ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Διαχείριση προτιμήσεων ιδιωτικότητας με χρήση τεχνολογίας ψηφιακών δικαιωμάτων

ΦΑΝΟΥΡΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Β. Λιουδάκης
Εντεταλμένος Διδάσκων

Λαμία 16 Οκτωβρίου έτος 2024

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Διαχείριση προτιμήσεων ιδιωτικότητας με χρήση τεχνολογίας ψηφιακών δικαιωμάτων

ΦΑΝΟΥΡΑΚΗΣ ΚΩΝΣΤΑΝΤΙΝΟΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΥΠΕΥΘΥΝΟΣ

Γεώργιος Β. Λιουδάκης
Εντεταλμένος Διδάσκων

Λαμία 16 Οκτωβρίου έτος 2024

UNIVERSITY OF
THESSALY

SCHOOL OF SCIENCE

DEPARTMENT OF COMPUTER SCIENCE & TELECOMMUNICATIONS

Privacy preferences management using digital rights technology

FANOURAKIS KONSTANTINOS

FINAL THESIS

ADVISOR

Georgios V. Lioudakis
Adjunct Professor

Lamia October 16 year 2024

«Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [(1)], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

*1. Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί **χωρίς να τα περικλείω σε εισαγωγικά** και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

*2. Δέχομαι ότι η αυτολεξεί **παράθεση χωρίς εισαγωγικά**, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια

4. Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.

Ημερομηνία: 16/10/2024

Ο Δηλών

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση
του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων
σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.»

ΠΕΡΙΛΗΨΗ

Η παρούσα πτυχιακή εργασία αναφέρεται στο σύγχρονο ζήτημα της ιδιωτικότητας στον ψηφιακό κόσμο, και συγκεκριμένα στο πώς μπορούν να περιγραφούν οι προτιμήσεις ιδιωτικότητας των υποκειμένων των δεδομένων. Αρχικά συνοψίζει το υποκείμενο νομικό πλαίσιο, όπως ορίζεται από το Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ). Στη συνέχεια, περιγράφει τις τεχνολογίες ψηφιακών δικαιωμάτων. Κατόπιν, εμβαθύνει στο σύστημα που δημιουργήθηκε στο πλαίσιο της εργασίας, το οποίο μετατρέπει τις προτιμήσεις ιδιωτικότητας των χρηστών σε προτιμήσεις ιδιωτικότητας βασισμένες σε μία εκ των τεχνολογιών ψηφιακών δικαιωμάτων, την Open Digital Rights Language (ODRL).

ABSTRACT

This thesis examines the contemporary issue of privacy in the digital world, specifically how the privacy preferences of data subjects can be described. It begins by summarizing the relevant legal framework as described by the General Data Protection Regulation (GDPR). Next, it describes digital rights technologies. Following that, it analyzes the system developed in the context of the thesis, which converts users' privacy preferences into privacy preferences based on one of the digital rights technologies, Open Digital Rights Language (ODRL).

Table of Contents

Table of Figures

Glossary

GDPR	General Data Protection Regulation, ευρωπαϊκός κανονισμός με σκοπό την προστασία των δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης.
IBE	Identity-Based Encryption, τύπος κρυπτογράφησης δημοσίου κλειδιού.
EPA	Enterprise Privacy Architecture, αρχιτεκτονική διασφάλισης της ασφάλειας και ιδιωτικότητας στις υπηρεσίες ενός οργανισμού .
E-P3P	Platform for Enterprise Privacy Practices, βελτίωση της EPA που διαχωρίζει την ανάπτυξη πολιτικών ασφαλείας από τους μηχανισμούς που διαχειρίζονται όλα τα δεδομένα μέσα σε ένα οργανισμό.
EPAL	Enterprise Privacy Authorization Language, γλώσσα δημιουργίας βελτιστοποιημένων πολιτικών ασφαλείας μέσα σε ένα οργανισμό.
RBAC	Role-Based Access Control, έλεγχος πρόσβασης βάσει ρόλου μέσα σε ένα οργανισμό.
PuRBAC	Purpose-aware Role Based Access Control, έλεγχος πρόσβασης βάσει ρόλου με επίγνωση στο σκοπό μέσα σε ένα οργανισμό.
SPACE	Sticky Policy and Access Control Engine, υπηρεσία όπου τα υποκείμενα των δεδομένων μπορούν να ορίσουν τις προτιμήσεις ιδιωτικότητας τους μέσα στο υπολογιστικό νέφος χρησιμοποιώντας Sticky πολιτικές.
ODRL	Open Digital Rights Language, γλώσσα που εκφράζει πολιτικές για την διαχείριση ψηφιακών δικαιωμάτων πάνω σε ορισμένο ψηφιακό περιεχόμενο .
IRIs	Internationalized Resource Identifiers, μία γενίκευση των URIs που επιτρέπει την χρήση διαφορετικών χαρακτήρων από τους ASCII στις διευθύνσεις ιστοσελίδων.
RDF	Resource Description Framework, μοντέλο περιγραφής οντοτήτων στο Παγκόσμιο Ιστό.
XML	eXtensible Markup Language, γλώσσα που ορίζει κανόνες για την κωδικοποίηση εγγράφων σε μορφότυπο αναγνώσιμο από τον άνθρωπο και την μηχανή ταυτόχρονα.
JSON-LD	JSON for Linked Data,δυνατότητα σύνδεσης των δεδομένων με τρόπο αναγνώσιμο από την μηχανή και τον άνθρωπο, εξασφαλίζοντας διαλειτουργικότητα μεταξύ διαφορετικών συστημάτων και εφαρμογών.
MPEG REL	MPEG Rights Expression Language, γλώσσα που ορίζει μηχανισμούς για την χρήση και κατανάλωση ψηφιακού περιεχομένου.
CC	Creative Commons, μη κερδοσκοπικός οργανισμός που δημιουργεί τις CC άδειες για την προστασία των πνευματικών δικαιωμάτων των δημιουργών.
ccREL	Creative Commons Rights Expression Language, γλώσσα που παράγει άδειες πνευματικής ιδιοκτησίας σε μορφή αναγνώσιμη από την μηχανή.
NIST	National Institute of Standards and Technology, Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ.
JAXB	Java™ Architecture for XML Binding, αρχιτεκτονική της γλώσσας προγραμματισμού Java που χρησιμοποιείται για την μετατροπή των αντικειμένων της σε XML και το αντίστροφο.
GUI	Graphical User Interface, γραφική διεπαφή που επιτρέπει στους χρήστες να αλληλεπιδρούν με τις ηλεκτρονικές συσκευές και το λογισμικό τους μέσω γραφικών στοιχείων.
NLP	Natural Language Processing, τομέας της τεχνητής νοημοσύνης με στόχο το να επιτρέψει στα υπολογιστικά συστήματα να κατανοούν, να ερμηνεύουν και να παράγουν φυσική γλώσσα όπως ο άνθρωπος.

