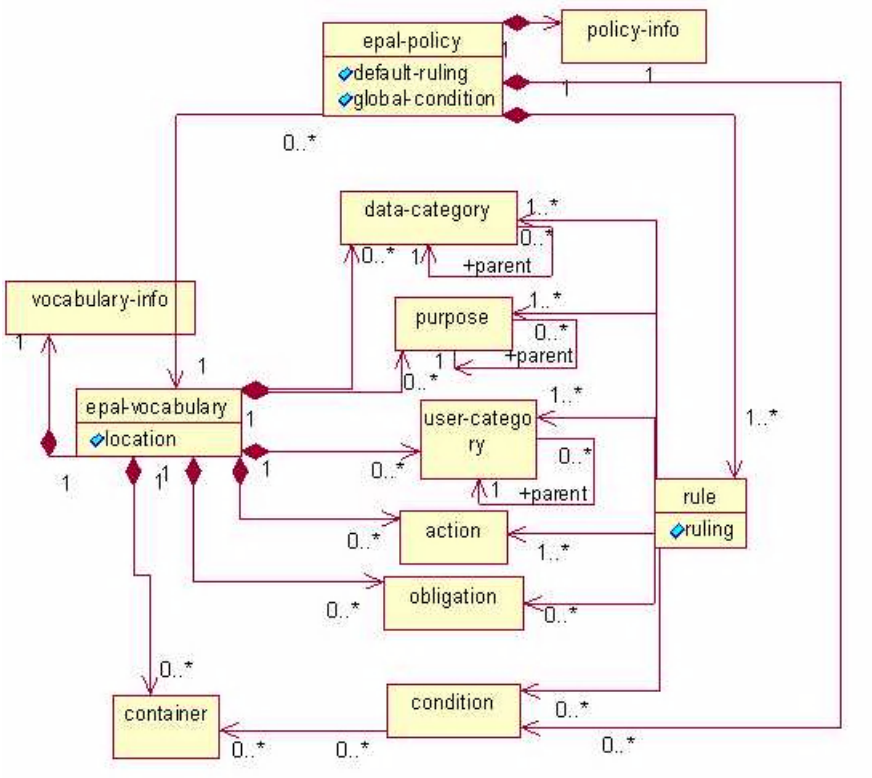
Συνθήκη (Condition) καθορίζει χαρακτηριστικά του Στόχου που πρέπει να πληρούνται προκειμένου να εφαρμόζεται η πολιτική, ενώ η Επίδραση (Effect) ορίζει τη συνέπεια της εφαρμογής. Τέλος, ο Αλγόριθμος Συνδυασμού Κανόνων (Rule-Combining Algorithm) ορίζει τη διαδικασία βάσει της οποίας πολλαπλοί Κανόνες καταλήγουν σε ένα συνδυαστικό αποτέλεσμα.

Στο Σχήμα 12 παρουσιάζεται ένα παράδειγμα XACML πολιτικής. Η πολιτική ελέγχει την πρόσβαση σε κάποιο εξυπηρετητή με όνομα `SampleServer` στον οποίο συνδέονται χρήστες (login). Ο πρώτος Κανόνας περιλαμβάνει μία Συνθήκη η οποία θέτει περιορισμό στο χρόνο κατά τον οποίο οι χρήστες μπορούν να συνδεθούν (09:00 – 17:00), ενώ εφόσον ο πρώτος κανόνας δεν ικανοποιηθεί, η πρόσβαση δε γίνεται δεκτή σύμφωνα με το δεύτερο Κανόνα.

3.1.5 Η Γλώσσα Επιχειρησιακής Εξουσιοδότησης για Ιδιωτικότητα (EPAL)

Η εταιρεία International Business Machines (IBM) έχει αναπτύξει τη Γλώσσα Επιχειρησιακής Εξουσιοδότησης για Ιδιωτικότητα (Enterprise Privacy Authorization Language – EPAL) [71][72][73][74][75]. Η γλώσσα EPAL αποτελεί μία φορμαλιστική γλώσσα για τον προσδιορισμό και την εφαρμογή πολιτικών ιδιωτικότητας και σε γενικές γραμμές χαρακτηρίζεται από αρκετά κοινά στοιχεία με τη γλώσσα XACML. Ανταποκρίνεται στις τέσσερις βασικές απαιτήσεις για τις δομημένες γλώσσες έκφρασης και εφαρμογής πολιτικών ιδιωτικότητας όπως αυτές συνοψίζονται στο [42], ενώ – όπως και το μοντέλο της γλώσσας XACML – ακολουθεί το γενικό μοντέλο που περιγράφεται στα [67][68][69]. Το Σχήμα 13 παρουσιάζει ένα UML μοντέλο μίας πολιτικής EPAL, το οποίο προέρχεται από τη βασική προδιαγραφή της EPAL [75].

Σε σχέση με την XACML, η γλώσσα EPAL παρουσιάζει το πλεονέκτημα της ιδέας του λεξιλογίου πολιτικής (policy vocabulary). Κάθε πολιτική EPAL περιλαμβάνει αναφορά σε κάποια αφηρημένη δομή, το λεξιλόγιο, το οποίο περιγράφει όλα τα χαρακτηριστικά, όπως τις υποχρεώσεις, συνθήκες και χαρακτηριστικά, που χρησιμοποιεί ή μπορεί να χρησιμοποιήσει η εν λόγω πολιτική. Επιπλέον, η γλώσσα EPAL ορίζει ιεραρχικές κατηγορίες οντοτήτων οι οποίες μπορούν να είναι συσχετισμένες με διάφορες επιτρεπτές ή απαγορευμένες ενέργειες και για τις οποίες είναι δυνατό να οριστούν κανόνες κληρονομικότητας.



Σχήμα 13: Μοντέλο Πολιτικής Γλώσσας EPAL

Ωστόσο, η γλώσσα EPAL παρουσιάζει και κάποιες ελλείψεις σε σχέση με την XACML. Σε αυτές περιλαμβάνεται η αδυναμία συνδυασμού των αποτελεσμάτων διαφορετικών πολιτικών και η έλλειψη της δυνατότητας αναφοράς σε εξωτερικές πολιτικές προκειμένου να αποτελέσουν μέρος κάποιας δεδομένης πολιτικής. Γενικά, η γλώσσα XACML έχει επικρατήσει έναντι της EPAL. Μία αναλυτική σύγκρισή τους περιλαμβάνεται στο [42].

3.2 Τεχνολογίες για την Προστασία της Ιδιωτικότητας

Οι τεχνολογίες για την προστασία της ιδιωτικότητας αποτελούν ως επί το πλείστον τεχνολογίες ασφάλειας οι οποίες μπορούν να χρησιμοποιηθούν συμπληρωματικά και σε συνδυασμό με κάποια τεχνολογία διαχείρισης της ιδιωτικότητας. Κατά συνέπεια, οι τεχνολογίες αυτές συνιστούν μία πολύ σημαντική εργαλειοθήκη και χρησιμοποιούνται σε μεγάλο βαθμό στο πλαίσιο της προτεινόμενης λύσης.

3.2.1 Κρυπτογραφικά Συστήματα

Όταν πραγματοποιείται μετάδοση προσωπικών δεδομένων σε κάποιο πάροχο υπηρεσίας, οι παραπάνω μέθοδοι Διαχείρισης της Ιδιωτικότητας καθίστανται άχρηστες εάν τα προσωπικά δεδομένα δε χαρακτηρίζονται από επαρκή βαθμό προστασίας από τις εξωτερικές οντότητες οι οποίες ενδέχεται να επιθυμούν να υποκλέψουν τη σχετική πληροφορία και να την επιβουλευτούν. Η αποτροπή τρίτων οντοτήτων από το να υποκλέψουν προσωπικά δεδομένα κατά τη φάση της μετάδοσής τους καθίσταται δυνατή μέσα από τη χρήση κρυπτογραφικών μεθόδων [76][77].

Επιπλέον, εφόσον προσωπικά δεδομένα έχουν διατεθεί σε κάποιο πάροχο υπηρεσιών, η αποθήκευσή τους πρέπει να χαρακτηρίζεται από υψηλό βαθμό ασφάλειας, ούτως ώστε να είναι δυνατό μόνο σε εξουσιοδοτημένες οντότητες να τα προσπελάσουν. Στην πράξη, αυτό μεταφράζεται σε δύο απαιτήσεις. Από τη μία, τα δεδομένα πρέπει να αποθηκεύονται κρυπτογραφημένα ούτως ώστε ακόμα και αν κάποιος αποκτήσει μη εξουσιοδοτημένη πρόσβαση στα σχετικά αρχεία να μην είναι σε θέση να διαβάσει το περιεχόμενο. Από την άλλη, απαιτούνται ισχυροί μηχανισμοί ταυτοποίησης και εξουσιοδότησης χρηστών, ούτως ώστε να διασφαλίζεται ότι εξουσιοδοτημένες οντότητες και μόνο είναι δυνατό να αποκτήσουν πρόσβαση στα αποθηκευμένα δεδομένα. Συνεπώς, η χρήση κρυπτογραφικών μεθόδων βρίσκει και εδώ εφαρμογή.

Τα συμβατικά, συμμετρικά κρυπτογραφικά συστήματα βασίζονται στο γεγονός ότι και τα δύο άκρα μίας κρυπτογραφημένης δικτυακής σύνδεσης μοιράζονται το ίδιο κρυπτογραφικό κλειδί. Αυτό σημαίνει ότι το κλειδί αυτό πρέπει να κρατηθεί μυστικό από κάθε τρίτη οντότητα και ότι ο αποστολέας και ο παραλήπτης του κρυπτογραφημένου μηνύματος πρέπει με κάποιο τρόπο να συμφωνήσουν αναφορικά με το συγκεκριμένο κρυπτογραφικό κλειδί πριν από την έναρξη της επικοινωνιακής συνόδου. Μερικοί ευρέως διαδεδομένοι αλγόριθμοι συμμετρικής κρυπτογραφίας είναι οι Data Encryption Standard (DES) [78], Triple Data Encryption Standard (Triple DES) [79], Advance Encryption Standard (AES) [80], International Data Encryption Algorithm (IDEA) [81], Blowfish [82], Rivest Cipher 2 (RC2) [83], Rivest Cipher 4 (RC4) [84], Rivest Cipher 5 (RC5) [85].

Το ζήτημα της διανομής των κρυπτογραφικών κλειδιών λύνεται με χρήση Κρυπτογραφίας Δημοσίου Κλειδιού (Public Key Cryptography) [86]. Η χρήση κρυπτογραφίας δημοσίου κλειδιού ή ασύμμετρης κρυπτογραφίας επιτρέπει στις εμπλεκόμενες οντότητες να συμφωνήσουν με ασφάλεια και μυστικότητα σε κάποιο

κρυπτογραφικό κλειδί χρησιμοποιώντας ένα μη ασφαλές επικοινωνιακό κανάλι. Η βασική ιδέα είναι η χρήση ενός ζεύγους κρυπτογραφικών κλειδιών, ενός ιδιωτικού κλειδιού (private key) και ενός δημοσίου κλειδιού (public key). Ενώ το πρώτο από αυτά διατηρείται μυστικό από τον κάτοχό του, το δεύτερο μπορεί να είναι (και σε μερικές περιπτώσεις χρήσης πρέπει να είναι) ευρέως διαδεδομένο.

Η μαθηματική ιδέα πίσω από την κρυπτογραφία δημοσίου κλειδιού είναι ότι η γνώση του ενός κλειδιού δεν μπορεί να οδηγήσει σε υπολογισμό του άλλου, ενώ το κάθε κλειδί χρησιμοποιείται για την αποκρυπτογράφηση μηνυμάτων τα οποία έχουν κρυπτογραφηθεί με χρήση του άλλου κλειδιού. Αυτό σημαίνει ότι δεδομένα τα οποία έχουν κρυπτογραφηθεί με χρήση του ιδιωτικού κλειδιού μπορούν να αποκρυπτογραφηθούν μόνο με χρήση του αντίστοιχου δημοσίου κλειδιού, ενώ δεδομένα τα οποία έχουν κρυπτογραφηθεί με χρήση του δημοσίου κλειδιού μπορούν να αποκρυπτογραφηθούν μόνο με χρήση του αντίστοιχου ιδιωτικού κλειδιού. Το γεγονός αυτό επιτρέπει τη χρήση του γενικού μηχανισμού όχι μόνο για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων αλλά και για τη δημιουργία ηλεκτρονικά υπογεγραμμένων μηνυμάτων τα οποία μπορούν να χρησιμοποιηθούν για την ταυτοποίηση του αποστολέα τους και για την εξακρίβωση της μη παραποίησης των μηνυμάτων αυτών από κάποια τρίτη οντότητα. Ιδιαίτερα διαδεδομένοι αλγόριθμοι οι οποίοι υλοποιούν την ιδέα αυτή είναι οι Diffie–Hellman [86], Rivest–Shamir–Adleman (RSA) [87], καθώς και – τα τελευταία χρόνια – οι αλγόριθμοι που βασίζονται σε ελλειπτικές καμπύλες [88].

Σημειώνεται ότι ο βαθμός της προσφερόμενης ασφάλειας από κάποιο κρυπτογραφικό σύστημα εξαρτάται από διάφορους παράγοντες, όπως είναι ο χρησιμοποιούμενος αλγόριθμος και το μέγεθος των χρησιμοποιούμενων κλειδιών. Επιπλέον, πέρα από την ανάγκη να παραμένει εντελώς μυστικό το ιδιωτικό κλειδί, η σωστή απόδοση ενός δημοσίου κλειδιού στο φερόμενο ως ιδιοκτήτη του απαιτεί τη χρήση μέσων διασφάλισης. Η Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure – PKI) [89][90] αποτελεί τη βάση για μία τέτοια διασφάλιση. Σε μία υποδομή PKI, μία έμπιστη οντότητα γνωστή ως Αρχή Πιστοποίησης (Certificate Authority) μπορεί να επιβεβαιώσει με τεχνικά μέσα τον κάτοχο ενός ζεύγους κλειδιών.

Συγκρινόμενα με τα συμβατικά κρυπτογραφικά συστήματα, τα συστήματα κρυπτογραφίας δημοσίου κλειδιού χαρακτηρίζονται από μεγαλύτερο βαθμό

πολυπλοκότητας και, κατά συνέπεια, από χαμηλότερες επιδόσεις αναφορικά με την ταχύτητά τους. Για το λόγο αυτό, στην πράξη χρησιμοποιούνται περισσότερο για την ασφαλή ανταλλαγή κρυπτογραφικών κλειδιών συμμετρικών αλγορίθμων καθώς και για τη δημιουργία και επαλήθευση ψηφιακών υπογραφών.

Η χρήση του δημοσίου κλειδιού κάποιου χρήστη για την κρυπτογράφηση κάποιας πληροφορίας διασφαλίζει ότι μόνο ο χρήστης αυτός, χρησιμοποιώντας το ιδιωτικό κλειδί του, μπορεί να την αποκρυπτογραφήσει. Βάσει της συμμετρίας των ιδιοτήτων των δύο κλειδιών, ιδιωτικού και δημοσίου, η χρήση του ιδιωτικού κλειδιού από το χρήστη – κάτοχό του για την κρυπτογράφηση κάποιας πληροφορίας καθιστά οποιονδήποτε άλλο χρήστη – γνώστη του αντίστοιχου δημοσίου κλειδιού ικανό να την αποκρυπτογραφήσει. Αν και αυτό είναι φαινομενικά άχρηστο σε ό,τι αφορά τη μυστικότητα της πληροφορίας, είναι ιδιαιτέρως χρήσιμο αναφορικά με τη διασφάλιση της αυθεντικότητας της πληροφορίας. Καθώς μόνο ο χρήστης – ιδιοκτήτης του ζεύγους κλειδιών έχει στην κατοχή του το ιδιωτικό κλειδί, η αποκρυπτογράφηση ενός μηνύματος από το δημόσιο κλειδί αποδεικνύει ότι το μήνυμα είναι αυθεντικό υπό την έννοια ότι ο δημιουργός του ταυτοποιείται ως ο ιδιοκτήτης του ζεύγους κλειδιών. Το γεγονός αυτό αποτελεί τη θεωρητική βάση των ψηφιακών υπογραφών.

Ο συνδυασμός των δύο ιδεών διασφαλίζει τόσο τη μυστικότητα όσο και την αυθεντικότητα και ακεραιότητα τη πληροφορίας. Ένας χρήστης μπορεί να χρησιμοποιήσει το ιδιωτικό του κλειδί και να κρυπτογραφήσει την πληροφορία κατ' αρχήν. Σε δεύτερη φάση, χρησιμοποιεί το δημόσιο κλειδί του τελικού αποδέκτη της πληροφορίας και κρυπτογραφεί και πάλι την πληροφορία. Ο τελικός αποδέκτης είναι τελικά ο μόνος που μπορεί να την αποκρυπτογραφήσει χρησιμοποιώντας το ιδιωτικό του κλειδί, ενώ η τελική αποκρυπτογράφηση χρησιμοποιώντας το ευρέως γνωστό δημόσιο κλειδί του αποστολέα της πληροφορίας αποδεικνύει τόσο την ταυτότητα του αποστολέα όσο και το γεγονός ότι η πληροφορία δεν παραποιήθηκε στην πορεία από κάποια τρίτη οντότητα. Επιπλέον, ο δημιουργός του μηνύματος δεν μπορεί να αρνηθεί τη δημιουργία και αποστολή του μηνύματος, εφόσον είναι ο μοναδικός γνώστης του ιδιωτικού του κλειδιού.

Σημειώνεται ότι στην πράξη οι ψηφιακές υπογραφές δε χρησιμοποιούν ολόκληρη την πληροφορία για τη δημιουργία τους. Για λόγους αύξησης της ταχύτητας δημιουργίας και επαλήθευσή τους, οι σχετικοί αλγόριθμοι λειτουργούν σε μία συνοπτική εκδοχή της

πληροφορίας, η οποία προκύπτει από την εφαρμογή κάποιας συνάρτησης κατακερματισμού (hash function), όπως είναι οι πολύ δημοφιλείς Message Digest 2 (MD2) [91] και 5 (MD5) [92] και η οικογένεια των αλγορίθμων Secure Hash Algorithm (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-1) [93].

Αξίζει να σημειωθεί ότι η Ευρωπαϊκή Ένωση, προκειμένου να εξασφαλίσει την ομαλή λειτουργία της εσωτερικής αγοράς, έχει θεσπίσει νομικό πλαίσιο για τις ψηφιακές υπογραφές. Για το σκοπό αυτό, έχει εκδώσει την Κοινοτική Οδηγία 1999/93/ΕΚ [94] με στόχο τη διευκόλυνση της χρήσης των ηλεκτρονικών υπογραφών και τη νομική αναγνώρισή τους. Η χώρα μας προσάρμοσε την Κοινοτική Οδηγία 1999/93/ΕΚ στο Ελληνικό Εθνικό Δίκαιο με το Προεδρικό Διάταγμα 150/2001 [95].

Τα κρυπτογραφικά συστήματα δημοσίου κλειδιού βρίσκουν εφαρμογή σε διάφορα πρωτόκολλα ασφάλειας στο Διαδίκτυο. Ιδιαίτερα σημαντικά μεταξύ αυτών είναι το πρωτόκολλο Secure Sockets Layer (SSL) [96] καθώς και ο διάδοχός του, το πρωτόκολλο Transport Layer Security (TLS) [97][98]. Τα πρωτόκολλα SSL και TLS χρησιμοποιούνται συνήθως για τη διασφάλιση επικοινωνιακών καναλιών που ακολουθούν το πρωτόκολλο Hypertext Transfer Protocol (HTTP) [99], αλλά μπορούν να χρησιμοποιηθούν σε συνδυασμό και με άλλα πρωτόκολλα, όπως το Simple Mail Transfer Protocol (SMTP) [100] για τη διασφάλιση των μηνυμάτων ηλεκτρονικού ταχυδρομείου.

Τα πρωτόκολλα SSL και TLS περιλαμβάνουν τρία βασικά βήματα προκειμένου να διασφαλίσουν μία επικοινωνιακή σύνδεση:

1. Διαπραγμάτευση των παραμέτρων του πρωτοκόλλου μεταξύ του πελάτη και του εξυπηρετητή.
2. Ανταλλαγή κρυπτογραφικών κλειδιών και ταυτοποίηση του εξυπηρετητή με χρήση κρυπτογραφίας δημοσίου κλειδιού και ψηφιακών πιστοποιητικών.
3. Συμφωνία σε κάποιο συμμετρικό κρυπτογραφικό κλειδί για την κρυπτογράφηση και αποκρυπτογράφηση της επικοινωνιακής κίνησης.

Τα πρωτόκολλα SSL και TLS μπορούν να υποστηρίξουν έναν αριθμό από διαφορετικούς αλγορίθμους προκειμένου να πραγματοποιήσουν την ανταλλαγή των κρυπτογραφικών κλειδιών και την κρυπτογράφηση των δεδομένων. Συνεπώς, οι σχετικές δυνατότητες του πελάτη και του εξυπηρετητή πρέπει να αντιστοιχηθούν προτού λάβει χώρα οποιαδήποτε κρυπτογράφηση δεδομένων. Έπειτα από το πρώτο αυτό

βήμα, ο εξυπηρετητής αποστέλλει ένα ψηφιακό πιστοποιητικό, το οποίο περιέχει το δημόσιο κλειδί του εξυπηρετητή και το οποίο είναι υπογεγραμμένο από κάποια αρχή πιστοποίησης. Έτσι, ο πελάτης είναι σε θέση να επαληθεύσει την ταυτότητα του εξυπηρετητή. Στη συνέχεια, ο πελάτης δημιουργεί ένα τυχαίο κρυπτογραφικό κλειδί, το οποίο αποστέλλει στον εξυπηρετητή, κρυπτογραφημένο με το δημόσιο κλειδί του εξυπηρετητή. Μέσω του κλειδιού αυτού και μετά από κάποια βήματα, δημιουργείται τελικά το κρυπτογραφικό κλειδί της επικοινωνιακής συνόδου.

Κατά συνέπεια, τα πρωτόκολλα SSL και TLS προσφέρουν στα πρωτόκολλα των ανώτερων στρωμάτων τις εξής υπηρεσίες ασφάλειας:

- *Εμπιστευτικότητα*, μέσω της κρυπτογράφησης όλων των μεταδιδόμενων δεδομένων.
- *Ταυτοποίηση του εξυπηρετητή* (και προαιρετικά του πελάτη), μέσω της χρήσης των ψηφιακών πιστοποιητικών.

3.2.2 Συστήματα Ανωνυμίας και Ψευδωνυμίας

Συχνά, η χρήση ανωνυμίας (anonymity) ή ψευδωνυμίας (pseudonymity) αποτελεί απαίτηση της νομοθεσίας. Για παράδειγμα, στην Ευρωπαϊκή Οδηγία 2002/58/ΕΚ [24] αναφέρεται ως στόχος η "χρήση ανώνυμων ή ψευδώνυμων δεδομένων, όπου αυτό είναι δυνατό".

Η ανωνυμία μπορεί να οριστεί σαν "η κατάσταση κατά την οποία κάποιο υποκείμενο δεν είναι αναγνωρίσιμο μεταξύ των μελών ενός συνόλου υποκειμένων, του *συνόλου ανωνυμίας*" [101]. Ιδιαίτερα στο Διαδίκτυο και τις προσφερόμενες μέσω αυτού υπηρεσίες, η προστασία της ανωνυμίας κάποιου αποτελεί ως επί το πλείστον ζήτημα της απόκρυψης της IP διεύθυνσής του, καθώς αυτή μπορεί να οδηγήσει στην ταυτότητα του χρήστη. Η απόκρυψη της IP διεύθυνσης κάποιου χρήστη στο επίπεδο δικτύου εφαρμόζεται σχετικά εύκολα και μπορεί να ενσωματωθεί σε οποιαδήποτε τεχνική λύση προστασίας προσωπικών δεδομένων, καθώς υλοποιείται χωριστά σε σχέση από την εκάστοτε υποδομή ιδιωτικότητας. Ωστόσο, η ανωνυμία στο επίπεδο του δικτύου δεν μπορεί να αποτρέψει την αναγνώριση κάποιου χρήστη μέσω των προσωπικών του πληροφοριών που είναι αποθηκευμένες ή μεταδίδονται στο πλαίσιο της παροχής κάποιας υπηρεσίας.

Μία εναλλακτική ή και συμπληρωματική λύση είναι η χρήση ψευδωνύμων, τα οποία επιτρέπουν την προσωποποίηση των παρεχομένων υπηρεσιών χωρίς να κάνουν χρήση της πραγματικής ταυτότητας κάποιου χρήστη. Ο Διεθνής Οργανισμός Προτυποποίησης (International Organization for Standardization – ISO) [66], στο πρότυπό του για την αξιολόγηση των κριτηρίων ασφάλειας για τις τεχνολογίες της πληροφορίας [102], ορίζει ότι "η ψευδωνυμία εξασφαλίζει ότι κάποιος χρήστης μπορεί να χρησιμοποιήσει κάποιο πόρο ή υπηρεσία, χωρίς να αποκαλύψει την πραγματική του ταυτότητα, παραμένοντας ωστόσο υπόλογος για τη χρήση".

Ένας από τους πιο δημοφιλείς τρόπους απόκρυψης της Διαδικτυακής διεύθυνσης κάποιου χρήστη είναι οι πληρεξούσιοι κόμβοι ανωνυμίας (anonymizing proxies), όπως είναι ο Anonymouse [103]. Η βασική ιδέα είναι η εξής: όταν κάποιος χρήστης θέλει να επικοινωνήσει με κάποιο εξυπηρετητή παροχής υπηρεσίας, η δρομολόγηση όλων των εξερχομένων από τον τερματικό εξοπλισμού του χρήστη πακέτων πραγματοποιείται μέσω ενός πληρεξούσιου κόμβου ανωνυμίας, ο οποίος αφαιρεί τη Διαδικτυακή διεύθυνση του χρήστη από τα πακέτα, διεκπεραιώνοντας ο ίδιος την επικοινωνία με τον αντίστοιχο εξυπηρετητή, για λογαριασμό του χρήστη. Στη συνέχεια, τα πακέτα – απαντήσεις του εξυπηρετητή λαμβάνονται από τον πληρεξούσιο κόμβο ανωνυμίας και αποστέλλονται από αυτόν στο χρήστη. Η απλή αυτή τεχνική παρουσιάζει το μειονέκτημα της ύπαρξης ενός μοναδικού σημείου αντιστοίχησης του χρήστη (δηλαδή της Διαδικτυακής διεύθυνσής του) με τη διεύθυνση ανωνυμίας του, γεγονός το οποίο αποτελεί πρόβλημα σε περίπτωση αποτυχίας του πληρεξούσιου κόμβου ανωνυμίας ή δικτυακής επίθεσης σε αυτόν.

Μία καλύτερη προσέγγιση αποτελεί η λύση των δικτύων τύπου Mix (Mix Networks), η ιδέα των οποίων προτάθηκε από τον David Chaum το 1981 [104]. Στο πλαίσιο των Mix Networks, η δρομολόγηση πραγματοποιείται μέσω πολλών διαδοχικών κόμβων ανωνυμίας, με τον τελευταίο από αυτούς να επικοινωνεί τελικά με τον αντίστοιχο εξυπηρετητή παροχής της υπηρεσίας. Κατά αυτόν τον τρόπο, καθίσταται εξαιρετικά πιο δύσκολη η εξακρίβωση της Διαδικτυακής διεύθυνσης του χρήστη που αποστέλλει κάποιο μήνυμα. Τα Mix Networks κάνουν επιπλέον χρήση Κρυπτογραφίας Δημοσίου Κλειδιού (Public Key Cryptography) [86]: ο χρήστης κρυπτογραφεί το μήνυμά του χρησιμοποιώντας το δημόσιο κλειδί του πρώτου κόμβου του Mix Network. Ο κόμβος αυτός αποκρυπτογραφεί το μήνυμα και το προωθεί στον επόμενο κόμβο, αφού πρώτα το

κρυπτογραφήσει με το δημόσιο κλειδί του τελευταίου. Η διαδικασία συνεχίζεται κατά αυτόν τον τρόπο, με την αλυσιδωτή κρυπτογράφηση και προώθηση του μηνύματος από τους κόμβους του Mix Network, μέχρι την τελική αποστολή του στον αντίστοιχο εξυπηρετητή παροχής της υπηρεσίας.

Διάφορες ερευνητικές προσπάθειες έχουν εξελίξει την αρχική ιδέα των Mix Networks. Εξέχουσα θέση κατέχει το σύστημα *Crowds* [105] το οποίο αναπτύχθηκε στα εργαστήρια της AT&T. Το σύστημα αυτό αίρει την ανάγκη της εκ των προτέρων δημιουργίας της αλυσίδας των κόμβων του Mix Network, καθώς δρομολογεί τα μηνύματα με τυχαίο τρόπο μεταξύ των κόμβων.

4 Γενική Περιγραφή της Προτεινόμενης Λύσης

Στο Κεφάλαιο αυτό παρουσιάζονται οι γενικές αρχές της προτεινόμενης λύσης. Πραγματοποιείται σύνοψη / κωδικοποίηση των βασικών αρχών για την προστασία των προσωπικών δεδομένων όπως ορίζονται από τη Νομοθεσία και περιγράφονται στο Κεφάλαιο 2 της παρούσας Διατριβής, ενώ ορίζονται διάφορες βασικές έννοιες, όπως είναι οι κατηγορίες των προσωπικών δεδομένων, οι τύποι δεδομένων, υπηρεσιών και ρόλων, οι Σύνοδοι και οι Συναλλαγές Ιδιωτικότητας. Επίσης, πραγματοποιείται μία εκτενής εισαγωγή στην προτεινόμενη λύση που έχει ως βασικό στόχο την περιγραφή του τρόπου με τον οποίο ολοκληρώνονται μεταξύ τους οι μηχανισμοί που περιγράφονται στα επόμενα Κεφάλαια.

4.1 Νομικές και Κανονιστικές Απαιτήσεις

Στο Κεφάλαιο 2 παρουσιάστηκε το Νομικό και Κανονιστικό Πλαίσιο που διέπει την προστασία των προσωπικών δεδομένων. Το πλαίσιο αυτό αντανακλά ουσιαστικά τις απαιτήσεις για το προτεινόμενο τεχνολογικό σύστημα που στοχεύει στην προστασία των προσωπικών δεδομένων σε έξυπνα περιβάλλοντα. Οι νομικές απαιτήσεις μπορούν να συνοψιστούν / κωδικοποιηθούν ως εξής:

- **Νομιμότητα της επεξεργασίας των δεδομένων**: Το σύστημα θα πρέπει να είναι σε θέση να εξετάζει εάν η συλλογή και επεξεργασία των δεδομένων βρίσκεται σε συμφωνία με τους ισχύοντες νόμους και κανονισμούς.
- **Σκοπός της επεξεργασίας των δεδομένων**: Το σύστημα θα πρέπει να παρέχει τα μέσα για την ταυτοποίηση των σκοπών της συλλογής και επεξεργασίας δεδομένων, οι οποίοι θα πρέπει να είναι έννομοι και να κοινοποιούνται με σαφήνεια στο υποκείμενο των δεδομένων. Επιπλέον, θα πρέπει το σύστημα να είναι σε θέση να πραγματοποιεί έλεγχο των σκοπών συλλογής και επεξεργασίας, ούτως ώστε να αποφεύγεται η περαιτέρω επεξεργασία δεδομένων για σκοπούς άλλους από εκείνους για τους οποίους πραγματοποιήθηκε η συλλογή τους.

- **Αναγκαιότητα, καταλληλότητα και αναλογικότητα των δεδομένων υπό επεξεργασία**: Το σύστημα θα πρέπει να είναι σε θέση να εγγυηθεί ότι υφίστανται επεξεργασία μόνο δεδομένα τα οποία είναι λειτουργικά, απαραίτητα, συναφή προς το θέμα και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους συλλέγονται.
- **Ποιότητα των δεδομένων υπό επεξεργασία**: Το σύστημα θα πρέπει να φροντίζει ότι τα δεδομένα υπό επεξεργασία είναι σωστά, ακριβή και ενημερωμένα. Σε αντίθετη περίπτωση, τα δεδομένα θα πρέπει διορθώνονται, ενημερώνονται ή διαγράφονται.
- **Ταυτοποιήσιμα δεδομένα**: Το σύστημα θα πρέπει να παρέχει τα μέσα ούτως ώστε τα δεδομένα που υφίστανται επεξεργασία να διατηρούνται σε μορφή που να ταυτοποιούν το υποκείμενο των δεδομένων μόνο για το χρονικό διάστημα το οποίο είναι απαραίτητο προκειμένου να επιτευχθούν οι σκοποί της επιδιωχθείσας επεξεργασίας.
- **Πληροφόρηση των υποκειμένων των δεδομένων – συγκατάθεση και δικαιώματα πρόσβασης των υποκειμένων των δεδομένων**: Το σύστημα θα πρέπει να έχει τη δυνατότητα να ενημερώνει τα υποκείμενα των δεδομένων αναφορικά με την επεξεργασία των δεδομένων τους. Επιπλέον, το σύστημα θα πρέπει να εγγυάται ότι η ρητή συγκατάθεση των υποκειμένων των δεδομένων θα απαιτείται προκειμένου να πραγματοποιηθεί επεξεργασία των δεδομένων, εφόσον η ισχύουσα νομοθεσία ορίζει σχετικά, ενώ η επεξεργασία οποιασδήποτε μορφής των δεδομένων θα λαμβάνει χώρα λαμβάνοντας υπόψη τις προτιμήσεις των υποκειμένων των δεδομένων αναφορικά με την ιδιωτικότητα. Επιπροσθέτως, το σύστημα θα πρέπει να παρέχει τη δυνατότητα στα υποκείμενα των δεδομένων να εξασκούν τα δικαιώματα πρόσβασης στα δεδομένα τους τα οποία προβλέπονται από την ισχύουσα νομοθεσία. Τέτοια δικαιώματα πρόσβασης αφορούν –για παράδειγμα– την ενημέρωση των δεδομένων τα οποία βρίσκονται αποθηκευμένα σε κάποια βάση δεδομένων, τη διαγραφή τους, το δικαίωμα αποτροπής της επεξεργασίας τους, κλπ.
- **Δεδομένα θέσης και κίνησης – ειδικές κατηγορίες δεδομένων**: Το σύστημα θα πρέπει να είναι σε θέση να εγγυηθεί ότι η επεξεργασία ειδικών κατηγοριών δεδομένων θα πραγματοποιείται σε συμφωνία με τις συγκεκριμένες απαιτήσεις

οι οποίες ορίζονται από την ισχύουσα νομοθεσία. Για παράδειγμα, ως ειδικές κατηγορίες δεδομένων θεωρούνται τα δεδομένα κίνησης και θέσης στο πλαίσιο κάποιας επικοινωνίας, δικαστικά και άλλα ευαίσθητα δεδομένα, κλπ.

- **Περιορισμός της πρόσβασης**: Το σύστημα τα πρέπει να παρέχει διαδικασίες εξουσιοδοτημένης πρόσβασης στα δεδομένα, το επίπεδο της οποίας θα πρέπει απαραιτήτως να διαφοροποιείται με βάση διάφορα κριτήρια. Επιπλέον, κάθε πρόσβαση σε δεδομένα θα πρέπει να καταγράφεται.

- **Ασφάλεια δεδομένων και εμπιστευτικότητα**: Το σύστημα τα πρέπει να είναι ασφαλές, ούτως ώστε να είναι σε θέση να εγγυηθεί την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα των δεδομένων. Επιπλέον, το σύστημα θα πρέπει να είναι σε θέση να αποτρέπει την οποιαδήποτε υποκλοπή ή παρακολούθηση των δεδομένων εκτός εάν υπάρχει η ρητή συγκατάθεση του υποκειμένου των δεδομένων ή εφόσον προβλέπεται από την ισχύουσα νομοθεσία για λόγους που τεκμηριώνονται από το δημόσιο συμφέρον.

- **Αποθήκευση δεδομένων**: Το σύστημα θα πρέπει να διαγράφει ή καθιστά ανώνυμα με αυτόματο τρόπο εκείνα τα δεδομένα για τα οποία η αναγκαιότητά τους για την επίτευξη κάποιου σκοπού έχει λήξει ή για τα οποία έχει παρέλθει το οριζόμενο βάσει της νομοθεσίας χρονικό διάστημα διατήρησής τους.

- **Ειδοποιήσεις και λοιπές αρμοδιότητες / εξουσιοδοτήσεις των αρμοδίων Αρχών**: Το σύστημα θα πρέπει να έχει τη δυνατότητα να παρακολουθεί τη συμμόρφωση με την απαίτηση για την παροχή ειδοποιήσεων προς την αρμόδια Αρχή Προστασίας Δεδομένων, καθώς και την παροχή οποιασδήποτε άλλης αρμοδιότητας / εξουσιοδότησης διαθέτει η Αρχή. Επιπλέον, το σύστημα θα πρέπει να παρέχει τα μέσα επικοινωνίας μεταξύ της Αρχής και του συστήματος.

- **Εποπτεία και επιβολή προστίμων**[1]: Οι αρμόδιες Αρχές Προστασίας Δεδομένων θα πρέπει να διαθέτουν τη δυνατότητα εποπτείας και ελέγχου όλων των ενεργειών συλλογής και επεξεργασίας προσωπικών δεδομένων.

[1] Εξυπακούεται ότι η επιβολή προστίμων δεν είναι δυνατό να αποτελεί αντικείμενο ενός τεχνολογικού συστήματος· αναφέρεται ωστόσο εδώ για λόγους πληρότητας.

- **Νόμιμη παρακολούθηση και συλλογή δεδομένων** (**Lawful Interception – LI**): Οι αρμόδιες Αρχές Προστασίας Δεδομένων θα πρέπει να διαθέτουν τη δυνατότητα πραγματοποίησης παρακολούθησης και συλλογής δεδομένων μέσω του συστήματος, εφόσον κάτι τέτοιο προβλέπεται από την ισχύουσα νομοθεσία και εφόσον πληρούνται οι σχετικές συνθήκες για την απόδοση τέτοιων εξουσιοδοτήσεων. Τα σχετικά επικοινωνιακά κανάλια και διεπαφές δε θα πρέπει σε καμία περίπτωση να διατίθενται σε άλλες οντότητες πέρα από τις αρμόδιες Αρχές.

Οι παραπάνω απαιτήσεις θα αποτελέσουν τη βάση για το σχεδιασμό της προτεινόμενης λύσης, όπως θα περιγραφεί αναλυτικά στη συνέχεια της Διατριβής.

4.2 Βασικές Αρχές της Προτεινόμενης Λύσης

Με βάση την παραπάνω κωδικοποίηση των Νομικών και Κανονιστικών απαιτήσεων, προκύπτουν οι εξής απαιτήσεις:

- **Έλεγχος πρόσβασης**: Όπως είναι μάλλον αυτονόητο, βασική προϋπόθεση για την προστασία της ιδιωτικότητας είναι η οποιαδήποτε πρόσβαση στα προσωπικά δεδομένα να είναι ελεγχόμενη.
- **Συμπληρωματικές ενέργειες**: Σε πολλές περιπτώσεις, η πρόσβαση σε δεδομένα θα πρέπει να συνοδεύεται από κάποιες συμπληρωματικές ενέργειες, όπως είναι η ενημέρωση του υποκειμένου των δεδομένων ή το αίτημα για παροχή ρητής συναίνεσης πριν την εκτέλεση της διαδικασίας.
- **Σημασιολογική βάση**: Ο έλεγχος πρόσβασης στα προσωπικά δεδομένα βασίζεται σε μεγάλο βαθμό στη σημασιολογική φύση των ίδιων των προσωπικών δεδομένων, του σκοπού συλλογής, επεξεργασίας και γενικά πρόσβασης σε αυτά, της οντότητας που τα συλλέγει ή/και τα επεξεργάζεται.
- **Ενεργός ρόλος της Αρχής Ιδιωτικότητας**: Θα πρέπει να παρέχονται διάφορες δυνατότητες στην Αρχή Ιδιωτικότητας ή κάποια άλλη εντεταλμένη αρχή. Οι δυνατότητες αυτές αφορούν την ενημέρωση της Αρχής για κρίσιμα συμβάντα, καθώς και την ενεργό εποπτεία και έλεγχο.
- **Συμμετοχή του υποκειμένου των δεδομένων**: Βάσει της Νομοθεσίας, ο χρήστης (υποκείμενο των δεδομένων) θα πρέπει να έχει τη δυνατότητα ενεργούς

συμμετοχής στην όλη διαδικασία. Η συμμετοχή του χρήστη αφορά τους εξής άξονες: ο χρήστης θα πρέπει να έχει πρόσβαση στα δεδομένα, θα πρέπει να ενημερώνεται για την επεξεργασία τους, να ζητείται η ρητή συναίνεσή του για κάθε ενέργεια συλλογής ή επεξεργασίας, καθώς και να λαμβάνονται υπόψη οι προτιμήσεις ιδιωτικότητας που έχει προσδιορίσει.

- **Μηχανισμοί ασφάλειας**: Όπως είναι φυσικό, η Νομοθεσία απαιτεί την ύπαρξη των κατάλληλων μηχανισμών για την προστασία των δεδομένων, τόσο κατά τη μετάδοση όσο και κατά την αποθήκευσή τους.

Πέρα από τα παραπάνω, η πρόταση που παρουσιάζεται βασίζεται σε δύο βασικές αρχές:

- Από τη στιγμή που κάποια πληροφορία διατεθεί σε κάποιον πάροχο υπηρεσίας, δεν υπάρχει κανένα τεχνικό μέσο που να μπορεί να διασφαλίσει ότι η περαιτέρω επεξεργασία και χρήση της θα είναι σύννομη και θεμιτή. Δηλαδή, τα προσωπικά δεδομένα καθίστανται αυτομάτως απροστάτευτα απέναντι σε ενδεχόμενη κατάχρηση από την πλευρά του παρόχου.
- Όποια Πολιτική Ιδιωτικότητας και να δηλώνει κάποιος πάροχος υπηρεσιών αναφορικά με τη χρήση των προσωπικών δεδομένων που βρίσκονται στην κατοχή του, η εφαρμογή της πολιτικής αυτής δεν μπορεί να διασφαλιστεί. Δηλαδή, οι χρήστες δε διαθέτουν καμία εγγύηση αναφορικά με την εφαρμογή ή μη από τον πάροχο της Πολιτικής Ιδιωτικότητας την οποία δηλώνει. Εξάλλου, υπάρχουν αναρίθμητα παραδείγματα όπου οι τελικές πρακτικές των παρόχων υπηρεσιών έρχονται σε πλήρη αντίθεση με τις δεδηλωμένες Πολιτικές Ιδιωτικότητας, π.χ. [106], [107], [108].

Ως εκ τούτου, η προτεινόμενη λύση φιλοδοξεί να διευθετήσει τα ως άνω περιγραφόμενα προβλήματα που χαρακτηρίζουν την κατοχή προσωπικών δεδομένων από κάποιο πάροχο υπηρεσιών. Προκειμένου να επιτευχθεί αυτό, η προτεινόμενη λύση υιοθετεί δύο πρακτικές:

- Ελαχιστοποίηση των προσωπικών δεδομένων τα οποία διατίθενται στους παρόχους υπηρεσιών. Σύμφωνα με την πρακτική αυτή, μόνο τα απολύτως απαραίτητα δεδομένα και στον απαραίτητο βαθμό ακρίβειας προκειμένου να

είναι δυνατή η παροχή της υπηρεσίας διατίθενται στον εκάστοτε πάροχο υπηρεσίας.

- Η Πολιτική Ιδιωτικότητας του κάθε παρόχου καταργείται, υπό την έννοια ότι εφαρμόζεται μία ενιαία Πολιτική Ιδιωτικότητας για όλους τους παρόχους υπηρεσιών. Η εφαρμογή της πολιτικής αυτής επιβάλλεται και ελέγχεται μέσω τεχνικής διαδικασίας η οποία δεν μπορεί να παραβιαστεί και η οποία εμπεριέχει όλες τις αρχές της Νομοθεσίας που διέπουν τη συλλογή και επεξεργασία των προσωπικών δεδομένων.

4.3 Κατηγορίες Προσωπικών Δεδομένων

Προκειμένου να οριστεί μία αποτελεσματική αρχιτεκτονική η οποία θα είναι σε θέση να διευθετήσει το ζήτημα της προστασίας των προσωπικών δεδομένων, κρίνεται σκόπιμος ο ορισμός μίας κατηγοριοποίησης των προσωπικών δεδομένων, βάσει κάποιων ιδιαίτερων χαρακτηριστικών τους.

Στο πλαίσιο αυτό, μπορούμε να κατηγοριοποιήσουμε τα προσωπικά δεδομένα στις εξής τρεις βασικές κατηγορίες:

- **Ενεργά προσωπικά δεδομένα**: χαρακτηρίζονται τα προσωπικά δεδομένα τα οποία ο χρήστης παρέχει οικιοθελώς και με τρόπο ο οποίος του δίνει τη δυνατότητα της παροχής τους ή μη. Τα δεδομένα αυτά συνήθως μεταδίδονται από το τερματικό του χρήστη. Για παράδειγμα, ο αριθμός της πιστωτικής κάρτας ενός χρήστη όταν συμπληρώνεται σε κάποια Διαδικτυακή φόρμα ως απαίτηση για τη χρέωση κάποιας υπηρεσίας αποτελεί ενεργό προσωπικό δεδομένο. Χαρακτηριστικό των ενεργών προσωπικών δεδομένων είναι ότι στις περισσότερες περιπτώσεις ταυτοποιούν το χρήστη που τα παρέχει, είτε αμέσως, είτε εμμέσως, δηλαδή σε συνδυασμό με άλλα δεδομένα οποιουδήποτε τύπου.

- **Ημιενεργά προσωπικά δεδομένα**: έτσι μπορούν να χαρακτηριστούν εκείνα τα προσωπικά δεδομένα τα οποία μεταδίδονται με τη μερική, έμμεση επί της ουσίας, συμμετοχή του χρήστη. Με αυτό εννοούνται είτε εκείνα τα δεδομένα τα οποία συλλέγονται από αισθητήρες ή RFIDs [7], είτε διάφορα μεταδεδομένα τα οποία συλλέγονται στο πλαίσιο διεξαγωγής ηλεκτρονικών επικοινωνιών, όπως για παράδειγμα η ημερομηνία και ώρα έναρξης μίας τηλεφωνικής κλήσης ή

διαδικτυακής συνόδου. Λαμβάνοντας υπόψη ότι τα δεδομένα από αισθητήρες και RFIDs έχουν στις περισσότερες περιπτώσεις σκοπό την αναγνώριση του χρήστη και ότι τα μεταδεδομένα των ηλεκτρονικών επικοινωνιών σχετίζονται με την ταυτότητα του χρήστη, μπορούμε να θεωρήσουμε ότι τα ημιενεργά προσωπικά δεδομένα γενικά ταυτοποιούν τους χρήστες. Σημαντική ιδιαιτερότητα των ημιενεργών δεδομένων αποτελεί το και γεγονός ότι γενικά συλλέγονται απευθείας από τον εμπλεκόμενο πάροχο υπηρεσίας, χωρίς να παρεμβάλλεται ο χρήστης ή να είναι εύκολη η παρεμβολή κάποιου συστήματος προστασίας της ιδιωτικότητας κατά τη συλλογή.

- **Παθητικά προσωπικά δεδομένα**: πρόκειται για εκείνα τα δεδομένα στα οποία ο χρήστης δεν έχει καμία ενεργό συμμετοχή στη συλλογή ή επεξεργασία τους. Χαρακτηριστικό παράδειγμα αποτελούν τα δεδομένα εκείνα τα οποία αποτελούν το αντικείμενο των μηχανών λήψης σταθερή ή κινούμενης εικόνας. Χαρακτηριστικά των δεδομένων αυτού του τύπου είναι ότι ο χρήστης δε διαθέτει στην πράξη κανένα μηχανισμό άμυνας απέναντι στη συλλογή και επεξεργασία τους και το ότι στη γενική περίπτωση δεν ταυτοποιούν τους χρήστες, παρά μόνο σε συνδυασμό με άλλα δεδομένα ταυτοποίησης.

Σημειώνεται ότι η κατηγορία στην οποία κατατάσσονται τα προσωπικά δεδομένα μπορεί να διαφέρει από περίπτωση σε περίπτωση. Για παράδειγμα, όταν κάποιος χρήστης για την παροχή κάποιας υπηρεσίας βασισμένης στη θέση (Location-Based Service – LBS) δηλώνει τη θέση του συμπληρώνοντας κάποιο σχετικό πεδίο σε μία Διαδικτυακή φόρμα, η θέση του αποτελεί ενεργό προσωπικό δεδομένο. Αντίθετα, όταν η θέση ενός χρήστη προκύπτει από το γεωγραφικό εντοπισμό ενός κινητού τερματικού κατά τη διάρκεια μίας συνόδου κινητής τηλεφωνίας, τότε η θέση αποτελεί ημιενεργό προσωπικό δεδομένο.

4.4 Τύποι Προσωπικών Δεδομένων, Υπηρεσιών και Ρόλων

Εκτός από την κατηγορία στην οποία κατατάσσονται κατά περίπτωση τα προσωπικά δεδομένα, πολύ σημαντική μπορεί να θεωρηθεί η ταξινόμησή τους με βάση τον τύπο τους. Ως τύπος ενός προσωπικού δεδομένου νοείται εκείνη η έννοια ή πληροφορία η οποία εκφράζεται μέσω του δεδομένου αυτού. Για παράδειγμα, η θέση

ενός χρήστη με τη μορφή γεωγραφικών συντεταγμένων εκφράζει κάτι πολύ συγκεκριμένο: την ακριβή τοποθεσία στην οποία βρίσκεται ο εν λόγω χρήστης. Είτε αποτελεί ενεργό είτε ημιενεργό προσωπικό δεδομένο (όπως φάνηκε στο παράδειγμα της προηγούμενης Ενότητας), ο τύπος του είναι συγκεκριμένος και καθορίζεται από το νόημα της πληροφορίας η οποία εξάγεται από αυτό αναφορικά με το υποκείμενο των δεδομένων.

Αναλόγως, μπορεί να οριστεί και μία ταξινόμηση των δυνατών διαθέσιμων υπηρεσιών σε σχέση με τον τύπο τους. Ο τύπος μίας υπηρεσίας αποτελεί φορμαλιστική έκφραση του περιεχομένου της υπηρεσίας, δηλαδή του τι ακριβώς η συγκεκριμένη υπηρεσία παρέχει. Έτσι, ένας τύπος υπηρεσίας "εύρεση φαρμακείων που διανυκτερεύουν σε συγκεκριμένη περιοχή" είναι διαφορετικός από τον τύπο "εύρεση φαρμακείων σε συγκεκριμένη περιοχή" (δηλαδή ανεξάρτητα από το αν τα φαρμακεία διανυκτερεύουν ή όχι), παρόλο που ο πρώτος τύπος μπορεί να θεωρηθεί υποπερίπτωση του δεύτερου, ενώ όλοι οι πάροχοι υπηρεσιών των οποίων το αντικείμενο αποτελεί η εύρεση για λογαριασμό του χρήστη των φαρμακείων που διανυκτερεύουν με δεδομένη τη θέση του χρήστη, παρέχουν υπηρεσία του τύπου "εύρεση φαρμακείων που διανυκτερεύουν σε συγκεκριμένη περιοχή". Μία τέτοια ταξινόμηση των δυνατών διαθέσιμων υπηρεσιών μπορεί να παραλληλιστεί με το Κοινό Λεξιλόγιο για τις Δημόσιες Συμβάσεις (Common Procurement Vocabulary – CPV) [109], το οποίο αποτελεί ένα ιεραρχικό σύστημα ταξινόμησης των δημοσίων συμβάσεων και προσφέρει ένα ενιαίο σύστημα αναφοράς στα κράτη – μέλη της Ευρωπαϊκής Κοινότητας.

Οι ταξινομήσεις των υπηρεσιών, των προσωπικών δεδομένων, αλλά και των ρόλων των εμπλεκομένων οντοτήτων είναι ιδιαιτέρως χρήσιμες για τον καθορισμό κανόνων αναφορικά με τους τύπους προσωπικών δεδομένων που είναι αναγκαίοι για την παροχή του κάθε τύπου υπηρεσίας, καθώς όπως τονίστηκε στην Ενότητα 4.2 υπάρχει η ανάγκη για σημασιολογική βάση. Σύμφωνα με τις βασικές αρχές για την προστασία των προσωπικών δεδομένων και τη σχετική Νομοθεσία, κάθε προσωπική πληροφορία πρέπει να συλλέγεται και να υφίσταται επεξεργασία προκειμένου να εξυπηρετήσει συγκεκριμένο σκοπό, για τον οποίο είναι απαραίτητη. Προκειμένου να οριστούν κανόνες αναφορικά με την αναγκαιότητα συλλογής και επεξεργασίας κάποιας προσωπικής πληροφορίας για την παροχή κάποιας υπηρεσίας από κάποια συγκεκριμένη οντότητα,

είναι απαραίτητη η ύπαρξη κάποιας φορμαλιστικής ταξινόμησης των προσωπικών δεδομένων, των υπηρεσιών και των ρόλων.

Περισσότερες πληροφορίες αναφορικά με τις φορμαλιστικές ταξινομήσεις των προσωπικών δεδομένων, των υπηρεσιών και των ρόλων παρέχονται στο Κεφάλαιο 5 "Οντολογία Ιδιωτικότητας" και ιδιαιτέρως στην περιγραφή του Σημασιολογικού Μοντέλου Πληροφοριών (Ενότητα 5.2).

4.5 Γενική Περιγραφή της Προτεινόμενης Αρχιτεκτονικής

Όπως προαναφέρθηκε, η προτεινόμενη αρχιτεκτονική βασίζεται σε δύο θεμελιώδεις αρχές:

- Ελαχιστοποίηση των προσωπικών δεδομένων τα οποία διατίθενται στους παρόχους υπηρεσιών.
- Επιβολή μίας ενιαίας Πολιτικής Ιδιωτικότητας για όλους τους παρόχους υπηρεσιών και επιβολή και έλεγχος της εφαρμογής της με χρήση τεχνολογικών μέσων.

Προκειμένου να επιτευχθεί ο πρώτος από τους παραπάνω στόχους – αρχές, είναι απαραίτητη η απομόνωση των προσωπικών δεδομένων από τους παρόχους υπηρεσιών. Δηλαδή, πρέπει να επιτευχθεί – στο μέτρο του δυνατού – ο διαχωρισμός του χώρου αποθήκευσης των προσωπικών δεδομένων από την επιχειρησιακή λογική της υπηρεσίας. Επιπλέον, εφόσον κάποια δεδομένα πρέπει αναπόφευκτα να διατεθούν στους παρόχους για την παροχή της υπηρεσίας, τα δεδομένα αυτά πρέπει να σχετίζονται στο μικρότερο δυνατό βαθμό και ιδανικά καθόλου με την ταυτότητα του χρήστη τον οποίο αφορά η υπηρεσία.

Από την άλλη, προκειμένου να επιτευχθεί ο δεύτερος από τους παραπάνω στόχους – αρχές, είναι απαραίτητη η ανάπτυξη ενός μηχανισμού ο οποίος θα είναι σε θέση να επιβάλλει την εφαρμογή μίας συγκεκριμένης Πολιτικής Ιδιωτικότητας, η οποία θα είναι βασισμένη στη σχετική Νομοθεσία περί της προστασίας των προσωπικών δεδομένων και δε θα αφήνει περιθώρια στον πάροχο κάποιας υπηρεσίας να επιβουλευθεί και εκμεταλλευτεί προς όφελός του τα προσωπικά δεδομένα τα οποία κάποιος χρήστης έχει παραχωρήσει αμέσως ή εμμέσως, προκειμένου να του παρασχεθεί

κάποια υπηρεσία. Η Πολιτική Ιδιωτικότητας συνίσταται στην εφαρμογή ελέγχου πρόσβασης στα δεδομένα, αλλά και τη συνακόλουθη εφαρμογή των απαραίτητων συμπληρωματικών ενεργειών (π.χ. αίτημα ρητής συναίνεσης από το υποκείμενο των δεδομένων).

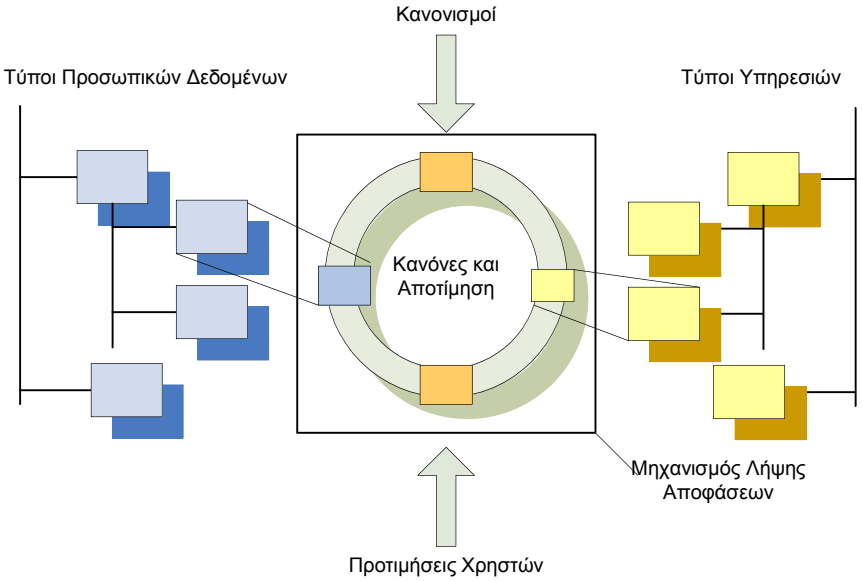
Στην ως άνω αναφερόμενη ενιαία Πολιτική Ιδιωτικότητας, πρέπει να προστεθεί και η ανάγκη για συμμετοχή του χρήστη στον καθορισμό της περαιτέρω χρήσης των προσωπικών του δεδομένων. Η συμμετοχή αυτή αφορά κυρίως το δικαίωμα της πρόσβασης, όπως αυτό ορίζεται από τη νομοθεσία. Το δικαίωμα αυτό αναφέρεται στην ενημέρωση του χρήστη όταν λαμβάνει χώρα επεξεργασία των προσωπικών του δεδομένων και ενημέρωση σχετικά με το σκοπό της επεξεργασίας, τους αποδέκτες της, ή οποιαδήποτε άλλη σχετική πληροφορία, τη ζήτηση της συναίνεσης του χρήστη, όπου αυτή είναι απαραίτητη, πριν από κάθε ενέργεια που αφορά σε χρήση των προσωπικών του δεδομένων, την παροχή της δυνατότητας της άμεσης επέμβασης του χρήστη στα προσωπικά του δεδομένα (τροποποίηση, διαγραφή, κλείδωμα, κλπ.), και γενικά την παροχή της δυνατότητας στο υποκείμενο των δεδομένων να καθορίζει το ίδιο τη μοίρα των προσωπικών του δεδομένων ακόμα και μετά τη στιγμή της συλλογής τους από κάποιο πάροχο υπηρεσίας.

Επιπλέον, δε θα πρέπει να παραλειφθεί ως απαίτηση από ένα τέτοιο σύστημα η συμμετοχή της Αρχής Ιδιωτικότητας, υπό την έννοια ενός ενεργού ρόλου στην εποπτεία και διαχείριση των λειτουργιών ιδιωτικότητας. Εδώ περιλαμβάνεται και η δυνατότητα για νόμιμη παρακολούθηση και συλλογή προσωπικών δεδομένων (Lawful Interception – LI), όπως ορίζεται από την Εθνική και Ευρωπαϊκή Νομοθεσία (π.χ., το Προεδρικό Διάταγμα 47/2005 [40]). Οι αρμόδιες Αρχές πρέπει να διαθέτουν τη δυνατότητα αυτή, με τρόπο τέτοιο όμως που να εξασφαλίζεται η νομιμότητα, η διαφάνεια και η εκπλήρωση των προϋποθέσεων που απαιτούνται για το σκοπό αυτό. Επιπλέον, θα πρέπει να καθίσταται αδύνατη η εκμετάλλευση της δυνατότητας αυτής από τρίτες οντότητες για μη θεμιτούς σκοπούς.

Μία σχετικά προφανής τεχνική λύση η οποία εξετάστηκε στο πλαίσιο της Διατριβής και η οποία θα ικανοποιούσε τις παραπάνω απαιτήσεις υπό την έννοια ότι απομονώνει τα προσωπικά δεδομένα από την επιχειρησιακή λογική των υπηρεσιών θα ήταν η διατήρηση όλων των προσωπικών δεδομένων στο τερματικό του χρήστη και η χρήση Κινητού Κώδικα (Mobile Code) [110] ιδιοκτησίας του παρόχου της εκάστοτε

υπηρεσίας, ο οποίος μεταναστεύοντας στο τερματικό του χρήστη θα μπορούσε να εκτελεί τις απαραίτητες διεργασίες για την παροχή της υπηρεσίας. Ωστόσο, μία τέτοια προσέγγιση κρίνεται ως μη πρακτική καθώς, πέρα από τα μεγάλα προβλήματα ασφάλειας τα οποία δημιουργεί [111], βρίσκει εφαρμογή μόνο σε ενεργά δεδομένα ενώ υπόκειται στους περιορισμούς που θέτει το τερματικό του χρήστη αναφορικά με ενεργειακή αυτονομία, επεξεργαστική ισχύ, υποστηριζόμενες τεχνολογίες κλπ. Αντίστοιχα, η προσέγγιση της υιοθέτησης μίας κεντρικής έμπιστης οντότητας της οποίας η παρεμβολή μεταξύ χρηστών και παρόχων δικτύωσης και υπηρεσιών θα διασφάλιζε την εφαρμογή των κανόνων ιδιωτικότητας παρουσιάζει μειονεκτήματα που καθιστούν μία τέτοια λύση μη πρακτική και ανεφάρμοστη. Τα μειονεκτήματα μίας τέτοιας προσέγγισης αναφέρονται αφενός στη δημιουργία ενός μοναδικού σημείου αποτυχίας (single point of failure) και αφετέρου στο διαχειριστικό κόστος που δημιουργεί.

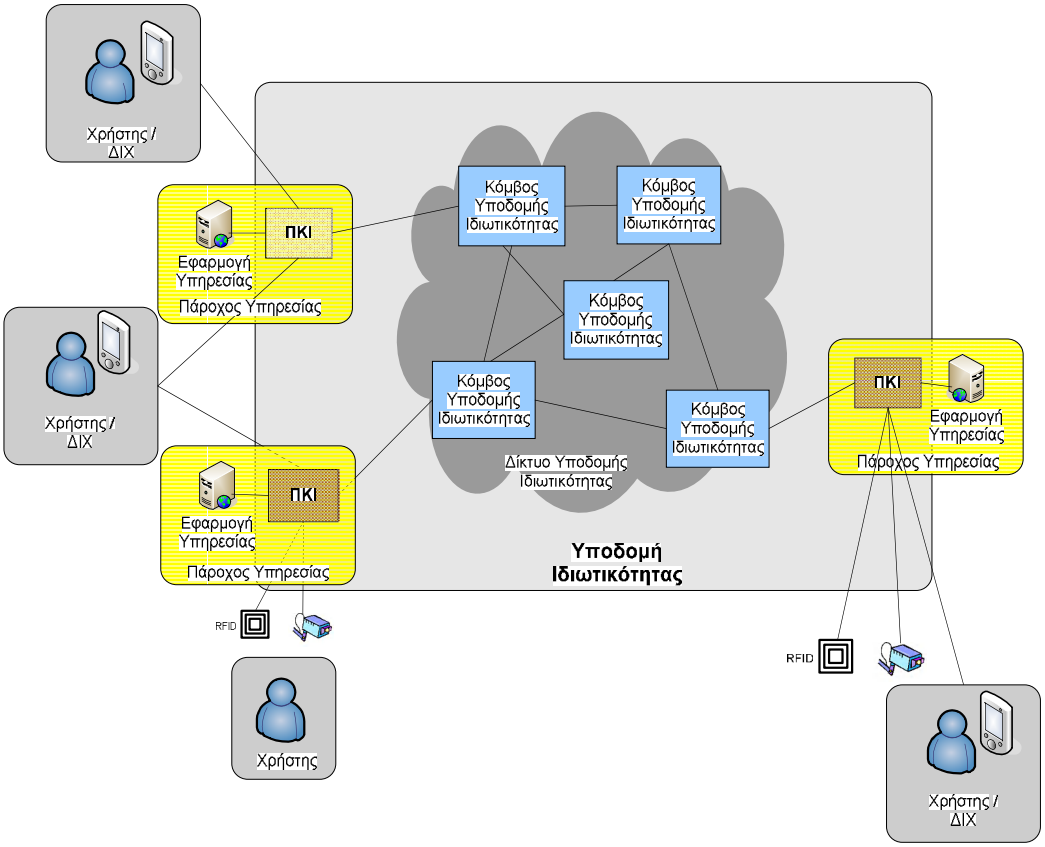
Για την εκπλήρωση των ως άνω περιγραφόμενων απαιτήσεων, η προτεινόμενη αρχιτεκτονική ορίζει ένα πλήρες σύνολο συστημάτων και λειτουργιών, τα οποία ενοποιούνται σε ένα κατανεμημένο σύστημα μεσισμικού. Το βασικότερο δομικό συστατικό του συστήματος αποτελεί ο Πληρεξούσιος Κόμβος Ιδιωτικότητας (ΠΚΙ), ο οποίος αποτελεί το σύνορο μεταξύ της υποδομής υλικού και λογισμικού του παρόχου υπηρεσιών και των υπολοίπων συστατικών της αρχιτεκτονικής, δηλαδή των δικτύων μετάδοσης, των τερματικών των χρηστών, των μηχανισμών συλλογής δεδομένων (π.χ. κάμερες, αισθητήρες, κλπ.) και των βοηθητικών λειτουργικών και διαχειριστικών δομικών συστατικών που εισάγονται από την παρούσα προτεινόμενη προσέγγιση. Ο ΠΚΙ αποτελεί επί της ουσίας έναν πληρεξούσιο εξυπηρετητή (proxy server), ο οποίος παρεμβάλλεται μεταξύ χρήστη και παρόχου υπηρεσίας και ελέγχεται από κάποια Αρχή Ιδιωτικότητας ή άλλη εντεταλμένη και εξουσιοδοτημένη για το σκοπό αυτό αρχή, μεριμνώντας για την εφαρμογή των νομικών κανόνων αναφορικά με την προστασία των προσωπικών δεδομένων αλλά και των αντίστοιχων προτιμήσεων των χρηστών. Προκειμένου να επιτευχθεί αυτό, ο ΠΚΙ ενσωματώνει ένα μηχανισμό λήψης αποφάσεων, ο οποίος βασίζεται στους κανόνες της νομοθεσίας, τις εκάστοτε προτιμήσεις των χρηστών, και στους τύπους των υπηρεσιών υπό παροχή και των διαφόρων τύπων προσωπικών δεδομένων, όπως αυτοί ορίστηκαν στην Ενότητα 4.4, ενώ λαμβάνει υπόψη τους ρόλους των εμπλεκομένων οντοτήτων. Η ιδέα αυτή απεικονίζεται στο Σχήμα 14:



Σχήμα 14: Μηχανισμός Λήψης Αποφάσεων του Πληρεξούσιου Κόμβου Ιδιωτικότητας.

Παρόλο που ο ΠΚΙ ελέγχεται από κάποια Αρχή Ιδιωτικότητας ή άλλη εντεταλμένη και εξουσιοδοτημένη αρχή, θεωρείται ότι αποτελεί μέρος του εξοπλισμού του παρόχου υπηρεσίας και ότι η εγκατάστασή του πραγματοποιείται στο – φυσικό ή λογικό – χώρο του τελευταίου. Ενσωματώνει το χώρο που αποθηκεύονται τα προσωπικά δεδομένα των χρηστών των παρεχομένων υπηρεσιών και, σύμφωνα με το μηχανισμό λήψης αποφάσεων που περιγράφεται παραπάνω, φροντίζει για την τήρηση της νομοθεσίας και των προτιμήσεων ιδιωτικότητας των χρηστών σε ό,τι αφορά τη διάθεση των δεδομένων και τη συνακόλουθη επεξεργασία τους, αλλά και την εφαρμογή των βασικών αρχών ιδιωτικότητας γενικότερα.

Τα υπόλοιπα δομικά στοιχεία που συμπληρώνουν την προτεινόμενη αρχιτεκτονική μεσισμικού είναι ο Διαχειριστής Ιδιωτικότητας Χρήστη και οι Κόμβοι Υποδομής Ιδιωτικότητας, οι οποίοι σχηματίζουν το Δίκτυο Υποδομής Ιδιωτικότητας. Συνολικά, η προτεινόμενη αρχιτεκτονική παρουσιάζεται στο Σχήμα 15.



Σχήμα 15: Αρχιτεκτονική Μεσισμικού Προστασίας Προσωπικών Δεδομένων.

Όπως φαίνεται στο σχήμα, η αρχιτεκτονική μπορεί να διαχωριστεί λειτουργικά σε τρεις τομείς: Ο πρώτος τομέας είναι εκείνος των χρηστών, δηλαδή ο τομέας από τον οποίο πηγάζουν τα προσωπικά δεδομένα. Το δομικό στοιχείο της αρχιτεκτονικής που αφορά στον τομέα των χρηστών είναι ο Διαχειριστής Ιδιωτικότητας Χρήστη (ΔΙΧ), ο οποίος αποτελεί μέρος του τερματικού του χρήστη. Ο σκοπός του ΔΙΧ είναι να αποτελέσει τη διεπαφή του χρήστη με το σύστημα αναφορικά με ζητήματα ιδιωτικότητας, ενσωματώνοντας λειτουργίες όπως ο ορισμός και η διαχείριση προτιμήσεων, η διαχείριση και προστασία προσωπικών δεδομένων σε πρώτο στάδιο, η διεκπεραίωση ζητημάτων ενημέρωσης και παροχής συναίνεσης και διάφορες άλλες λειτουργίες.

Ο δεύτερος λειτουργικός τομέας της αρχιτεκτονικής είναι αυτός του παρόχου υπηρεσιών. Εκεί εδράζουν οι εφαρμογές λογισμικού για την παροχή της υπηρεσίας, δηλαδή οι εφαρμογές που συλλέγουν και επεξεργάζονται προσωπικά δεδομένα.

Τέλος, ο τρίτος λειτουργικός τομέας της προτεινόμενης αρχιτεκτονικής είναι η έμπιστη Υποδομή Ιδιωτικότητας, δηλαδή το μέρος εκείνο του συστήματος που ελέγχεται από κάποια Αρχή Ιδιωτικότητας ή άλλη εντεταλμένη και εξουσιοδοτημένη αρχή. Οι Κόμβοι Υποδομής Ιδιωτικότητας (ΚΥΙ) αποτελούν τα δομικά συστατικά της αρχιτεκτονικής στον τομέα αυτό και οποία συνιστούν τα σημεία εισόδου της Αρχής Ιδιωτικότητας στο όλο σύστημα, εξυπηρετώντας τους σκοπούς της διαχείρισης και εποπτείας των ΠΚΙ, της διάδοσης των τελευταίων εκδόσεων της σχετικής νομοθεσίας στα ΠΚΙ και της διεξαγωγής της νόμιμης παρακολούθησης. Οι ΚΥΙ σχηματίζουν το Δίκτυο Υποδομής Ιδιωτικότητας (ΔΥΙ) που αποτελεί ένα πλέγμα από διασυνδεδεμένες οντότητες οι οποίες συνεργάζονται για την εκπλήρωση των παραπάνω σκοπών.

Ο ΠΚΙ αποτελεί το συνδετικό στοιχείο των τριών αυτών τομέων. Η τοποθέτησή του στο σύνορο μεταξύ του τομέα της Υποδομής Ιδιωτικότητας και του παρόχου υπηρεσίας εκφράζει τη διττή υπόστασή του: από τη μία πλευρά αποτελεί λειτουργικό μέρος της παρεχόμενης υπηρεσίας αποθηκεύοντας τα δεδομένα που αυτή χρησιμοποιεί και εκτελώντας μέρος της επιχειρησιακής της λειτουργίας, ενώ από την άλλη αποτελεί μέρος της έμπιστης υποδομής, ενσωματώνοντας νομικούς κανόνες και φροντίζοντας για την εφαρμογή τους. Επιπλέον, ο ΠΚΙ αποτελεί το σημείο διεπαφής μεταξύ του χρήστη και της υπηρεσίας, καθώς παρεμβάλλεται ανάμεσά τους, φιλτράροντας όλη την επικοινωνιακή κίνηση μεταξύ τους με σκοπό τη διασφάλιση της ιδιωτικότητας.

Ο ΠΚΙ περιγράφεται αναλυτικά στην Ενότητα 7.1. Για λόγους ροής του κειμένου, τα βασικά δομικά του στοιχεία είναι, συνοπτικά, τα παρακάτω (βλ. και Σχήμα 22 στη σελίδα 134):

- **Διαχειριστής Επικοινωνίας**: Πρόκειται για το δομικό συστατικό του ΠΚΙ το οποίο έχει ως αρμοδιότητα τη διαχείριση της επικοινωνίας του ΠΚΙ με τα υπόλοιπα στοιχεία της προτεινόμενης αρχιτεκτονικής, δηλαδή το Διαχειριστή Ιδιωτικότητας Χρήστη και τους Κόμβους Υποδομής Ιδιωτικότητας. Αποτελεί δηλαδή τη βασική διεπαφή του ΠΚΙ.
- **Αποθετήριο Κανονισμών**: Αποτελεί το δομικό στοιχείο του ΠΚΙ στο οποίο είναι αποθηκευμένη η Οντολογία Ιδιωτικότητας (Κεφάλαιο 5). Από εκεί ο ΠΚΙ αντλεί τους κανόνες που πηγάζουν από τη Νομοθεσία, καθώς και όλες τις απαραίτητες πληροφορίες που αφορούν τη σημασιολογική βάση του συστήματος.

- **Αποθετήριο Προσωπικών Δεδομένων**: Είναι το δομικό στοιχείο του ΠΚΙ στο οποίο αποθηκεύονται όλα τα προσωπικά δεδομένα, εφόσον συντρέχει λόγος αποθήκευσής τους. Με τον τρόπο αυτό, τα προσωπικά δεδομένα διατηρούνται απομονωμένα από τον πάροχο της υπηρεσίας και επιδίδονται μόνο εφόσον αυτό είναι θεμιτό βάσει των κανόνων της Νομοθεσίας και των προτιμήσεων του αντίστοιχου υποκειμένου των δεδομένων. Μαζί με τα προσωπικά δεδομένα, στο Αποθετήριο Προσωπικών Δεδομένων αποθηκεύονται και οι προτιμήσεις ιδιωτικότητας του χρήστη, εφόσον υφίστανται.
- **Μηχανή Πολιτικών**: Έχοντας ως είσοδο τους κανόνες οι οποίοι πηγάζουν από τη Νομοθεσία καθώς και τις προτιμήσεις ιδιωτικότητας των υποκειμένων των δεδομένων, η Μηχανή Πολιτικών αποτελεί το δομικό στοιχείο του ΠΚΙ που λαμβάνει τις αποφάσεις αναφορικά με τις ενέργειες που εκτελούνται εσωτερικά στον ΠΚΙ αλλά και την επικοινωνία του ΠΚΙ με τα υπόλοιπα στοιχεία της αρχιτεκτονικής. Ως έξοδο, η Μηχανή Πολιτικών παράγει τη ροή εργασιών για τη δεδομένη συναλλαγή ιδιωτικότητας, διαμορφωμένη ως ένα έγγραφο της Γλώσσας Περιγραφής Ροής Εργασιών Ιδιωτικότητας (ΓΠΡΕΙ) (βλ. Ενότητα 6.2).
- **Διαχειριστής Συνόδων**: Αποτελεί το κεντρικό δομικό στοιχείο του ΠΚΙ, το στοιχείο εκείνο το οποίο συντονίζει τη λειτουργία των υπολοίπων. Ο Διαχειριστής επικοινωνίας διαβιβάζει τα μηνύματα που λαμβάνει στο Διαχειριστή Συνόδων, ο οποίος καλεί τη Μηχανή Πολιτικών με τα κατάλληλα ορίσματα, ανάλογα με την περίπτωση. Στη συνέχεια, αναλαμβάνει την κλήση και το συντονισμό των υπολοίπων δομικών συστατικών του ΠΚΙ για την απρόσκοπτη εκτέλεση της ροής εργασιών που γεννά η Μηχανή Πολιτικών.
- **Ενσωματωμένες Λειτουργικές Μονάδες**: Πρόκειται για δομικά στοιχεία του ΠΚΙ τα οποία αναλαμβάνουν την εκτέλεση εσωτερικά στον ΠΚΙ διαφόρων λειτουργιών που υπό άλλες συνθήκες θα εκτελούνταν από τον πάροχο των υπηρεσιών. Οι λειτουργίες αυτές μπορεί να είναι είτε λειτουργίες επεξεργασίας δεδομένων (π.χ. η μετατροπή ενός τύπου δεδομένων σε κάποιον άλλο λιγότερο λεπτομερή), οπότε ονομάζονται Ενσωματωμένοι Τελεστές, είτε ολόκληρα τμήματα υπηρεσιών (π.χ. πραγματοποίηση χρηματικής χρέωσης), οπότε ονομάζονται Ενσωματωμένες Υπηρεσίες.

4.6 Υπηρεσίες, Σύνοδοι και Συναλλαγές Ιδιωτικότητας

Όπως προαναφέρθηκε, ως *υπηρεσία* στο πλαίσιο της Διατριβής εννοείται η κάθε διακριτή λειτουργία που ξεκινάει με κάποιο μήνυμα – αίτηση προς παροχή από κάποια οντότητα (συνήθως το χρήστη) και τελειώνει με το μήνυμα – απάντηση στην αίτηση. Δηλαδή, μιλώντας με όρους του πρωτοκόλλου Hypertext Transfer Protocol (HTTP)[1] [99], η παροχή μίας υπηρεσίας αρχίζει με ένα μήνυμα τύπου HTTP Request και ολοκληρώνεται με το αντίστοιχο μήνυμα τύπου HTTP Response.

Στο πλαίσιο της προτεινόμενης λύσης, σε κάθε αλληλουχία μηνυμάτων που αφορά την παροχή μίας υπηρεσίας παρεμβάλλεται ο Πληρεξούσιος Κόμβος Ιδιωτικότητας. Διακρίνουμε δύο περιπτώσεις:

- Υπηρεσίες που παρέχονται από τον πάροχο υπηρεσίας σε κάποιο χρήστη, οπότε ο ΠΚΙ μεσολαβεί μεταξύ χρήστη και παρόχου υπηρεσίας.
- Υπηρεσίες που παρέχονται από τον ΠΚΙ προς τους χρήστες (π.χ. διαγραφή δεδομένων), την Αρχή Ιδιωτικότητας (π.χ. LI) ή τον πάροχο υπηρεσιών (π.χ. εξαγωγή στατιστικών στοιχείων). Στις περιπτώσεις αυτές, συμμετέχουν μόνο δύο οντότητες, η μία από τις οποίες είναι ο ΠΚΙ.