ΚΕΦΑΛΑΙΟ 1 Εισαγωγή

Είναι γεγονός, πως τα τελευταία χρόνια η χρήση του Διαδικτύου έχει εξαπλωθεί και πλέον η αλληλεπίδραση των χρηστών με τις διαδικτυακές εφαρμογές θεωρείται δεδομένη. Αυτό έχει φέρει την ανησυχία για την προστασία των δεδομένων των χρηστών, αφού η αλληλεπίδραση αυτή σημαίνει ότι και περισσότερες πληροφορίες για τους χρήστες εισάγονται στις πλατφόρμες και αργότερα ρέουν στο διαδίκτυο. Με αυτό το τρόπο δημιουργείται η ανάγκη για την προστασία των προσωπικών δεδομένων. Φυσικά, η προστασία των προσωπικών δεδομένων δεν είναι κάτι νέο αφού ακόμα και από το 1890 υπάρχει η αναφορά στο ατομικό δικαίωμα στην ιδιωτικότητα στις Η.Π.Α [1].

Η μη σωστή οργάνωση και προστασία των δεδομένων των χρηστών μπορεί να οδηγήσει στην εκμετάλλευση των δεδομένων τους από τρίτους άμεσα ή έμμεσα [2]. Το γεγονός αυτό, έφερε την δημιουργία ορισμένων νομικών πλαισίων σε διάφορες χώρες ανά το κόσμο για την εξασφάλιση της προστασίας των προσωπικών δεδομένων των πολιτών. Για παράδειγμα, η Κίνα δημιούργησε το Personal Information Protection Law (PIPL), το Ηνωμένο Βασίλειο το Data Protection Act 2018 (αντικαθιστώντας το παλαιότερο Data Protection Act 1998). Μέρος αυτής της πτυχιακής εργασίας είναι η εκτενής αναφορά που γίνεται στο Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) που δημιούργησε η Ευρωπαϊκή Ένωση για την προστασία των προσωπικών δεδομένων των πολιτών της.

Ταυτόχρονα, αξιοσημείωτη πρόοδος έχει παρατηρηθεί και στις τεχνολογίες ψηφιακών δικαιωμάτων ή γενικότερα στην διαχείριση των ψηφιακών δικαιωμάτων [3]. Αυτές, έκαναν την εμφάνιση τους στα μέσα της δεκαετίας του ‘90 και αποτελούν κατηγορία λογισμικού με κύριο σκοπό τον ορισμό των δικαιωμάτων που διευκρινίζουν οι δημιουργοί τους. Μία τέτοια τεχνολογία μπορεί να επιτρέπει ή να απαγορεύει την χρήση, το διαμοιρασμό και άλλες λειτουργίες σε ό,τι αφορά ένα ορισμένο περιεχόμενο. Τα δικαιώματα περιγράφονται μέσω των εκφράσεων δικαιωμάτων ή πιο περίπλοκα και δομημένα μέσω των Γλωσσών Εκφράσεων Δικαιωμάτων (Rights Expression Languages-RELs) όπως η ODRL, MPEG-REL, ccREL.

Συνδυάζοντας το φλέγον ζήτημα της προστασίας δεδομένων με τις τεχνολογίες ψηφιακών δικαιωμάτων και συγκεκριμένα την Open Digital Rights Language (ODRL) γίνεται ανάλυση του συστήματος που αναπτύχθηκε στα πλαίσια της πτυχιακής εργασίας το οποίο έχει βασικό στόχο την μετατροπή προτιμήσεων ιδιωτικότητας των χρηστών σε ODRL προτιμήσεις ιδιωτικότητας με XML μορφότυπο [4].