Κάθε παροχή υπηρεσίας συνιστά μία **Συναλλαγή Ιδιωτικότητας**. Στην τυπική περίπτωση, μία υπηρεσία δεν παρέχεται μόνη της, αλλά σε συνδυασμό με άλλες υπηρεσίες. Για παράδειγμα, μία πράξη ηλεκτρονικών αγορών από κάποιο Διαδικτυακό κατάστημα, περιλαμβάνει διάφορες υπηρεσίες: είσοδο στο σύστημα, περιήγηση στα διαθέσιμα προϊόντα, πράξεις τύπου "προσθήκη στο καλάθι", εισαγωγή των απαραίτητων στοιχείων για τη χρέωση των αγορών, πραγματοποίηση της χρέωσης· η κάθε υπηρεσία από αυτές αποτελεί μία Συναλλαγή Ιδιωτικότητας.

Εκτός από τη Συναλλαγή Ιδιωτικότητας, η Διατριβή εισάγει και τον όρο **Σύνοδος Ιδιωτικότητας**, προκειμένου να περιγράψει το σύνολο των Συναλλαγών Ιδιωτικότητας που εκτελούνται ακολουθιακά και αφορούν την παροχή υπηρεσιών από τη στιγμή που

[1] Η αναφορά στο πρωτόκολλο HTTP δεν είναι τυχαία· αφενός, στο πλαίσιο της Διατριβής οι υπηρεσίες υλοποιήθηκαν με τη χρήση του HTTP ενώ, αφετέρου, το HTTP γίνεται όλο και πιο δημοφιλές στην παροχή των ηλεκτρονικών υπηρεσιών.

κάποια οντότητα συνδέεται με κάποια άλλη ζητώντας την παροχή κάποιας υπηρεσίας, μέχρι τη στιγμή της τελικής αποσύνδεσης. Σε σχέση με το παράδειγμα των ηλεκτρονικών αγορών της προηγούμενης παραγράφου, η Σύνοδος Ιδιωτικότητας ορίζεται από την πρώτη σύνδεση του χρήστη με το Διαδικτυακό κατάστημα (δηλαδή από την αποστολή του πρώτου HTTP Request μηνύματος) μέχρι την τελική αποσύνδεσή του (δηλαδή τη λήψη του τελικού HTTP Response).

Οι έννοιες της Συνόδου Ιδιωτικότητας και της Συναλλαγής Ιδιωτικότητας παίζουν πολύ σημαντικό ρόλο στη λειτουργία της προτεινόμενης λύσης και ιδιαιτέρως στην λειτουργία του ΠΚΙ, όπως θα φανεί στη συνέχεια της Διατριβής. Σε κάθε Σύνοδο Ιδιωτικότητας, ο ΠΚΙ (συγκεκριμένα ο Διαχειριστής Συνόδων) διατηρεί την κατάσταση (state) του συστήματος (π.χ. τα προσωπικά δεδομένα που έχει διαθέσει ο χρήστης στον ΠΚΙ ή ο ΠΚΙ στον πάροχο της υπηρεσίας). Επιπλέον, σε κάθε Συναλλαγή Ιδιωτικότητας, ο Διαχειριστής Συνόδων καλεί ακριβώς μία φορά τη Μηχανή Πολιτικών και παράγεται ακριβώς ένα έγγραφο ροής εργασιών.

Οι υπηρεσίες ακολουθούν συγκεκριμένα πρότυπα αναφορικά με τη λειτουργική τους δομή καθώς και τον αριθμό και τη φύση των μηνυμάτων που ανταλλάσσονται. Για το λόγο αυτό, στο πλαίσιο της Διατριβής έχουν οριστεί συγκεκριμένα υποδείγματα (patterns) των διαφόρων κατηγοριών υπηρεσιών. Συνολικά, έχουν θεωρηθεί πέντε υποδείγματα· τα τέσσερα από αυτά αναφέρονται στην παροχή υπηρεσιών ορίζοντας τα πρότυπα των εξής περιπτώσεων:

- Παροχή υπηρεσίας από πάροχο υπηρεσίας σε χρήστη.
- Παροχή υπηρεσίας από τον ΠΚΙ σε χρήστη.
- Παροχή υπηρεσίας από τον ΠΚΙ σε Αρχή Ιδιωτικότητας.
- Παροχή υπηρεσίας από τον ΠΚΙ σε πάροχο υπηρεσίας.

Το πέμπτο υπόδειγμα αναφέρεται και αυτό στην πρώτη περίπτωση (παροχή υπηρεσίας από πάροχο υπηρεσίας σε χρήστη), με τη θεμελιώδη διαφορά ότι δεν αντιστοιχεί σε κάποια πραγματική υπηρεσία, αλλά στην υπηρεσία `Welcome`. Πρόκειται για ψεύτικη υπηρεσία, η οποία έχει ως σκοπό την αμοιβαία αναγνώριση μεταξύ του ΠΚΙ και του Διαχειριστή Ιδιωτικότητας Χρήστη και την αρχικοποίηση των διαφόρων παραμέτρων. Η υπηρεσία `Welcome` είναι πάντοτε η πρώτη Συναλλαγή Ιδιωτικότητας που λαμβάνει χώρα στο πλαίσιο της κάθε Συνόδου Ιδιωτικότητας που εμπλέκει τόσο το

χρήστη όσο και τον πάροχο υπηρεσίας. Σημειώνεται ότι η κατηγορία στην οποία εντάσσεται η κάθε υπηρεσία, δηλαδή το υπόδειγμα που ακολουθεί, περιλαμβάνεται μεταξύ των πληροφοριών που περιέχει η Οντολογία Ιδιωτικότητας (Κεφάλαιο 5), ενώ ο ΠΚΙ περιλαμβάνει τα υποδείγματα των διαφόρων κατηγοριών σε μορφή εγγράφων – μητρών της Γλώσσας Περιγραφής Ροής Εργασιών Ιδιωτικότητας.

4.7 Πλαίσιο Επικοινωνίας

Στα πλαίσια της Διατριβής, έχουν προδιαγραφεί οι μηχανισμοί για την επικοινωνία και διαλειτουργικότητα μεταξύ των δομικών συστατικών της αρχιτεκτονικής της προτεινόμενης λύσης. Οι μηχανισμοί αφορούν τον Πληρεξούσιο Κόμβο Ιδιωτικότητας, το Διαχειριστή Ιδιωτικότητας Χρήστη, τους Κόμβους Υποδομής Ιδιωτικότητας και τις εφαρμογές του παρόχου υπηρεσιών.

Το πλαίσιο επικοινωνίας της προτεινόμενης λύσης έχει υλοποιηθεί εξ ολοκλήρου με βάση το πρωτόκολλο Hypertext Transfer Protocol (HTTP) [99]. Η επιλογή αυτή βασίστηκε στο γεγονός ότι όχι μόνο αποτελεί το πρωτόκολλο των διαδικτυακών υπηρεσιών, αλλά αποτελεί και τη βάση των σύγχρονων Υπηρεσιών Ιστού (Web Services) [112]. Επιπλέον, άλλα σύγχρονα πρωτόκολλα ακολουθούν το μοντέλο του HTTP. Για παράδειγμα, το Πρωτόκολλο Έναρξης Συνόδου (Session Initiation Protocol – SIP) [113] το οποίο χρησιμοποιείται – μεταξύ άλλων – στην πλειοψηφία των υπηρεσιών Διαδικτυακής Τηλεφωνίας (Voice Over IP – VoIP) [114] βασίζεται στο HTTP.

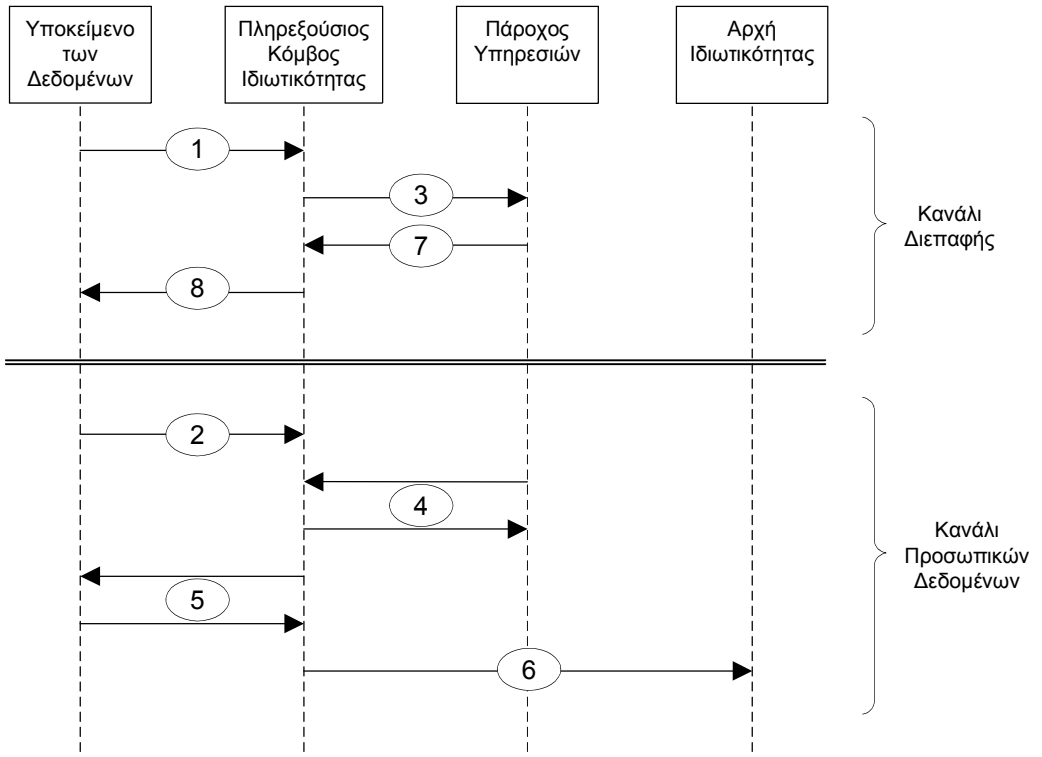
Μεταξύ των χαρακτηριστικών του πλαισίου επικοινωνίας περιλαμβάνονται:

- Η χρήση δύο καναλιών ανταλλαγής πληροφοριών τα οποία λειτουργούν παράλληλα.
- Η χρήση ειδικών HTTP επικεφαλίδων που προδιαγράφηκαν στο πλαίσιο της Διατριβής.
- Η φύση των ροών των δεδομένων που βασίζεται στις έννοιες της Συναλλαγής και Συνόδου Ιδιωτικότητας.

Τα δύο κανάλια τα οποία χρησιμοποιούνται από την προτεινόμενη λύση ονομάζονται, αντίστοιχα, **Κανάλι Διεπαφής** και **Κανάλι Προσωπικών Δεδομένων**. Το Κανάλι Διεπαφής αποτελεί το κανάλι μέσω του οποίου μεταφέρονται τα υφιστάμενα μηνύματα που έχουν να κάνουν με την παροχή υπηρεσιών. Το Κανάλι Προσωπικών

Δεδομένων είναι εκείνο το κανάλι μέσω του οποίου μεταδίδονται τα μηνύματα που έχουν προδιαγραφεί στο πλαίσιο της Διατριβής και σχετίζονται με την Ιδιωτικότητα. Τέτοια μηνύματα είναι εκείνα τα οποία μεταφέρουν προσωπικά δεδομένα από το Διαχειριστή Ιδιωτικότητας Χρήστη προς τον Πληρεξούσιο Κόμβο Ιδιωτικότητας και αντίστροφα, μέσα σε ειδικές δομές που προδιαγράφηκαν στο πλαίσιο της Διατριβής. Οι δομές αυτές χαρακτηρίζονται σαν **Κέλυφος Ιδιωτικότητας** και περιγράφονται στην Ενότητα 4.8, ενώ η γλώσσα που χρησιμοποιείται είναι η Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας (βλ. Ενότητα 6.1). Επιπλέον, από το Κανάλι Προσωπικών Δεδομένων μεταδίδονται τα μηνύματα μέσω των οποίων ο πάροχος υπηρεσίας υποβάλλει αιτήματα στον Πληρεξούσιο Κόμβο Ιδιωτικότητας που αφορούν προσωπικά δεδομένα, τα μηνύματα που αφορούν την παροχή ενημέρωσης ή αιτήματα για συγκατάθεση, καθώς και τα μηνύματα μέσω των οποίων η Αρχή Ιδιωτικότητας αλληλεπιδρά με τον Πληρεξούσιο Κόμβο Ιδιωτικότητας.

Το παρακάτω Σχήμα 16 παρουσιάζει μία περίπτωση παροχής υπηρεσίας η οποία περιλαμβάνει όλες τις οντότητες του συστήματος (χρήστη, Αρχή Ιδιωτικότητας και πάροχο υπηρεσιών) και η οποία επιδεικνύει τη χρήση των δύο καναλιών επικοινωνίας.



Σχήμα 16: Κανάλια Επικοινωνίας

Ο χρήστης υποβάλει αρχικά το αίτημα για υπηρεσία μέσω του Καναλιού Διεπαφής (μήνυμα 1), ενώ, σχεδόν ταυτόχρονα, μέσω του Καναλιού Προσωπικών Δεδομένων μεταδίδει τα προσωπικά δεδομένα μαζί με τα μεταδεδομένα – προτιμήσεις ιδιωτικότητας (μήνυμα 2). Ο Πληρεξούσιος Κόμβος Ιδιωτικότητας, αφού πραγματοποιήσει την κατά περίπτωση απαραίτητη επεξεργασία, προωθεί το αίτημα παροχής της υπηρεσίας (μήνυμα 3). Στη συνέχεια, μέσω του Καναλιού Προσωπικών Δεδομένων ξεκινά μία διαδικασία κατά την οποία ο πάροχος των υπηρεσιών υποβάλλει αιτήματα προς τον Πληρεξούσιο Κόμβο Ιδιωτικότητας που αφορούν πρόσβαση σε δεδομένα ή σε Ενσωματωμένες Λειτουργικές Μονάδες (μηνύματα 4). Θεωρώντας ότι η εν λόγω υπηρεσία απαιτεί την παροχή ρητής συναίνεσης από το υποκείμενο των δεδομένων, η σχετική ανταλλαγή μηνυμάτων (μηνύματα 5) λαμβάνει χώρα από το Κανάλι Προσωπικών Δεδομένων. Το ίδιο ισχύει και με την ενημέρωση της Αρχής Ιδιωτικότητας (μήνυμα 6). Μετά την ολοκλήρωση της επεξεργασίας, ο πάροχος υπηρεσίας αποστέλλει το μήνυμα παροχής υπηρεσίας το οποίο μέσω του Πληρεξούσιου Κόμβου Ιδιωτικότητας διαβιβάζεται στο χρήστη (μηνύματα 7 και 8). Τα μηνύματα αυτά μεταδίδονται μέσω του Καναλιού Διεπαφής.

4.8 Κέλυφος Ιδιωτικότητας

Το **Κέλυφος Ιδιωτικότητας** αποτελεί τη δομή δεδομένων που προδιαγράφηκε στο πλαίσιο της Διατριβής για τη μεταφορά προσωπικών δεδομένων από το Διαχειριστή Ιδιωτικότητας Χρήστη στον Πληρεξούσιο Κόμβο Ιδιωτικότητας (και αντίστροφα). Ο σκοπός του Κελύφους Ιδιωτικότητας είναι διπλός:

- Να εξασφαλίσει την ασφαλή μετάδοση των προσωπικών δεδομένων.
- Να καταστήσει δυνατή τη μετάδοση μεταδεδομένων μαζί με τα προσωπικά δεδομένα· τα μεταδεδομένα αφορούν τις προτιμήσεις ιδιωτικότητας του χρήστη.

Το Κέλυφος Ιδιωτικότητας αποτελεί ένα αντικείμενο, το οποίο μεταδίδεται μέσω του Καναλιού Προσωπικών Δεδομένων. Στο πλαίσιο της Διατριβής χρησιμοποιήθηκε κρυπτογραφία δημοσίου κλειδιού και πιο συγκεκριμένα ο αλγόριθμος Rivest–Shamir–Adleman (RSA) [87] με μήκος κλειδιού 2048 δυαδικά ψηφία, ενώ η σχετική υλοποίηση έλαβε χώρα με χρήση των βιβλιοθηκών του Java™ Cryptography Architecture, έκδοση 6 [115]. Ωστόσο, το Κέλυφος Ιδιωτικότητας θα μπορούσε και να μην είναι

κρυπτογραφημένο, καθώς το Κανάλι Προσωπικών Δεδομένων είναι από μόνο του κρυπτογραφημένο.

Σημειώνεται ότι το Κέλυφος Ιδιωτικότητας μπορεί να χρησιμοποιηθεί για τη μετάδοση μεταδεδομένων ακόμα και χωρίς τα δεδομένα αυτά καθαυτά. Κάτι τέτοιο μπορεί να λάβει χώρα για παράδειγμα όταν το υποκείμενο των δεδομένων επιθυμεί να ορίσει τις προτιμήσεις του αναφορικά με την ιδιωτικότητα ημιενεργών προσωπικών δεδομένων (Ενότητα 4.3).

Στο Κεφάλαιο 8, παρουσιάζονται κάποια παραδείγματα της δομής του Κελύφους Ιδιωτικότητας.

5 Οντολογία Ιδιωτικότητας

5.1 Εισαγωγή

Όπως συνάγεται από τις νομικές και κανονιστικές απαιτήσεις (βλ. Κεφάλαιο 2 καθώς και Ενότητα 4.1), η συγκεκριμενοποίηση των απαιτήσεων αυτών οδηγεί στον ορισμό κανόνων ελέγχου πρόσβασης σε άμεση σχέση με τον τύπο των προσωπικών δεδομένων, το σκοπό συλλογής και επεξεργασίας τους και το ρόλο της οντότητας που αιτείται των δεδομένων, πιθανότατα σε συνδυασμό με την εκτέλεση κάποιων συμπληρωματικών ενεργειών, όπως επεξεργασία των δεδομένων πριν από την εκχώρησή τους ή ενημέρωση του υποκειμένου των δεδομένων. Η Οντολογία Ιδιωτικότητας αποτελεί ένα ενιαίο σύστημα για το φορμαλιστικό ορισμό των κανόνων αυτών που διέπουν την παροχή ηλεκτρονικών υπηρεσιών αναφορικά με την ιδιωτικότητα. Η Οντολογία Ιδιωτικότητας αποτελεί τη γνωσιακή βάση για την εξαγωγή συμπερασμάτων και τη λήψη αποφάσεων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας (ΠΚΙ) αναφορικά με τη συλλογή, επεξεργασία και περαιτέρω μετάδοση των προσωπικών δεδομένων.

Σαν τεχνικό μέσο για τον προσδιορισμό των κανόνων επιλέχτηκε η χρήση μίας οντολογίας [116] λόγω των πλεονεκτημάτων που παρουσιάζει, όπως είναι η σημασιολογική διαλειτουργικότητα. Πράγματι, γλώσσες προδιαγραφής πολιτικών όπως είναι η OASIS XACML [63] και η IBM EPAL [75] που παρουσιάστηκαν στο Κεφάλαιο 3 μειονεκτούν αναφορικά με την εκφραστική δύναμη των φορμαλισμών που χρησιμοποιούν για να περιγράψουν πόρους και οντότητες που αιτούνται των πόρων αυτών. Η χρήση οντολογιών επιτρέπει τον ορισμό πολύπλοκων δομών και κανόνων, ενώ παρουσιάζει διάφορα πλεονεκτήματα, όπως οι δυνατότητες εξαγωγής λογικών συμπερασμάτων (reasoning), η δυνατότητα αξιολόγησης των κανόνων ως προς τη συνέπειά τους και η δυνατότητα ολοκλήρωσης με άλλα σημασιολογικά μοντέλα τα οποία περιγράφουν συμπληρωματικές έννοιες.

Η υλοποίηση της Οντολογίας Ιδιωτικότητας βασίζεται στη διαδεδομένη γλώσσα OWL (Web Ontology Language) [117], η οποία έχει προτυποποιηθεί από τον οργανισμό W3C [45]. Το συντακτικό της βασίζεται στο διαδεδομένο πρότυπο Σύστημα Περιγραφής Πόρων (Resource Description Framework – RDF) [118], ενώ για την εξαγωγή

συμπερασμάτων μπορούν να χρησιμοποιηθούν διάφορες γλώσσες ερωτήσεων, όπως είναι η Γλώσσα Ερωτήσεων RDQL (RDF Data Query Language) [119]. Για την υλοποίηση της Οντολογίας Ιδιωτικότητας, χρησιμοποιήθηκε το ελεύθερο και ανοιχτού κώδικα εργαλείο λογισμικού Protégé [120], το οποίο έχει αναπτυχθεί από το Πανεπιστήμιο Stanford.

Αναφορικά με τη δομή της, η Οντολογία Ιδιωτικότητας αποτελείται από επτά κλάσεις, τις παρακάτω:

- `PersonalData`, η οποία περιέχει τους τύπους προσωπικών δεδομένων.
- `Services`, η οποία περιέχει τους τύπους υπηρεσιών.
- `Actors`, η οποία περιέχει τους διάφορους ρόλους των οντοτήτων.
- `Rules`, τα μέλη της οποίας συνιστούν τους κανόνες που απορρέουν από το Νομοθετικό και Κανονιστικό Πλαίσιο και αφορούν είτε σε πρόσβαση (ανάγνωσης και εγγραφής) σε δεδομένα, είτε σε εκτέλεση Ενσωματωμένων Λειτουργικών Μονάδων του Πληρεξούσιου Κόμβου Ιδιωτικότητας.
- `Components`, η οποία αντανακλά τις διάφορες Ενσωματωμένες Λειτουργικές Μονάδες του Πληρεξούσιου Κόμβου Ιδιωτικότητας.
- `Patterns`, η οποία χρησιμοποιείται για την αντιστοίχηση των υπηρεσιών με το υπόδειγμα στο οποίο εντάσσονται (βλ. Ενότητα 4.6).
- `DataTransformations`, η οποία ορίζει τους μετασχηματισμούς που μπορούν να πραγματοποιηθούν μεταξύ των διαφόρων τύπων των δεδομένων με χρήση των Ενσωματωμένων Λειτουργικών Μονάδων του Πληρεξούσιου Κόμβου Ιδιωτικότητας.

Από τις παραπάνω κλάσεις, οι τρεις πρώτες συνιστούν το Σημασιολογικό Μοντέλο Πληροφοριών του προτεινόμενου συστήματος και περιγράφονται αναλυτικά στην Ενότητα 5.2. Η κλάση `Rules` χρησιμοποιείται για τη φορμαλιστική περιγραφή των κανόνων, ο τρόπος ορισμού των οποίων περιγράφεται στην Ενότητα 5.3. Οι υπόλοιπες κλάσεις περιέχουν κυρίως βοηθητικές πληροφορίες για την εκτέλεση των συνόδων ιδιωτικότητας, όπως περιγράφεται στην Ενότητα 5.4.

5.2 Σημασιολογικό Μοντέλο Πληροφοριών

Όπως έχει αναφερθεί παραπάνω, σύμφωνα με τη νομοθεσία περί προστασίας προσωπικών δεδομένων, το δικαίωμα πρόσβασης σε κάποιο προσωπικό δεδομένο αποτελεί συνάρτηση τριών παραμέτρων: του τύπου του προσωπικού δεδομένου, του σκοπού για τον οποίο το δεδομένο συλλέγεται ή/και υφίσταται επεξεργασία, καθώς και του ρόλου της οντότητας που αιτείται του δεδομένου. Ως εκ τούτου, το Σημασιολογικό Μοντέλο Πληροφοριών του προτεινόμενου συστήματος περιέχει σημασιολογικούς ορισμούς των τριών αυτών τύπων πληροφορίας. Οι ορισμοί αυτοί αντιστοιχούν σε τρεις υπογράφους της Οντολογίας Ιδιωτικότητας, οι οποίοι αποτελούνται από μέλη[1] των κλάσεων `PersonalData`, `Services` και `Actors`, αντίστοιχα. Οι υπογράφοι αυτοί παρουσιάζονται στη συνέχεια.

Οι διάφοροι τύποι προσωπικών δεδομένων αποτελούν μέλη της κλάσης `PersonalData`, συνιστούν υπογράφο και είναι οργανωμένοι σε τρεις διαφορετικές ιεραρχίες, με χρήση αντικειμενικών ιδιοτήτων (object properties). Η βασική ιεραρχία στην οποία ανήκουν όλα τα μέλη της κλάσης αναφέρεται σε και προσδιορίζει την κληρονομικότητα των χαρακτηριστικών. Ως μέλος–ρίζα της ιεραρχίας αυτής, έχει οριστεί ένας γενικός τύπος, ο `AllPersonalData` από τον οποίο κληρονομούν όλα τα μέλη της ιεραρχίας. Τα παιδιά πρώτης τάξης του τύπου αυτού ως προς την εν λόγω ιεραρχία αποτελούν γενικές κατηγορίες προσωπικών δεδομένων και – ενδεικτικά – περιλαμβάνουν τα παρακάτω: `Age`, `BillingData`, `Contact`, `Identity`, `LawEnforcementData`, `Location`, `Preferences`, `ShoppingData`, `TransportData`.

Η ιεραρχία αυτή ορίζεται μέσω της αντικειμενικής ιδιότητας `inheritsFromData`, καθώς και από την αντίστροφή της.

Σημειώνεται ότι αυτά ισχύουν για την οντολογία που υλοποιήθηκε στα πλαίσια της εκπόνησης της παρούσας διατριβής· οι διάφοροι τύποι θα μπορούσαν να είναι πολύ περισσότεροι, ούτως ώστε να καλύπτουν το σύνολο των δυνατών προσωπικών δεδομένων που χρησιμοποιούνται κατά την παροχή ηλεκτρονικών υπηρεσιών. Όπως προαναφέρθηκε, η λογική πίσω από το Σημασιολογικό Μοντέλο Πληροφοριών είναι να

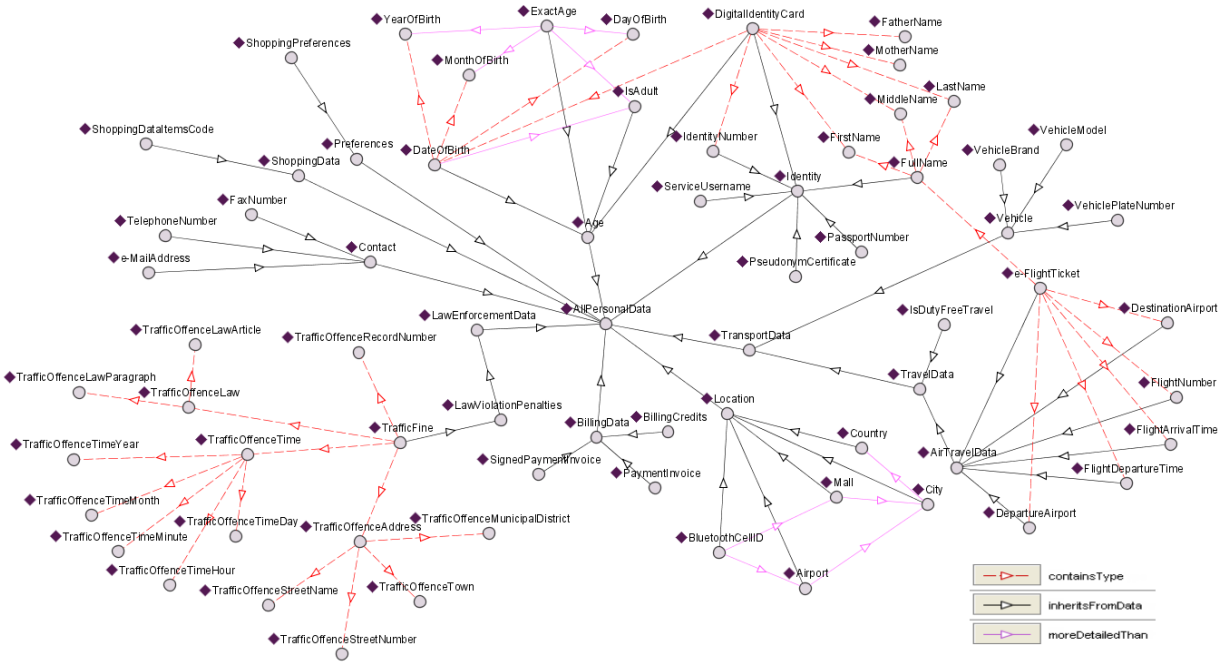
[1] Ο όρος "μέλος" επιλέχθηκε ως ο πλέον αντιπροσωπευτικός για το νόημα που στην Αγγλική γλώσσα αποδίδεται από τον όρο "instance".

αποτελέσει μία ταξινόμηση προσωπικών δεδομένων, υπηρεσιών και ρόλων τόσο εξαντλητική όσο και το Κοινό Λεξιλόγιο για τις Δημόσιες Συμβάσεις (Common Procurement Vocabulary – CPV) [109].

Η δεύτερη ιεραρχία η οποία ορίζεται στον υπογράφο των προσωπικών δεδομένων της Οντολογίας ιδιωτικότητας αναφέρεται στο βαθμό λεπτομέρειας των προσωπικών δεδομένων και υλοποιείται με τις αντικειμενικές ιδιότητες `lessDetailedThan` και `moreDetailedThan`, οι οποίες είναι αντίστροφες μεταξύ τους. Για παράδειγμα, το έτος γεννήσεως κάποιου (τύπος `YearOfBirth`) αποτελεί προσωπικό δεδομένο που χαρακτηρίζεται από μικρότερο βαθμό λεπτομέρειας από την ακριβή του ηλικία (τύπος `ExactAge`), ενώ οι γεωγραφικές συντεταγμένες (τύπος `GeographicalCoordinates`) αποτελούν προσωπικό δεδομένο που χαρακτηρίζεται από μεγαλύτερο βαθμό λεπτομέρειας από κάποια ευρύτερη γεωγραφική περιοχή όπως η χώρα (τύπος `Country`) στην οποία βρίσκεται κάποιος, αναφορικά με την τοποθεσία (π.χ. δεδομένα θέσης τηλεπικοινωνιακών υπηρεσιών).

Η τρίτη και τελευταία ιεραρχία που ορίζεται για τον υπογράφο προσωπικών δεδομένων αφορά τον ορισμό δομών προσωπικών δεδομένων από επιμέρους τύπους. Οι αντίστοιχες σχέσεις μεταξύ των τύπων προσωπικών δεδομένων υλοποιούνται με τις αντικειμενικές ιδιότητες `containsType` και `isContainedToType`, οι οποίες είναι αντίστροφες μεταξύ τους. Για παράδειγμα, το όνομα (τύπος `FirstName`), το επώνυμο (τύπος `LastName`) και το μεσαίο όνομα (τύπος `MiddleName`) κάποιου συναποτελούν το πλήρες όνομά του (τύπος `FullName`).

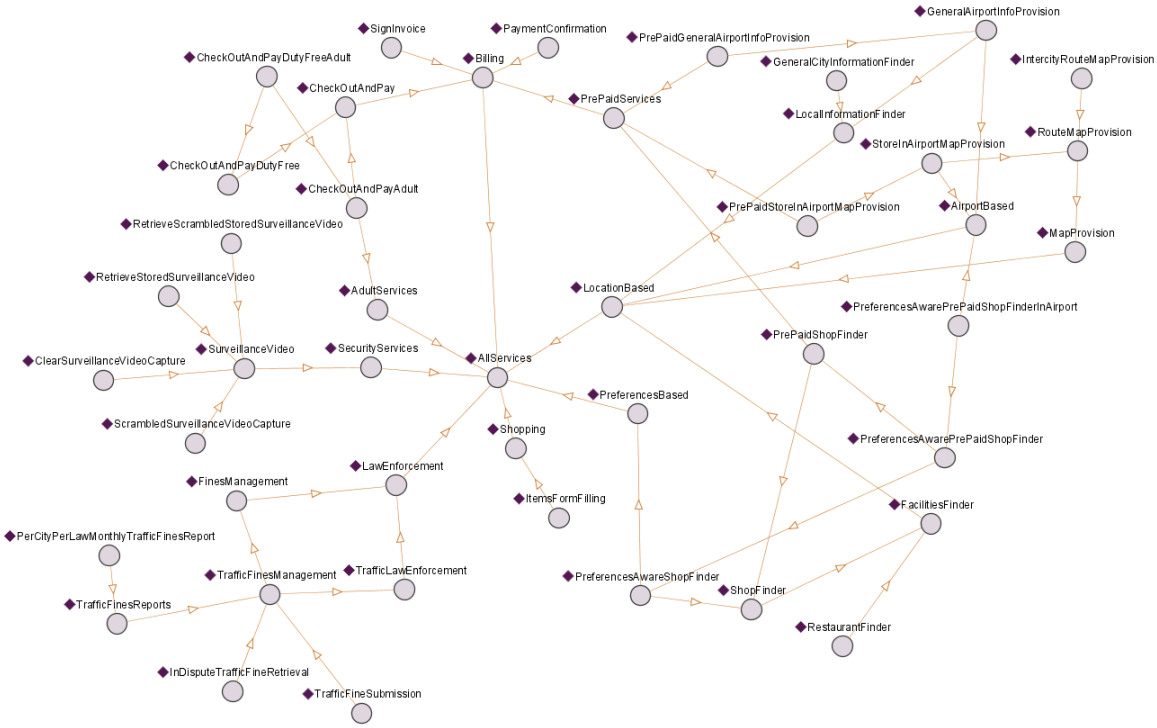
Το Σχήμα 17 παρέχει τη γραφική αναπαράσταση ενός τμήματος του υπογράφου προσωπικών δεδομένων της Οντολογίας Ιδιωτικότητας, μαζί με τις ως άνω περιγραφόμενες ιεραρχίες των μελών του υπογράφου.



Σχήμα 17: Οντολογία Ιδιωτικότητας – Υπογράφος Προσωπικών Δεδομένων

Οι διάφοροι σκοποί συλλογής και επεξεργασίας προσωπικών δεδομένων εκφράζονται μέσω των αντίστοιχων υπηρεσιών. Υπενθυμίζεται εδώ ότι ως "υπηρεσία" στο πλαίσιο της Διατριβής εννοείται η κάθε διακριτή λειτουργία που ξεκινάει με κάποιο μήνυμα – αίτηση προς παροχή από κάποια οντότητα (συνήθως το χρήστη) και τελειώνει με το μήνυμα – απάντηση στην αίτηση. Οι υπηρεσίες αυτές αποτελούν μέλη της κλάσης `Services` της Οντολογίας Ιδιωτικότητας και σχηματίζουν ιεραρχία αναφορικά με την κληρονομικότητα των διαφόρων χαρακτηριστικών. Η ιεραρχία έχει ως μέλος – ρίζα το γενικό τύπο υπηρεσίας `AllServices`, ενώ ως παιδιά πρώτου επιπέδου έχουν – μεταξύ άλλων – θεωρηθεί τα: `AdultServices`, `Billing`, `LawEnforcement`, `LocationBased`, `PreferencesBased`, `SecurityServices`, `Shopping`.

Τέλος, ο τρίτος υπογράφος του Σημασιολογικού Μοντέλου Πληροφοριών αναφέρεται στους ρόλους των διαφόρων οντοτήτων που συμμετέχουν στην παροχή των υπηρεσιών με οποιοδήποτε τρόπο. Οι οντότητες αυτές μπορούν να αναφέρονται στην πλευρά του χρήστη, του παρόχου της υπηρεσίας (π.χ. υπάλληλος με συγκεκριμένη θέση) ή της Αρχής Ιδιωτικότητας. Στο πλαίσιο της διατριβής και χωρίς βλάβη της γενικότητας, θεωρήθηκε ένα απλοποιημένο μοντέλο, με τρεις ρόλους που αντιστοιχούν σε μέλη της κλάσης `Actors` της Οντολογίας Ιδιωτικότητας:



Σχήμα 18: Οντολογία Ιδιωτικότητας – Υπογράφος Υπηρεσιών

- Ρόλος χρήστη (τύπος `DataSubject`)
- Ρόλος παρόχου υπηρεσίας (τύπος `ServiceProvider`)
- Ρόλος Αρχής Ιδιωτικότητας (τύπος `PrivacyAuthority`)

Ορίζεται επιπλέον ο τύπος `AllActors`, προκειμένου να δηλωθούν άπαντες οι ρόλοι που περιλαμβάνονται στον υπογράφο.

Σημειώνεται ότι το απλό αυτό μοντέλο γενικεύεται πολύ εύκολα ούτως ώστε, ειδικά αναφορικά με τον πάροχο της υπηρεσίας και την Αρχή Ιδιωτικότητας, να οριστούν γράφοι ρόλων.

5.3 Κανόνες Οντολογίας Ιδιωτικότητας

Η Οντολογία Ιδιωτικότητας ορίζει δύο τύπους κανόνων:

- **Κανόνες Δικαιώματος Πρόσβασης**: αναφέρονται στη διάθεση ή όχι κάποιου τύπου προσωπικού δεδομένου σε οντότητα που ανήκει σε κάποιο ρόλο στο πλαίσιο της παροχής κάποιας υπηρεσίας.

- **Κανόνες Δικαιώματος Εκτέλεσης**: αναφέρονται στο δικαίωμα εκτέλεσης κάποιας Ενσωματωμένης Υπηρεσίας από οντότητα που ανήκει σε κάποιο ρόλο στο πλαίσιο της παροχής κάποιας υπηρεσίας.

Κάθε κανόνας υλοποιείται ως μέλος της κλάσης `Rules` της Οντολογίας Ιδιωτικότητας. Οι διάφοροι κανόνες δε συσχετίζονται μεταξύ τους με κάποια αντικειμενική ιδιότητα· ωστόσο, όλοι οι κανόνες συνδέονται με μέλη των κλάσεων των υπηρεσιών, των ρόλων και των προσωπικών δεδομένων ή των Ενσωματωμένων Λειτουργικών Μονάδων.

Πιο συγκεκριμένα, τα μέλη της κλάσης `Rules` της Οντολογίας Ιδιωτικότητας που αντιστοιχούν σε Κανόνες Δικαιώματος Πρόσβασης, αναφέρονται πάντοτε σε τριάδες {τύπος προσωπικού δεδομένου, τύπος υπηρεσίας, τύπος ρόλου}. Προκειμένου να πραγματοποιηθεί ο συσχετισμός μεταξύ των μελών των αντίστοιχων υπογράφων της Οντολογίας Ιδιωτικότητας, χρησιμοποιούνται οι παρακάτω αντικειμενικές ιδιότητες:

- Για τη διασύνδεση των μελών των υπογράφων των κλάσεων `Rules` και `PersonalData`, χρησιμοποιείται η αντικειμενική ιδιότητα `refersToData` και η αντίστροφή της.
- Για τη διασύνδεση των μελών των υπογράφων των κλάσεων `Rules` και `Services`, χρησιμοποιείται η αντικειμενική ιδιότητα `refersToService` και η αντίστροφή της.
- Για τη διασύνδεση των μελών των υπογράφων των κλάσεων `Rules` και `Actors`, χρησιμοποιείται η αντικειμενική ιδιότητα `refersToActor` και η αντίστροφή της.

Ο κάθε κανόνας χαρακτηρίζεται από μία ή περισσότερες ιδιότητες επισημείωσης (annotation properties) που αποτελούν ουσιαστικά το σώμα του κανόνα. Οι ιδιότητες αυτές είναι οι παρακάτω:

- `DisclosureOfData`: Εκφράζει το εάν η οντότητα στην οποία αναφέρεται ο κανόνας διαθέτει δικαίωμα ανάγνωσης του τύπου προσωπικού δεδομένου για την παροχή του τύπου της υπηρεσίας, στους οποίους αναφέρεται ο κανόνας. Μπορεί να λάβει τις τιμές `YES` και `NO`, επιτρέποντας ή μη την αποκάλυψη του δεδομένου στην οντότητα από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας.

- `RetentionPeriod`: Εκφράζει το χρονικό διάστημα διατήρησης των δεδομένων συγκεκριμένου τύπου στις βάσεις δεδομένων του παρόχου της υπηρεσίας. Για παράδειγμα, η Ευρωπαϊκή Οδηγία 2006/24/ΕΚ [25] ορίζει συγκεκριμένα χρονικά διαστήματα για τη διατήρηση των μεταδεδομένων επικοινωνίας. Μπορεί να λάβει κάποια ακέραια αριθμητική τιμή, η οποία εκφράζει τον αριθμό των χιλιοστών του δευτερολέπτου που πρέπει να κρατηθούν τα δεδομένα, ή την τιμή `INDEFINITE`, η οποία υπονοεί διατήρηση των δεδομένων επ' αόριστο.

- `ModificationPermission`: Εκφράζει το εάν η οντότητα στην οποία αναφέρεται ο κανόνας διαθέτει δικαίωμα τροποποίησης του τύπου προσωπικού δεδομένου για την παροχή του τύπου της υπηρεσίας, στους οποίους αναφέρεται ο κανόνας. Μπορεί να λάβει τις τιμές `YES` και `NO`, δίνοντας ή όχι το σχετικό δικαίωμα. Σημειώνεται ότι σε περίπτωση αντίθεσης με τον κανόνα `RetentionPeriod`, υπερισχύει ο `RetentionPeriod`.

Οι παραπάνω ιδιότητες αφορούν το δικαίωμα πρόσβασης στα προσωπικά δεδομένα, καθώς και το εάν πρέπει να λαμβάνει χώρα διατήρηση αυτών στη βάση δεδομένων του Πληρεξούσιου Κόμβου Ιδιωτικότητας και για πόσο χρονικό διάστημα. Επιπλέον και αναφορικά με τις συμπληρωματικές ενέργειες που ενδεχομένως πρέπει να πραγματοποιηθούν, ορίζονται οι παρακάτω ιδιότητες επισημείωσης:

- `DataSubjectInformation`: Αναφέρεται στην απαίτηση να ενημερωθεί το υποκείμενο των δεδομένων του τύπου στον οποίο αναφέρεται ο κανόνας, εφόσον ζητείται να πραγματοποιηθεί η πράξη που ορίζεται από τον κανόνα (αποκάλυψη δεδομένων, τροποποίηση κλπ.) στο πλαίσιο της παροχής της υπηρεσίας και από οντότητα των τύπων (υπηρεσίας και ρόλου) στους οποίους αναφέρεται ο κανόνας. Μπορεί να λάβει τις τιμές `YES` και `NO`· εφόσον δεν προσδιορίζεται κάποια τιμή, θεωρείται ότι δεν υπάρχει απαίτηση για ενημέρωση του υποκειμένου των δεδομένων.

- `DataSubjectConsent`: Αναφέρεται στην απαίτηση να ζητηθεί η παροχή ρητής συναίνεσης από το υποκείμενο των δεδομένων του τύπου στον οποίο αναφέρεται ο κανόνας, προκειμένου να πραγματοποιηθεί η πράξη που ορίζεται από τον κανόνα (αποκάλυψη δεδομένων, τροποποίηση κλπ.) στο πλαίσιο της παροχής της υπηρεσίας και από οντότητα των τύπων (υπηρεσίας και ρόλου) στους οποίους αναφέρεται ο κανόνας. Μπορεί να λάβει τις τιμές `YES` και `NO`· εφόσον δεν

προσδιορίζεται κάποια τιμή, θεωρείται ότι δεν υπάρχει απαίτηση για παροχή ρητής συναίνεσης από το υποκειμένου των δεδομένων (π.χ., θεωρείται ότι η συναίνεση υπάρχει ήδη). Σημειώνεται ότι η ύπαρξη μίας τέτοιας απαίτησης θα πρέπει να προκαλέσει την αναστολή της εκτέλεσης της πράξης που ορίζεται από τον κανόνα μέχρι την παροχή της συναίνεσης, ή μέχρι τη χρονική λήξη της συνόδου.

- `AuthorityNotification`: Αναφέρεται στην απαίτηση να ενημερωθεί η Αρχή Ιδιωτικότητας, εφόσον ζητείται να πραγματοποιηθεί η πράξη που ορίζεται από τον κανόνα (αποκάλυψη δεδομένων, τροποποίηση κλπ.) στο πλαίσιο της παροχής της υπηρεσίας και από οντότητα των τύπων (υπηρεσίας και ρόλου) στους οποίους αναφέρεται ο κανόνας. Μπορεί να λάβει τις τιμές `YES` και `NO`· εφόσον δεν προσδιορίζεται κάποια τιμή, θεωρείται ότι δεν υπάρχει απαίτηση για ενημέρωση της Αρχής Ιδιωτικότητας.

Τέλος, ένα κανόνας μπορεί να χαρακτηρίζεται και από τις παρακάτω δευτερεύουσες ιδιότητες επισημείωσης, οι οποίες του προσδίδουν κάποια επιπλέον χαρακτηριστικά:

- `appliesToPersonalDataDescendants`: Λαμβάνει τις τιμές `YES` και `NO` και δηλώνει εάν ο προσδιοριζόμενος κανόνας βρίσκει εφαρμογή στα προσωπικά δεδομένα των οποίων ο τύπος είναι απόγονος του τύπου που ορίζεται στον κανόνα. Εφόσον παραλείπεται στον ορισμό κάποιου κανόνα, υπονοείται η τιμή `NO`.
- `appliesToServiceDescendants`: Λαμβάνει τις τιμές `YES` και `NO` και δηλώνει εάν ο προσδιοριζόμενος κανόνας βρίσκει εφαρμογή στις υπηρεσίες των οποίων ο τύπος είναι απόγονος του τύπου που ορίζεται στον κανόνα. Εφόσον παραλείπεται στον ορισμό κάποιου κανόνα, υπονοείται η τιμή `YES`.
- `appliesToActorDescendants`: Λαμβάνει τις τιμές `YES` και `NO` και δηλώνει εάν ο προσδιοριζόμενος κανόνας βρίσκει εφαρμογή στις οντότητες ο τύπος του ρόλου των οποίων είναι απόγονος του τύπου που ορίζεται στον κανόνα. Εφόσον παραλείπεται στον ορισμό κάποιου κανόνα, υπονοείται η τιμή `NO`.
- `overrideDataSubjectPreferences`: Σε κάποιες περιπτώσεις, είναι φυσικό οι προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων να έρχονται σε

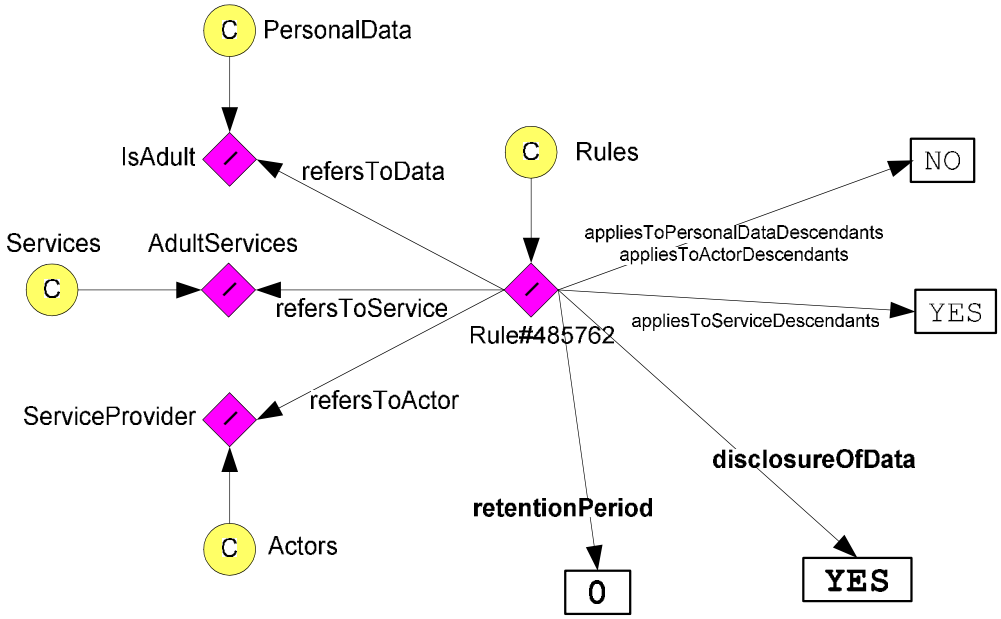
αντίθεση με κάποιο κανόνα που έχει προσδιοριστεί στην Οντολογία Ιδιωτικότητας. Η ιδιότητα `overrideDataSubjectPreferences` ορίζει μέσω κάποιας δυαδικής τιμής `YES` ή `NO` εάν ο κανόνας της Οντολογίας Ιδιωτικότητας υπερισχύει της προτίμησης του χρήστη. Εφόσον δεν προσδιορίζεται κάποια τιμή, θεωρείται ότι η προτίμηση του χρήστη υπερισχύει του κανόνα της Οντολογίας Ιδιωτικότητας (τιμή `NO`).

Επιπλέον, το πεδίο `<rdfs:comment>` των οντολογιών OWL χρησιμοποιείται για τη λεκτική περιγραφή του περιεχομένου του κανόνα.

Το Σχήμα 19 παρουσιάζει το παράδειγμα ενός Κανόνα Δικαιώματος Πρόσβασης. Το νόημα του κανόνα είναι το εξής: "*προκειμένου για υπηρεσίες που απευθύνονται σε ενήλικες (τύπος* `AdultServices`*), όταν κάποια οντότητα τύπου παρόχου υπηρεσίας (*`ServiceProvider`*) θέλει να προσπελάσει προσωπικό δεδομένο τύπου* `IsAdult`[1] *του υποκειμένου του δεδομένου, το δεδομένο θα πρέπει να δοθεί, αλλά να μην κρατηθεί περαιτέρω χρονικό διάστημα στη βάση δεδομένων του Πληρεξούσιου Κόμβου Ιδιωτικότητας. Επιπλέον, ο κανόνας έχει ισχύ για όλους του τύπους υπηρεσιών που είναι απόγονοι της υπηρεσίας τύπου* `AdultServices`*, ενώ δεν έχει ισχύ για τα προσωπικά δεδομένα των τύπων που αποτελούν απογόνους του τύπου* `IsAdult` *καθώς και για τις οντότητες των οποίων ο τύπος του ρόλου τους είναι απόγονος του τύπου* `ServiceProvider`."

Παρόμοια είναι η λογική και των Κανόνων Δικαιώματος Εκτέλεσης. Πιο συγκεκριμένα, τα μέλη της κλάσης `Rules` της Οντολογίας Ιδιωτικότητας που αντιστοιχούν σε Κανόνες Δικαιώματος Εκτέλεσης, αναφέρονται πάντοτε σε τριάδες {τύπος ενσωματωμένης λειτουργικής μονάδας, τύπος υπηρεσίας, τύπος ρόλου}. Όπως περιγράφεται στην επόμενη Ενότητα 5.4, η σημασιολογική αναπαράσταση των Ενσωματωμένων Λειτουργικών Μονάδων του Πληρεξούσιου Κόμβου Ιδιωτικότητας παρέχεται από τα μέλη της κλάσης `Components` της Οντολογίας Ιδιωτικότητας. Προκειμένου να πραγματοποιηθεί ο συσχετισμός μεταξύ των μελών των αντίστοιχων υπογράφων της Οντολογίας Ιδιωτικότητας, χρησιμοποιούνται οι παρακάτω αντικειμενικές ιδιότητες:

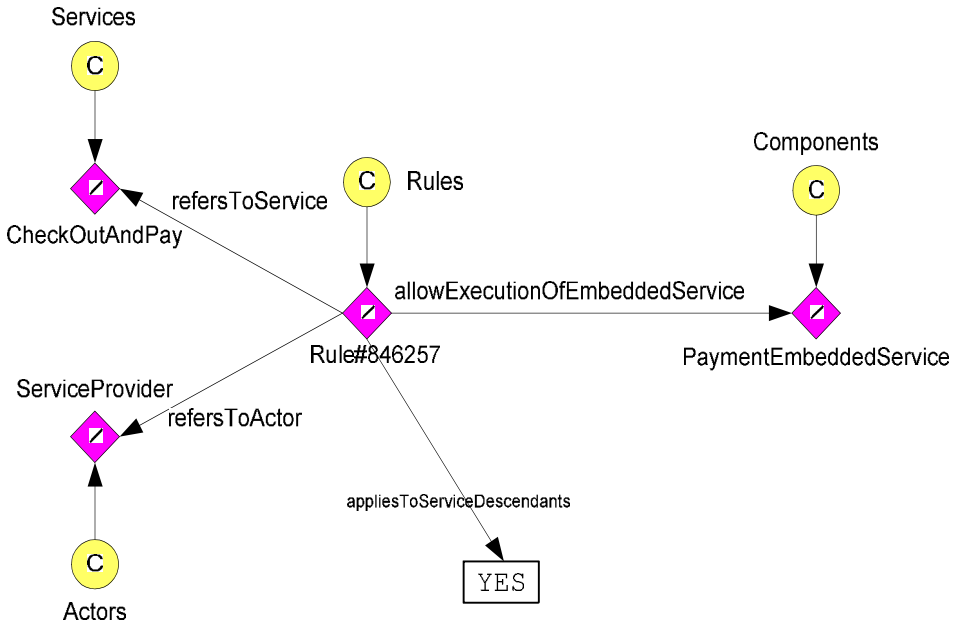
[1] Ο τύπος προσωπικού δεδομένου `IsAdult` αποτελεί μία δυαδική μεταβλητή η οποία εκφράζει εάν το υποκείμενο του δεδομένου είναι ενήλικας ή όχι.



Σχήμα 19: Οντολογία Ιδιωτικότητας – Παράδειγμα Κανόνα Δικαιώματος Πρόσβασης

- Για τη διασύνδεση των μελών των υπογράφων των κλάσεων `Rules` και `Components`, χρησιμοποιείται η αντικειμενική ιδιότητα `allowsExecutionOfEmbeddedService` και η αντίστροφή της.
- Για τη διασύνδεση των μελών των υπογράφων των κλάσεων `Rules` και `Services`, χρησιμοποιείται η αντικειμενική ιδιότητα `refersToService` και η αντίστροφή της.
- Για τη διασύνδεση των μελών των υπογράφων των κλάσεων `Rules` και `Actors`, χρησιμοποιείται η αντικειμενική ιδιότητα `refersToActor` και η αντίστροφή της.

Οι Κανόνες Δικαιώματος Εκτέλεσης είναι αυτοπεριγραφικοί υπό την έννοια ότι περιγράφουν τα δικαιώματα εκτέλεσης χωρίς να χρειάζονται τον ορισμό σχετικών ιδιοτήτων επισημείωσης. Οι ιδιότητες επισημείωσης που μπορεί να χαρακτηρίζουν έναν Κανόνα Δικαιώματος Εκτέλεσης προκειμένου να προσδιορίσουν τα ιδιαίτερα χαρακτηριστικά του αποτελούν υποσύνολο αυτών των Κανόνων Δικαιώματος Πρόσβασης και είναι οι εξής: `DataSubjectInformation`, `DataSubjectConsent`, `AuthorityNotification`, `appliesToServiceDescendants` και `appliesToActorDescendants`, ενώ το πεδίο `<rdfs:comment>` των οντολογιών OWL χρησιμοποιείται για τη λεκτική περιγραφή του περιεχομένου του κανόνα.



Σχήμα 20: Οντολογία Ιδιωτικότητας – Παράδειγμα Κανόνα Δικαιώματος Εκτέλεσης

Το Σχήμα 20 παρουσιάζει το παράδειγμα ενός Κανόνα Δικαιώματος Εκτέλεσης. Το νόημα του κανόνα είναι το εξής: "*προκειμένου για υπηρεσίες που αφορούν την ολοκλήρωση της διαδικασίας αγοράς και τη συνακόλουθη πληρωμή (τύπος* `CheckOutAndPay`*), όταν κάποια οντότητα τύπου παρόχου υπηρεσίας* (`ServiceProvider`) *θέλει να εκτελέσει την Ενσωματωμένη Λειτουργική Μονάδα που πραγματοποιεί την πληρωμή (τύπος* `PaymentEmbeddedService`*), θα πρέπει να του αποδοθούν τα αντίστοιχα δικαιώματα εκτέλεσης. Επιπλέον, ο κανόνας έχει ισχύ για όλους του τύπους υπηρεσιών που είναι απόγονοι της υπηρεσίας τύπου* `CheckOutAndPay`."

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι υπάρχουν κάποιοι γενικοί, "εξ ορισμού" κανόνες οι οποίοι έχουν ενσωματωθεί στην Οντολογία Ιδιωτικότητας και πιο συγκεκριμένα στα μέλη – ρίζες των υπογράφων και οι οποίοι – με την εφαρμογή των καταλλήλων σχέσεων κληρονομικότητας – ισχύουν για όλα τα μέλη της εφόσον δεν αναιρούνται από άλλους, πιο εξειδικευμένους κανόνες. Οι κανόνες αυτοί είναι:

- Το κάθε υποκείμενο δεδομένων διαθέτει πλήρη πρόσβαση στα δεδομένα του.
- Ο πάροχος υπηρεσίας κάθε τύπου, για κάθε τύπο προσωπικών δεδομένων και για κάθε υπηρεσία, δε διαθέτει δικαίωμα πρόσβασης, είτε ανάγνωσης είτε τροποποίησης / διαγραφής.

- Η Αρχή Ιδιωτικότητας για κάθε τύπο προσωπικών δεδομένων και για κάθε υπηρεσία, δε διαθέτει δικαίωμα πρόσβασης, είτε ανάγνωσης είτε τροποποίησης / διαγραφής.
- Ο κάθε πάροχος υπηρεσίας δε διαθέτει δικαίωμα εκτέλεσης καμίας Ενσωματωμένης Λειτουργικής Μονάδας στο πλαίσιο όλων των τύπων υπηρεσιών.
- Το χρονικό διάστημα διατήρησης όλων των τύπων προσωπικών δεδομένων στις βάσεις δεδομένων του Πληρεξούσιου Κόμβου Ιδιωτικότητας είναι ίσο με μηδέν.

5.4 Βοηθητικές Κλάσεις

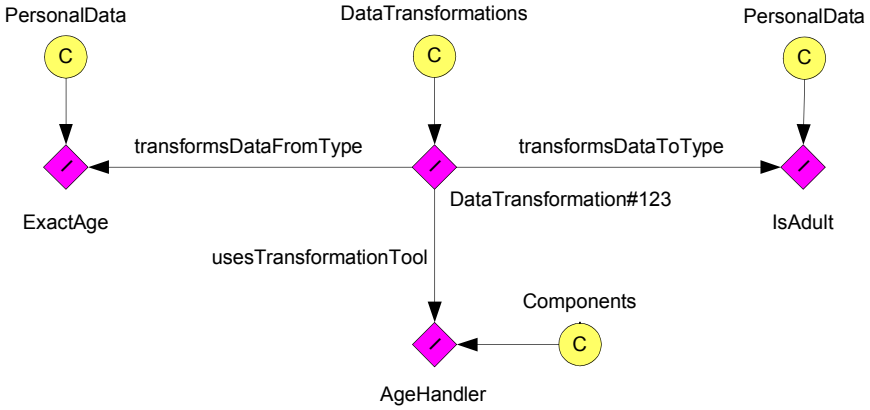
Όπως αναφέρθηκε στην προηγούμενη Ενότητα, η κλάση `Components` αντανακλά τις Ενσωματωμένες Λειτουργικές Μονάδες οι οποίες αποτελούν δομικά συστατικά του Πληρεξούσιου Κόμβου Ιδιωτικότητας. Στην προηγούμενη Ενότητα πραγματοποιήθηκε η περιγραφή του τρόπου με τον οποίο τα μέλη της κλάσης `Components` χρησιμοποιούνται για τον προσδιορισμό των Κανόνων Δικαιώματος Εκτέλεσης.

Η δεύτερη χρήση της κλάσης `Components` είναι ο προσδιορισμός σχέσεων μετασχηματισμών μεταξύ των διαφόρων τύπων προσωπικών δεδομένων. Στο πλαίσιο αυτό, χρησιμοποιείται η κλάση `DataTransformations`, της οποίας τα μέλη ορίζουν τους μετασχηματισμούς που μπορούν να πραγματοποιηθούν μεταξύ των διαφόρων τύπων των δεδομένων με χρήση των Ενσωματωμένων Λειτουργικών Μονάδων του Πληρεξούσιου Κόμβου Ιδιωτικότητας. Το κάθε μέλος της κλάσης `DataTransformations` χαρακτηρίζεται από τρεις αντικειμενικές ιδιότητες:

- `transformsDataFromType`: Έχει ως πεδίο τιμών την κλάση `PersonalData` και εκφράζει τον τύπο προσωπικών δεδομένων που υφίσταται μετασχηματισμό. Ως αντίστροφη έχει την αντικειμενική ιδιότητα `isTransformedBy`.
- `transformsDataToType`: Έχει ως πεδίο τιμών την κλάση `PersonalData` και εκφράζει τον τύπο προσωπικών δεδομένων που αποτελεί το αποτέλεσμα του μετασχηματισμού. Ως αντίστροφη έχει την αντικειμενική ιδιότητα `resultsFromTransformation`.

- `usesTransformationTool`: Έχοντας ως πεδίο τιμών την κλάση `Components`, υποδεικνύει την Ενσωματωμένη Λειτουργική Μονάδα η οποία χρησιμοποιείται για το μετασχηματισμό. Ως αντίστροφη έχει την αντικειμενική ιδιότητα `isUsedAsTransformationTool`.

Το Σχήμα 21 παρουσιάζει ένα παράδειγμα μετασχηματισμού δεδομένων. Σύμφωνα με το παράδειγμα, η Ενσωματωμένη Λειτουργική Μονάδα (Ενσωματωμένος Τελεστής) `AgeHandler` χρησιμοποιείται για το μετασχηματισμό της ακριβούς ηλικίας του υποκειμένου των δεδομένων (τύπος `ExactAge`) σε μία δυαδική μεταβλητή η οποία εκφράζει εάν το υποκείμενο του δεδομένου είναι ενήλικας ή όχι (τύπος `IsAdult`).



Σχήμα 21: Παράδειγμα Μετασχηματισμού Δεδομένων

Τέλος, η κλάση `Patterns` χρησιμοποιείται για την αντιστοίχηση των υπηρεσιών με το υπόδειγμα στο οποίο εντάσσονται (βλ. Ενότητα 4.6). Για το σκοπό αυτό, χρησιμοποιείται η αντικειμενική ιδιότητα `characterizesServices` καθώς και η αντίστροφή της αντικειμενική ιδιότητα `followsPattern`. Στο πλαίσιο της Διατριβής, θεωρήθηκαν τα ακόλουθα υποδείγματα:

- `Pattern#0`: Αντιστοιχεί στο υπόδειγμα που χαρακτηρίζει την παροχή υπηρεσίας από πάροχο υπηρεσίας σε χρήστη και χρησιμοποιείται μόνο για την αμοιβαία αναγνώριση μεταξύ Διαχειριστή Ιδιωτικότητας Χρήστη και Πληρεξούσιου Κόμβου Ιδιωτικότητας, καθώς και την αρχικοποίηση των διαφόρων παραμέτρων ιδιωτικότητας.
- `Pattern#1`: Αντιστοιχεί στο υπόδειγμα που χαρακτηρίζει την παροχή υπηρεσίας από πάροχο υπηρεσίας σε χρήστη.

- `Pattern#2`: Αντιστοιχεί στο υπόδειγμα που χαρακτηρίζει την παροχή υπηρεσίας από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας σε χρήστη.
- `Pattern#3`: Αντιστοιχεί στο υπόδειγμα που χαρακτηρίζει την παροχή υπηρεσίας από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας σε Αρχή Ιδιωτικότητας.
- `Pattern#4`: Αντιστοιχεί στο υπόδειγμα που χαρακτηρίζει την παροχή υπηρεσίας από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας σε πάροχο υπηρεσίας.

5.5 Σύνοψη Ιδιοτήτων OWL της Οντολογίας Ιδιωτικότητας

Επειδή ο αριθμός των ιδιοτήτων OWL – αντικειμενικών και επισημείωσης – που χαρακτηρίζουν την Οντολογία Ιδιωτικότητας είναι μεγάλος, ο Πίνακας 1 συνοψίζει τα πεδία ορισμού και τιμών τους.

Πίνακας 1: Σύνοψη Ιδιοτήτων OWL της Οντολογίας Ιδιωτικότητας

Ιδιότητα OWL	Πεδίο Ορισμού (Κλάση)	Πεδίο Τιμών (Κλάση)
containsType	PersonalData	PersonalData
isContainedToType	PersonalData	PersonalData
inheritsFromData	PersonalData	PersonalData
inheritsFromService	Services	Services
moreDetailedThan	PersonalData	PersonalData
lessDetailedThan	PersonalData	PersonalData
usesTransformationTool	DataTransformations	Components
isUsedAsTransformationTool	Components	DataTransformations
refersToData	Rules	PersonalData
followsPattern	Services	Patterns
characterizesServices	Patterns	Services
refersToActor	Rules	Actors
resultsFromTransformation	PersonalData	DataTransformations
transformDataToType	DataTransformations	PersonalData

Ιδιότητα OWL	Πεδίο Ορισμού (Κλάση)	Πεδίο Τιμών (Κλάση)
transformsDataFromType	DataTransformations	PersonalData
refersToService	Rules	Services
isTransformedBy	PersonalData	DataTransformations
allowExecutionOfEmbeddedService	Rules	Components
isAllowedToBeExecuted	Components	Rules
RetentionPeriod	Rules	
ModificationPermission	Rules	
DisclosureOfData	Rules	
appliesToPersonalDataDescendants	Rules	
appliesToServiceDescendants	Rules	
appliesToActorDescendants	Rules	
DataSubjectInformation	Rules	
DataSubjectConsent	Rules	
AuthorityNotification	Rules	
overrideDataSubjectPreferences	Rules	

6 Οι Γλώσσες Περιγραφής Κανόνων Ιδιωτικότητας και Ροής Εργασιών Ιδιωτικότητας

Στο Κεφάλαιο αυτό, περιγράφονται δύο πρωτότυπες περιγραφικές γλώσσες, βασισμένες στην XML [46], οι οποίες ορίστηκαν στο πλαίσιο της Διατριβής. Η **Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας** χρησιμοποιείται για τον προσδιορισμό των προτιμήσεων των υποκειμένων των δεδομένων αναφορικά με την ιδιωτικότητα. Επιπλέον, στη γλώσσα αυτή εκφράζονται στην τελική τους μορφή οι κανόνες οι οποίοι προκύπτουν από την Οντολογία Ιδιωτικότητας, προκειμένου συνδυαστούν με τις προτιμήσεις του χρήστη. Από την άλλη πλευρά, η **Γλώσσα Περιγραφής Ροής Εργασιών Ιδιωτικότητας** χρησιμοποιείται από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας προκειμένου να περιγραφούν και συγχρονιστούν οι ενέργειες οι οποίες θα λάβουν χώρα για τη διασφάλιση της ιδιωτικότητας στο πλαίσιο της εξυπηρέτησης κάποιου αιτήματος για παροχή υπηρεσίας. Η εκάστοτε ροή εργασιών προκύπτει έπειτα από την επεξεργασία τόσο των κανόνων που περιέχονται στην Οντολογία Ιδιωτικότητας, όσο και των προτιμήσεων του χρήστη, εφόσον υπάρχουν.

6.1 Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας

Προκειμένου ο χρήστης να μπορεί να προσδιορίσει δικούς του κανόνες για το βαθμό και τον τρόπο επεξεργασίας καθώς και για την περαιτέρω μετάδοση των προσωπικών του δεδομένων, στο πλαίσιο της διατριβής αναπτύχθηκε η Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας (ΓΠΚΙ). Η ΓΠΚΙ βασίζεται στη γλώσσα XML [46] και επιτρέπει στο χρήστη να ορίσει κανόνες αναφορικά με:

- Τη συλλογή, επεξεργασία και περαιτέρω μετάδοση των προσωπικών του δεδομένων.
- Το επιθυμητό χρονικό διάστημα διατήρησης των προσωπικών του δεδομένων στις βάσεις δεδομένων του παρόχου κάποιας υπηρεσίας.
- Την επιθυμία του για ενημέρωση σε πραγματικό χρόνο κάθε φορά που κάποιο προσωπικό του δεδομένο πρόκειται να υποστεί επεξεργασία.

- Την επιθυμία του για αίτημα παροχής συναίνεσης σε πραγματικό χρόνο κάθε φορά που κάποιο προσωπικό του δεδομένο πρόκειται να υποστεί επεξεργασία.

Οι κανόνες του χρήστη συντάσσονται με χρήση της γλώσσας ΓΠΚΙ και αποστέλλονται σαν μεταδεδομένα τα οποία συνοδεύουν τα προσωπικά δεδομένα, σύμφωνα με την προκαθορισμένη δομή του Κελύφους Ιδιωτικότητας, όπως περιγράφεται στην Ενότητα 4.8. Εξυπακούεται ότι αυτό βρίσκει εφαρμογή μόνο στα ενεργά προσωπικά δεδομένα. Για τα ημιενεργά προσωπικά δεδομένα η γλώσσα ΓΠΚΙ μπορεί να χρησιμοποιηθεί για τον προσδιορισμό αντίστοιχων κανόνων ασύγχρονα σε σχέση με τη μετάδοση των προσωπικών δεδομένων, ενώ για τα παθητικά προσωπικά δεδομένα δεν υπάρχει δυνατότητα ορισμού προτιμήσεων ιδιωτικότητας από την πλευρά των χρηστών, καθώς δεν υπάρχει άμεσος συσχετισμός μεταξύ των δεδομένων και των χρηστών.

Πέρα από τον ορισμό των προτιμήσεων ιδιωτικότητας των χρηστών, η ΓΠΚΙ χρησιμοποιείται για την έκφραση των τελικών κανόνων ιδιωτικότητας όπως αυτοί προκύπτουν από την Οντολογία Ιδιωτικότητας, εσωτερικά στον Πληρεξούσιο Κόμβο Ιδιωτικότητας (ΠΚΙ). Οι κανόνες αυτοί, οι οποίοι προκύπτουν από τη Νομοθεσία, μεταφράζονται σε ΓΠΚΙ από το Αποθετήριο Κανονισμών και πριν από την παράδοσή τους στο Διαχειριστή Συνόδων και ακολούθως στη Μηχανή Πολιτικών, προκειμένου να είναι δυνατός ο άμεσος συνδυασμός τους με τις προτιμήσεις ιδιωτικότητας του χρήστη και η εξαγωγή των τελικών κανόνων που θα εφαρμοστούν από τον ΠΚΙ.

Όπως έχει προαναφερθεί στην Ενότητα 4.8, το Κέλυφος Ιδιωτικότητας αποτελεί επί της ουσίας μία ΓΠΚΙ δομή, η οποία έχει ως ρίζα το στοιχείο `PRIVACY_LOCK`. Ένα Κέλυφος Ιδιωτικότητας μπορεί να περιέχει οποιοδήποτε αριθμό δεδομένων. Ως εκ τούτου, η ΓΠΚΙ ορίζει το στοιχείο `LOCK`, το οποίο περικλείει κάθε διακριτό τύπο δεδομένων. Κάθε στοιχείο `LOCK` πρέπει να περιέχει τουλάχιστον ένα στοιχείο `DATA` και, προαιρετικά, ακριβώς ένα στοιχείο `META`:

- Το στοιχείο `DATA` περικλείει το τμήμα δεδομένων του αντίστοιχου στοιχείου `LOCK`. Μέσα στο `DATA`, τουλάχιστον ένα στοιχείο `DATA_TYPE` πρέπει να υφίσταται, περιγράφοντας τον τύπο του εν λόγω προσωπικού δεδομένου· όπως είναι φυσικό, το στοιχείο `DATA_TYPE` λαμβάνει τιμές από τον υπογράφο προσωπικών δεδομένων της Οντολογίας Ιδιωτικότητας. Δύο περιπτώσεις υπάρχουν:

- Υφίσταται μετάδοση δεδομένων, οπότε, είτε ένα στοιχείο DATA_VALUE είτε ένα στοιχείο OBJECT είναι παρόν. Το πρώτο χρησιμοποιείται για δεδομένα τύπου συμβολοσειράς (γράμματα, αριθμοί, κλπ.) και περιέχει την αντίστοιχη πληροφορία. Το στοιχείο τύπου OBJECT χρησιμοποιείται στην περίπτωση που το εν λόγω προσωπικό δεδομένο χαρακτηρίζεται από πολύπλοκη φύση / δομή, όπως για παράδειγμα εάν περιέχει πληροφορία τύπου εικόνας, οπότε και δεν μπορεί να περιληφθεί στη δομή της ΓΠΚΙ. Τότε, το στοιχείο OBJECT υποδεικνύει το αντίστοιχο αντικείμενο που περιέχεται στη δομή του Κελύφους Ιδιωτικότητας.
- Δεν υφίσταται μετάδοση δεδομένων, παρά μόνο μετάδοση προτιμήσεων ιδιωτικότητας. Στην περίπτωση αυτή, μόνο το στοιχείο τύπου DATA_TYPE που εκφράζει τον τύπο των προσωπικών δεδομένων που αποτελεί το αντικείμενο των προτιμήσεων πρέπει να είναι παρόν. Στην περίπτωση κατά την οποία ο τύπος που δηλώνεται στο DATA_TYPE αποτελεί τη ρίζα ενός υπογράφου στον υπογράφο προσωπικών δεδομένων της Οντολογίας Ιδιωτικότητας και οι προτιμήσεις αφορούν τους απογόνους του (δηλαδή τα μέλη του υπογράφου), ένα στοιχείο τύπου DATA_TYPE_DESCENDANTS εκφράζει τη σχετική κληρονομικότητα των προτιμήσεων, λαμβάνοντας είτε την τιμή YES είτε την τιμή NO (με προκαθορισμένη τιμή τη YES). Σημειώνεται επίσης ότι στην περίπτωση αυτή, το DATA_TYPE μπορεί επίσης να λάβει την τιμή AllPersonalData, οπότε και αναφέρεται σε όλους τους τύπους προσωπικών δεδομένων.

- Το στοιχείο META περικλείει τις προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων για τους τύπους δεδομένων που περιέχονται στο στοιχείο DATA του LOCK. Αποτελείται από μία σειρά στοιχείων PREF_RULE, όπως περιγράφεται παρακάτω. Σημειώνεται ωστόσο ότι η παρουσία του στοιχείου META είναι προαιρετική, καθώς το υποκείμενο των δεδομένων μπορεί να μεταδώσει δεδομένα χωρίς να εκφράσει προτιμήσεις ιδιωτικότητας.

Οι προτιμήσεις του υποκειμένου των δεδομένων μέσα σε ένα Κέλυφος Ιδιωτικότητας περικλείονται από στοιχεία τύπου PREF_RULE, τα οποία περιέχονται μέσα στο τμήμα META ενός LOCK. Η κάθε προτίμηση ιδιωτικότητας βρίσκει εφαρμογή στα προσωπικά δεδομένα που περιέχονται στο τμήμα DATA του ίδιου LOCK.

Μέσα σε κάθε στοιχείο τύπου PREF_RULE, τουλάχιστον ένα στοιχείο τύπου SERVICE πρέπει να περιέχεται, περικλείοντας τις υπηρεσίες τις οποίες αφορά η προτίμηση ιδιωτικότητας. Κάθε στοιχείο SERVICE περιέχει:

- Τουλάχιστον ένα στοιχείο SERVICE_TYPE, το οποίο εκφράζει τον τύπο της υπηρεσίας στον οποία αναφέρεται η προτίμηση ιδιωτικότητας και λαμβάνει τιμές από τον αντίστοιχο υπογράφο της Οντολογίας Ιδιωτικότητας. Μπορεί επίσης να λάβει την τιμή AllServices, οπότε και αναφέρεται σε όλους τους τύπους υπηρεσιών.
- SERVICE_DESCENDANTS: Δηλώνει εάν ο οριζόμενος κανόνας κληρονομείται από τους απογόνους του δεδομένου τύπου SERVICE_TYPE στην ιεραρχία των κλάσεων του αντίστοιχου υπογράφου της Οντολογίας Ιδιωτικότητας. Μπορεί να λάβει τις τιμές YES και NO.

Σε πλήρη αντιστοιχία, ορίζονται και τα στοιχεία ACTORS, ACTOR και ACTOR_DESCENDANTS. Ωστόσο, καθώς στο πλαίσιο της Διατριβής έχει οριστεί ένα πολύ απλό μοντέλο ρόλων οντοτήτων, δε χρησιμοποιούνται επί της ουσίας.

Εκτός από το πλαίσιο αναφοράς της προτίμησης ιδιωτικότητας (τύπος δεδομένου, τύπος υπηρεσίας και τύπος ρόλου), το κάθε στοιχείο τύπου PREF_RULE περιέχει ακριβώς μία φορά κάθε ένα από τα παρακάτω στοιχεία, τα οποία συναποτελούν το σώμα της προτίμησης ιδιωτικότητας[1]:

- DISCLOSURE: Καθορίζει εάν τα προσωπικά δεδομένα των προσδιορισμένων τύπων για υπηρεσίες των προσδιορισμένων τύπων πρέπει να γνωστοποιηθούν στον πάροχο της υπηρεσίας για την παροχή της. Οι πιθανές τιμές που μπορεί να λάβει είναι YES, NO και MIN, με την τελευταία να δηλώνει την επιθυμία του χρήστη για τη γνωστοποίηση όσο το δυνατό μικρότερης ποσότητας πληροφορίας. Ως προκαθορισμένη τιμή ορίζεται η MIN.
- MODIFICATION_PERMISSION: Καθορίζει εάν ο πάροχος υπηρεσίας έχει δικαίωμα τροποποίησης των προσωπικών δεδομένων των προσδιορισμένων τύπων στο

[1] Η ενδεχόμενη απουσία κάποιου από τα στοιχεία αυτά υπονοεί εφαρμογή της προκαθορισμένης τιμής.

πλαίσιο της παροχής κάποιας υπηρεσίας μεταξύ των προσδιορισμένων τύπων. Μπορεί να λάβει τις τιμές `YES` και `NO`. Ως προκαθορισμένη τιμή ορίζεται η `NO`.

- `INFORMATION`: Καθορίζει εάν το υποκείμενο των δεδομένων επιθυμεί να ενημερωθεί σε πραγματικό χρόνο κάθε φορά που κάποιο προσωπικό του δεδομένο μεταξύ των προσδιορισμένων τύπων πρόκειται να υποστεί επεξεργασία. Μπορεί να λάβει τις τιμές `YES` και `NO`. Ως προκαθορισμένη τιμή ορίζεται η `NO`.
- `CONSENT`: Καθορίζει εάν το υποκείμενο των δεδομένων επιθυμεί να παράσχει συναίνεση σε πραγματικό χρόνο κάθε φορά που κάποιο προσωπικό του δεδομένο μεταξύ των προσδιορισμένων τύπων πρόκειται να υποστεί επεξεργασία. Μπορεί να λάβει τις τιμές `YES` και `NO`. Ως προκαθορισμένη τιμή ορίζεται η `NO`.
- `RETENTION_PERIOD`: Προσδιορίζει το χρονικό διάστημα διατήρησης των προσωπικών δεδομένων των προσδιορισμένων τύπων στη βάση δεδομένων του ΠΚΙ. Μπορεί να λάβει κάποια ακέραια αριθμητική τιμή, η οποία εκφράζει τον αριθμό των χιλιοστών του δευτερολέπτου που πρέπει να κρατηθούν τα δεδομένα, την τιμή `LAW_DEFINED` που ορίζει ως τιμή εκείνη που προκύπτει από τους αντίστοιχους κανόνες που περιέχονται στην Οντολογία Ιδιωτικότητας, ή την τιμή `INDEFINITE`, η οποία υπονοεί διατήρηση των δεδομένων επ' αόριστο. Ως προκαθορισμένη τιμή ορίζεται η `LAW_DEFINED`.