ΚΕΦΑΛΑΙΟ 2 Προτιμήσεις Ιδιωτικότητας

Υποκεφάλαιο 2.1 Νομικά Θέματα

Ενότητα 2.1.α Γενικός Κανονισμός Προστασίας Δεδομένων

Ο **Γενικός Κανονισμός Προστασίας Δεδομένων - General Data Protection Regulation (GDPR)** [5] αφορά την προστασία των προσωπικών δεδομένων των πολιτών της Ευρωπαϊκής Ένωσης. Οργανισμοί που έχουν στην κατοχή τους ή επεξεργάζονται δεδομένα Ευρωπαίων πολιτών άσχετα με το αν εκείνοι δεν βρίσκονται στην Ευρώπη, είναι υποχρεωμένοι να τηρήσουν τον GDPR. Ο GDPR ορίστηκε από το Ευρωπαϊκό Κοινοβούλιο το 2016 και από τις 25 Μαΐου του 2018 κάθε οργανισμός πρέπει να τον τηρεί.

Ιστορικά, για την Ευρωπαϊκή Ένωση η έννοια «δικαίωμα στην ιδιωτικότητα» δεν είναι καινούργια. Όμως, η ραγδαία ανάπτυξη του ψηφιακού κόσμου έφερε την ανάγκη για την δημιουργία ενός τέτοιου κανονισμού.

Πριν προχωρήσουμε αναλυτικά στο τι ορίζει ο Γενικός Κανονισμός Προστασίας Δεδομένων είναι χρήσιμο να ορίσουμε τους εξής όρους:

- Υποκείμενο δεδομένων (Data Subject): Το φυσικό πρόσωπο που αφορούν οι πληροφορίες.
- Υπεύθυνος επεξεργασίας των δεδομένων (Data Controller): Το φυσικό ή νομικό πρόσωπο, μία δημόσια αρχή ή κάποιος φορέας όπου μόνα τους ή από κοινού με άλλα καθορίζουν το σκοπό και τα μέσα της επεξεργασίας των προσωπικών δεδομένων.
- Υπεύθυνος προστασίας δεδομένων (Data Protection Officer): Το πρόσωπο που είναι υπεύθυνο στο να διαβεβαιώνει την τήρηση του GDPR μέσα σε ένα οργανισμό.

Αρχές Προστασίας Δεδομένων:

Το άρθρο 5 του κανονισμού ορίζει τις παρακάτω επτά (7) αρχές προστασίας δεδομένων που πρέπει να τηρούν οι φορείς που επεξεργάζονται τα δεδομένα:

1)**Νομιμότητα, αντικειμενικότητα, διαφάνεια**, δηλαδή η επεξεργασία των δεδομένων θα πρέπει να είναι σύμφωνη με ό,τι ορίζει ο κανονισμός (νομιμότητα), θα πρέπει τα δεδομένα που θα δεχθούν επεξεργασία να είναι τα ίδια με αυτά που αναφέρονται (αντικειμενικότητα) και το υποκείμενο θα πρέπει να γνωρίζει για την σχετική επεξεργασία των δεδομένων του (διαφάνεια).

2)**Περιορισμός του σκοπού**, δηλαδή η περισυλλογή και η επεξεργασία των δεδομένων θα γίνεται μόνο για νόμιμους σκοπούς και το υποκείμενο των δεδομένων θα πρέπει να λαμβάνει γνώση.

3)**Ελαχιστοποίηση των δεδομένων**, δηλαδή τα δεδομένα τα οποία περισυλλέγονται και δέχονται επεξεργασία θα πρέπει να είναι τα απολύτως απαραίτητα για τον κάθε σκοπό που εξυπηρετούν.

4)**Ακρίβεια**, όπου θα πρέπει να γίνεται επικαιροποίηση των δεδομένων ανά πάσα στιγμή.

5)**Περιορισμός της αποθήκευσης**, όπου τα δεδομένα θα αποθηκεύονται μόνο για το χρονικό διάστημα του σκοπού που εξυπηρετούν.

6)**Ακεραιότητα και εμπιστευτικότητα**, όπου η επεξεργασία των δεδομένων θα πρέπει να γίνεται με τέτοιο τρόπο έτσι ώστε να εξασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα τους. Πρέπει δηλαδή να παρέχονται μέτρα προστασίας των δεδομένων από τροποποίηση ή απώλεια αλλά και από την πρόσβαση σε αυτά από μη εξουσιοδοτημένα πρόσωπα.

7)**Λογοδοσία**, όπου ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει να συμμορφωθεί με όλες τις παραπάνω αρχές σε ό,τι αφορά τα δεδομένα που διαχειρίζεται.

Νομιμότητα της επεξεργασίας δεδομένων:

Το άρθρο 6 του κανονισμού ορίζει την νομιμότητα της επεξεργασίας των δεδομένων αν τηρείται έστω και ένας όρος από τους παρακάτω:

- Ο ιδιοκτήτης των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων του.
- Η επεξεργασία είναι απαραίτητη όταν το υποκείμενο των δεδομένων αποτελεί μέρος κάποιας σύμβασης που πρόκειται να γίνει.
- Η επεξεργασία γίνεται σύμφωνα με κάποια νομική υποχρέωση.
- Η επεξεργασία γίνεται με σκοπό να σωθεί η ζωή κάποιου ατόμου.
- Η επεξεργασία είναι απαραίτητη για σκοπό που εξυπηρετεί το κοινό συμφέρον.
- Εάν υπάρχει ενδιαφέρον επεξεργασίας από τον φορέα, πάντα με νόμιμο τρόπο, εκτός και αν θίγει τα θεμελιώδη δικαιώματα και τις ελευθερίες του υποκείμενου των δεδομένων.