Τέλος, ορίζεται το προαιρετικό στοιχείο `OVERRIDE_LAW` το οποίο μπορεί να περιλαμβάνεται σε κάθε προτίμηση του υποκειμένου των δεδομένων. Το νόημά του είναι να δηλωθεί εάν το υποκείμενο των δεδομένων επιθυμεί η εν λόγω προτίμηση να υπερισχύσει του αντίστοιχου κανόνα που απορρέει από την Οντολογία Ιδιωτικότητας, σε περίπτωση μεταξύ τους αντίθεσης. Σημειώνεται ωστόσο ότι σε περίπτωση που υπάρχει αντίστοιχος μετακανόνας στην Οντολογία Ιδιωτικότητας ο οποίος ορίζει υπεροχή του κανόνα της Οντολογίας Ιδιωτικότητας έναντι της προτίμησης του υποκειμένου των δεδομένων, εφαρμόζεται τελικά ο κανόνας της Οντολογίας Ιδιωτικότητας, ανεξάρτητα από την επιθυμία του υποκειμένου των δεδομένων.

Αναφορικά με την έκφραση στη γλώσσα ΓΠΚΙ των κανόνων που απορρέουν από την Οντολογία Ιδιωτικότητας, ο κάθε κανόνας περιέχεται σε ένα στοιχείο τύπου `REG_RULE`, το οποίο είναι χωρισμένο σε τέσσερα τμήματα:

- Τμήμα τύπων προσωπικών δεδομένων, που ορίζεται από το στοιχείο DATA.
- Τμήμα τύπων υπηρεσιών, που ορίζεται από το στοιχείο SERVICE.
- Τμήμα τύπων ρόλων οντοτήτων, που ορίζεται από το στοιχείο ACTORS.
- Τμήμα σώματος κανόνα, που δεν ορίζεται από κάποιο στοιχείο· δηλαδή, το σώμα του κανόνα περιλαμβάνεται μεταξύ των στοιχείων παιδιών του REG_RULE.

Ένα στοιχείο τύπου DATA περιλαμβάνει:

- DATA_TYPE (υποχρεωτικό): Υποδεικνύει τον τύπο των προσωπικών δεδομένων στον οποίο αναφέρεται ο κανόνας. Λαμβάνει τιμές από τον αντίστοιχο υπογράφο της Οντολογίας Ιδιωτικότητας. Σημειώνεται ότι μπορεί επίσης να λάβει την τιμή AllPersonalData, οπότε και αναφέρεται σε όλους τους τύπους προσωπικών δεδομένων.
- DATA_TYPE_DESCENDANTS (προαιρετικό): Δηλώνει εάν ο οριζόμενος κανόνας κληρονομείται από τους απογόνους του δεδομένου τύπου DATA_TYPE στην ιεραρχία του αντίστοιχου υπογράφου της Οντολογίας Ιδιωτικότητας. Μπορεί να λάβει τις τιμές YES και NO[1].

Ένα στοιχείο τύπου SERVICE περιλαμβάνει:

- SERVICE_TYPE (υποχρεωτικό): Εκφράζει τον τύπο της υπηρεσίας και λαμβάνει τιμές από τον αντίστοιχο υπογράφο της Οντολογίας Ιδιωτικότητας. Μπορεί επίσης να λάβει την τιμή AllServices, οπότε και αναφέρεται σε όλους τους τύπους υπηρεσιών.
- SERVICE_DESCENDANTS (προαιρετικό): Δηλώνει εάν ο οριζόμενος κανόνας κληρονομείται από τους απογόνους του δεδομένου τύπου SERVICE_TYPE στην ιεραρχία του αντίστοιχου υπογράφου της Οντολογίας Ιδιωτικότητας. Μπορεί να λάβει τις τιμές YES και NO.

Ένα στοιχείο τύπου ACTORS περιλαμβάνει:

[1] Σημειώνεται ότι εδώ δεν έχει νόημα η έννοια της προκαθορισμένης τιμής. Οι προκαθορισμένες τιμές ορίζονται στην Οντολογία Ιδιωτικότητας.

- `ACTOR` (υποχρεωτικό): Εκφράζει τον τύπο του ρόλου της δεδομένης οντότητας και λαμβάνει τιμές από τον αντίστοιχο υπογράφο της Οντολογίας Ιδιωτικότητας. Μπορεί επίσης να λάβει την τιμή `AllActors`, οπότε και αναφέρεται σε όλους τους τύπους ρόλων.
- `ACTOR_DESCENDANTS` (προαιρετικό): Δηλώνει εάν ο οριζόμενος κανόνας κληρονομείται από τους απογόνους της οντότητας τύπου `ACTOR` στην ιεραρχία του αντίστοιχου υπογράφου της Οντολογίας Ιδιωτικότητας. Μπορεί να λάβει τις τιμές `YES` και `NO`.

Αναφορικά με το σώμα του κανόνα και σε αντιστοιχία με τις προτιμήσεις του χρήστη, στην ΓΠΕΙ ορίζονται τα παρακάτω στοιχεία:

- `DISCLOSURE`: Καθορίζει εάν τα προσωπικά δεδομένα των προσδιορισμένων τύπων για υπηρεσίες των προσδιορισμένων τύπων πρέπει να γνωστοποιηθούν στους τύπους ρόλων οντοτήτων που προσδιορίζονται. Οι πιθανές τιμές που μπορεί να λάβει είναι `YES`, `NO`[1].
- `MODIFICATION_PERMISSION`: Καθορίζει οι οντότητες των τύπων των ρόλων που προσδιορίζονται έχουν δικαίωμα τροποποίησης των προσωπικών δεδομένων των προσδιορισμένων τύπων στο πλαίσιο της παροχής κάποιας υπηρεσίας μεταξύ των προσδιορισμένων τύπων. Μπορεί να λάβει τις τιμές `YES` και `NO`.
- `INFORMATION`: Καθορίζει εάν το υποκείμενο των δεδομένων θα πρέπει να ενημερωθεί σε πραγματικό χρόνο κάθε φορά που κάποιο προσωπικό του δεδομένο μεταξύ των προσδιορισμένων τύπων πρόκειται να υποστεί επεξεργασία. Μπορεί να λάβει τις τιμές `YES` και `NO`.
- `CONSENT`: Καθορίζει εάν το υποκείμενο των δεδομένων θα πρέπει να παράσχει συναίνεση σε πραγματικό χρόνο κάθε φορά που κάποιο προσωπικό του δεδομένο μεταξύ των προσδιορισμένων τύπων πρόκειται να υποστεί επεξεργασία. Μπορεί να λάβει τις τιμές `YES` και `NO`.

[1] Εδώ, σε αντίθεση με τις προτιμήσεις του υποκειμένου των δεδομένων, δεν έχει νόημα η τιμή `MIN`. Ως μικρότερη ποσότητας πληροφορίας θεωρείται εδώ εκείνος ο τύπος προσωπικών δεδομένων σε κάποιο μονοπάτι του αντίστοιχου υπογράφου της Οντολογίας Ιδιωτικότητας για τον οποίο ορίζεται τιμή `YES`.

- `RETENTION_PERIOD`: Προσδιορίζει το χρονικό διάστημα διατήρησης των προσωπικών δεδομένων των προσδιορισμένων τύπων στη βάση δεδομένων του ΠΚΙ. Μπορεί να λάβει κάποια ακέραια αριθμητική τιμή, η οποία εκφράζει τον αριθμό των χιλιοστών του δευτερολέπτου που πρέπει να κρατηθούν τα δεδομένα, την τιμή `USER_DEFINED` που ορίζει ως τιμή εκείνη που προκύπτει από τις αντίστοιχες προτιμήσεις του υποκειμένου των δεδομένων, ή την τιμή `INDEFINITE`, η οποία υπονοεί διατήρηση των δεδομένων επ' αόριστο. Ως προκαθορισμένη τιμή ορίζεται η τιμή 0· δηλαδή, η μη διατήρηση των δεδομένων.

Τέλος, ορίζεται το στοιχείο `OVERRIDE_USER`. Το νόημά του είναι παρόμοιο με αυτό του `OVERRIDE_LAW` και σκοπό έχει εάν ο κανόνας θα υπερισχύσει ενδεχόμενης αντίστοιχης προτίμησης ιδιωτικότητας του υποκειμένου του δεδομένου. Εφόσον οι δύο αυτοί μετακανόνες έρχονται σε αντίθεση, υπερισχύει ο κανόνας που ορίζεται στην Οντολογία Ιδιωτικότητας.

6.2 Γλώσσα Περιγραφής Ροής Εργασιών Ιδιωτικότητας

Προκειμένου να καλυφθεί η ανάγκη του φορμαλιστικού προσδιορισμού των ενεργειών που πραγματοποιούνται από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας στο πλαίσιο της εξυπηρέτησης κάποιου αιτήματος αλλά και του συγχρονισμού της εκτέλεσής του, στο πλαίσιο της διατριβής προδιαγράφηκε μία πρωτότυπη γλώσσα για την περιγραφή της σχετικής ροής εργασιών. Η Γλώσσα Περιγραφής Ροής Εργασιών Ιδιωτικότητας (ΓΠΡΕΙ) είναι βασισμένη στη γλώσσα XML [46] και σε κάποιο βαθμό είναι παρόμοια με τις διάφορες γλώσσες περιγραφής ροής εργασιών, όπως είναι η δημοφιλής Γλώσσα Εκτέλεσης Επιχειρησιακών Διεργασιών (Business Process Execution Language – BPEL) [121].

Η ΓΠΡΕΙ χρησιμοποιείται εσωτερικά στον Πληρεξούσιο Κόμβο Ιδιωτικότητας (ΠΚΙ). Συγκεκριμένα, η Μηχανή Πολιτικών του ΠΚΙ, αφού αξιολογήσει για κάθε συναλλαγή ιδιωτικότητας τους κανόνες της Οντολογίας Ιδιωτικότητας και τις προτιμήσεις ιδιωτικότητας του χρήστη (εφόσον υπάρχουν), παράγει την απαιτούμενη ροή εργασιών την οποία προδιαγράφει με τη χρήση της ΓΠΡΕΙ και την οποία διαβιβάζει στον αντίστοιχο Διαχειριστή Συνόδων του ΠΚΙ προκειμένου οι εργασίες αυτές να εκτελεστούν και να παρασχεθεί η υπηρεσία. Δηλαδή, η ΓΠΡΕΙ αποτελεί επί της ουσίας τη

γλώσσα για τη διαλειτουργικότητα μεταξύ του Διαχειριστή Συνόδων και της Μηχανής Πολιτικών του ΠΚΙ. Στο σημείο αυτό, θα πρέπει να σημειωθεί ότι η ΓΠΡΕΙ βασίζεται στο σημασιολογικό μοντέλο το οποίο ορίζεται από την Οντολογία Ιδιωτικότητας, προκειμένου να αναφερθεί σε τύπους υπηρεσιών, προσωπικών δεδομένων και ρόλων, αλλά και Ενσωματωμένων Λειτουργικών Μονάδων του ΠΚΙ και μετασχηματισμών μεταξύ των διαφόρων τύπων προσωπικών δεδομένων.

Στη συνέχεια, παρουσιάζονται τα στοιχεία (elements) της γλώσσας ΓΠΡΕΙ. Αναφορικά με το συγχρονισμό των εργασιών, η γλώσσα ΓΠΡΕΙ ορίζει τα παρακάτω στοιχεία:

- `SEQUENCE`: Στο εσωτερικό ενός στοιχείου `<SEQUENCE>`, όλες οι οριζόμενες ενέργειες εκτελούνται ακολουθιακά, με βάση τη σειρά με την οποία αναφέρονται.
- `FLOW`: Το στοιχείο αυτό προσφέρει συγχρονισμό και ταυτοχρονισμό. Όλες οι ενέργειες που ορίζονται στο εσωτερικό ενός στοιχείου `<FLOW>` είναι δυνατό να εκτελεστούν ταυτόχρονα ή και με τυχαία σειρά, ενώ η εκτέλεση της καθεμίας μπορεί να πραγματοποιηθεί περισσότερες της μίας φορές.
- `INTERRUPT`: Το στοιχείο αυτό είναι πάντοτε παρόν στο εσωτερικό ενός στοιχείου `<FLOW>`, προσδιορίζοντας τις αναγκαίες συνθήκες διακοπής του `FLOW`. Η εκτέλεση της ενέργειας που αντιστοιχεί στις συνθήκες αυτές προκαλεί τη διακοπή του και τη συνέχιση της εκτέλεσης της ροής εργασιών εκτός του `FLOW`.
- `SWITCH`: Το στοιχείο αυτό προσφέρει τη δυνατότητα στις ροές εργασίας να επιλέγουν την εργασία εκτέλεσης βάσει της πλήρωσης διαφόρων συνθηκών. Το εσωτερικό ενός στοιχείου `<SWITCH>` αποτελείται από "κλαδιά" εκτέλεσης τα οποία ορίζονται από στοιχεία `<CASE>` καθώς και από ένα μοναδικό και προαιρετικό στοιχείο `<OTHERWISE>`.
- `CASE`: Κάθε στοιχείο `<CASE>` προσδιορίζει ένα σύνολο από ενέργειες που πρόκειται να εκτελεστούν εφόσον ικανοποιούνται οι υποκείμενες συνθήκες. Οι υποκείμενες συνθήκες ορίζονται από ένα ή περισσότερα XML γνωρίσματα (attributes). Για παράδειγμα, όταν κάποιος πάροχος υπηρεσίας υποβάλει αίτημα για κάποιο προσωπικό δεδομένο, το `data-type` αναγνωριστικό χρησιμοποιείται

προκειμένου να διαφοροποιηθούν οι περιπτώσεις εκτέλεσης ανάλογα με τον τύπο του προσωπικού δεδομένου.

- `OTHERWISE`: Οι ενέργειες που προδιαγράφονται μάσα στο στοιχείο <OTHERWISE> είναι εκείνες που εκτελούνται εφόσον καμία από τις αναγκαίες συνθήκες που ορίζονται από τα διάφορα στοιχεία τύπου <CASE> μέσα στο <SWITCH> δεν ικανοποιείται.
- `TERMINATE`: Η παρουσία του στοιχείου <TERMINATE> προκαλεί τον τερματισμό της εκτέλεσης των ενεργειών που ορίζονται μέσα στο στοιχείο το οποίο περιλαμβάνει το <TERMINATE>.

Αναφορικά με την επικοινωνία του ΠΚΙ με τις υπόλοιπες οντότητες που απαρτίζουν το σύστημα, ορίζονται τα παρακάτω ΓΠΡΕΙ στοιχεία:

- `RECEIVE`: Το στοιχείο <RECEIVE> χρησιμοποιείται για τον ορισμό ενός κλειδώματος αναμονής (blocking wait), αναφορικά με τη λήψη κάποιου μηνύματος από κάποια από τις οντότητες του συστήματος. Δύο αναγνωριστικά συνοδεύουν κάποιο στοιχείο <RECEIVE>:
  - `from`: καταδεικνύει την οντότητα – πηγή του μηνύματος που αναμένεται. Μπορεί να πάρει ως τιμή οποιαδήποτε εγγραφή του υπογράφου της κλάσης `Actors` της Οντολογίας Ιδιωτικότητας (Ενότητα 5.2).
  - `message-type`: εκφράζει τον τύπο του μηνύματος που αναμένεται. Μπορεί να πάρει ως τιμή οποιαδήποτε από τις παρακάτω:
    - `DATA_READ_REQUEST`: αναφέρεται στα αιτήματα για ανάγνωση δεδομένων.
    - `DATA_WRITE_REQUEST`: αναφέρεται στα αιτήματα για εγγραφή / τροποποίηση / διαγραφή δεδομένων.
    - `EMBEDDED_SERVICE_EXECUTION_REQUEST`: αναφέρεται στα αιτήματα για εκτέλεση κάποιας Ενσωματωμένης Λειτουργικής Μονάδας.
    - `SERVICE_PROVISION`: αναφέρεται στα μηνύματα που αφορούν το αποτέλεσμα των ενεργειών για την παροχή της ζητούμενης υπηρεσίας.

- `RELAY`: Το στοιχείο `<RELAY>` χρησιμοποιείται για να δηλώσει τη διαβίβαση ενός μηνύματος που ελήφθη σε κάποια άλλη οντότητα, πιθανότατα έπειτα από κάποια στάδια επεξεργασίας. Τα δύο γνωρίσματα τα οποία συνοδεύουν κάποιο στοιχείο `<RELAY>` είναι τα παρακάτω:
  - `to`: καταδεικνύει την οντότητα – αποδέκτη του μηνύματος που διαβιβάζεται. Μπορεί να πάρει ως τιμή οποιαδήποτε εγγραφή του υπογράφου της κλάσης `Actors` της Οντολογίας Ιδιωτικότητας (Ενότητα 5.2).
  - `channel`: εκφράζει το κανάλι μέσω του οποίου θα διαβιβαστεί το μήνυμα. Μπορεί να πάρει ως τιμή είτε την `INTERFACE_CHANNEL`, οπότε το μήνυμα θα διαβιβαστεί μέσω του Καναλιού Διεπαφής, είτε την τιμή `PERSONAL_DATA_CHANNEL`, οπότε το κανάλι που θα χρησιμοποιηθεί θα είναι το Κανάλι Προσωπικών Δεδομένων (βλ. Ενότητα 4.7).
- `REPLY`: Το στοιχείο `<REPLY>` χρησιμοποιείται για να δηλώσει την αποστολή απάντησης σε μήνυμα που ελήφθη από κάποια οντότητα, πιθανότατα έπειτα από κάποια στάδια επεξεργασίας. Χρησιμοποιείται κυρίως στις περιπτώσεις όπου ο Πληρεξούσιος Κόμβος Ιδιωτικότητας παίζει όχι το ρόλο του διαμεσολαβητή μεταξύ παρόχου υπηρεσιών και υποκειμένου των δεδομένων, αλλά το ρόλο του παρόχου υπηρεσίας, εξυπηρετώντας κάποια από τις άλλες οντότητες.

Αναφορικά με την κλήση των Ενσωματωμένων Λειτουργικών Μονάδων, η γλώσσα ΓΠΡΕΙ ορίζει το στοιχείο `<INVOKE>`. Περικλείει τον προσδιορισμό κάποιας λειτουργίας, περιλαμβάνοντας τα ακόλουθα γνωρίσματα:

- `embedded_component`: Προσδιορίζει την Ενσωματωμένη Λειτουργική Μονάδα που πρόκειται να χρησιμοποιηθεί. Μπορεί να αφορά είτε Ενσωματωμένο Τελεστή είτε Ενσωματωμένη Υπηρεσία.
- `source_data_type`: Όταν η κλήση ενός Ενσωματωμένου Τελεστή αφορά το μετασχηματισμό ενός τύπου προσωπικού δεδομένου σε κάποιον άλλο τύπο, το αναγνωριστικό αυτό δηλώνει τον τύπο – "πηγή", δηλαδή τον τύπο που πρόκειται να υποστεί μετασχηματισμό. Εξυπακούεται ότι το αναγνωριστικό αυτό δε χρησιμοποιείται όταν η κλήση αφορά κάποια Ενσωματωμένη Υπηρεσία.

- `target_data_type`: Όταν η κλήση ενός Ενσωματωμένου Τελεστή αφορά το μετασχηματισμό ενός τύπου προσωπικού δεδομένου σε κάποιον άλλο τύπο, το αναγνωριστικό αυτό δηλώνει τον τύπο – "στόχο", δηλαδή τον τύπο που πρόκειται να αποτελέσει το αποτέλεσμα του μετασχηματισμού. Εξυπακούεται ότι το αναγνωριστικό αυτό δε χρησιμοποιείται όταν η κλήση αφορά κάποια Ενσωματωμένη Υπηρεσία.

Σε ό,τι αφορά τα δικαιώματα πρόσβασης των διαφόρων οντοτήτων στα προσωπικά δεδομένα αλλά και στις Ενσωματωμένες Λειτουργικές Μονάδες του ΠΚΙ, η γλώσσα ΓΠΡΕΙ ορίζει τα ακόλουθα στοιχεία:

- `DISCLOSE`: Ορίζει ότι τα προσωπικά δεδομένα του δεδηλωμένου τύπου θα πρέπει να δοθούν στην οντότητα που ζήτησε την απόκτησή τους.
- `WRITE`: Ορίζει ότι κάποια οντότητα διαθέτει δικαιώματα εγγραφής / τροποποίησης / διαγραφής σε κάποιο τύπο προσωπικών δεδομένων. Το στοιχείο αυτό μπορεί να χρησιμοποιηθεί και χωρίς να ζητήσει κάποια οντότητα την εγγραφή των δεδομένων, αλλά να επιβληθεί από τον ΠΚΙ για λόγους που αφορούν την υποχρέωση διατήρησης των εν λόγω δεδομένων.
- `EXECUTE`: Ενεργοποιεί την εκτέλεση κάποιας Ενσωματωμένης Υπηρεσίας, όπως έχει ζητηθεί από κάποια οντότητα.
- `REJECT`: Απορρίπτει το αίτημα οποιουδήποτε είδους (ανάγνωσης προσωπικών δεδομένων, εγγραφής / διαγραφής / τροποποίησης, εκτέλεσης Ενσωματωμένης Υπηρεσίας, κλπ.).

Επιπλέον, σε σχέση με τις απαιτήσεις για ενημέρωση χρηστών ή / και της Αρχής Ιδιωτικότητας, αλλά και για παροχή ρητής συγκατάθεσης από κάποιο υποκείμενο των δεδομένων αναφορικά με κάποια πράξη συλλογής ή επεξεργασίας προσωπικών δεδομένων, η γλώσσα ΓΠΡΕΙ ορίζει τα παρακάτω στοιχεία:

- `INFORMATION`: Ενεργοποιεί την ενέργεια ενημέρωσης κάποιας οντότητας αναφορικά με την πραγματοποίηση κάποιας πράξης κοινοποίησης ή επεξεργασίας προσωπικών δεδομένων. Το αναγνωριστικό `to` υποδεικνύει την οντότητα στην οποία θα σταλεί η εν λόγω ενημέρωση.

- `ASK-CONSENT`: Προκαλεί την υποβολή αιτήματος για ρητή συγκατάθεση σε κάποια οντότητα (συνήθως το υποκείμενο των δεδομένων) αναφορικά με τη συλλογή ή επεξεργασία κάποιων προσωπικών δεδομένων. Το αναγνωριστικό `from` υποδεικνύει την οντότητα από την οποία πρέπει να ζητηθεί η ρητή συγκατάθεση.

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι η ΓΠΡΕΙ δεν αποτελεί μία γλώσσα περιγραφής ροής εργασιών γενικού σκοπού, αλλά έχει σχεδιαστεί συγκεκριμένα στο πλαίσιο της διατριβής και για την υποστήριξη της λειτουργίας του ΠΚΙ. Για το λόγο αυτό, διάφορα χαρακτηριστικά των προσδιοριζόμενων ενεργειών δεν περιγράφονται από τη γλώσσα, αλλά αποτελούν μέρος της εσωτερικής λογικής του ΠΚΙ. Για παράδειγμα, η αφαίρεση των προσωπικών δεδομένων από τα αιτήματα των χρηστών για την παροχή κάποιας υπηρεσίας προτού τα αιτήματα αυτά διαβιβαστούν στον πάροχο της υπηρεσίας δεν προδιαγράφεται από την ΓΠΡΕΙ, αλλά πραγματοποιείται από τον ΠΚΙ ούτως ή άλλως.

Κάθε έγγραφο της γλώσσας ΓΠΡΕΙ περικλείεται από ένα στοιχείο τύπου `<WORKFLOW>`, το οποίο ορίζει την αρχή και το τέλος του. Επιπλέον, το στοιχείο αυτό περιλαμβάνει δύο αναγνωριστικά:

- `SessionID`: Αποτελεί μία συμβολοσειρά η οποία ταυτοποιεί τη συγκεκριμένη Σύνοδο Ιδιωτικότητας, στο πλαίσιο της οποίας δημιουργείται το ΓΠΡΕΙ έγγραφο.
- `TransactionID`: Αποτελεί τη συμβολοσειρά η οποία ταυτοποιεί τη συγκεκριμένη Συναλλαγή της Συνόδου Ιδιωτικότητας, στο πλαίσιο της οποίας δημιουργείται το ΓΠΡΕΙ έγγραφο.

Στο Κεφάλαιο 8, παρουσιάζονται κάποια παραδείγματα εγγράφων ροής εργασιών εκφρασμένα σε ΓΠΡΕΙ.

7 Αρχιτεκτονική Μεσισμικού

Το Κεφάλαιο αυτό παρουσιάζει την αρχιτεκτονική του Συστήματος Μεσισμικού το οποίο παρεμβάλλεται μεταξύ υποκειμένου των δεδομένων, παρόχου υπηρεσίας και Αρχής Ιδιωτικότητας και μεριμνά για την εφαρμογή των απαιτήσεων της Νομοθεσίας περί προστασίας προσωπικών δεδομένων, τόσο σε ό,τι αφορά τους κανόνες ελέγχου πρόσβασης σε προσωπικά δεδομένα που περιέχονται στην Οντολογία Ιδιωτικότητας, όσο και αναφορικά με την εκτέλεση των απαραίτητων συμπληρωματικών ενεργειών. Όπως προαναφέρθηκε, το βασικότερο στοιχείο της προτεινόμενης αρχιτεκτονικής είναι ο Πληρεξούσιος Κόμβος Ιδιωτικότητας, ο οποίος παρουσιάζεται στην Ενότητα 7.1, ενώ στη συνέχεια παρουσιάζονται ο Διαχειριστής Ιδιωτικότητας Χρήστη και ο Κόμβος Υποδομής Ιδιωτικότητας.

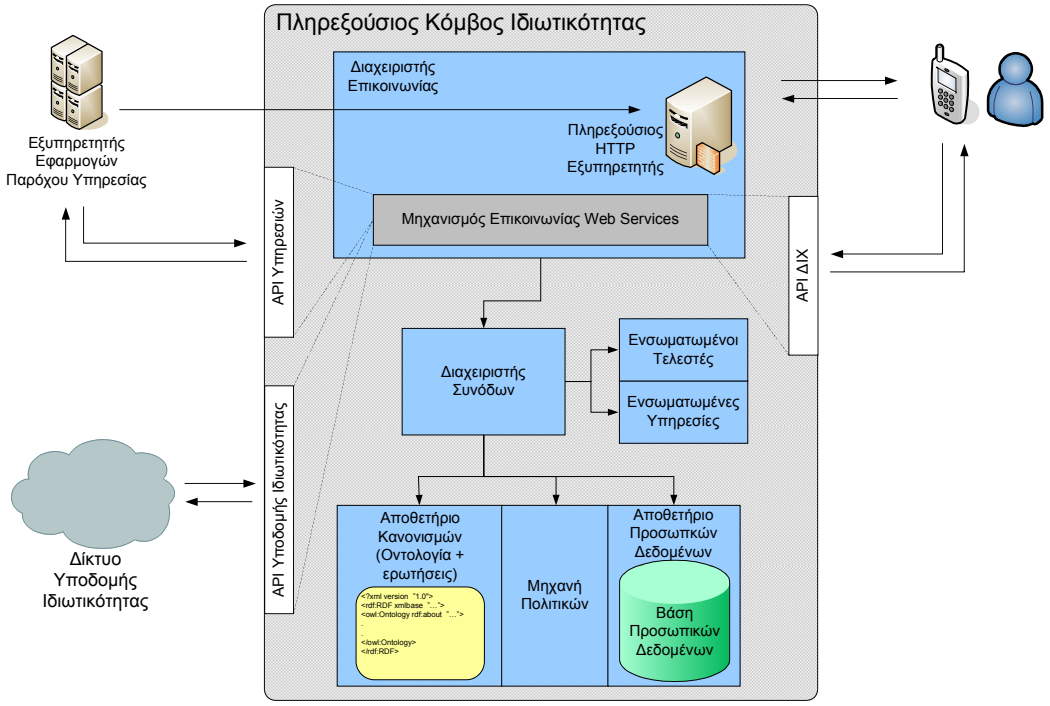
7.1 Πληρεξούσιος Κόμβος Ιδιωτικότητας

Ο Πληρεξούσιος Κόμβος Ιδιωτικότητας (ΠΚΙ) αποτελεί το βασικό συστατικό της προτεινόμενης αρχιτεκτονικής. Αποτελεί το δομικό στοιχείο της προτεινόμενης λύσης το οποίο παρεμβάλλεται μεταξύ του υποκειμένου των δεδομένων, του παρόχου των υπηρεσιών και της Αρχής Ιδιωτικότητας και φροντίζει για την εφαρμογή των κανόνων της ενιαίας πολιτικής ιδιωτικότητας που προδιαγράφεται από την Οντολογία Ιδιωτικότητας.

Η εσωτερική λογική δομή του ΠΚΙ απεικονίζεται στο Σχήμα 22, ενώ η περιγραφή των δομικών συστατικών του και της λειτουργίας τους παρατίθεται στη συνέχεια.

7.1.1 Διαχειριστής Επικοινωνίας

Ο Διαχειριστής Επικοινωνίας είναι εκείνο το δομικό συστατικό του ΠΚΙ που υλοποιεί την επικοινωνία του ΠΚΙ με τα υπόλοιπα στοιχεία της αρχιτεκτονικής, δηλαδή το Διαχειριστή Ιδιωτικότητας Χρήστη, τους Κόμβους Υποδομής Ιδιωτικότητας, αλλά και τις εφαρμογές των παρόχων υπηρεσιών. Επιπλέον, ο Διαχειριστής Επικοινωνίας πραγματοποιεί ένα μέρος της διαχείρισης συνόδων εσωτερικά στον ΠΚΙ, σε άμεση συνέργεια με το Διαχειριστή Συνόδων.



Σχήμα 22: Πληρεξούσιος Κόμβος Ιδιωτικότητας

Όταν κάποιος χρήστης προσπαθεί να συνδεθεί σε κάποια υπηρεσία και δεν είναι συμβατός με την προτεινόμενη λύση, ο ΠΚΙ καθίσταται ένας διάφανος διαβιβαστής των μηνυμάτων, μη συμμετέχοντας περαιτέρω στη διαδικασία. Όταν ο Διαχειριστής Επικοινωνίας δέχεται μήνυμα από έναν Διαχειριστή Ιδιωτικότητας Χρήστη, τότε ενεργοποιεί τις διαδικασίες της προτεινόμενης λύσης. Αρχικοποιεί τις σχετικές παραμέτρους που ορίζουν τη Σύνοδο Ιδιωτικότητας και τη Συναλλαγή Ιδιωτικότητας και ενεργοποιεί ένα Διαχειριστή Συνόδων που θα αναλάβει τη διαχείριση των Συνόδων Ιδιωτικότητας για όλες τις υπηρεσίες και για όσο διάστημα διαρκέσει η Σύνοδος Ιδιωτικότητας. Για κάθε μήνυμα που θα λαμβάνει ο Διαχειριστής Επικοινωνίας και από οποιαδήποτε οντότητα που θα αφορά την εν λόγω Σύνοδο Ιδιωτικότητας, ο Διαχειριστής Επικοινωνίας θα ενεργοποιεί τον αντίστοιχο Διαχειριστή Συνόδων, συμμετέχοντας με τον τρόπο αυτό στη διαχείριση συνόδων.

Ο Διαχειριστής Επικοινωνίας υλοποιεί από την πλευρά του ΠΚΙ και τα δύο κανάλια επικοινωνίας που ορίστηκαν στην Ενότητα 4.7, δηλαδή το Κανάλι Διεπαφής και το Κανάλι Προσωπικών Δεδομένων. Για το λόγο αυτό, στην υλοποίησή του περιλαμβάνεται ένα Java Servlet [122] για την υλοποίηση του Καναλιού Διεπαφής και μία

σειρά από Υπηρεσίες Ιστού (Web Services) βασισμένες στην προσέγγιση Apache Axis2 [123].

7.1.2 Αποθετήριο Κανονισμών

Το Αποθετήριο Κανονισμών αποτελεί το δομικό συστατικό του ΠΚΙ που δίνει τη δυνατότητα στον ΠΚΙ να λαμβάνει αποφάσεις σχετικά με τη διαχείριση των προσωπικών δεδομένων λαμβάνοντας υπόψη τους κανόνες που απορρέουν από τη Νομοθεσία. Αποτελεί το δομικό συστατικό που διαχειρίζεται την Οντολογία Ιδιωτικότητας (Κεφάλαιο 5) και τροφοδοτεί τον ΠΚΙ με τους κανόνες και όλες τις πληροφορίες που η Οντολογία Ιδιωτικότητας περιλαμβάνει.

Το Αποθετήριο Κανονισμών εκτελεί ουσιαστικά δύο λειτουργίες:

- Ενημέρωση της Οντολογίας Ιδιωτικότητας.
- Παροχή στο Διαχειριστή Συνόδων πληροφοριών που περιέχονται στην Οντολογία Ιδιωτικότητας.

Αναφορικά με την πρώτη λειτουργία, η Αρχή Ιδιωτικότητας είναι η μόνη οντότητα του συστήματος η οποία διαθέτει δικαιώματα πρόσβασης εγγραφής στην Οντολογία Ιδιωτικότητας. Όταν για κάποιο λόγο η Οντολογία Ιδιωτικότητας τροποποιηθεί (π.χ., μεταβολή κανόνων, προσθήκη νέων τύπων προσωπικών δεδομένων, προσθήκη νέων τύπων υπηρεσιών, κλπ.), η Αρχή Ιδιωτικότητας διανέμει τη νέα έκδοση του μέσω Δικτύου Υποδομής Ιδιωτικότητας και μέσω της διεπαφής μεταξύ του ΠΚΙ και του Κόμβου Υποδομής Ιδιωτικότητας. Το σχετικό αίτημα λαμβάνεται από το Διαχειριστή Επικοινωνίας και μέσω του Διαχειριστή Συνόδων, το αίτημα φτάνει στο Αποθετήριο Κανονισμών το οποίο ενημερώνει την Οντολογία Ιδιωτικότητας.

Αναφορικά με τη δεύτερη λειτουργία, το Αποθετήριο Κανονισμών προσφέρει στο Διαχειριστή Ιδιωτικότητας μία διεπαφή για την υποβολή των σχετικών ερωτημάτων. Τα ερωτήματα τα οποία είναι σε θέση να εξυπηρετήσει το Αποθετήριο Κανονισμών είναι:

- Για δεδομένο τύπο προσωπικών δεδομένων, εύρεση του υποδέντρου που ορίζει.
- Για δεδομένο τύπο προσωπικών δεδομένων, εύρεση των μονοπατιών που συνδέουν τον τύπο αυτό με τον τύπο `AllPersonalData`.
- Για δεδομένο τύπο υπηρεσίας, εύρεση του υποδέντρου που ορίζει.

- Για δεδομένο τύπο υπηρεσίας, εύρεση των μονοπατιών που συνδέουν τον τύπο αυτό με τον τύπο `AllServices`.
- Για δεδομένο τύπο υπηρεσίας, εύρεση του υποδείγματος το οποίο ακολουθεί.
- Για δεδομένο τύπο προσωπικών δεδομένων, εύρεση των κανόνων που τον διέπουν.
- Για δεδομένο τύπο υπηρεσίας, εύρεση των κανόνων που τον διέπουν.

Το Αποθετήριο Κανονισμών υλοποιήθηκε στο πλαίσιο της διατριβής σαν ένα Enterprise Java Bean [124], ενώ για την προσπέλαση της Οντολογίας Ιδιωτικότητας χρησιμοποιήθηκε η βιβλιοθήκη Jena [125] που αναπτύχθηκε στα ερευνητικά εργαστήρια για το Σημασιολογικό Ιστό (Semantic Web) της Hewlett Packard [126].

Τέλος, σημειώνεται ότι το Αποθετήριο Κανονισμών παρέχει στο Διαχειριστή Συνόδων τους ζητούμενους κανόνες υπό μορφή της Γλώσσας Περιγραφής Κανόνων Ιδιωτικότητας (Ενότητα 6.1), προκειμένου αυτοί να είναι άμεσα συγκρίσιμοι με τις προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων. Για το σκοπό αυτό, μία από τις εσωτερικές λειτουργίες του Αποθετηρίου Κανονισμών είναι η μετάφραση των κανόνων στη μορφή αυτή.

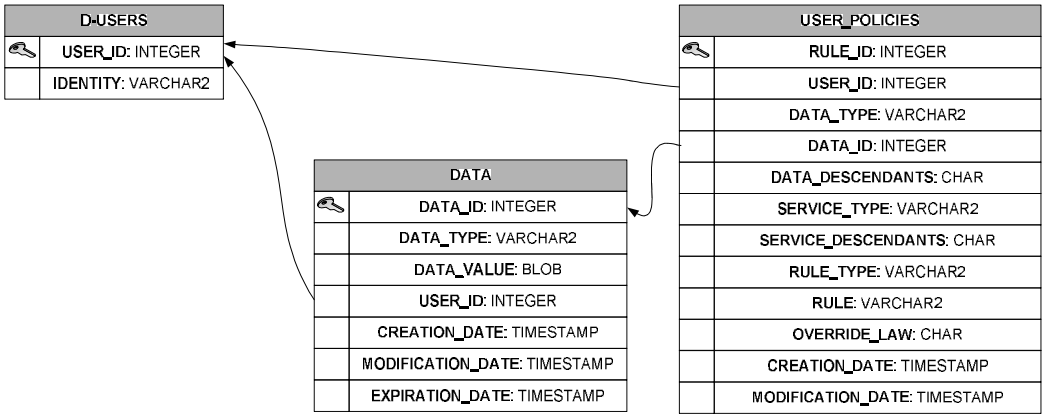
7.1.3 Αποθετήριο Προσωπικών Δεδομένων

Το Αποθετήριο Προσωπικών Δεδομένων αποτελεί ένα πολύ σημαντικό δομικό στοιχείο του ΠΚΙ, καθώς εκεί αποθηκεύονται τα προσωπικά δεδομένα όταν υπάρχει λόγος για κάτι τέτοιο. Αποτελείται από δύο βασικά δομικά στοιχεία:

- Βάση Προσωπικών Δεδομένων.
- Διαχειριστής Συναλλαγών Αποθετηρίου Προσωπικών Δεδομένων.

Η Βάση Προσωπικών Δεδομένων αποτελεί μία Σχεσιακή Βάση Δεδομένων (Relational Database Management System – RDBMS) [127] στην οποία βρίσκονται αποθηκευμένα τα προσωπικά δεδομένα. Το προϊόν που επιλέχθηκε ήταν το Oracle Database 10g Release 2 [128], λόγω των εξαιρετικών χαρακτηριστικών ασφάλειας που προσφέρει, καθώς και λόγω της αξιοπιστίας και των επιδόσεών του.

Το Σχήμα 23 παρουσιάζει το σχήμα της Βάσης Προσωπικών Δεδομένων.



Σχήμα 23: Σχήμα Βάσης Προσωπικών Δεδομένων

Όπως φαίνεται στο Σχήμα 23, το σχήμα της Βάσης Προσωπικών Δεδομένων είναι αρκετά απλό, καθώς αποτελείται από τρεις μόνο πίνακες. Οι τρεις πίνακες αφορούν αντίστοιχα τα υποκείμενα των δεδομένων (πίνακας `D-USERS`), τα προσωπικά δεδομένα τους (πίνακας `DATA`) και τις προτιμήσεις ιδιωτικότητας (πίνακας `USER_POLICIES`).

Κάτι το οποίο πρέπει να σημειωθεί εδώ είναι ότι τα προσωπικά δεδομένα τα οποία αποθηκεύονται στη Βάση Προσωπικών Δεδομένων μπορεί να είναι οποιασδήποτε μορφής, όπως κείμενο, εικόνα, βίντεο, οποιοδήποτε κρυπτογραφημένο αντικείμενο, κλπ. Για το λόγο αυτό, η στήλη `DATA_VALUE` του πίνακα `DATA` είναι τύπου Binary Large Object (BLOB), δηλαδή αποθηκεύει τα δεδομένα ανεξάρτητα από τον τύπο τους σαν δυαδικά αντικείμενα. Έτσι, μπορεί να αποθηκεύσει δεδομένα οποιασδήποτε μορφής. Το μειονέκτημα ασφαλώς μίας τέτοιας προσέγγισης είναι ότι η αναζήτηση καθίσταται εξαιρετικά δύσκολη υπό την έννοια ότι απαιτεί την κατανάλωση αρκετών πόρων του συστήματος. Ωστόσο, το μειονέκτημα αυτό δεν ισχύει στην περίπτωση της Βάσης Προσωπικών Δεδομένων, καθώς η αναζήτηση πραγματοποιείται στη συντριπτική πλειοψηφία των περιπτώσεων με βάση τη δυάδα {αναγνωριστικό χρήστη, τύπος δεδομένων}.

Ο Διαχειριστής Συναλλαγών Αποθετηρίου Προσωπικών Δεδομένων αποτελεί το υποσύστημα λογισμικού που διαχειρίζεται τη Βάση Προσωπικών Δεδομένων και επικοινωνεί με το Διαχειριστή Συνόδων. Είναι υλοποιημένος σαν Enterprise Java Bean [124] και προσφέρει στο Διαχειριστή Συνόδων μεθόδους για:

- Την ανάκτηση δεδομένων και μεταδεδομένων.
- Την αποθήκευση δεδομένων και μεταδεδομένων.

- Την τροποποίηση δεδομένων και μεταδεδομένων.
- Τη διαγραφή δεδομένων και μεταδεδομένων.

Επιπλέον, ο Διαχειριστής Συναλλαγών Αποθετηρίου Προσωπικών Δεδομένων διαγράφει με αυτόματο τρόπο τα προσωπικά δεδομένα όταν ο χρόνος ζωής τους (όπως υποδεικνύεται από τη στήλη `EXPIRATION_DATE` του πίνακα `DATA`) έχει παρέλθει.

Τέλος, σημειώνεται ότι ο Διαχειριστής Συναλλαγών Αποθετηρίου Προσωπικών Δεδομένων καταγράφει όλα τα ερωτήματα που υποβάλλονται στη Βάση Προσωπικών Δεδομένων και τα καταχωρεί σε κρυπτογραφημένο αρχείο το οποίο βρίσκεται στη διάθεση της Αρχής Ιδιωτικότητας.

7.1.4 Μηχανή Πολιτικών

Η Μηχανή Πολιτικών αποτελεί το δομικό στοιχείο του ΠΚΙ που λαμβάνει τις αποφάσεις αναφορικά με την εκτέλεση των απαραιτήτων ενεργειών που θα εξασφαλίσουν την προστασία της ιδιωτικότητας του υποκειμένου δεδομένων κατά την παροχή κάποιας υπηρεσίας. Η Μηχανή Πολιτικών λαμβάνει ως είσοδο τους κανόνες που απορρέουν από τη Νομοθεσία όπως αυτοί προδιαγράφονται στην Οντολογία Ιδιωτικότητας καθώς και τις αντίστοιχες προτιμήσεις του χρήστη, υπό μορφή Γλώσσα Περιγραφής Κανόνων Ιδιωτικότητας. Μετά από την επεξεργασία τους, η Μηχανή Πολιτικών παράγει ένα έγγραφο της Γλώσσας Περιγραφής Ροής Εργασιών Ιδιωτικότητας το οποίο διαβιβάζει στο Διαχειριστή Συνόδων, ο οποίος μεριμνά για την εκτέλεση των προσδιορισμένων ενεργειών.

Πιο συγκεκριμένα, η Μηχανή Πολιτικών λαμβάνει ως είσοδο την παρακάτω πληροφορία:

- Τον τύπο της ζητούμενης υπηρεσίας, σημασιολογικά προσδιορισμένο σύμφωνα με το σημασιολογικό μοντέλο της Οντολογίας Ιδιωτικότητας, καθώς και το ρόλο της οντότητας από την οποία ζητείται η παροχή της.
- Το υπόδειγμα το οποίο ακολουθεί η εν λόγω υπηρεσία κατά την παροχή της.
- Τους κανόνες που περιέχονται στην Οντολογία Ιδιωτικότητας αναφορικά με τη ζητούμενη υπηρεσία.
- Τις προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων, εφόσον ασφαλώς υφίστανται.

- Τους κατά περίπτωση διαθέσιμους τύπους προσωπικών δεδομένων, προκειμένου να προσδιοριστούν οι μετασχηματισμοί που είναι δυνατό ή / και που επιβάλλεται να πραγματοποιηθούν.

Λαμβάνοντας υπόψη τα παραπάνω, παράγει και διαβιβάζει στο Διαχειριστή Συνόδων τη ροή εργασιών που πρέπει να εκτελεστεί.

7.1.5 Διαχειριστής Συνόδων

Ο Διαχειριστής Συνόδων έχει ως αποστολή το συντονισμό της λειτουργίας των υπολοίπων δομικών στοιχείων του ΠΚΙ στο πλαίσιο της εξυπηρέτησης των Συνόδων Ιδιωτικότητας. Είναι υλοποιημένος σαν Enterprise Java Bean [124] το οποίο διατηρεί την κατάστασή του (stateful) και παραμένει ενεργός καθόλη τη διάρκεια μίας Συνόδου Ιδιωτικότητας. Πραγματοποιεί επίσης λεπτομερή καταγραφή όλων των συμβάντων που λαμβάνουν χώρα κατά τον κύκλο ζωής του.

Ο κύκλος λειτουργίας του Διαχειριστή Συνόδων συνοψίζεται στα παρακάτω βήματα:

1. Αρχικοποίηση ή επαναρχικοποίηση.
2. Εξακρίβωση του υποδείγματος της υπηρεσίας προς παροχή.
3. Ανάκτηση των κανόνων που απορρέουν από τη Νομοθεσία από το Αποθετήριο Κανονισμών.
4. Υποβολή των κανόνων και των προτιμήσεων ιδιωτικότητας του υποκειμένου των δεδομένων στη Μηχανή Πολιτικών και ανάκτηση της ροής εργασιών.
5. Εκτέλεση της ροής εργασιών.

Αξίζει να σημειωθεί ότι καθώς ο Διαχειριστής Συνόδων λαμβάνει και στέλνει ασύγχρονα μεγάλο αριθμό μηνυμάτων από και σε μεγάλο αριθμό άλλων αρχιτεκτονικών οντοτήτων, κατά την υλοποίησή του χρησιμοποιήθηκε εκτενώς η τεχνολογία Java Message Service [129].

7.1.6 Ενσωματωμένες Λειτουργικές Μονάδες

Οι Ενσωματωμένες Λειτουργικές Μονάδες είναι δομικά στοιχεία του ΠΚΙ τα οποία αναλαμβάνουν την εκτέλεση εσωτερικά στον ΠΚΙ διαφόρων λειτουργιών που υπό

άλλες συνθήκες θα εκτελούνταν από τον πάροχο των υπηρεσιών. Χωρίζονται σε δύο κατηγορίες:

- **Ενσωματωμένοι Τελεστές**: Πρόκειται για λειτουργίες επεξεργασίας δεδομένων (π.χ. η μετατροπή ενός τύπου δεδομένων σε κάποιον άλλο λιγότερο λεπτομερή) ή για λειτουργίες διαχείρισης πολύπλοκων τύπων δεδομένων.
- **Ενσωματωμένες Υπηρεσίες**: Πρόκειται για ολόκληρα "αυτόνομα" τμήματα υπηρεσιών, οι οποίες γενικά απαιτούν την επεξεργασία προσωπικών δεδομένων με υψηλό βαθμό ευαισθησίας (π.χ. πραγματοποίηση χρηματικής χρέωσης). Ο σκοπός τους είναι να αποτρέψουν την κοινοποίηση των αντίστοιχων τύπων προσωπικών δεδομένων στον πάροχο των υπηρεσιών. Αντί αυτού, ο πάροχος των υπηρεσιών ζητά από τον ΠΚΙ την εκτέλεση των Ενσωματωμένων Υπηρεσιών.

Ενδεικτικά, στο πλαίσιο της Διατριβής υλοποιήθηκαν μεταξύ άλλων οι παρακάτω Ενσωματωμένοι Τελεστές:

- **Διαχειριστής Ψηφιακού Δελτίου Ταυτότητας**: Πρόκειται για λειτουργικό συστατικό το οποίο επεξεργάζεται αντικείμενα του τύπου Ψηφιακό Δελτίο Ταυτότητας (ορισμένα στην Οντολογία Ιδιωτικότητας σαν `DigitalIdentityCard`). Το Ψηφιακό Δελτίο Ταυτότητας αποτελεί μία δομή δεδομένων το οποίο αποτελεί το ψηφιακό ανάλογο του Δελτίου Ταυτότητας και περιέχει τις ίδιες πληροφορίες σε ψηφιακή μορφή. Θεωρούμε ότι το Ψηφιακό Δελτίο Ταυτότητας εκδίδεται από κάποια αρμόδια Δημόσια Αρχή και ότι η ακεραιότητά του διασφαλίζεται με κρυπτογραφικά μέσα. Ο Ενσωματωμένος Τελεστής εκτελεί την αποκρυπτογράφηση της δομής, την εξακρίβωση της αυθεντικότητάς καθώς και την εξαγωγή των επιμέρους πεδίων, τα οποία είναι σε θέση να παράσχει στο Διαχειριστή Ιδιωτικότητας.
- **Διαχειριστής Ηλικίας**: Πρόκειται για λειτουργικό συστατικό το οποίο πραγματοποιεί την επεξεργασία όλων των τύπων δεδομένων που σχετίζονται με την ηλικία του υποκειμένου των δεδομένων, κάνοντας μετατροπές από κάποιο τύπο σε κάποιον άλλο. Για παράδειγμα, από την ημερομηνία γέννησης του υποκειμένου των δεδομένων (τύπος `DateOfBirth`) εξάγει μία δυαδική μεταβλητή η οποία εκφράζει εάν το υποκείμενο του δεδομένου είναι ενήλικας ή όχι (τύπος `IsAdult`).

- **Διαχειριστής Θέσης**: Πρόκειται για λειτουργικό συστατικό το οποίο πραγματοποιεί την επεξεργασία όλων των τύπων δεδομένων που σχετίζονται με δεδομένα θέσης του υποκειμένου των δεδομένων, κάνοντας μετατροπές από κάποιο τύπο σε κάποιον άλλο. Για παράδειγμα, από τις λεπτομερείς γεωγραφικές συντεταγμένες της θέσης του υποκειμένου των δεδομένων (τύπος `GeographicCoordinates`) εξάγει λιγότερο λεπτομερείς πληροφορίες, όπως είναι η πόλη στην οποία βρίσκεται το υποκείμενο των δεδομένων (τύπος `City`).
- **Επεξεργαστής Εικόνας**: Πρόκειται για λειτουργικό συστατικό το οποίο επεξεργάζεται σταθερή ή κινούμενη εικόνα και αποκρύπτει την πληροφορία που αναφέρεται στα πρόσωπα των ανθρώπων που περιλαμβάνονται στην εικόνα. Στο πλαίσιο της Διατριβής, χρησιμοποιήθηκε για την επεξεργασία βίντεο που λαμβάνεται για λόγους ασφάλειας.

Επιπλέον, στο πλαίσιο της Διατριβής υλοποιήθηκαν ενδεικτικά οι παρακάτω Ενσωματωμένες Υπηρεσίες:

- **Υπηρεσία Πληρωμών**: Εκτελεί εσωτερικά στον ΠΚΙ τις χρεώσεις των υποκειμένων των δεδομένων για την παροχή κάποιας υπηρεσίας. Υπόκεινται σε Κανόνες Δικαιώματος Εκτέλεσης, όπως αυτοί ορίζονται στην Οντολογία Ιδιωτικότητας (βλ. Ενότητα 5.3). Για την πραγματοποίηση της χρέωσης η Ενσωματωμένη Υπηρεσία Πληρωμών (`PaymentEmbeddedService` στην Οντολογία Ιδιωτικότητας) χρησιμοποιεί τη μέθοδο που περιγράφεται στο [130].
- **Υπηρεσία Αποστολής Μηνυμάτων Ηλεκτρονικού Ταχυδρομείου**: Προκειμένου να μη δοθούν διευθύνσεις ηλεκτρονικού ταχυδρομείου σε κάποιον Υπεύθυνο για την Επεξεργασία, η εν λόγω Ενσωματωμένη Υπηρεσία πραγματοποιεί την αποστολή των μηνυμάτων εσωτερικά στον ΠΚΙ. Δέχεται ως ορίσματα τα τυπικά πεδία των μηνυμάτων ηλεκτρονικού ταχυδρομείου καθώς και κωδικοποιημένα τα σημεία στα οποία πρέπει να τοποθετηθούν προσωπικά δεδομένα που βρίσκονται αποθηκευμένα στο Αποθετήριο Προσωπικών Δεδομένων μαζί με τους αντίστοιχους τύπους δεδομένων. Έτσι, αποφεύγεται η κοινοποίηση διευθύνσεων και ο συνακόλουθος κίνδυνος για αποστολή ανεπιθύμητων μηνυμάτων αλλά και ο κίνδυνος ταυτοποίησης του χρήστη που ζήτησε κάποια υπηρεσία.

7.2 Διαχειριστής Ιδιωτικότητας Χρήστη

Ο Διαχειριστής Ιδιωτικότητας Χρήστη (ΔΙΧ) αποτελεί το δομικό στοιχείο της αρχιτεκτονικής μεσισμικού που εδρεύει στο τερματικό του υποκειμένου των δεδομένων. Αποτελεί επί της ουσίας ένα είδος "βοηθού" του χρήστη, αναφορικά με την προστασία της ιδιωτικότητας των προσωπικών του δεδομένων. Πιο συγκεκριμένα, οι λειτουργίες του ΔΙΧ είναι οι παρακάτω:

- Ελέγχει όλη την επικοινωνιακή κίνηση από και προς το τερματικό του χρήστη.
- Εγκαθιστά και διαχειρίζεται την επικοινωνία του τερματικού του χρήστη με τους Πληρεξούσιους Κόμβους Ιδιωτικότητας
- Διαχειρίζεται όλη την επικοινωνία με το υποκείμενο των δεδομένων, αναφορικά με θέματα ιδιωτικότητας. Πιο συγκεκριμένα:
  - Λαμβάνει τις ενημερώσεις από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας.
  - Λαμβάνει τα αιτήματα για παροχή ρητής συναίνεσης και αποστέλλει τη σχετική απάντηση.
  - Επιτρέπει στο χρήστη να ορίσει τις προτιμήσεις ιδιωτικότητας.
- Κατασκευάζει τις δομές δεδομένων που συνδυάζουν τα προσωπικά δεδομένα με τις αντίστοιχες προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων.
- Διαχειρίζεται τα Κελύφη Ιδιωτικότητας.

Ο ΔΙΧ είναι υλοποιημένος σαν Enterprise Java Bean [124], ενώ το γραφικό περιβάλλον είναι χωριστό από το κυρίως μέρος του. Αυτό βασίζεται στη λογική ότι ο χρήστης μπορεί να χρησιμοποιεί τερματικά τα οποία δεν είναι σε θέση να αντέξουν το υπολογιστικό βάρος του ΔΙΧ. Στην περίπτωση αυτή, το γραφικό περιβάλλον μπορεί να εδρεύει στο τερματικό και το κυρίως μέρος να λειτουργεί ως πληρεξούσιος εξυπηρετητής. Για την επικοινωνία μεταξύ του ΔΙΧ και των χωριστών γραφικών περιβαλλόντων έχουν χρησιμοποιηθεί Υπηρεσίες Ιστού της τεχνολογίας Apache Axis2 [123].

7.3 Κόμβος Υποδομής Ιδιωτικότητας

Ο Κόμβος Υποδομής Ιδιωτικότητας (ΚΥΙ) αποτελεί το δομικό στοιχείο της αρχιτεκτονικής που αφορά την πρόσβαση της Αρχής Ιδιωτικότητας. Διαθέτει ένα τριπλό ρόλο στην προδιαγραφή της προτεινόμενης λύσης:

- Διαχείριση και εποπτεία των Πληρεξούσιων Κόμβων Ιδιωτικότητας.
- Προδιαγραφή, ενημέρωση και διάδοση της Οντολογίας Ιδιωτικότητας.
- Πραγματοποίηση νόμιμης παρακολούθησης και συλλογής προσωπικών δεδομένων (LI).

Για την υλοποίηση των παραπάνω λειτουργιών χρησιμοποιήθηκαν έτοιμα εργαλεία, όπως είναι το ελεύθερο και ανοιχτού κώδικα εργαλείο λογισμικού Protégé [120], το οποίο έχει αναπτυχθεί από το Πανεπιστήμιο Stanford και το οποίο χρησιμοποιήθηκε για τη διαχείριση της Οντολογίας Ιδιωτικότητας.

Στις δε περιπτώσεις που απαιτείται η συνέργεια με τον Πληρεξούσιο Κόμβο Ιδιωτικότητας, χρησιμοποιήθηκαν απλές διεπαφές HTTP [99] και Υπηρεσίες Ιστού της τεχνολογίας Apache Axis2 [123], σε κάθε περίπτωση πάνω από κρυπτογραφημένες ζεύξεις.

8 Παραδείγματα Χρήσης

Στο παρόν Κεφάλαιο παρουσιάζονται τρία παραδείγματα χρήσης, τα οποία επιδεικνύουν τη λειτουργία της προτεινόμενης λύσης. Λαμβάνοντας υπόψη τις διαφορές μεταξύ των ενεργών, ημιενεργών και παθητικών προσωπικών δεδομένων (βλ. Ενότητα 4.3), το κάθε ένα από τα τρία παραδείγματα εστιάζει, αντίστοιχα, στις τρεις αυτές διαφορετικές κατηγορίες δεδομένων.

8.1 Παράδειγμα Χρήσης Ενεργών Προσωπικών Δεδομένων

Θεωρούμε έναν πάροχο υπηρεσιών, ο οποίος παρέχει υπηρεσίες βασισμένες στη θέση του χρήστη (Location-Based Services – LBS). Οι υπηρεσίες καλύπτουν ένα μεγάλο εύρος, το οποίο αφορά την παροχή χαρτών, την εύρεση σημείων ενδιαφέροντος, κλπ. Επιπλέον, θεωρούμε ότι οι υπηρεσίες απευθύνονται σε εγγεγραμμένους χρήστες και ότι παρέχονται με πληρωμή.

Βρισκόμενος για πρώτη φορά σε κάποια πόλη, ο χρήστης του σεναρίου επιθυμεί να αναζητήσει τα μπαρ που βρίσκονται στη γειτονιά του ξενοδοχείου του και έχουν καταχωρηθεί ως μπαρ που παίζουν μουσική Jazz. Ως εκ τούτου, ο χρήστης θα ζητήσει την παροχή της υπηρεσίας `JazzBarFinder`, η οποία παρέχεται από τον εν λόγω πάροχο υπηρεσιών. Θεωρούμε επιπλέον ότι η υπηρεσία `JazzBarFinder` απευθύνεται σε ενήλικες.

Η σειρά με την οποία ο χρήστης προσπελαύνει τις υπηρεσίες είναι η παρακάτω:

1. `Welcome`
2. `ServiceSelector`
3. `JazzBarFinder`
4. `Payment`

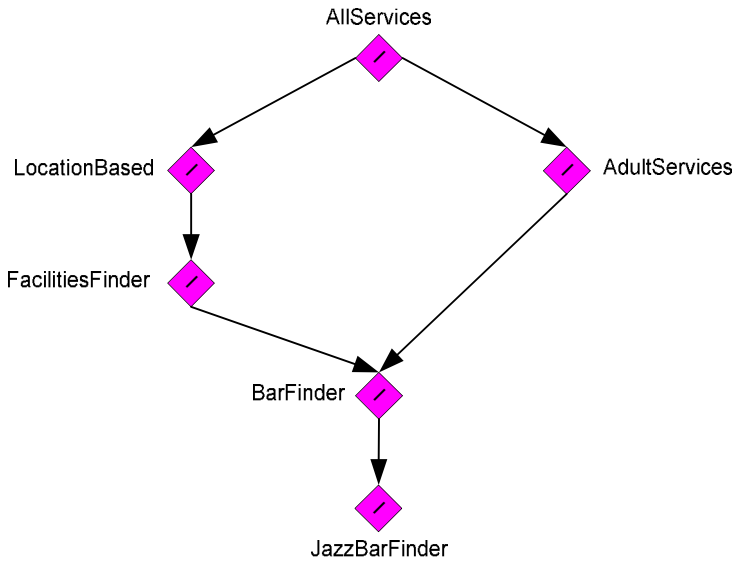
Η εκτέλεση των υπηρεσιών `Welcome` και `ServiceSelector` μπορεί να θεωρηθεί τετριμμένη· πράγματι, ο χρήστης δεν υποβάλλει προσωπικά δεδομένα για την παροχή των υπηρεσιών αυτών. Κατά την εκτέλεση της `Welcome`, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας αναγνωρίζει την ύπαρξη του Διαχειριστή Ιδιωτικότητας Χρήστη και

αρχικοποιεί τις παραμέτρους `SessionID` και `TransactionID`. Η υπηρεσία `ServiceSelector` είναι μία απλή υπηρεσία περιήγησης που επιτρέπει στο χρήστη να διαλέξει την υπηρεσία που επιθυμεί, δηλαδή εν προκειμένω την `JazzBarFinder`.

Ως υπηρεσία, η `JazzBarFinder` είναι ενταγμένη στον υπογράφο των υπηρεσιών της Οντολογίας Ιδιωτικότητας. Όπως φαίνεται στο Σχήμα 24, συνδέεται με το μέλος – ρίζα του υπογράφου μέσω των παρακάτω μονοπατιών κληρονομικότητας:

- `AllServices` → `LocationBased` → `FacilitiesFinder` → `BarFinder` → `JazzBarFinder`
- `AllServices` → `AdultServices` → `BarFinder` → `JazzBarFinder`

Κληρονομεί δηλαδή χαρακτηριστικά και κανόνες τόσο από τις υπηρεσίες βασισμένες στη θέση του χρήστη όσο και από τις υπηρεσίες που απευθύνονται σε ενήλικες.



Σχήμα 24: Οντολογία Ιδιωτικότητας – Υπηρεσία `JazzBarFinder`

Η υπηρεσία χρειάζεται δύο τύπους πληροφορίας προκειμένου να παρασχεθεί. Ως υπηρεσία που βασίζεται στη θέση του χρήστη, χρειάζεται ως είσοδο κάποια πληροφορία θέσης· από την άλλη, ως υπηρεσία που απευθύνεται σε ενήλικες, έχει ανάγκη από κάποια απόδειξη ότι ο χρήστης είναι ενήλικας. Αναφορικά με την πληροφορία θέσης, θεωρούμε ότι το τερματικό του χρήστη είναι εξοπλισμένο με κάποιο δορυφορικό σύστημα εντοπισμού θέσης, όπως είναι το καθιερωμένο Παγκόσμιο Σύστημα Εντοπισμού Θέσης (Global Positioning System – GPS) [131], ή το νεότερο Ευρωπαϊκό

Galileo [132][133]. Επιπλέον, για την πιστοποίηση της ηλικίας του χρήστη, θεωρούμε μία δομή δεδομένων, το Ψηφιακό Δελτίο Ταυτότητας, το οποίο αποτελεί το ψηφιακό ανάλογο του Δελτίου Ταυτότητας και περιέχει τις ίδιες πληροφορίες σε ψηφιακή μορφή. Θεωρούμε ότι το Ψηφιακό Δελτίο Ταυτότητας εκδίδεται από κάποια αρμόδια Δημόσια Αρχή και ότι η ακεραιότητά του διασφαλίζεται με κρυπτογραφικά μέσα. Ως εκ τούτου, ο χρήστης μεταδίδει στον Πληρεξούσιο Κόμβο Ιδιωτικότητας αυτούς τους τύπους πληροφορίας, μέσα σε Κέλυφος Ιδιωτικότητας, όπως φαίνεται στο Σχήμα 25.

```
<PRIVACY_LOCK>
        <LOCK>
                <DATA>
                        <DATA_TYPE>GeographicCoordinates<DATA_TYPE>
                        <DATA_VALUE>52.31.15, 13.24.34<DATA_VALUE>
                </DATA>
                <META>
                        <SERVICE>
                                <TYPE>LocationBased</TYPE>
                                <SERVICE_DESCENDANTS>YES</SERVICE_DESCENDANTS>
                        </SERVICE>
                        <PREF_RULE>
                                <DISCLOSURE>MIN</DISCLOSURE>
                                <INFORMATION>YES</INFORMATION>
                        </PREF_RULE>
                </META>
        </LOCK>
        <LOCK>
                <DATA>
                        <DATA_TYPE>DigitalIdentityCard<DATA_TYPE>
                        <OBJECT>@DIGITAL_IDENTITY_CARD</OBJECT>
                </DATA>
                <META>
                        <SERVICE>
                                <TYPE>AllServices</TYPE>
                                <SERVICE_DESCENDANTS>YES</SERVICE_DESCENDANTS>
                        </SERVICE>
                        <PREF_RULE>
                                <DISCLOSURE>NO</DISCLOSURE>
                        </PREF_RULE>
                </META>
        </LOCK>
</PRIVACY_LOCK>
```

Σχήμα 25: Κέλυφος Ιδιωτικότητας

Σύμφωνα με το Σχήμα 25, ο χρήστης αποστέλλει τις γεωγραφικές συντεταγμένες που χαρακτηρίζουν τη θέση του (τύπος `GeographicCoordinates`) με τις προτιμήσεις ιδιωτικότητας αφενός να παρέχεται πάντοτε και κατά περίπτωση η ελάχιστη δυνατή πληροφορία και αφετέρου ο χρήστης να ενημερώνεται για την οποιαδήποτε παροχή πληροφορίας που πηγάζει από την πληροφορία της θέσης του. Επιπλέον, οι προτιμήσεις αυτές ισχύουν μόνο για τις υπηρεσίες που βασίζονται στη θέση του χρήστη (τύπος `LocationBased` καθώς και οι απόγονοι αυτού στον υπογράφο των υπηρεσιών της Οντολογίας Ιδιωτικότητας).

```
<WORKFLOW SessionID="20931316" TransactionID="20881622">
   <SEQUENCE>
      <RELAY to="ServiceProvider" channel="INTERFACE_CHANNEL"/>
      <FLOW>
         <RECEIVE from="ServiceProvider"
             message-type="DATA_READ_REQUEST">
            <SWITCH>
               <CASE data-type="CityQuarter">
                  <INVOKE embedded_component="LocationHandler"
                    source_data_type="GeographicCoordinates"
                    target_data_type="CityQuarter"/>
                   <INFORMATION to=”DataSubject”/>
                  <DISCLOSE/>
               </CASE>
               <CASE data-type="City">
                  <INVOKE embedded_component="LocationHandler"
                    source_data_type="GeographicCoordinates"
                    target_data_type="City"/>
                   <INFORMATION to=”DataSubject”/>
                  <DISCLOSE/>
               </CASE>
               <CASE data-type="Country">
                  <INVOKE embedded_component="LocationHandler"
                    source_data_type="GeographicCoordinates"
                    target_data_type="Country"/>
                   <INFORMATION to=”DataSubject”/>
                  <DISCLOSE/>
               </CASE>
               <CASE data-type="IsAdult">
                  <INVOKE embedded_component="DICHandler"
                    source_data_type="DigitalIdentityCard"
                    target_data_type="DateOfBirth"/>
                 <INVOKE embedded_component="AgeHandler"
                    source_data_type="DateOfBirth"
                    target_data_type="IsAdult"/>
                  <DISCLOSE/>
               </CASE>
               <OTHERWISE>
                  <REJECT/>
               </OTHERWISE>
            </SWITCH>
         </RECEIVE>
         <INTERRUPT>
            <RECEIVE from="SERVICE_PROVIDER"
               message-type="SERVICE_PROVISION"/>
         </INTERRUPT>
      </FLOW>
      <RELAY to="DataSubject" channel="INTERFACE_CHANNEL"/>
   </SEQUENCE>
</WORKFLOW>
```

Σχήμα 26: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `JazzBarFinder`

Όταν δέχεται τη σχετική αίτηση, ο Διαχειριστής Επικοινωνίας του Πληρεξούσιου Κόμβου Ιδιωτικότητας, καλεί το Διαχειριστή Συνόδων ο οποίος είναι ταγμένος στην εξυπηρέτηση της εν λόγω Συνόδου Ιδιωτικότητας, ήδη από τη γέννησή της, δηλαδή από την κλήση της υπηρεσίας τύπου `Welcome`. Ο Διαχειριστής Συνόδων υποβάλλει σχετικό ερώτημα στο Αποθετήριο Κανονισμών και λαμβάνει αφενός το υπόδειγμα το οποίο

ακολουθεί η υπηρεσία `JazzBarFinder` και αφετέρου τους κανόνες που διέπουν την παροχή της. Ο Διαχειριστής Συνόδων διαβιβάζει ακολούθως τις πληροφορίες αυτές μαζί με τις προτιμήσεις ιδιωτικότητας του χρήστη στη Μηχανή Πολιτικών, η οποία του επιστρέφει την πλήρη προδιαγραφή της ροής εργασιών που πρέπει να εκτελεστούν. Η σχετική ροή εργασιών παρουσιάζεται στο Σχήμα 26, υπό μορφή εγγράφου της Γλώσσας Περιγραφής Ροής Εργασιών Ιδιωτικότητας.

Η ροή εργασιών που περιγράφει το Σχήμα 26 ορίζει τα παρακάτω:

1. Πρέπει να διαβιβαστεί το μήνυμα – αίτημα παροχής της υπηρεσίας στον πάροχο της υπηρεσίας.
2. Στη συνέχεια, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας μπαίνει σε κατάσταση αναμονής μηνυμάτων από τον πάροχο, μέσω του Καναλιού Προσωπικών Δεδομένων. Διακρίνουμε τις εξής περιπτώσεις:
    a. Εάν ληφθεί μήνυμα τύπου ανάγνωσης (`DATA_READ_REQUEST`) και ζητηθεί το προσωπικό δεδομένο τύπου `CityQuarter`, `City`, ή `Country`, τότε ο Διαχειριστής Συνόδων θα καλέσει κατ' αρχήν την Ενσωματωμένη Λειτουργική Μονάδα και θα πραγματοποιήσει το μετασχηματισμό από τις γεωγραφικές συντεταγμένες· ακολούθως θα παραχωρήσει την πληροφορία στον πάροχο, αφού πρώτα ενημερώσει σχετικά το υποκείμενο των δεδομένων.
    b. Εάν ληφθεί μήνυμα τύπου ανάγνωσης (`DATA_READ_REQUEST`) και ζητηθεί το προσωπικό δεδομένο τύπου `IsAdult`, τότε θα κληθούν με τη σειρά δύο Ενσωματωμένες Λειτουργικές Μονάδες: αρχικά η `DICHandler`, οπότε και θα εξαχθεί από το Ψηφιακό Δελτίο Ταυτότητας (τύπος `DigitalIdentityCard`) η ημερομηνία γέννησης του υποκειμένου των δεδομένων (τύπος `DateofBirth`) και στη συνέχεια η `AgeHandler`, οπότε θα μετασχηματιστεί η ημερομηνία γέννησης στη δυαδική μεταβλητή η οποία εκφράζει εάν το υποκείμενο του δεδομένου είναι ενήλικας ή όχι (τύπος `IsAdult`).
    c. Εάν ζητηθεί οποιοσδήποτε άλλος τύπος προσωπικού δεδομένου, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας θα αρνηθεί την παραχώρησή του.

d. Εάν το μήνυμα – αίτηση του παρόχου είναι άλλου τύπου (π.χ., `DATA_WRITE_REQUEST`), ο Πληρεξούσιος Κόμβος Ιδιωτικότητας θα αρνηθεί την πρόσβαση.

3. Ο Πληρεξούσιος Κόμβος Ιδιωτικότητας και η ροή εργασιών θα εξέλθει από την κατάσταση αναμονής μηνύματος όταν λάβει το μήνυμα παροχής της υπηρεσίας από τον πάροχο (`SERVICE_PROVISION`).

4. Το μήνυμα παροχής της υπηρεσίας θα διαβιβαστεί στο χρήστη, μέσω του Καναλιού Διεπαφής.

Στη συνέχεια, ο χρήστης καλείται να καταβάλει το αντίτιμο για την παροχή της υπηρεσίας. Αυτό λαμβάνει χώρα μέσω της υπηρεσίας `Payment`. Το Σχήμα 27 παρουσιάζει τη ροή εργασιών που αποτελεί την έξοδο της Μηχανής Πολιτικών για την εν λόγω υπηρεσία.

```
<WORKFLOW SessionID="20931316" TransactionID="20881754">
   <SEQUENCE>
      <RELAY to="SERVICE_PROVIDER" channel="INTERFACE_CHANNEL"/>
      <FLOW>
         <RECEIVE from="ServiceProvider"
              message-type="EMBEDDED_SERVICE_EXECUTION_REQUEST">
            <SWITCH>
               <CASE embedded-service="PaymentEmbeddedService">
                  <EXECUTE/>
               </CASE>
               <OTHERWISE>
                  <REJECT/>
               </OTHERWISE>
            </SWITCH>
         </RECEIVE>
         <INTERRUPT>
            <RECEIVE from="SERVICE_PROVIDER"
                message-type="SERVICE_PROVISION"/>
         </INTERRUPT>
      </FLOW>
      <RELAY to="DataSubject" channel="INTERFACE_CHANNEL"/>
   </SEQUENCE>
</WORKFLOW>
```

Σχήμα 27: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `Payment`

Όπως φαίνεται στο Σχήμα 27, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας δε θα παραχωρήσει απολύτως κανένα δεδομένο στον πάροχο της υπηρεσίας στο πλαίσιο της παροχής της υπηρεσίας `Payment`. Εκείνο το οποίο θα επιτρέψει είναι η κλήση της Ενσωματωμένης Υπηρεσίας `PaymentEmbeddedService`, μέσω της οποίας θα πραγματοποιηθεί η χρέωση του χρήστη από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας, χωρίς να δοθούν δεδομένα στον πάροχο της υπηρεσίας. Υπενθυμίζεται ότι η

Ενσωματωμένης Υπηρεσίας `PaymentEmbeddedService` χρησιμοποιεί τη μέθοδο που περιγράφεται στο [130] για την πραγματοποίηση της χρέωσης. Σημειώνεται ότι το μήνυμα `SERVICE_PROVISION` της εν λόγω υπηρεσίας θα είναι εκείνο που θα γνωστοποιήσει στο χρήστη τις επιλογές που έχει για Jazz μπαρ στη γειτονιά της διαμονής του.

Τέλος, θα πρέπει να σημειωθεί ότι στο συγκεκριμένο παράδειγμα δεν πραγματοποιείται καμία απολύτως αποθήκευση προσωπικών δεδομένων στο Αποθετήριο Προσωπικών του Πληρεξούσιου Κόμβου Ιδιωτικότητας.

8.2 Παράδειγμα Χρήσης Ημιενεργών Προσωπικών Δεδομένων

Ως παράδειγμα χρήσης ημιενεργών δεδομένων, θεωρούμε την υπηρεσία αυτόματης αναγνώρισης οχημάτων με χρήση συσκευών ραδιοσυχνότητας για προσδιορισμό ταυτότητας (Radio Frequency Identification – RFID) [7] και της συνακόλουθης διέλευσης από σταθμό διοδίων. Η μέθοδος διαχείρισης διελεύσεων σε σταθμούς διοδίων με χρήση RFIDs εφαρμόζεται σε πολλές περιπτώσεις, όπως για παράδειγμα στο σύστημα E-ZPASS των διοδίων της Νέας Υόρκης [134]. Θεωρούμε ότι ο χρήστης διαθέτει στο όχημά του μία ετικέτα RFID (RFID tag), ενώ οι σταθμοί διοδίων είναι εξοπλισμένοι με αναγνώστες RFID (RFID readers).

Εκείνο το οποίο διαφοροποιεί ουσιαστικά το συγκεκριμένο παράδειγμα από το προηγούμενο είναι ότι ο χρήστης δεν έχει ενεργό συμμετοχή στη μετάδοση των δεδομένων. Παρόλο που είναι η συσκευή RFID tag που ενεργοποιεί την παροχή της υπηρεσίας, η συσκευή RFID reader αποτελεί μέρος του εξοπλισμού του παρόχου της υπηρεσίας διέλευσης διοδίων, οπότε είναι ο πάροχος η οντότητα που ενεργοποιεί επί της ουσίας την παροχή της υπηρεσίας. Επιπλέον, στο παράδειγμα αυτό έχουμε διατήρηση προσωπικών δεδομένων στο Αποθετήριο Προσωπικών του Πληρεξούσιου Κόμβου Ιδιωτικότητας, καθώς και τροποποίησή τους από τον πάροχο των υπηρεσιών.

Κατ' αρχήν και μόλις η συσκευή RFID reader αναγνωρίσει κάποιο RFID tag, ο πάροχος της υπηρεσίας υποβάλλει στον Πληρεξούσιο Κόμβο Ιδιωτικότητας αίτημα ενεργοποίησης της υπηρεσίας `RFIDElectronicTollCollection`. Η ροή εργασιών που παράγεται στη Μηχανή Πολιτικών του Πληρεξούσιου Κόμβου Ιδιωτικότητας παρουσιάζεται στο Σχήμα 28.

```
<WORKFLOW SessionID="30431316" TransactionID="53481754">
   <SEQUENCE>
      <RECEIVE from="ServiceProvider"
             message-type="DATA_READ_REQUEST">
         <SWITCH>
            <CASE data-type="RemainingCredits">
               <DISCLOSE/>
            </CASE>
            <OTHERWISE>
               <REJECT/>
            </OTHERWISE>
         </SWITCH>
      </RECEIVE>
      <RECEIVE from="ServiceProvider"
             message-type="DATA_WRITE_REQUEST">
         <SWITCH>
            <CASE data-type="RemainingCredits">
               <INFORMATION to=”DataSubject”/>
               <WRITE/>
            </CASE>
            <OTHERWISE>
               <REJECT/>
            </OTHERWISE>
         </SWITCH>
      </RECEIVE>
      <REPLY to="ServiceProvider"/>
   </SEQUENCE>
</WORKFLOW>
```

Σχήμα 28: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `RFIDElectronicTollCollection`

Όπως φαίνεται στο Σχήμα 28, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας θα επιτρέψει στον πάροχο της υπηρεσίας όχι μόνο την ανάγνωση αλλά και την τροποποίηση των δεδομένων του τύπου `RemainingCredits`. Αντίθετα, ενώ θα επέτρεπε την ανάγνωση θα απαγόρευε την τροποποίηση των δεδομένων αυτών από το υποκείμενο των δεδομένων. Επιπλέον, θεωρώντας ότι το υποκείμενο των δεδομένων έχει εκφράσει ως προτίμηση ιδιωτικότητας την επιθυμία του για ενημέρωση σε κάθε τροποποίηση των δεδομένων τύπου `RemainingCredits`, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας θα προβεί στην ενημέρωση αυτή όπως φαίνεται από την προδιαγραφή `<INFORMATION to=”DataSubject”/>` της ροής εργασιών.