Συναίνεση:

Όσον αφορά την συναίνεση που ορίζει το υποκείμενο, αυτή ορίζεται από τους εξής κανόνες:

- Η συναίνεση πρέπει να προσφέρεται ελεύθερα, με συγκεκριμένο και ξεκάθαρο τρόπο.
- Τα αιτήματα για συναίνεση θα πρέπει να διαφοροποιούνται από κάθε άλλο ζήτημα.
- Τα υποκείμενα θα πρέπει να μπορούν να αναιρέσουν οποιαδήποτε προηγούμενη συναίνεση έχουν δώσει.
- Ανήλικοι κάτω των 13 ετών μπορούν να συναινούν με άδεια από τον κηδεμόνα τους.
- Οι συναινέσεις των υποκειμένων θα πρέπει να αρχειοθετούνται.

Δικαιώματα Ιδιωτικότητας:

1)*Δικαίωμα στην ενημέρωση (ή στην διαφανή ενημέρωση) (Άρθρο 12-14)*

Εάν τα προσωπικά δεδομένα συλλέγονται από το υποκείμενο άμεσα (Άρθρο 13 του Κανονισμού), το υποκείμενο θα πρέπει να ενημερωθεί την ακριβή στιγμή που γίνεται η περισυλλογή των δεδομένων του. Ο υπεύθυνος της επεξεργασίας δεδομένων θα πρέπει να ενημερώσει το υποκείμενο σχετικά με την ταυτότητα και τα στοιχεία επικοινωνίας του ίδιου, τα στοιχεία επικοινωνίας του Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer, DPO) (εάν υπάρχει), το σκοπό επεξεργασίας των δεδομένων, την νόμιμη αρχή που βασίζεται η επεξεργασία, τους τρίτους και τις χώρες που ενδέχεται να λάβουν τα δεδομένα, την χρονική διάρκεια που αυτά θα διατηρούνται, τα δικαιώματα που έχει το υποκείμενο των δεδομένων, την δυνατότητα του να αναιρέσει κάποια συναίνεση αλλά και επίσης το δικαίωμα του υποκειμένου να υποβάλλει καταγγελία σε κάποια αρχή.

Εάν τα προσωπικά δεδομένα δεν συλλέγονται άμεσα (Άρθρο 14 του Κανονισμού), ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώσει το υποκείμενο σε σύντομο χρονικό διάστημα, μέχρι και ένα μήνα αργότερα. Όσον αφορά την ενημέρωση του υποκειμένου από τον υπεύθυνο επεξεργασίας, ισχύουν οι ίδιοι όροι όπως και στην περίπτωση που τα προσωπικά δεδομένα συλλέγονται άμεσα, με την εξαίρεση ότι εδώ ο υπεύθυνος επεξεργασίας δεν είναι η αρμόδια αρχή για την λήψη αποφάσεων. Παρόλα αυτά θα πρέπει ενημερώσει επίσης το υποκείμενο σχετικά με τις πηγές από όπου προέρχονται τα δεδομένα του και εάν υπάρχει ελεύθερη πρόσβαση σε αυτές.

2)*Δικαίωμα πρόσβασης (Άρθρο 15)*

Ορίζεται ως το δικαίωμα του υποκειμένου των δεδομένων να γνωρίζει σχετικά με την επεξεργασία των δεδομένων του από τον υπεύθυνο επεξεργασίας.

Αρχικά, ο υπεύθυνος επεξεργασίας θα πρέπει να ελέγξει αν και εφόσον τα δεδομένα του υποκειμένου δέχονται επεξεργασία μετά από το αίτημα του υποκειμένου. Αν όντως υπάρχει σχετική επεξεργασία θα πρέπει να γίνει η ενημέρωση του υποκειμένου σχετικά με τον σκοπό της επεξεργασίας, τους παραλήπτες των δεδομένων, το χρονικό διάστημα διατήρησης τους, τα δικαιώματα του υποκειμένου σχετικά με τα δεδομένα του, το δικαίωμα του για καταγγελία σε αρμόδια αρχή, το δικαίωμα του για διόρθωση, διαγραφή ή και περιορισμό της επεξεργασίας.

3)*Δικαίωμα Διαγραφής (Άρθρο 17)*

Ορίζεται ως το δικαίωμα του υποκειμένου για το αίτημα διαγραφής των δεδομένων του από τον υπεύθυνο επεξεργασίας εάν τα δεδομένα του πλέον δεν είναι απαραίτητα για την αρχική ορισμένη επεξεργασία, είτε διότι το υποκείμενο ζήτησε ανάκληση συναίνεσης για επεξεργασία, είτε γιατί ανακλήθηκε η επεξεργασία για νομικούς λόγους .

Μέσα στο δικαίωμα διαγραφής συμπεριλαμβάνεται και το δικαίωμα στη «λήθη» όπου βρίσκεται και αυτό στο Άρθρο 17 του Κανονισμού. Αν ο υπεύθυνος επεξεργασίας έχει δημοσιοποιήσει τα δεδομένα του υποκειμένου, έπειτα από αίτημα του υποκειμένου για διαγραφή, ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώσει όλους τους άλλους αρμόδιους υπεύθυνους επεξεργασίας που λαμβάνουν μέρος στην επεξεργασία των δεδομένων του υποκειμένου και με αυτό το τρόπο θα γίνει η διαγραφή των δεδομένων.

4)*Δικαίωμα Διόρθωσης (Άρθρο 16)*

Ορίζεται ως το δικαίωμα του υποκειμένου για διόρθωση των προσωπικών δεδομένων του χωρίς να χρειαστεί αρκετή καθυστέρηση.

Είναι σημαντικό να αναφερθεί πως το υποκείμενο έχει το δικαίωμα να μην παραχωρήσει επακριβώς τα προσωπικά του δεδομένα και να παραχωρήσει μόνο τα απολύτως απαραίτητα για την επεξεργασία. Οπότε και το δικαίωμα διόρθωσης στην συγκεκριμένη περίπτωση μπορεί να χρησιμοποιηθεί εποικοδομητικά.

5)*Δικαίωμα περιορισμού της επεξεργασίας (Άρθρο 18)*

Ορίζεται ως το δικαίωμα του υποκειμένου να υποβάλλει αίτημα περιορισμού της επεξεργασίας στο υπεύθυνο επεξεργασίας όταν τουλάχιστον ένας από τους παρακάτω όρους ισχύει :

- Όταν αμφισβητείται η ακρίβεια των δεδομένων από το υποκείμενο.
- Η επεξεργασία κρίνεται παράνομη και το υποκείμενο απαιτεί την διαγραφή και το περιορισμό χρήσης των δεδομένων του.

- Ο υπεύθυνος επεξεργασίας των δεδομένων δεν χρειάζεται άλλο τα δεδομένα του υποκειμένου για επεξεργασία.
- Το υποκείμενο των δεδομένων αμφισβητεί νομικά την επεξεργασία τους.

Επίσης είναι σημαντικό να αναφερθεί πως εφόσον έχει υπάρξει περιορισμός της επεξεργασίας, οποιαδήποτε άλλη επεξεργασία δεχθούν τα δεδομένα, είναι εφικτή μόνο με την συναίνεση του υποκειμένου.

6*)Δικαίωμα στην φορητότητα των δεδομένων (Άρθρο 20)*

Ορίζεται ως το δικαίωμα του υποκειμένου να λαμβάνει τα δεδομένα που έχει παραχωρήσει στο υπεύθυνο επεξεργασίας των δεδομένων σε δομημένη, αναγνώσιμη από μηχανή μορφή και έπειτα να μπορεί να μεταβιβάσει τα δεδομένα αυτά σε κάποιο άλλο υπεύθυνο επεξεργασίας των δεδομένων όταν αυτό είναι τεχνικά εφικτό.

Στα παραπάνω υπάρχουν περιορισμοί όταν το δικαίωμα αυτό του υποκειμένου θίγει το δημόσιο συμφέρον, ή την άσκηση δημόσιας εξουσίας από το υπεύθυνο επεξεργασίας των δεδομένων ή επηρεάζει τα δικαιώματα και τις ελευθερίες άλλων ατόμων.

7)*Δικαίωμα στην αντίρρηση (Άρθρο 21)*

Ορίζεται ως το δικαίωμα του υποκειμένου να φέρει αντίρρηση οποιαδήποτε στιγμή σε ό,τι αφορά την επεξεργασία των προσωπικών του δεδομένων. Εάν η επεξεργασία δεδομένων γίνεται για εμπορικούς σκοπούς, το υποκείμενο των δεδομένων ανά πάσα στιγμή έχει το δικαίωμα για αντίρρηση. Γενικότερα, ο υπεύθυνος επεξεργασίας των δεδομένων έπειτα, δεν μπορεί να επεξεργάζεται τα δεδομένα εκτός και αν τον υποστηρίζει το νομικό πλαίσιο απέναντι στις επιθυμίες του υποκειμένου δεδομένων.

Ομοίως εάν η επεξεργασία των δεδομένων γίνεται για επιστημονική ή ιστορική έρευνα ή ακόμα και για στατιστικούς λόγους, το υποκείμενο των δεδομένων έχει δικαίωμα να φέρει αντίρρηση.

Στην περίπτωση που η επεξεργασία των δεδομένων πραγματοποιείται για το κοινό συμφέρον, μόνο τότε το υποκείμενο δεν μπορεί να φέρει σχετική αντίρρηση.

8)*Δικαίωμα σε ό,τι αφορά την αυτοματοποιημένη λήψη αποφάσεων (Άρθρο 22)*

Ορίζεται ως το δικαίωμα του υποκειμένου να μην παίρνει μέρος σε απόφαση που λαμβάνεται αποκλειστικά μέσω αυτοματοποιημένης επεξεργασίας συμπεριλαμβανομένης και της κατάταξης του σε κάποιο προφίλ.