8.3 Παράδειγμα Χρήσης Παθητικών Προσωπικών Δεδομένων

Το χαρακτηριστικότερο ίσως παράδειγμα προσωπικών δεδομένων που εντάσσονται στην κατηγορία των παθητικών προσωπικών δεδομένων είναι τα δεδομένα τα οποία προκύπτουν από τη λήψη βίντεο για λόγους ασφάλειας κτιρίων και κρίσιμων υποδομών. Στο πλαίσιο της εκπόνησης της Διατριβής, υλοποιήθηκε ένα σύστημα που

υποστηρίζει τέτοιου είδους συστήματα παρακολούθησης με τρόπο που σέβεται την ιδιωτικότητα των υποκειμένων των δεδομένων.

Συγκεκριμένα, θεωρήθηκαν δύο υπηρεσίες:

- `ScrambledSurveillanceVideoCapture`: Αναφέρεται στην παροχή στον Υπεύθυνο της Επεξεργασίας βίντεο που έχει υποστεί επεξεργασία υπό την έννοια της απόκρυψης της πληροφορίας που αναφέρεται στα πρόσωπα των ανθρώπων που περιλαμβάνονται στην εικόνα με χρήση ειδικής βιβλιοθήκης της εταιρείας Intel.
- `ClearSurveillanceVideoCapture`: Αναφέρεται στη λήψη και συνακόλουθη παροχή καθαρού βίντεο στον Υπεύθυνο της Επεξεργασίας, δηλαδή του πρωτογενούς υλικού που δεν έχει υποστεί οποιαδήποτε επεξεργασία.

Η ροή εργασιών ιδιωτικότητας των δύο αυτών υπηρεσιών παρουσιάζεται στο Σχήμα 29 και στο Σχήμα 30, αντίστοιχα.

```
<WORKFLOW SessionID="97693769" TransactionID="78954810">
   <SEQUENCE>
      <FLOW>
         <RECEIVE from="ServiceProvider"
                message-type="DATA_READ_REQUEST">
            <SWITCH>
               <CASE data-type="ScrambledSurveillanceVideo">
                  <WRITE data-type="ClearSurveillanceVideo"/>
                  <INVOKE embedded_component="ImageScrambler"
                           source_data_type="ClearSurveillanceVideo"
                           target_data_type="ScrambledSurveillanceVideo"/>
                  <DISCLOSE/>
               </CASE>
               <OTHERWISE>
                  <REJECT/>
               </OTHERWISE>
            </SWITCH>
         </RECEIVE>
         <RECEIVE from="ServiceProvider"
                message-type="DATA_WRITE_REQUEST">
            <SWITCH>
               <CASE data-type="ClearSurveillanceVideo">
                  <WRITE/>
               </CASE>
               <OTHERWISE>
                  <REJECT/>
               </OTHERWISE>
            </SWITCH>
         </RECEIVE>
      </FLOW>
      <REPLY to="ServiceProvider"/>
   </SEQUENCE>
</WORKFLOW>
```

Σχήμα 29: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `ScrambledSurveillanceVideoCapture`

```
<WORKFLOW SessionID="30431419" TransactionID="90781754">
   <SEQUENCE>
      <FLOW>
         <RECEIVE from="ServiceProvider"
                 message-type="DATA_READ_REQUEST">
            <SWITCH>
               <CASE data-type="ClearSurveillanceVideo">
                  <INFORMATION to=”PrivacyAuthority”/>
                  <DISCLOSE/>
                  <WRITE/>
               </CASE>
               <OTHERWISE>
                  <REJECT/>
               </OTHERWISE>
            </SWITCH>
         </RECEIVE>
      </FLOW>
      <REPLY to="ServiceProvider"/>
   </SEQUENCE>
</WORKFLOW>
```

Σχήμα 30: Ροή Εργασιών Ιδιωτικότητας για Υπηρεσία `ClearSurveillanceVideoCapture`

Όπως φαίνεται στα σχήματα, μεταξύ των δύο ροών εργασίας υπάρχουν δύο βασικές διαφορές:

- Στην περίπτωση της υπηρεσίας `ScrambledSurveillanceVideoCapture`, πριν το βίντεο δοθεί στον Υπεύθυνο της Επεξεργασίας, καλείται η Ενσωματωμένη Λειτουργική Μονάδα `ImageScrambler`, η οποία πραγματοποιεί την απόκρυψη της ευαίσθητης πληροφορίας, κάτι το οποίο δε συμβαίνει στην περίπτωση της υπηρεσίας `ClearSurveillanceVideoCapture`.
- Στην περίπτωση της υπηρεσίας `ClearSurveillanceVideoCapture`, πριν το βίντεο δοθεί στον Υπεύθυνο της Επεξεργασίας, το σύστημα προβαίνει στην ενημέρωση της Αρχής Ιδιωτικότητας, κάτι το οποίο δε συμβαίνει στην περίπτωση της υπηρεσίας `ScrambledSurveillanceVideoCapture`. Ο λόγος της ενημέρωσης είναι ότι για κάποιο λόγο, ο Υπεύθυνο της Επεξεργασίας ζήτησε την παροχή καθαρού βίντεο, οπότε πρόκειται για περίπτωση ενδεχόμενης παραβίασης της ιδιωτικότητας των ανθρώπων που περιλαμβάνονται στην εικόνα.

Κάτι το οποίο αξίζει επιπλέον να αναφερθεί είναι ότι η ενέργεια αποθήκευσης του βίντεο στην περίπτωση της υπηρεσίας `ScrambledSurveillanceVideoCapture` βρίσκεται σε συμφωνία με τη Νομοθεσία, καθώς η “Οδηγία για τα κλειστά κυκλώματα τηλεόρασης” [135] που εξέδωσε το 2000 η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, επιτρέπει την αποθήκευση του βίντεο για χρονικό διάστημα ίσο με 15

ημέρες. Ως εκ τούτου, αποδίδονται στον Υπεύθυνο της Επεξεργασίας τα αντίστοιχα δικαιώματα εγγραφής.

Από την άλλη πλευρά, στην περίπτωση της υπηρεσίας `ClearSurveillanceVideoCapture`, η εγγραφή του βίντεο επιβάλλεται από το σύστημα, προκειμένου να είναι σε θέση η Αρχή Ιδιωτικότητας να πραγματοποιήσει έλεγχο της σκοπιμότητας πίσω από το αίτημα λήψης από τον Υπεύθυνο της Επεξεργασίας του καθαρού βίντεο.

9 Αξιολόγηση της Προτεινόμενης Λύσης

Το Κεφάλαιο αυτό παρουσιάζει την αξιολόγηση της προτεινόμενης λύσης. Η αξιολόγηση πραγματοποιείται σε δύο βάσεις: τις Νομικές και Κανονιστικές απαιτήσεις όπως συνοψίστηκαν στην Ενότητα 4.1 και τα διεθνώς αναγνωρισμένα κριτήρια που έχουν οριστεί από το Ανεξάρτητο Κέντρο για την Προστασία της Ιδιωτικότητας και αποτελούν τη βάση για την προδιαγραφή της "Ευρωπαϊκής Σφραγίδας Ιδιωτικότητας".

9.1 Αξιολόγηση σε Σχέση με τις Νομικές και Κανονιστικές Απαιτήσεις

Με βάση το Κεφάλαιο 2, στην Ενότητα 4.1 κωδικοποιήθηκαν οι απαιτήσεις που απορρέουν από το Νομικό και Κανονιστικό Πλαίσιο αναφορικά με την ορθή χρήση των προσωπικών δεδομένων σε συγκεκριμένες αρχές. Η Ενότητα αυτή αναφέρεται στον τρόπο με τον οποίο η προτεινόμενη λύση ανταποκρίνεται αποτελεσματικά στις απαιτήσεις αυτές.

9.1.1 Νομιμότητα της Επεξεργασίας των Δεδομένων

Η προτεινόμενη λύση λαμβάνει υπόψη σε κάθε απόφαση που αφορά επεξεργασία προσωπικών δεδομένων τους κανόνες που πηγάζουν από τη Νομοθεσία καθώς αυτοί βρίσκονται ενσωματωμένοι στην Οντολογία Ιδιωτικότητας. Επιπλέον, προσδιορίζει το τεχνικό πλαίσιο για την εφαρμογή των κανόνων αυτών. Πράγματι, η συνέπεια ως προς τη Νομοθεσία αποτελεί βασικό κατευθυντήριο άξονα για τον ορισμό της προτεινόμενης λύσης.

9.1.2 Σκοπός της Επεξεργασίας των Δεδομένων

Η προτεινόμενη λύση ορίζει ένα σημασιολογικό πλαίσιο, τόσο για τους τύπους προσωπικών δεδομένων, όσο και για τους τύπους υπηρεσιών και ρόλων των εμπλεκομένων οντοτήτων. Το σημασιολογικό πλαίσιο υλοποιείται από την Οντολογία Ιδιωτικότητας. Οι τύποι των υπηρεσιών περιγράφονται από το σημασιολογικό μοντέλο με μεγάλη λεπτομέρεια και, ως εκ τούτου, αποτελούν ουσιαστικά τους διαφορετικούς σκοπούς πίσω από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Το

σύστημα που περιγράφει η προτεινόμενη λύση δεν επιτρέπει πρόσβαση στα προσωπικά δεδομένα για σκοπούς άλλους εκτός από εκείνους που περιγράφει με αυστηρά καθορισμένο τρόπο εν είδει κανόνων ελέγχου πρόσβασης. Επιπλέον, τα προσωπικά δεδομένα που παραχωρούνται σε κάποιο πάροχο υπηρεσιών είναι σε κάθε περίπτωση τα ελάχιστα δυνατά για την παροχή της ζητούμενης υπηρεσίας. Μάλιστα, η παρουσία των Ενσωματωμένων Λειτουργικών Μονάδων του Πληρεξούσιου Κόμβου Ιδιωτικότητας αποτρέπει την παραχώρηση δεδομένων που ταυτοποιούν το υποκείμενο των δεδομένων. Ως εκ τούτου, τα δεδομένα που τελικά παραχωρούνται είναι στη γενική περίπτωση άχρηστα για οποιοδήποτε άλλο σκοπό εκτός από εκείνον για τον οποίο παραχωρούνται ή και για σκοπούς που χαρακτηρίζονται ως ακίνδυνοι σε σχέση με την παραβίαση της ιδιωτικότητας του υποκειμένου των δεδομένων.

9.1.3 Αναγκαιότητα, Καταλληλότητα και Αναλογικότητα των Δεδομένων

Τα προσωπικά δεδομένα τα οποία υφίστανται συλλογή ή / και επεξεργασία είναι πάντοτε τα αναγκαία και κατάλληλα, συναρτήσει του σκοπού για τον οποίο τα παραχωρεί το υποκείμενο των δεδομένων. Αυτό προκύπτει από την Οντολογία Ιδιωτικότητας, το Σημασιολογικό Μοντέλο Πληροφοριών που αυτή ορίζει και τους κανόνες που έχουν προσδιοριστεί με βάση το μοντέλο αυτό. Η αναλογικότητα προκύπτει από τους εν λόγω κανόνες πρόσβασης, οι οποίοι επιτρέπουν μόνο τα απαραίτητα δεδομένα για την παροχή κάποιας υπηρεσίας να παρασχεθούν στον Υπεύθυνο της Επεξεργασίας.

9.1.4 Ποιότητα των Δεδομένων

Οποιαδήποτε ενέργεια πρόσβασης σε προσωπικά δεδομένα ελέγχεται από το πλαίσιο ελέγχου πρόσβασης που ορίζεται στην προτεινόμενη λύση και που έχει ως βάση του τους κανόνες που περιγράφονται στην Οντολογία Ιδιωτικότητας, τις αντίστοιχες προτιμήσεις του υποκειμένου των δεδομένων και το μηχανισμό εφαρμογής αυτών μέσω του πληρεξούσιου Κόμβου Ιδιωτικότητας. Συνεπώς, η κακόβουλη τροποποίηση αποτρέπεται. Επιπλέον, το υποκείμενο των δεδομένων διαθέτει τη δυνατότητα άμεσης πρόσβασης στα δεδομένα του, ούτως ώστε να διασφαλίζει τη συνέπειά τους, της ακρίβειας και της ενημερωμένης κατάστασής τους. Επιπλέον, το υποκείμενο των δεδομένων συμμετέχει στον κατά περίπτωση προσδιορισμό της αναγκαιότητας,

καταλληλότητας και αναλογικότητας των δεδομένων, μέσω του κατάλληλου μηχανισμού που ορίζει η προτεινόμενη λύση για τη φορμαλιστική περιγραφή των προτιμήσεων του υποκειμένου των δεδομένων αναφορικά με την ιδιωτικότητα. Επιπροσθέτως, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας ενσωματώνει τους μηχανισμούς για την αυτόματη διαγραφή των δεδομένων που βρίσκονται αποθηκευμένα στο Αποθετήριο Προσωπικών Δεδομένων μόλις παρέλθει ο χρόνος ζωής τους, όπως αυτός προσδιορίζεται τόσο από τη Νομοθεσία μέσω της Οντολογίας Ιδιωτικότητας, όσο και από τις προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων. Ασφαλώς, πολύ σημαντικό ρόλο για τη διασφάλιση της ποιότητας των δεδομένων παίζει το ζήτημα της ασφάλειάς τους, τόσο κατά το στάδιο της μετάδοσής τους, όσο και κατά το στάδιο που αυτά βρίσκονται αποθηκευμένα. Χωρίς το θέμα της ασφάλειας αυτής καθαυτής να αποτελεί αντικείμενο της Διατριβής, η προτεινόμενη λύση χαρακτηρίζεται από δύο βασικούς μηχανισμούς ασφάλειας: την κρυπτογραφημένη αποθήκευση και την κρυπτογραφημένη μετάδοση των δεδομένων, λαμβάνοντας υπόψη τα ασφαλή κανάλια επικοινωνίας μεταξύ των εμπλεκομένων οντοτήτων καθώς και το μηχανισμό του Κελύφους Ιδιωτικότητας.

9.1.5 Ταυτοποιήσιμα Δεδομένα

Η όλη φιλοσοφία της προτεινόμενης λύσης είναι να μην πραγματοποιείται παραχώρηση ταυτοποιήσιμων δεδομένων στους εκάστοτε Υπευθύνους της Επεξεργασίας. Για το σκοπό αυτό, τα σημασιολογικά χαρακτηρισμένα προσωπικά δεδομένα διέπονται από κανόνες που αποτρέπουν την εκχώρησή τους, κανόνες οι οποίοι εφαρμόζονται από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας. Επιπλέον και καθώς ορισμένες ενέργειες επεξεργασίας ταυτοποιήσιμων δεδομένων είναι απαραίτητες για την παροχή συγκεκριμένων υπηρεσιών, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας διαθέτει Ενσωματωμένες Λειτουργικές Μονάδες, οι οποίες πραγματοποιούν εσωτερικά τις ευαίσθητες πράξεις επεξεργασίας οι οποίες χρησιμοποιούν ταυτοποιήσιμα δεδομένα.

9.1.6 Πληροφόρηση των Υποκειμένων των Δεδομένων – Συγκατάθεση και Δικαιώματα Πρόσβασης των Υποκειμένων των Δεδομένων

Η προτεινόμενη λύση παρέχει τα μέσα για την ενημέρωση των υποκειμένων των δεδομένων αναφορικά με τις πράξεις παραχώρησης και επεξεργασίας των προσωπικών

τους δεδομένων. Αυτό επιτυγχάνεται κυρίως με τη χρήση του σχετικού μηχανισμού που παρέχεται. Η απαίτηση για ενημέρωση περιέχεται στην Οντολογία Ιδιωτικότητας αλλά μπορεί να οριστεί και από το υποκείμενο των δεδομένων. Στη συνέχεια, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας αναλαμβάνει την εκτέλεση των σχετικών απαιτήσεων, αποστέλλοντας σε πραγματικό χρόνο τις ζητούμενες ενημερώσεις. Παρόμοια είναι και η λογική αναφορικά με την παροχή ρητής συγκατάθεσης από το υποκείμενο των δεδομένων για τις περιπτώσεις παραχώρησης και επεξεργασίας τους. Ο Πληρεξούσιος Κόμβος Ιδιωτικότητας αναλαμβάνει την αποστολή προς το υποκείμενο των δεδομένων των σχετικών μηνυμάτων τα οποία ζητούν τη ρητή συγκατάθεσή του για κάποια πράξης παραχώρησης ή επεξεργασίας των δεδομένων. Η πράξη δεν εκτελείται μέχρι να παρασχεθεί η συγκατάθεση. Τέλος, η προδιαγραφή της προτεινόμενης λύσης παρέχει στα υποκείμενα των δεδομένων να έχουν απ' ευθείας πρόσβαση στα δεδομένα τους που βρίσκονται αποθηκευμένα στο Αποθετήριο Προσωπικών Δεδομένων του Πληρεξούσιου Κόμβου Ιδιωτικότητας, μέσω μίας κατάλληλης διεπαφής. Η πρόσβαση μπορεί να αφορά την ανάγνωση ή και την τροποποίηση / διαγραφή, εφόσον αυτό είναι επιτρεπτό. Οι κανόνες πρόσβασης των υποκειμένων των δεδομένων καθορίζονται λεπτομερώς από την Οντολογία Ιδιωτικότητας.

9.1.7 Δεδομένα Θέσης και Κίνησης – Ειδικές Κατηγορίες Δεδομένων

Στο πλαίσιο της προτεινόμενης λύσης, κάθε προσωπικό δεδομένο χαρακτηρίζεται από το σημασιολογικό ορισμό του, βάσει του Σημασιολογικού Μοντέλου Πληροφοριών της Οντολογίας Ιδιωτικότητας. Επιπλέον, ο σημασιολογικός τύπος του κάθε προσωπικού δεδομένου λαμβάνεται υπόψη σε κάθε ενέργεια συλλογής ή επεξεργασίας του. Κατά συνέπεια και βάσει των κανόνων που ορίζονται στην Οντολογία Ιδιωτικότητας, το κάθε δεδομένο ειδικής κατηγορίας, όπως είναι τα δεδομένα κίνησης και θέσης στο πλαίσιο κάποιας επικοινωνίας, τα δικαστικά και άλλα ευαίσθητα δεδομένα, υφίσταται συλλογή και επεξεργασία που βασίζεται σε κάθε περίπτωση στον ιδιαίτερο τύπο του.

9.1.8 Περιορισμός της Πρόσβασης

Ο έλεγχος της πρόσβασης στο πλαίσιο της προτεινόμενης λύσης πραγματοποιείται βάσει ενός μοντέλου κανόνων που απορρέουν από τη Νομοθεσία και

καλύπτουν όλους τους τύπους προσωπικών δεδομένων, υπηρεσιών και ρόλων των εμπλεκομένων οντοτήτων. Οι κανόνες εκτελούνται από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας ο οποίος λαμβάνει επιπροσθέτως υπόψη τις προτιμήσεις ιδιωτικότητας των υποκειμένων των δεδομένων. Κάθε πράξη πρόσβασης σε προσωπικά δεδομένα καταγράφεται από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας. Η πρόσβαση στα αρχεία καταγραφής είναι επίσης ελεγχόμενη, βάσει του ίδιου μοντέλου.

9.1.9 Ασφάλεια Δεδομένων και Εμπιστευτικότητα

Χωρίς το θέμα της ασφάλειας αυτής καθαυτής να αποτελεί το κύριο αντικείμενο της Διατριβής, η προτεινόμενη λύση χαρακτηρίζεται από δύο βασικούς μηχανισμούς ασφάλειας: την κρυπτογραφημένη αποθήκευση και την κρυπτογραφημένη μετάδοση των δεδομένων, λαμβάνοντας υπόψη τα ασφαλή κανάλια επικοινωνίας μεταξύ των εμπλεκομένων οντοτήτων καθώς και το μηχανισμό του Κελύφους Ιδιωτικότητας.

9.1.10 Αποθήκευση Δεδομένων

Όπως υπαγορεύεται από τους κανόνες πρόσβασης που περιέχονται στην Οντολογία Ιδιωτικότητας και απορρέουν από τη Νομοθεσία, όταν ο Πληρεξούσιος Κόμβος Ιδιωτικότητας παραχωρεί προσωπικά δεδομένα σε κάποιο Υπεύθυνο της Επεξεργασίας, δεν παραχωρεί δεδομένα που ταυτοποιούν το υποκείμενο των δεδομένων, καθιστώντας κατά αυτόν τον τρόπο τα δεδομένα ανώνυμα. Επιπλέον, σε κάθε δεδομένο που τελικά αποθηκεύεται στο Αποθετήριο Προσωπικών Δεδομένων του Πληρεξούσιου Κόμβου Ιδιωτικότητας ανατίθεται καθορισμένος χρόνος ζωής, ο οποίος προκύπτει από τους κανόνες της Οντολογίας Ιδιωτικότητας, καθώς και από τις αντίστοιχες προτιμήσεις του υποκειμένου των δεδομένων. Μετά το πέρας του εν λόγω χρόνου ζωής, το σύστημα προβαίνει σε αυτόματη διαγραφή των δεδομένων.

9.1.11 Ειδοποιήσεις και λοιπές Αρμοδιότητες / Εξουσιοδοτήσεις των Αρμοδίων Αρχών

Σύμφωνα με την προτεινόμενη λύση, η Αρχή Ιδιωτικότητας εφοδιάζεται με ένα εξειδικευμένο σύστημα, τον Κόμβο Υποδομής Ιδιωτικότητας. Ο Κόμβος Υποδομής Ιδιωτικότητας προσφέρει τις διεπαφές για την εποπτεία από την Αρχή Ιδιωτικότητας, συμπεριλαμβανομένων και των ειδοποιήσεων σε πραγματικό χρόνο για τα συμβάντα που λαμβάνουν χώρα. Αυτό επιτυγχάνεται μέσω της λειτουργικότητας του

Πληρεξούσιου Κόμβου Ιδιωτικότητας σε συνδυασμό με τους σχετικούς κανόνες που περιέχει η Οντολογία Ιδιωτικότητας. Επιπλέον, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας πραγματοποιεί λεπτομερή καταγραφή των συμβάντων που λαμβάνουν χώρα στο πλαίσιο της λειτουργίας του. Τα σχετικά αρχεία καταγραφής είναι προσβάσιμα από την Αρχή Ιδιωτικότητας και συνιστούν μέσο για την ειδοποίησή της.

9.1.12 Εποπτεία και Επιβολή Προστίμων

Η προτεινόμενη λύση φιλοδοξεί να καταστήσει εγγενές χαρακτηριστικό των συστημάτων την εποπτεία των ζητημάτων της ιδιωτικότητας από την αρμόδια Αρχή Ιδιωτικότητας. Στο πλαίσιο αυτό, η Αρχή Ιδιωτικότητας εφοδιάζεται με ένα εξειδικευμένο για το σκοπό αυτό σύστημα, τον Κόμβο Υποδομής Ιδιωτικότητας. Ο Κόμβος Υποδομής Ιδιωτικότητας προσφέρει τις διεπαφές για την εποπτεία από την Αρχή Ιδιωτικότητας. Επιπλέον, ο Πληρεξούσιος Κόμβος Ιδιωτικότητας πραγματοποιεί λεπτομερή καταγραφή των συμβάντων που λαμβάνουν χώρα στο πλαίσιο της λειτουργίας του. Τα σχετικά αρχεία καταγραφής είναι προσβάσιμα από την Αρχή Ιδιωτικότητας και προστατευμένα από ενδεχόμενες παραποιήσεις. Επιπροσθέτως, η προτεινόμενη λύση ενσωματώνει μηχανισμό για την ειδοποίηση σε πραγματικό χρόνο της Αρχής Ιδιωτικότητας εφόσον λάβει χώρα κάποιο ουσιαστικό συμβάν. Αυτό επιτυγχάνεται μέσω της λειτουργικότητας του Πληρεξούσιου Κόμβου Ιδιωτικότητας σε συνδυασμό με τους σχετικούς κανόνες που περιέχει η Οντολογία Ιδιωτικότητας. Αναφορικά με την επιβολή προστίμων, ασφαλώς δεν είναι δυνατό να αποτελεί αντικείμενο ενός τεχνολογικού συστήματος. Ωστόσο, η προτεινόμενη λύση παρέχει τα μέσα τόσο για την ανίχνευση των γεγονότων που χρίζουν επιβολή προστίμου, όσο και για την τεκμηρίωση των προστίμων.

9.1.13 Νόμιμη Παρακολούθηση και Συλλογή Δεδομένων

Η Αρχή Ιδιωτικότητας αποτελεί οντότητα η οποία συμμετέχει στη λειτουργία του συστήματος και διαθέτει κατά περίπτωση πρόσβαση στα προσωπικά δεδομένα τα οποία μεταδίδονται ή είναι αποθηκευμένα στο Αποθετήριο Προσωπικών Δεδομένων του Πληρεξούσιου Κόμβου Ιδιωτικότητας. Η Αρχή Ιδιωτικότητας αποτελεί έναν από τους ρόλους για τους οποίους ορίζονται στην Οντολογία Ιδιωτικότητας κανόνες πρόσβασης στα προσωπικά δεδομένα. Οι διάφορες πράξεις νόμιμης παρακολούθησης και συλλογής αποτελούν υπηρεσίες οι οποίες παρέχονται στην Αρχή Ιδιωτικότητας από τον Πληρεξούσιο Κόμβο Ιδιωτικότητας. Ως εκ τούτου, υπόκεινται σε κανόνες οι οποίοι

περιέχονται στην Οντολογία Ιδιωτικότητας και οι οποίοι απορρέουν από τη Νομοθεσία. Η πρόσβαση πραγματοποιείται μέσω του Κόμβου Υποδομής Ιδιωτικότητας, ο οποίος αποτελεί το μόνο σημείο εισόδου για πραγματοποίηση νόμιμης παρακολούθησης και συλλογής δεδομένων (LI). Η εφαρμογή των καταλλήλων μηχανισμών ελεγχόμενης πρόσβασης με χρήση ισχυρών μηχανισμών αυθεντικοποίησης και εξουσιοδότησης βασισμένων σε κρυπτογραφικά συστήματα μπορεί να διασφαλίσει την αποκλειστικότητα της Αρχής Ιδιωτικότητας σε ό,τι αφορά την παρακολούθηση και συλλογή των δεδομένων μέσω των σχετικών καναλιών. Τέλος, σημειώνεται ότι στο πλαίσιο της μελλοντικής εργασίας, πρόκειται να πραγματοποιηθεί η σχεδίαση και υλοποίηση των καταλλήλων συστημάτων λογισμικού και διεπαφών, ούτως ώστε η προτεινόμενη λύση να καταστεί συμμορφούμενη με τα διεθνή πρότυπα σχετικά με τη νόμιμη παρακολούθηση και συλλογή δεδομένων, και ιδίως με εκείνα του Ευρωπαϊκού Ινστιτούτου Τηλεπικοινωνιακών Προτύπων (European Telecommunications Standards Institute – ETSI) [136][137][138][139] [140][141][142].

9.2 Αξιολόγηση με Βάση τα Κριτήρια του Ανεξάρτητου Κέντρου για την Προστασία της Ιδιωτικότητας

Αναφορικά με την αξιολόγηση προϊόντων και υπηρεσιών πληροφορικής, υφίστανται διάφορα κριτήρια για την ανάλυση της ασφάλειας των δεδομένων, αλλά ελάχιστα λαμβάνουν υπόψη το ζήτημα της ιδιωτικότητας. Η κλάση της ιδιωτικότητας (privacy class) των "Κοινών Κριτηρίων για την Αξιολόγησης της Ασφάλειας των Τεχνολογιών Πληροφορικής" (Common Criteria for Information Technology Security Evaluation) [143][144][145] που έχουν αναπτυχθεί από το Διεθνή Οργανισμό Προτυποποίησης (International Organization for Standardization – ISO) [66] προσφέρει τη δυνατότητα αξιολόγησης αναφορικά με τις απαιτήσεις για ανωνυμία, ψευδωνυμία, κλπ. Ωστόσο, απαιτήσεις όπως η νομιμότητα και η αναλογικότητα, καθώς και η διαφάνεια για τα υποκείμενα των δεδομένων δεν είναι δυνατό να εκφραστούν μέσω των Κοινών Κριτηρίων.

Στο πλαίσιο της Διατριβής, ελήφθησαν υπόψη για την αξιολόγηση τόσο της προτεινόμενης λύσης όσο και των υπηρεσιών που παρέχονται μέσω αυτής, τα κριτήρια που αναφέρονται ως "Κατάλογος Απαιτήσεων για τη Σφραγίδα Ποιότητας των

Προϊόντων Πληροφορικής Αναφορικά με την Προστασία των Προσωπικών Δεδομένων" (Anforderungskatalog zum Datenschutz-Gütesiegel für IT-Produkte) [146]. Τα κριτήρια αυτά έχουν προδιαγραφεί από τον Οργανισμό "Ανεξάρτητο Κέντρο για την Προστασία της Ιδιωτικότητα" (Unabhängigen Landeszentrum für Datenschutz – ULD) [147] που αποτελεί την Αρχή Προστασίας Προσωπικών Δεδομένων του "κρατιδίου" (Länder) Schleswig-Holstein της Γερμανίας. Τα κριτήρια ιδιωτικότητας του ULD έχουν σκοπό να πιστοποιήσουν τη συμβατότητα και συμμόρφωση ενός προϊόντος ή υπηρεσίας πληροφορικής με τη Νομοθεσία περί προστασίας προσωπικών δεδομένων, μέσω μίας επίσημης διαδικασίας πιστοποίησης. Τα κριτήρια του ULD είναι αναγνωρισμένα σε διεθνές επίπεδο και μάλιστα αποτελούν τη βάση για τα κριτήρια της Ευρωπαϊκής Σφραγίδας Ιδιωτικότητας (European Privacy Seal) η οποία θα αποτελέσει το προϊόν του Προγράμματος EuroPriSe [148], το οποίο ξεκίνησε τον Ιούνιο του 2007 και αναμένεται να ολοκληρωθεί το Νοέμβριο του 2008. Η τρέχουσα – προκαταρκτική – έκδοση των κριτηρίων της Ευρωπαϊκής Σφραγίδας Ιδιωτικότητας ([149]) βασίζεται σε μεγάλο βαθμό στα κριτήρια ιδιωτικότητας του ULD και χρησιμοποιήθηκε επιπλέον στο πλαίσιο της Διατριβής.

Τα κριτήρια ιδιωτικότητας του ULD είναι οργανωμένα σε τέσσερις Ενότητες, οι οποίες καλύπτουν το σύνολο των Νομικών και Κανονιστικών απαιτήσεων, όπως περιγράφηκαν στην Ενότητα 4.1. Οι τέσσερις Ενότητες είναι:

- Θεμελιώδης Τεχνικός Σχεδιασμός Προϊόντων Πληροφορικής
- Νομιμότητα της Επεξεργασίας Δεδομένων
- Τεχνικά – Οργανωτικά Μέτρα: Συμπληρωματικά Μέτρα για την Προστασία του Υποκειμένου των Δεδομένων
- Δικαιώματα του Υποκειμένου των Δεδομένων

Οι Πίνακες 2, 3, 4 και 5 που ακολουθούν συνοψίζουν την αντιστοίχηση μεταξύ των απαιτήσεων των κριτηρίων του ULD και των λειτουργιών της προτεινόμενης λύσης.

Πίνακας 2: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 1 – "Θεμελιώδης Τεχνικός Σχεδιασμός Προϊόντων Πληροφορικής"

Ενότητα 1 – "Θεμελιώδης Τεχνικός Σχεδιασμός Προϊόντων Πληροφορικής"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
1.1	Οικονομία δεδομένων / αποφυγή δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Ανωνυμία / Ψευδωνυμία
1.2	Έγκαιρη, ανωνυμία ή ψευδωνυμία δεδομένων	▪ Διαχείριση αποθήκευσης δεδομένων ▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Ανωνυμία / Ψευδωνυμία
1.3	Διαφάνεια και περιγραφή	▪ Μηχανισμός ενημέρωσης του υποκειμένου των δεδομένων ▪ Μηχανισμός παροχής ρητής συγκατάθεσης ▪ Σημασιολογικός χαρακτηρισμός προσωπικών δεδομένων, υπηρεσιών και ρόλων των οντοτήτων ▪ Τεκμηρίωση συστήματος

Πίνακας 3: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 2 – "Νομιμότητα της Επεξεργασίας Δεδομένων"

Ενότητα 2 – "Νομιμότητα της Επεξεργασίας Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
2.1	Γενικές Απαιτήσεις περί Νομιμότητας	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες
2.2	Συγκατάθεση	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Μηχανισμός παροχής ρητής συγκατάθεσης
2.3	Νομιμότητα στα διαφορετικά στάδια της επεξεργασίας	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες
2.4	Αποθήκευση και περαιτέρω επεξεργασία	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Διαχείριση αποθήκευσης δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες

Ενότητα 2 – "Νομιμότητα της Επεξεργασίας Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
2.5	Παραχώρηση των δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες
2.6	Επεξεργασία δεδομένων μόνο για το σκοπό για τον οποίο συλλέχτηκαν νομίμως – επεξεργασία για άλλους σκοπούς	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες
2.7	Διαγραφή των δεδομένων έπειτα από τη διακοπή της απαίτησης	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Διαχείριση αποθήκευσης δεδομένων
2.8	Θεώρηση των χρονικών ορίων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Διαχείριση αποθήκευσης δεδομένων

Ενότητα 2 – "Νομιμότητα της Επεξεργασίας Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
2.9	Εποπτεία των Νόμων για τη χρήση συγκεκριμένων τεχνικών μέσων (π.χ., χρήση βίντεο)	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Ενσωματωμένες Λειτουργικές Μονάδες του Πληρεξούσιου Κόμβου Ιδιωτικότητας

Πίνακας 4: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 3 – "Τεχνικά – Οργανωτικά Μέτρα: Συμπληρωματικά Μέτρα για την Προστασία του Υποκειμένου των Δεδομένων"

Ενότητα 3 – "Τεχνικά – Οργανωτικά Μέτρα: Συμπληρωματικά Μέτρα για την Προστασία του Υποκειμένου των Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
3.1	Εξουσιοδοτημένη πρόσβαση σε / επεξεργασία προσωπικών δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Διαχείριση αποθήκευσης δεδομένων
3.2	Κρυπτογραφία	▪ Διαλειτουργικότητα Πληρεξούσιου Κόμβου Ιδιωτικότητας ↔ Διαχειριστή Ιδιωτικότητας Χρήστη ▪ Κέλυφος Ιδιωτικότητας ▪ Διαχείριση αποθήκευσης δεδομένων
3.3	Μηχανισμοί για την αύξηση της ευαισθησίας των χρηστών στο θέμα της ιδιωτικότητας	▪ Σημασιολογικός χαρακτηρισμός προσωπικών δεδομένων, υπηρεσιών και ρόλων των οντοτήτων ▪ Τεκμηρίωση συστήματος

Ενότητα 3 – "Τεχνικά – Οργανωτικά Μέτρα: Συμπληρωματικά Μέτρα για την Προστασία του Υποκειμένου των Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
3.4	Καταγραφή των διαδικασιών επεξεργασίας δεδομένων	▪ Καταγραφή συμβάντων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας
3.5	Μέτρα για τη διασφάλιση της ακεραιότητας των δεομένων	▪ Διαχείριση αποθήκευσης δεδομένων
3.6	Δυνατότητες για τη διασφάλιση της διαθεσιμότητας των δεδομένων	▪ Διαχείριση αποθήκευσης δεδομένων
3.7	Διευκόλυνση της Αρχής Ιδιωτικότητας αναφορικά με τη διεξαγωγή ελέγχων, σύμφωνα με το Άρθρο 20 της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ [22]	▪ Διαλειτουργικότητα Πληρεξούσιου Κόμβου Ιδιωτικότητας ↔ Κόμβου Υποδομής Ιδιωτικότητας ▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας)
3.8	Άλλη υποστήριξη στην Αρχή Ιδιωτικότητας	▪ Διαλειτουργικότητα Πληρεξούσιου Κόμβου Ιδιωτικότητας ↔ Κόμβου Υποδομής Ιδιωτικότητας ▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καταγραφή συμβάντων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας
3.9	Διευκόλυνση / υποστήριξη για ψευδώνυμα και ψευδωνυμία	▪ Διαχείριση αποθήκευσης δεδομένων ▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Ανωνυμία / Ψευδωνυμία

Πίνακας 5: Κριτήρια Ιδιωτικότητας του ULD – Ενότητα 4 – "Δικαιώματα του Υποκειμένου των Δεδομένων"

Ενότητα 4 – "Δικαιώματα του Υποκειμένου των Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
4.1	Ενημέρωση και ειδοποίηση	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Απ' ευθείας πρόσβαση υποκειμένου των δεδομένων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας ▪ Μηχανισμός ενημέρωσης του υποκειμένου των δεδομένων ▪ Σημασιολογικός χαρακτηρισμός προσωπικών δεδομένων, υπηρεσιών και ρόλων των οντοτήτων ▪ Διαλειτουργικότητα Πληρεξούσιου Κόμβου Ιδιωτικότητας ↔ Διαχειριστή Ιδιωτικότητας Χρήστη ▪ Καταγραφή συμβάντων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας

Ενότητα 4 – "Δικαιώματα του Υποκειμένου των Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
4.2	Ενημέρωση του υποκειμένου των δεδομένων, σύμφωνα με το Άρθρο 12 της Ευρωπαϊκής Οδηγίας 95/46/ΕΚ [22]	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Απ' ευθείας πρόσβαση υποκειμένου των δεδομένων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας ▪ Μηχανισμός ενημέρωσης του υποκειμένου των δεδομένων ▪ Σημασιολογικός χαρακτηρισμός προσωπικών δεδομένων, υπηρεσιών και ρόλων των οντοτήτων ▪ Διαλειτουργικότητα Πληρεξούσιου Κόμβου Ιδιωτικότητας ↔ Διαχειριστή Ιδιωτικότητας Χρήστη ▪ Καταγραφή συμβάντων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας
4.3	Διόρθωση προσωπικών δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Απ' ευθείας πρόσβαση υποκειμένου των δεδομένων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας

Ενότητα 4 – "Δικαιώματα του Υποκειμένου των Δεδομένων"		
	Απαίτηση	**Λειτουργία Προτεινόμενης Λύσης**
4.4	Πλήρης διαγραφή προσωπικών δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Απ' ευθείας πρόσβαση υποκειμένου των δεδομένων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας
4.5	Αποκλεισμός προσωπικών δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Απ' ευθείας πρόσβαση υποκειμένου των δεδομένων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας
4.6	Αντίρρηση στην επεξεργασία προσωπικών δεδομένων	▪ Μοντελοποίηση Νομοθεσίας (Οντολογία Ιδιωτικότητας) ▪ Καθορισμός προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων ▪ Μηχανισμός λήψης αποφάσεων για πρόσβαση και ενέργειες ▪ Απ' ευθείας πρόσβαση υποκειμένου των δεδομένων στον Πληρεξούσιο Κόμβο Ιδιωτικότητας ▪ Μηχανισμός παροχής ρητής συγκατάθεσης

10 Συμπεράσματα – Μελλοντική Εργασία

Ως βάση και κίνητρο για την πραγματοποίηση της παρούσας Διατριβής στάθηκε η παρακάτω διπλή παρατήρηση:

- Από τη στιγμή που κάποια πληροφορία διατεθεί σε κάποιον πάροχο υπηρεσίας, δεν υπάρχει κανένα τεχνικό μέσο που να μπορεί να διασφαλίσει ότι η περαιτέρω επεξεργασία και χρήση της θα είναι σύννομη και θεμιτή. Δηλαδή, τα προσωπικά δεδομένα καθίστανται αυτομάτως απροστάτευτα απέναντι σε ενδεχόμενη κατάχρηση από την πλευρά του παρόχου.
- Όποια Πολιτική Ιδιωτικότητας και να δηλώνει κάποιος πάροχος υπηρεσιών αναφορικά με τη χρήση των προσωπικών δεδομένων που βρίσκονται στην κατοχή του, η εφαρμογή της πολιτικής αυτής δεν μπορεί να διασφαλιστεί. Δηλαδή, οι χρήστες δε διαθέτουν καμία εγγύηση αναφορικά με την εφαρμογή ή μη από τον πάροχο της Πολιτικής Ιδιωτικότητας την οποία δηλώνει. Εξάλλου, υπάρχουν αναρίθμητα παραδείγματα όπου οι τελικές πρακτικές των παρόχων υπηρεσιών έρχονται σε πλήρη αντίθεση με τις δεδηλωμένες Πολιτικές Ιδιωτικότητας.