Αυτό το δικαίωμα αναιρείται εάν τα παραπάνω είναι απαραίτητα για την σύμβαση μεταξύ του υποκειμένου και του υπεύθυνου επεξεργασίας δεδομένων, είτε εάν επιτρέπονται από την σχετική νομοθεσία της Ευρωπαϊκής Ένωσης ή του συγκεκριμένου κράτους-μέλους της ΕΕ, είτε εάν βασίζονται στην συναίνεση του υποκειμένου των δεδομένων.

Προστασία δεδομένων από το σχεδιασμό (by design) και εξ 'ορισμού (by default) (Άρθρο 25):

Ο Κανονισμός δίνει έμφαση σε αυτό που ονομάζεται προστασία από το σχεδιασμό και προστασία εξ' ορισμού . Ο υπεύθυνος επεξεργασίας των δεδομένων πρέπει να οργανώνει την επεξεργασία τους με τέτοιο τρόπο έτσι ώστε οι αρχές προστασίας δεδομένων του κανονισμού να εφαρμόζονται από την αρχή της επεξεργασίας (Προστασία από το σχεδιασμό(by design)).

Ταυτόχρονα, ο υπεύθυνος επεξεργασίας πρέπει να διαβεβαιώνει το γεγονός πως η επεξεργασία των δεδομένων χρησιμοποιεί τα απολύτως απαραίτητα δεδομένα που ορίζει ο σκοπός της (Προστασία εξ' ορισμού(by default)).

Υποχρέωση ειδοποίησης σε περίπτωση τροποποίησης, διαγραφής ή και περιορισμού της επεξεργασίας δεδομένων (Άρθρο 19):

Οποιαδήποτε τροποποίηση, διαγραφή των δεδομένων ή περιορισμός της επεξεργασίας των δεδομένων γίνει, ο υπεύθυνος επεξεργασίας των δεδομένων είναι υποχρεωμένος να ενημερώσει όλους τους φορείς που λαμβάνουν μέρος στην επεξεργασία, εκτός και αν αυτό είναι αδύνατο.

Εάν το υποκείμενο των δεδομένων ζητήσει να ενημερωθεί για τα παραπάνω, τότε επίσης ο υπεύθυνος επεξεργασίας των δεδομένων θα πρέπει να το ενημερώσει.

Περιορισμοί (Άρθρο 23):

Ο υπεύθυνος επεξεργασίας των δεδομένων υπόκειται σε κάποιους περιορισμούς από την νομοθεσία της Ευρωπαϊκής Ένωσης ή του κράτους-μέλους της ΕΕ με σκοπό την διασφάλιση:

- της εθνικής ασφάλειας.
- της εθνικής άμυνας.
- της δημόσιας ασφάλειας.
- της προτροπής, έρευνας, ανίχνευσης ή δίωξης ποινικών αδικημάτων.
- ό,τι αφορά το δημόσιο συμφέρον της ΕΕ και των μελών κρατών της σε θέματα δημόσιας υγείας αλλά και οικονομικού και κοινωνικού ζητήματος.
- της προστασίας του υποκειμένου των δεδομένων .
- των δικαιωμάτων του ατόμου.

Πρόστιμα (Άρθρο 83):

Οι εθνικές αρχές κάθε χώρας μπορούν να ορίσουν σχετικά πρόστιμα για παραβιάσεις της προστασίας των δεδομένων σε ό,τι ορίζει ο GDPR. Φυσικά, κάθε παραβίαση είναι διαφορετική και λαμβάνει διαφορετική διαχείριση όσον αφορά τα πρόστιμα.

Για παράδειγμα, όπως αναφέρεται στο Άρθρο 83 του Κανονισμού, για ακραίες περιπτώσεις παραβιάσεων το ποσό του προστίμου μπορεί να ξεπεράσει τα 20 εκατομμύρια ευρώ ή να οριστεί η δέσμευση του 4% των παγκόσμιων εσόδων του οργανισμού που παραβίασε το Κανονισμό.

Ενότητα 2.1.β Προκλήσεις εφαρμογής

Η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων φέρνει αρκετές προκλήσεις [6] που πρέπει να αντιμετωπίσουν οι υπεύθυνοι επεξεργασίας δεδομένων για να συμμορφωθούν με τις νομικές απαιτήσεις του. Από την στιγμή που η ΕΕ επέβαλε στους οργανισμούς την εφαρμογή του κανονισμού, ελάχιστοι οργανισμοί κατάφεραν να συμμορφωθούν πλήρως με αυτόν. Αυτό οφείλεται στο γεγονός ότι παρόλο που ο κανονισμός είναι ένα δομημένο και αναλυτικό νομικό έγγραφο, δεν υπάρχει τεχνική υποστήριξη στους οργανισμούς που θα κληθούν να τον εφαρμόσουν.

Η προστασία των προσωπικών δεδομένων όσον αφορά τους οργανισμούς είναι αμιγώς ένα τεχνικό ζήτημα. Από την στιγμή που μαζί με το κανονισμό δεν ορίστηκε κάποια τεχνική καθοδήγηση ή κάποια συγκεκριμένη τεχνολογία για την διευκόλυνση των οργανισμών, τόσο και πιο δύσκολη είναι η εφαρμογή του κανονισμού σε κάθε οργανισμό ατομικά. Επίσης η προσθήκη επιπλέον μηχανισμών οι οποίοι εφαρμόζουν τεχνικά τον κανονισμό μπορεί να αποτελέσει ένα μεγάλο κόστος για κάθε οργανισμό.

Συγκεκριμένα το δικαίωμα στην «λήθη» που ορίζει ο κανονισμός, τεχνικά είναι δύσκολο για τους οργανισμούς να τον τηρήσουν αφού διατηρούν συστήματα αντιγράφων ασφαλείας σε περίπτωση απώλειας δεδομένων ή φυσικών καταστροφών. Οπότε, στην συγκεκριμένη περίπτωση οι οργανισμοί θα πρέπει να διαγράφουν τα δεδομένα των υποκειμένων και από τα συστήματα αντιγράφων ασφαλείας όταν αυτό ζητείται, γεγονός που κρύβει κινδύνους για σφάλματα σε αυτή την διαγραφή ή και πιθανή εκμετάλλευση των δεδομένων.

Ταυτόχρονα ο κανονισμός ορίζει και την ενσωμάτωση του PSD2 [1] σε χρηματοοικονομικούς οργανισμούς . Με αυτόν το τρόπο, οι συγκεκριμένοι οργανισμοί επικοινωνούν συνεχώς με τρίτους με σκοπό την ισχυρή ταυτοποίηση των πελατών τους με το να συλλέγουν και να επεξεργάζονται

[1] PSD2: Payment Service Directive 2, αφορά τον Ευρωπαϊκό κανονισμό για την εξασφάλιση ασφαλών ηλεκτρονικών πληρωμών . Σχετικό URL: https://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/14575

ευαίσθητα προσωπικά δεδομένα, καταπατώντας σε πολλές περιπτώσεις τις υποχρεώσεις που ορίζει ο ίδιος ο κανονισμός.

Επίσης είναι σημαντικό να αναφερθεί πως πλέον οι σύγχρονες εφαρμογές βασίζονται στην αλληλεπίδραση που έχουν τα υποκείμενα των δεδομένων με αυτές, οπότε και πολλές φορές το περιεχόμενο τους βασίζεται στην περισυλλογή και επεξεργασία δεδομένων των υποκειμένων δεδομένων για να προσφέρουν μία καλύτερη και πιο προσιτή εμπειρία σε αυτά . Αυτό λοιπόν έρχεται σε αντίθεση με ό,τι ορίζει ο GDPR, δηλαδή στην υποχρεωτική συναίνεση των υποκειμένων σε ό,τι αφορά την περισυλλογή και επεξεργασία των δεδομένων τους. Με αυτόν τον τρόπο, οι ενδεχόμενες επιλογές των υποκειμένων των δεδομένων για το μέλλον των δεδομένων τους αλλοιώνουν την ποιότητα και το περιβάλλον που προσφέρει η κάθε εφαρμογή σε αυτά.

Ενότητα 2.1.γ Περιπτώσεις παραβάσεων του Κανονισμού

Στην συγκεκριμένη ενότητα θα γίνουν ορισμένες αναφορές στις πιο πρόσφατες παραβάσεις του GDPR. Με την βοήθεια του CMS.Law GDPR Enforcement Tracker [7] είναι δυνατόν να παρατηρούμε τις ποινές και τα πρόστιμα που λαμβάνουν συγκεκριμένοι οργανισμοί από τις αρμόδιες αρχές προστασίας δεδομένων της ανάλογης χώρας της ΕΕ που βρίσκονται.

1)Στις 20 Ιουνίου 2024, η CUI ZSQ FOOD, S.L., ως υπεύθυνος επεξεργασίας λαμβάνει πρόστιμο του ύψους των 42 χιλιάδων ευρώ από την Ισπανική αρχή προστασίας δεδομένων, έπειτα από καταγγελία υπαλλήλου για εμφάνιση βίντεο από το σύστημα παρακολούθησης της εταιρείας σε ομάδα συνομιλίας της εταιρείας. Στην συγκεκριμένη περίπτωση[2], το αρχικό πρόστιμο ήταν το ποσό των 70 χιλιάδων ευρώ αλλά μειώθηκε μετά την άμεση ανάληψη της ευθύνης από την εταιρεία. Ο συγκεκριμένος υπεύθυνος επεξεργασίας δεδομένων δεν συμμορφώθηκε με τις βασικές αρχές του κανονισμού σχετικά με την επεξεργασία δεδομένων (Άρθρο 5 (1) f) του GDPR).

2)Στις 11 Απριλίου 2024, το Ιταλικό Ινστιτούτο Κοινωνικής Ασφάλισης, ως υπεύθυνος επεξεργασίας λαμβάνει πρόστιμο του ύψους των 20 χιλιάδων ευρώ από την Ιταλική αρχή προστασίας δεδομένων, έπειτα από την κίνηση του Ινστιτούτου να δημοσιεύσει στην ιστοσελίδα του, τα προσωπικά δεδομένα συμμετεχόντων σε κάποιον διαγωνισμό επιλογής χωρίς την αρμόδια νομική βάση[3]. Ο υπεύθυνος επεξεργασίας δεν συμμορφώθηκε με τις βασικές αρχές του κανονισμού σχετικά με την επεξεργασία δεδομένων (Άρθρο 2, Άρθρο 5, Άρθρο 6 του GDPR).