Ως εκ τούτου, αναζητήθηκε ο τρόπος αφενός να απομονωθούν τα δεδομένα από τον Υπεύθυνο της Επεξεργασίας και αφετέρου η πρόσβαση στα προσωπικά δεδομένα όχι απλώς να είναι ελεγχόμενη, αλλά να βασίζεται στις απαιτήσεις του Νομικού και Κανονιστικού Πλαισίου που διέπει τη συλλογή και επεξεργασία των προσωπικών δεδομένων.

Τα παραπάνω δημιουργούν τις εξής ανάγκες:

- Εφαρμογή ελέγχου πρόσβασης που θα λαμβάνει υπόψη τις απαιτήσεις τις Νομοθεσίας.
- Εκτέλεση όλων των απαραίτητων συμπληρωματικών ενεργειών που πρέπει να συνοδεύουν τις πράξεις συλλογής και επεξεργασίας προσωπικών δεδομένων.

- Εκτέλεση της κάθε πράξης συλλογής και επεξεργασίας λαμβάνοντας υπόψη τα ιδιαίτερα χαρακτηριστικά του κάθε τύπου προσωπικών δεδομένων, υπηρεσίας και ρόλου των εμπλεκομένων οντοτήτων.
- Ενεργό ρόλο για το υποκείμενο των δεδομένων.
- Ενεργό ρόλο για την Αρχή Ιδιωτικότητας.

Η Διατριβή παρουσιάζει την προτεινόμενη λύση, η οποία προέκυψε έπειτα από ανάλυση του Νομικού και Κανονιστικού Πλαισίου και τη συνακόλουθη θεώρηση των σχετικών απαιτήσεων. Οι βασικές συνεισφορές της προτεινόμενης λύσης και – συνεπώς – της Διατριβής είναι οι παρακάτω:

- Ο ορισμός ενός μοντέλου ελέγχου πρόσβασης που βασίζεται στον προσδιορισμό κανόνων που απορρέουν από τη Νομοθεσία. Το μοντέλο περιέχει τους σημασιολογικούς ορισμούς των τύπων των προσωπικών δεδομένων, των υπηρεσιών και των ρόλων των εμπλεκομένων οντοτήτων και ορίζει κανόνες πρόσβασης βασιζόμενο στους ορισμούς αυτούς. Ορίζει επιπλέον όλες τις συμπληρωματικές πράξεις που πρέπει να εκτελεστούν.
- Ο ορισμός ενός συστήματος για την εφαρμογή του παραπάνω μοντέλου ελέγχου πρόσβασης. Ιδιαίτερο χαρακτηριστικό του συστήματος αυτού είναι ότι απομονώνει τα προσωπικά δεδομένα από τους εν δυνάμει Υπεύθυνους της Επεξεργασίας και δεν παραχωρεί δεδομένα που ταυτοποιούν τα υποκείμενα των δεδομένων. Για το σκοπό αυτό, ενσωματώνει λειτουργικές μονάδες επεξεργασίας που πραγματοποιούν πράξεις επεξεργασίας δεδομένων εσωτερικά στο σύστημα εξαλείφοντας την ανάγκη παραχώρησης των εν λόγω δεδομένων. Επιπλέον, λαμβάνει υπόψη τις προτιμήσεις ιδιωτικότητας των χρηστών, τις οποίες καθιστά ουσιαστικά μέρος του μοντέλου ελέγχου πρόσβασης. Ο ενεργός ρόλος των υποκειμένων των δεδομένων συμπληρώνεται από τη δυνατότητα για απ' ευθείας πρόσβαση στα δεδομένα τους μετά από τη συλλογή τους, την ενημέρωσή τους αναφορικά με πράξεις συλλογής και επεξεργασίας δεδομένων, καθώς και από τη δυνατότητα παραχώρησης ή μη ρητής συγκατάθεσης σε πραγματικό χρόνο. Επιπροσθέτως, η Αρχή Ιδιωτικότητας αποκτά επίσης ενεργό ρόλο, έχοντας τη δυνατότητα σε πραγματικό ή μη χρόνο να εποπτεύει την προστασία της ιδιωτικότητας από τους Υπευθύνους της Επεξεργασίας και – κυρίως – όντας η

ίδια η Αρχή Ιδιωτικότητας η οντότητα που καθορίζει τους κανόνες συλλογής και επεξεργασίας, μέσω της Οντολογίας Ιδιωτικότητας.

Βασικά εργαλεία για την πραγματοποίηση των ανωτέρω είναι η Οντολογία Ιδιωτικότητας, η αρχιτεκτονική μεσισμικού και οι γλώσσες περιγραφής κανόνων και ροών εργασιών ιδιωτικότητας που προδιαγράφηκαν στο πλαίσιο της εκπόνησης της Διατριβής.

Η τρέχουσα και μελλοντική ερευνητική εργασία κινείται στους παρακάτω άξονες:

- Εξειδίκευση της προτεινόμενης λύσης σε ειδικούς τύπους υπηρεσιών. Ως παραδείγματα μπορούν να αναφερθούν οι εφαρμογές Διαδικτυακής Τηλεφωνίας (Voice Over IP – VoIP) και οι μηχανισμού παρακολούθησης δικτύων για λόγους όπως είναι η ανίχνευση εισβολών (Intrusion Detection), η παρακολούθηση της απόδοσης, η χρέωση των συνδρομητών, κλπ. Σε ό,τι αφορά την παρακολούθηση δικτύων, η προτεινόμενη λύση έχει ήδη αρχίσει να προσαρμόζεται στις ειδικές ανάγκες τους· έχουν επιπλέον προκύψει δύο σχετικές δημοσιεύσεις στα πρακτικά αναγνωρισμένων διεθνών συνεδρίων [150][151]. Στο ίδιο πλαίσιο εντάσσεται και η ολοκλήρωση της προτεινόμενης λύσης με τα διεθνή πρότυπα για τη νόμιμη παρακολούθηση και συλλογή προσωπικών δεδομένων [136][137][138][139][140][141][142].
- Δημιουργία ενός πλαισίου για την ημιαυτόματη δημιουργία υπηρεσιών που εκμεταλλεύονται την προτεινόμενη λύση. Σκοπός είναι η δημιουργία ενός περιβάλλοντος σύνθεσης υπηρεσιών που θα είναι εγγενώς συμβατές με την προτεινόμενη λύση και θα συμμορφώνονται με τη Νομοθεσία. Ο τελικός στόχος είναι να μπει ένα επίπεδο αφαίρεσης αναφορικά με την προστασία των προσωπικών δεδομένων και η συμμόρφωση με τις αντίστοιχες αρχές να είναι διάφανη για το δημιουργό των υπηρεσιών. Στο πλαίσιο αυτό, θα επιδιωχθεί η ολοκλήρωση με σύγχρονες τεχνικές και μεθοδολογίες της μηχανικής λογισμικού, όπως είναι η υλοποίηση βασισμένη σε όψεις (Aspect–Oriented Software Development) [152] και οι Μοντελοκεντρικές Αρχιτεκτονικές (Model–Driven Architectures) [153].

Βιβλιογραφία

[1] S. D. Warren and L. D. Brandeis, "The Right to Privacy", *Harvard Law Review*, Vol. IV, No. 5, pp. 193–220, December 1890.

[2] The European Opinion Research Group, "European Union citizens' views about privacy", *Special Eurobarometer 196*, December 2003.

[3] Mark Weiser, "The computer for the 21st century", *Scientific American*, 265(3), pp. 66–75, September 1991.

[4] European Union, Information Society Technology Advisory Group – ISTAG, homepage: http://cordis.europa.eu/ist/istag.htm.

[5] Information Society Technology Advisory Group, "Orientations for Workprogramme 2000 and Beyond", September 1999.

[6] R. Cucchiara, "Multimedia surveillance systems", in *Proc. 3rd ACM Intl. Workshop on Video Surveillance & Sensor Networks*, Singapore, 2005, pp. 3–10.

[7] R. Weinstein, "RFID: A Technical Overview and Its Application to the Enterprise", *IEEE IT Professional*, Vol. 7, No. 3, pp. 27–33, May 2005.

[8] Wikipedia, *List of Google acquisitions*, online: http://en.wikipedia.org/wiki/List_of_Google_acquisitions.

[9] R. Kimball and M. Ross, *The Data Warehouse Toolkit: The Complete Guide to Dimensional Modeling*, John Wiley & Sons, 2002.

[10] J. Han and M. Kamber, *Data mining: Concepts and Techniques*, Morgan-Kaufman, 2000.

[11] E. Thomsen, *OLAP Solutions: Building Multidimensional Information Systems*, John Wiley & Sons, 2002.

[12] Ηνωμένα Έθνη, "Οικουμενική Διακήρυξη για τα Ανθρώπινα Δικαιώματα", 10 Δεκεμβρίου 1948, διαθέσιμο στο http://www.unhchr.ch/udhr/lang/grk.pdf.

[13] A. F. Westin, *Privacy and Freedom*, Atheneum, 1967.

[14] E. Lundin and E. Jonsson, "Anomaly-based Intrusion Detection: Privacy Concerns and other Problems", *Elsevier Computer Networks*, Volume 34, Issue 4, pp. 623–640, October 2000.

[15] The Information and Privacy Commissioner/Ontario, Deloitte & Touche, "The Security-Privacy Paradox: Issues, Misconceptions, and Strategies", Joint Report, August 2003.

[16] Gesetz- und Verordnungsblatt für das Land Hessen - Teil I - Nr. 4, Wiesbaden 12.Oktober 1970, 625ff.

[17] Public Law No. 93-579, 88 Stat. 1897 (Dec. 31, 1974), 5 U.S.C. 552a.

[18] Public Law No. 100-503, Oct. 18, 1988, 5 U.S.C. 552a.

[19] Public Law No. 107-56, H. R. 3162, Oct. 21, 2001

[20] Organisation for Economic Co-operation and Development, homepage: http://www.oecd.org/.

[21] Organisation for Economic Co-operation and Development, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", September 1980.

[22] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, "Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη διακίνηση των δεδομένων αυτών", *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 281, σελ. 31 – 50, Νοέμβριος 1995.

[23] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, "Οδηγία 97/66/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Δεκεμβρίου 1997 περί επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και προστασίας της ιδιωτικής ζωής στον τηλεπικοινωνιακό τομέα", *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 24, σελ. 1 – 8, Δεκέμβριος 1997.

[24] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, "Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Ιουλίου 2002 σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την

προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)", *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 201, σελ. 37 – 47, Ιούλιος 2002.

[25] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, "Οδηγία 2006/24/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 15ης Μαρτίου 2006 για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ", *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 105, σελ. 54 – 63, Απρίλιος 2006.

[26] Ζ' Αναθεωρητική Βουλή των Ελλήνων, "Το Σύνταγμα της Ελλάδας", Αθήνα, 6 Απριλίου 2001, online: http://www.parliament.gr/politeuma/syntagma.pdf.

[27] Βουλή των Ελλήνων, "Νόμος 2472/1997: Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 50, Τεύχος Πρώτο, 10 Απριλίου 1997.

[28] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, homepage: http://www.dpa.gr/.

[29] Βουλή των Ελλήνων, "Νόμος 3115/2003: Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 47, Τεύχος Πρώτο, 27 Φεβρουαρίου 2003.

[30] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, homepage: http://www.adae.gr.

[31] Βουλή των Ελλήνων, "Νόμος 2474/1999: Προστασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 287, Τεύχος Πρώτο, 22 Δεκεμβρίου 1999.

[32] Βουλή των Ελλήνων, "Νόμος 3471/2006: Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του Νόμου 2472/1997", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 133, Τεύχος Πρώτο, 28 Ιουνίου 2006.

[33] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση Απορρήτου κατά την Παροχή Κινητών Τηλεπικοινωνιακών Υπηρεσιών", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 87, Τεύχος Δεύτερο, 26 Ιανουαρίου 2005.

[34] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση Απορρήτου κατά την παροχή Σταθερών Τηλεπικοινωνιακών Υπηρεσιών", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 87, Τεύχος Δεύτερο, 26 Ιανουαρίου 2005.

[35] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση Απορρήτου κατά την παροχή Τηλεπικοινωνιακών Υπηρεσιών μέσω Ασυρμάτων Δικτύων", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 87, Τεύχος Δεύτερο, 26 Ιανουαρίου 2005.

[36] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου στις Διαδικτυακές Επικοινωνίες και τις συναφείς Υπηρεσίες και Εφαρμογές", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 88, Τεύχος Δεύτερο, 26 Ιανουαρίου 2005.

[37] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου Διαδικτυακών Υποδομών", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 88, Τεύχος Δεύτερο, 26 Ιανουαρίου 2005.

[38] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, "Κανονισμός για τη Διασφάλιση του Απορρήτου Εφαρμογών και Χρήστη Διαδικτύου", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 88, Τεύχος Δεύτερο, 26 Ιανουαρίου 2005.

[39] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Code of practice for information security management", International Standard ISO/IEC 17799, December 2000.

[40] Πρόεδρος της Ελληνικής Δημοκρατίας, "Προεδρικό Διάταγμα Υπ. Αριθ. 47: Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του", *Εφημερίδα της*

Κυβέρνησης της Ελληνικής Δημοκρατίας, Αριθμός Φύλλου 64, Τεύχος Πρώτο, 10 Μαρτίου 2005.

[41] META Group, "Privacy Enhancing Technologies", META Group Report v. 1.1 for Danish Ministry of Science, Technology and Innovation, March 2005.

[42] A. Anderson, "A Comparison of Two Privacy Policies Languages: EPAL and XACML", in *Proceedings of the 3rd ACM Workshop on Secure Web Services* (*SWS'06)*, Alexandria, Virginia, USA, November 3 2006.

[43] D. F. Ferraiolo, R. Sandhu, S. Gavrila, R.D. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control", *ACM Transactions on Information and System Security*, Vol. 4, No. 3, August 2001.

[44] The World Wide Web Consortium (W3C), The Platform for Privacy Preferences (P3P) Project, online: http://www.w3.org/P3P/.

[45] The World Wide Web Consortium (W3C), homepage: http://www.w3.org/.

[46] The World Wide Web Consortium (W3C), Extensible Markup Language (XML) 1.0 (Fourth Edition) Specification, *W3C Recommendation*, August 2006, online: http://www.w3.org/TR/2006/REC-xml-20060816.

[47] T. Berners-Lee, R. Fielding, and L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax and Semantics", *IETF Request For Comments 2396*, August 1998.

[48] The World Wide Web Consortium (W3C), P3P 1.0 Implementations, online: http://www.w3.org/P3P/compliant_sites.php3.

[49] Privacy Finder, homepage: http://www.privacyfinder.org/.

[50] The World Wide Web Consortium (W3C), A P3P Preference Exchange Language 1.0 (APPEL 1.0), *W3C Working Draft*, April 2002, online: http://www.w3.org/TR/P3P-preferences/.

[51] R. Agrawal, J. Kiernan, R. Srikant and Yirong Xu, "XPref: a preference language for P3P", *Elsevier Computer Networks*, Vol. 48, Issue 5, pp. 809–827, August 2005.

[52] The World Wide Web Consortium (W3C), XML Path Language (XPath) Version 1.0 Specification, *W3C Recommendation*, November 1999, online: http://www.w3.org/TR/xpath.

[53] The World Wide Web Consortium (W3C), XML Path Language (XPath) Version 2.0 Specification, *W3C Recommendation*, January 2007, online: http://www.w3.org/TR/xpath20/.

[54] E. Bertino, J. Byun and N. Li, "Privacy-Preserving Database Systems", *Foundations of Security Analysis and Design III,* Lecture Notes in Computer Science, Vol. 3655, Springer-Verlag, 2005.

[55] G. Hogben, "A technical analysis of problems with P3P v1.0 and possible solutions", in *W3C Workshop on the Future of P3P*, Dulles, Virginia, USA, November 12-13 2002.

[56] M. Schunter, E. Van Herreweghen and M. Waidner, "Expressive Privacy Promises - How to Improve the Platform for Privacy Preferences (P3P)", in *W3C Workshop on the Future of P3P*, Dulles, Virginia, USA, November 12-13 2002.

[57] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, "Hippocratic databases", in *Proceedings of the 28th International Conference on Very Large Databases (VLDB' 2002)*, Hong Kong, China, August 20 – 23, 2002.

[58] K. LeFevre, R. Agrawal, V. Ercegovac, R. Ramakrishnan, Y. Xu, D. DeWitt, "Limiting Disclosure in Hippocratic databases", in *Proceedings of the 30th International Conference on Very Large Databases (VLDB' 2004)*, pp.108-119, Toronto, Canada, August 31 – September 3, 2004.

[59] J.-W. Byun, E. Bertino, N. Li, "Purpose Based Access Control for Privacy Protection in Relational Database Systems", *Technical Report 2004-52*, Purdue University, 2004.

[60] J.-W. Byun, E. Bertino, N. Li, "Purpose Based Access Control of Complex Data for Privacy Protection", in *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05)*, pp.102-110, Stockholm, Sweden, June 01 – 03, 2005.

[61] J.-W. Byun and N. Li, "Purpose Based Access Control for Privacy Protection in Relational Database Systems", *The VLDB Journal*, Vol.17, No.4, pp.603-619, July 2008.

[62] Organization for the Advancement of Structured Information Standards (OASIS), homepage: http://www.oasis-open.org/.

[63] OASIS eXtensible Access Control Markup Language (XACML) 2.0 Specification Set, online: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml.

[64] M. Kudo and S. Hada, "XML document security based on provisional authorization" in *Proceedings of the 7th ACM Conference on Computer and Communications Security (CCS'00)*, Athens, Greece, 01 – 04 November 2000.

[65] The Internet Engineering Task Force (IETF), homepage: http://www.ietf.org/.

[66] International Organization for Standardization (ISO), homepage: http://www.iso.org.

[67] A. Westerinen, J. Schnizlein, J. Strassner, et al., "Terminology for Policy-Based Management", *IETF Request For Comments 3198*, November 2001.

[68] R. Yavatkar, D. Pendarakis, and R. Guerin, "A Framework for Policy-Based Admission Control", *IETF Request For Comments 2753*, January 2000.

[69] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Open Systems Interconnection — Security frameworks for open systems: Access control framework", International Standard ISO/IEC 10181-3, September 1996.

[70] T. Moses (editor), "OASIS eXtensible Access Control Markup Language (XACML) 2.0 Specification Document", February 2005.

[71] G. Karjoth, M. Schunter, "A Privacy Policy Model for Enterprises", in *Proceedings of the 15th IEEE Computer Foundations Workshop*, 2002.

[72] G. Karjoth, M. Schunter, M. Waidner, "Platform for Enterprise Privacy Practices: Privacy-enabled Management of Customer Data", in *Proceedings of the 2nd Workshop on Privacy Enhancing Technologies (PET 2002)*, Lecture Notes in Computer Science, Vol. 2482, Springer-Verlag, 2002.

[73] M. Schunter, P. Ashley, "The Platform for Enterprise Privacy Practices", IBM Zurich Research Laboratory, 2002.

[74] G. Karjoth, M. Schunter, M. Waidner, "Privacy-enabled Services for Enterprises", in *Proceedings of the International Workshop on Trust and Privacy in Digital Business 2002 (TrustBus 2002)*, Aix-en-Provence, France, September 2-6 2002.

[75] International Business Machines, Enterprise Privacy Authorisation Language (EPAL 1.2) Specification, *IBM Research Report*, June 2003, online: http://www.zurich.ibm.com/security/enterprise-privacy/epal/Specification/.

[76] A. J. Menejes, P. C. Van Oorschot and C. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[77] B. Schneier, *Applied Cryptography*, John Wiley & Sons, 1996.

[78] National Institute of Standards and Technology, "Data Encryption Standard (DES)", Federal Information Processing Standard Publication 46-3, October 1999.

[79] National Institute of Standards and Technology, "Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", Special Publication 800-67, May 2004.

[80] National Institute of Standards and Technology, "Advance Encryption Standard (AES)", Federal Information Processing Standard Publication 197, November 2001.

[81] X. Lai and J. L. Massey, "A Proposal for a New Block Encryption Standard," in *Advances in Cryptology - EUROCRYPT '90: Workshop on the Theory and Application of Cryptographic Techniques*, Aarhus, Denmark, May 1990, Lecture Notes in Computer Science, Vol. 473, Springer-Verlang, pp. 389–404, 1991.

[82] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)", in *Proceedings of Fast Software Encryption Cambridge Security Workshop 1993*, Lecture Notes in Computer Science, Vol. 809, Springer-Verlang, pp. 191–204, 1994.

[83] R. Rivest, "A Description of the RC2(r) Encryption Algorithm", *IETF Request For Comments 2268*, March 1998.

[84] R. Rivest, "The RC4 encryption algorithm", RSA Data Security, Inc., March 1992.

[85] R. Baldwin and R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", *IETF Request For Comments 2040*, October 1996.

[86] W. Diffie and M. E. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Volume 22, Issue 6 pp. 644–654, November 1976.

[87] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol . 21 no. 2, pp. 120–126, February 1978.

[88] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, 48(177): 203 - 209, January 1987.

[89] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, Addison-Wesley, 2002.

[90] National Institute of Standards and Technology, "Introduction to Public Key Technology and the Federal PKI Infrastructure", Special Publication 800-32, February 2001.

[91] B. Kaliski, "The MD2 Message-Digest Algorithm", *IETF Request For Comments 1319*, April 1992.

[92] R. Rivest, "The MD5 Message-Digest Algorithm", *IETF Request For Comments 1321*, April 1992.

[93] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", Federal Information Processing Standard Publication 180-2, August 2002.

[94] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, "Οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 13ης Δεκεμβρίου 1999 σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές", *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 13, σελ. 12 – 20, Ιανουάριος 2000.

[95] Πρόεδρος της Ελληνικής Δημοκρατίας, "Προεδρικό Διάταγμα Υπ. Αριθ. 150: Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές", *Εφημερίδα της Κυβέρνησης της Ελληνικής Δημοκρατίας*, Αριθμός Φύλλου 125, Τεύχος Πρώτο, 25 Ιουνίου 2001.

[96] A. O. Freier, P. Karlton and P. C. Kocher, "The SSL Protocol Version 3.0", Internet Draft draft-freier-ssl-version3-02, IETF, November 1996.

[97] T. Dierks and E. Rescorla, "The TLS Protocol Version 1.1", *IETF Request For Comments 4346*, April 2006.

[98] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", *IETF Request For Comments 5246*, August 2008.

[99] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", *IETF Request For Comments 2616*, June 1999.

[100] J. Klensin (editor), "Simple Mail Transfer Protocol", *IETF Request For Comments 2821*, April 2001.

[101] A. Pfitzmann and M. Köhntopp, "Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology", in *Designing Privacy Enhancing Technologies: Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, USA, July 2000, Lecture Notes in Computer Science, Vol. 2009, Springer-Verlag, 2001, pp. 1–9.

[102] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques — Evaluation criteria for IT security", International Standard ISO/IEC 15408-2, Second Edition, October 2005.

[103] Anonymouse anonymization proxy, homepage: http://anonymouse.org/.

[104] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms", *Communications of the ACM*, Volume 24, Issue 2, pp. 84–88, February 1981.

[105] M. K. Reiter and Aviel D. Rubin, "Anonymous Web transactions with Crowds", *Communications of the ACM*, Volume 42 Issue 2, pp. 32–48, February 1999.

[106] U.S.A. Federal Trade Commission, "Eli Lilly Settles FTC Charges Concerning Security Breach", *File No. 012 3214 In the Matter of Eli Lilly and Company*, January 2002, online: http://www.ftc.gov/opa/2002/01/elililly.htm.

[107] U.S.A. Federal Trade Commission, "FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors", FTC File No. 002 3274, July 2000, online: http://www.ftc.gov/opa/2000/07/toysmart.htm.

[108] M. Barbaro and T. Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times*, 9 August 2006.

[109] Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο, "Κανονισμός 2195/2002 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 5ης Νοεμβρίου 2002 περί του κοινού

λεξιλογίου για τις δημόσιες συμβάσεις", *Επίσημη Εφημερίδα των Ευρωπαϊκών Κοινοτήτων*, Αρ. L. 340, σελ. 1 – 562, Δεκέμβριος 2006.

[110] A. Fuggetta, G. P. Picco and G. Vigna, "Understanding Code Mobility," *IEEE Transactions on Software Engineering*, Vol. 24, No. 5, pp. 342–361, May 1998.

[111] J. Claessens, B. Preneel, J. Vandewalle, "(How) can mobile agents do secure electronic transactions on untrusted hosts? A survey of the security issues and the current solutions", *ACM Transactions on Internet Technology*, Vol. 3 No. 1, pp. 28–48, February 2003.

[112] The World Wide Web Consortium (W3C), Web Services Architecture, *W3C Working Group Note*, February 2004, online: http://www.w3.org/TR/ws-arch/.

[113] J. Rosenberg, H. Schulzrinne, G. Camarillo, et al, "SIP: Session Initiation Protocol", *IETF Request For Comments 3261*, June 2002.

[114] P. Sherburne and C. Fitzgerald, "You Don't Know Jack About VoIP". *ACM Queue*, Volume 2, Issue 6, pp. 30–38, September 2004.

[115] Sun Microsystems, "Java™ Cryptography Architecture for Java™ Platform Standard Edition 6", online: http://java.sun.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html

[116] N. F. Noy, D. L. McGuinness, "Ontology Development 101: A Guide to Creating Your First Ontology", *Stanford Medical Informatics Technical Report SMI-2001-0880*, March 2001.

[117] The World Wide Web Consortium (W3C), "Web Ontology Language (OWL)", online: http://www.w3.org/2004/OWL/.

[118] The World Wide Web Consortium (W3C), "Resource Description Framework (RDF)", online: http://www.w3.org/RDF/.

[119] A. Seaborn, "RDQL - A query language for RDF", W3C Member Submission, Jan. 2004, online: http://www.w3.org/Submission/RDQL/.

[120] Stanford Center for Biomedical Informatics Research, Protégé ontology editor, homepage: http://protege.stanford.edu/.

[121] D. Jordan, J. Evdemon (chairs), "OASIS Web Services Business Process Execution Language Version 2.0 (BPEL) 2.0 Specification Document", OASIS Standard, April 2007.

[122] Sun Microsystems, "Java Servlet Technology", online: http://java.sun.com/products/servlet/.

[123] The Apache Software Foundation, Apache Axis2, online: http://ws.apache.org/axis2/.

[124] Sun Microsystems, "Enterprise JavaBeans Technology", online: http://java.sun.com/products/ejb/.

[125] Jena – A Semantic Web Framework for Java, online: http://jena.sourceforge.net/.

[126] Hewlett Packard Labs, Semantic Web Research, homepage: http://www.hpl.hp.com/semweb/.

[127] E. F. Codd, *The Relational Model for Database Management: Version 2*, Addison-Wesley Longman Publishing Co., 1990.

[128] Oracle Database, homepage: http://www.oracle.com/technology/software/products/database/index.html.

[129] Sun Microsystems, "Java Message Service (JMS)", online: http://java.sun.com/products/jms/.

[130] V. Falletta, F. S. Proto, S. Teofili, G. Bianchi, "Privacy-Aware Accounting and Billing" *17th ICT Mobile & Wireless Communications Summit 2008*, Stockholm, Sweden, 10 – 12 June 2008.

[131] P. Daly, "Navstar GPS and GLONASS: Global Satellite Navigation Systems", *IEEE Electronics & Communication Engineering Journal*, Volume 5, Issue 6, pp. 349–357, December 1993.

[132] European Commission, Directorate of Energy and Transport: Galileo, homepage: http://ec.europa.eu/dgs/energy_transport/galileo/index_en.htm.

[133] European Space Agency (ESA): Galileo, homepage: http://www.esa.int/esaNA/galileo.html.

[134] E-ZPASS, New York Service Center, homepage: http://www.e-zpassny.com.

[135] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), "Οδηγία για τα Κλειστά Κυκλώματα Τηλεόρασης", Απόφασης της ΑΠΔΠΧ, Αριθ. Πρωτ. 1122, Σεπτέμβριος 2000.

[136] European Telecommunication Standards Institute. Lawful Interception; Requirements of Law Enforcement Agencies. Technical Specification 101.331, v1.2.1, June 2006.

[137] European Telecommunication Standards Institute. Lawful Interception; Concepts of Interception in a Generic Network Architecture. Technical Report 101.943, v1.1.1, July 2001.

[138] European Telecommunication Standards Institute. Lawful Interception; Issues on IP Interception. Technical Report 101.944, v1.1.2, December 2001.

[139] European Telecommunication Standards Institute. Lawful Interception; Handover Specification for IP Delivery. Technical Specification 102.232, v1.5.1, October 2006.

[140] European Telecommunication Standards Institute. Lawful interception; Service-specific details for e-mail services. Technical Specification 102.233, v1.1.1, February 2004.

[141] European Telecommunication Standards Institute. Lawful Interception; Service-specific details for internet access services. Technical Specification 102.234, v1.1.1, February 2004.

[142] European Telecommunication Standards Institute. Lawful Interception; Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data. Technical Specification 102.656, v1.1.2, December 2007.

[143] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model", International Standard ISO/IEC 15408-1:2005, October 2005.

[144] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements", International Standard ISO/IEC 15408-2:2005, October 2005.

[145] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), "Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements", International Standard ISO/IEC 15408-3:2005, October 2005.

[146] Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, "Anforderungskatalog zum Datenschutz-Gütesiegel für IT-Produkte", Version 1.2, August 2005, online: https://www.datenschutzzentrum.de/download/anford.pdf.

[147] Ανεξάρτητο Κέντρο για την Προστασία της Ιδιωτικότητας (Unabhängigen Landeszentrum für Datenschutz), Kiel, Schleswig-Holstein, Germany, homepage: https://www.datenschutzzentrum.de/.

[148] eTEN Project European Privacy Seal (EuroPriSe), homepage: http://www.european-privacy-seal.eu/.

[149] eTEN EuroPriSe, "EuroPriSe Criteria Catalogue", Version 0.3 (June 2008), avalable at: http://www.european-privacy-seal.eu/criteria.

[150] Giuseppe Bianchi, Elisa Boschi, Dimitra I. Kaklamani, Eleftherios A. Koutsoloukas, Georgios V. Lioudakis, Francesco Oppedisano, Martin Petraschek, Fabio Ricciato, Carsten Schmoll, "Towards Privacy-Preserving Network Monitoring: Issues and Challenges", *The 18th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2007)*, Athens, Greece, September 3 - 7 2007.

[151] Giuseppe Bianchi, Elisa Boschi, Francesca Gaudino, Eleftherios A. Koutsoloukas, Georgios V. Lioudakis, Sathya Rao, Fabio Ricciato, Carsten Schmoll, Felix Strohmeier, "Privacy-Preserving Network Monitoring: Challenges and Solutions", *17th ICT Mobile & Wireless Communications Summit 2008*, Stockholm, Sweden, June 10 – 12 2008.

[152] R. Filman, L. Cranor, A. Chowdhury, *Aspect-Oriented Software Development*, Addison-Wesley, 2004.

[153] D. Frankel, *Model Driven Architecture*, Wiley, 2002.

Παράρτημα Α' – Δημοσιεύσεις

Διεθνή Περιοδικά

[1] Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Nikolaos Dellas, Nikolaos Tselikas, Sofia Kapellaki, George N. Prezerakos, Dimitra I. Kaklamani, Iakovos S. Venieris, "A Middleware Architecture for Privacy Protection", *Computer Networks*, Volume 51, Issue 16, pp. 4679-4696, November 2007.

[2] Vaggelis Nikas, Georgios V. Lioudakis, Nikos Dellas, Iakovos S. Venieris, Christoph Pollak, Richard Wisenocker, "SIP as a Unified Signalling Solution in a Beyond 3G System", *Computer Communications*, Volume 29, Issue 16, pp. 3226–3237, October 2006.

Πρακτικά Διεθνών Συνεδρίων

[3] Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Nikolaos Dellas, Georgia M. Kapitsaki, Dimitra I. Kaklamani, Iakovos S. Venieris, "A Semantic Framework for Privacy-Aware Access Control", in *Proceedings of The 3rd International Workshop on Secure Information Systems (SIS'08)*, Wisla, Poland, October 20 – 22 2008.

[4] Giuseppe Bianchi, Elisa Boschi, Francesca Gaudino, Eleftherios A. Koutsoloukas, Georgios V. Lioudakis, Sathya Rao, Fabio Ricciato, Carsten Schmoll, Felix Strohmeier, "Privacy-Preserving Network Monitoring: Challenges and Solutions", in *Proceedings of The 17th ICT Mobile & Wireless Communications Summit 2008*, Stockholm, Sweden, June 10 – 12 2008.

[5] Georgia M. Kapitsaki, Dimitris A. Kateros, Georgios V. Lioudakis, Iakovos S. Venieris, "Extending Reusable Asset Specification to Describe Simple Mobile Services", in *Proceedings of The 17th ICT Mobile & Wireless Communications Summit 2008*, Stockholm, Sweden, June 10 – 12 2008.

[6] Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Nikolaos L. Dellas, Francesca Gaudino, Dimitra I. Kaklamani, Iakovos S. Venieris, "Technical Enforcement of Privacy Legislation", in *Proceedings of The 18th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2007)*, Athens, Greece, September 3 – 7 2007.

[7] Giuseppe Bianchi, Elisa Boschi, Dimitra I. Kaklamani, Eleftherios A. Koutsoloukas, Georgios V. Lioudakis, Francesco Oppedisano, Martin Petraschek, Fabio Ricciato, Carsten Schmoll, "Towards Privacy-Preserving Network Monitoring: Issues and Challenges", in *Proceedings of The 18th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2007)*, Athens, Greece, September 3 – 7 2007.

[8] Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Francesca Gaudino, Nikolaos L. Dellas, Dimitra I. Kaklamani, Iakovos S. Venieris, "A Technical Realization of Privacy Legislation", in *Proceedings of ACSIS INTER: A European Cultural Studies Conference 2007*, Norrköping, Sweden, June 11 – 13 2007.

[9] Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Nikolaos Dellas, Sofia Kapellaki, George N. Prezerakos, Dimitra I. Kaklamani, Iakovos S. Venieris, "A Proxy for Privacy: the Discreet Box", in *Proceedings of The IEEE Eurocon 2007*, Warsaw, Poland, September 9 – 12 2007.

[10] Alexander De Luca, Giuseppe Tropea, Georgios V. Lioudakis, Eleftherios A. Koutsoloukas, Nikolaos L. Dellas, Fabio Testa, Markus Blanchebarbe, "A Framework for Adapting Services' Design and Execution to Privacy Regulations", in *Proceedings of The 16th IST Mobile & Wireless Communications Summit 2007*, Budapest, Hungary, July 1 – 5 2007.

[11] Nikolaos L. Dellas, Eleftherios A. Koutsoloukas, Georgios V. Lioudakis, Dimitra I. Kaklamani, Iakovos S. Venieris, "A Performance Comparison of Ontology Reasoning and Rule Engines", in *Proceedings of The 16th IST Mobile & Wireless Communications Summit 2007*, Budapest, Hungary, July 1 – 5 2007.

[12] Eleftherios Koutsoloukas, Georgios V. Lioudakis, Sofia Kapellaki, Nikolaos L. Dellas, Christos Katsigiannis, George N. Prezerakos, Dimitra I. Kaklamani, Iakovos S. Venieris, "A Middleware Architecture for Privacy Protection in Smart Environments", in *Proceedings of The 15th IST Mobile & Wireless Communication Summit 2006*, Mykonos, Greece, June 4 – 8 2006.

[13] Vaggelis Nikas, Georgios V. Lioudakis, Nikos Dellas, Iakovos S. Venieris, Dimitra I. Kaklamani, Christoph Pollak, Richard Wisenocker, "Evolving UMTS towards IP:

Evaluation of the SIPRAN Architecture", in *Proceedings of The IEEE International Conference on Communications (ICC) 2006*, Istanbul, Turkey, June 11 – 15 2006.

[14] Georgios V. Lioudakis, Ioannis E. Foukarakis, George N. Prezerakos, Dimitra I. Kaklamani, and Iakovos S. Venieris, "eDocuments Intelligent Enrichment from Distributed Knowledge Resources", in *Proceedings of The IEEE Eurocon 2005*, Belgrade, Serbia & Montenegro, November 21 – 24 2005.

[15] Georgios V. Lioudakis, Vaggelis Nikas, Christoph Pollak, Richard Wisenocker, Nikos Dellas, Iakovos S. Venieris, "Unified Signalling Using SIP in a B3G System", in *Proceedings of The 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC 2005)*, Berlin, Germany, September 11 – 14 2005.

[16] Georgios V. Lioudakis, Vaggelis Nikas, Christoph Pollak, Richard Wisenocker, Nick Dellas, "SIP as a Unified Signalling Solution in a Beyond 3G System", in *Proceedings of The IST Mobile & Wireless Communication Summit 2005*, Dresden, Germany, June 19 – 23 2005.

[17] Vaggelis Nikas, Georgios V. Lioudakis, Georgios Leoleis, Iakovos S. Venieris, "IP-based Video Streaming service provision over Satellite UMTS", in *Proceedings of The Interworking 2004*, Ottawa, Canada, November 29 – December 1 2004.

[18] Lila Dimopoulou, Vaggelis Nikas, Georgios Leoleis, Georgios V. Lioudakis, Iakovos S. Venieris, "Mobility Management using SIP in a beyond 3G System", in *Proceedings of The IST Mobile & Wireless Communication Summit 2004*, Lyon, France, June 27 – 30 2004.

[19] Vaggelis Nikas, Georgios V. Lioudakis, Lila Dimopoulou, Georgios Leoleis, Iakovos S. Venieris, "QoS provision for real-time services over Satellite UMTS", in *Proceedings of The IST Mobile & Wireless Communication Summit 2004*, Lyon, France, June 27 - 30 2004.

[20] Christoph Pollak, Seoug Hoon Oh, Arnoldo Giralda, Vaggelis Nikas, Georgios V. Lioudakis, Jose Manuel Sanchez, "A SIP based concept for NAS signaling in combination with an all-IP core network architecture", in *Proceedings of The IST Mobile & Wireless Communication Summit 2004*, Lyon, France, June 27 – 30 2004.