3)Στις 24 Ιουνίου 2024, η Avanza Bank AB, ως υπεύθυνος επεξεργασίας λαμβάνει πρόστιμο ύψους 1,3 εκατομμύρια ευρώ από την Σουηδική αρχή προστασίας δεδομένων, έπειτα από την κίνηση της

[2] https://www.enforcementtracker.com/ETid-2371
[3] https://www.enforcementtracker.com/ETid-2382

συγκεκριμένης τράπεζας να χρησιμοποιήσει στην ιστοσελίδα και στις εφαρμογές της μία τεχνολογία η οποία έστελνε τα προσωπικά δεδομένα των χρηστών στο οργανισμό Meta. Τα δεδομένα στέλνονταν στην Meta από το Νοέμβριο του 2019 μέχρι και το Ιούνιο του 2021[4]. Ο υπεύθυνος επεξεργασίας εδώ, δεν διασφάλισε την προστασία των δεδομένων των χρηστών παραβιάζοντας το Άρθρο 5 (1) f) και το Άρθρο 32 (1) του GDPR.

Υποκεφάλαιο 2.2 Sticky Policies

Η ονομασία τους, «κολλητικές» πολιτικές, προκύπτει από το γεγονός ότι οι κανόνες και οι περιορισμοί για την αντιμετώπιση των δεδομένων, είτε αυτή είναι η χρήση, η επεξεργασία ή ο διαμοιρασμός τους, είναι προσκολλημένοι πάνω στα ίδια τα δεδομένα [8].

Με εκείνες, όταν υποβάλλεται ένα τμήμα δεδομένων σε κάποια υπηρεσία, το υποκείμενο των δεδομένων επιλέγει τις προτιμήσεις ιδιωτικότητας του και σύμφωνα με αυτές δημιουργούνται ανάλογες πολιτικές. Αποτελούν λοιπόν ένα πρακτικό τρόπο προστασίας των προσωπικών δεδομένων τόσο για επιχειρήσεις όσο και για ιδιώτες.

Για τα υποκείμενα των δεδομένων, τα παραπάνω σημαίνουν πως εκείνοι θα πρέπει να εμπιστεύονται τους καταναλωτές δεδομένων οι οποίοι με βάση τις συμφωνημένες πολιτικές θα χρησιμοποιήσουν ανάλογα τα δεδομένα.

Στο σύστημα στο οποίο μπορεί να γίνεται η περισυλλογή, η επεξεργασία ή και ο διαμοιρασμός των δεδομένων ακολουθούνται οι συμφωνημένοι κανόνες που ορίζει η κάθε πολιτική. Το ίδιο ισχύει και για υπηρεσίες τρίτων που μπορεί να λαμβάνουν μέρος στη διαδικασία. Είναι σημαντικό να αναφερθεί πως για κάθε πολιτική, μπορεί αυτή να υποβληθεί σε τροποποίηση ή και σε ανάκληση όπου και θα ακολουθεί η ανάλογη ενημέρωση της σε κάθε εμπλεκόμενο καταναλωτή δεδομένων.

Τα παραπάνω επιτυγχάνονται με την εξής διαδικασία:

το υποκείμενο των δεδομένων, στέλνει τα δεδομένα κρυπτογραφημένα μαζί με την αντίστοιχη sticky πολιτική, οι καταναλωτές των δεδομένων επικοινωνούν με μία εμπιστεύσιμη αρχή η οποία διαχειρίζεται τις πολιτικές με σκοπό να αποκτήσουν πρόσβαση στα δεδομένα. Με τον παραπάνω τρόπο, τα υποκείμενα των δεδομένων πρέπει να εμπιστεύονται αυτές τις αρχές προστατεύοντας τα

[4] https://www.enforcementtracker.com/ETid-2377

δεδομένα τους από άλλες ενέργειες που θα μπορούσαν να προβούν οι καταναλωτές των δεδομένων για δικό τους όφελος, π.χ., πώληση των δεδομένων για κέρδος.

Μία sticky πολιτική καθορίζει το μέλλον των σχετικών δεδομένων με το να ορίζει το υποκείμενο των δεδομένων, το περιεχόμενο των δεδομένων, το σκοπό χρήσης των δεδομένων, το σημείο και την χρονική διάρκεια που τα δεδομένα θα είναι διαθέσιμα, καθώς επίσης τις υποχρεώσεις και τους περιορισμούς για κάθε μέρος που συμμετέχει στην πολιτική.

Επίσης πρέπει να αναφερθεί πως μία sticky πολιτική, πρέπει να μπορεί να είναι σύμφωνη και με την τρέχουσα νομοθεσία της κάθε χώρας στο ζήτημα της προστασίας των προσωπικών δεδομένων. Οι περισσότεροι σχετικοί κανονισμοί ορίζονται από τον Οργανισμό Οικονομικής Συνεργασίας και Ανάπτυξης (ΟΟΣΑ) είτε από το Ευρωπαϊκό Κοινοβούλιο σε ό,τι αφορά τον GDPR.

Ενότητα 2.2.α Περιοχές εφαρμογής

Εφαρμογές ή Πλατφόρμες Οργανισμών:

Όταν ένας χρήστης εισέρχεται σε μια ηλεκτρονική υπηρεσία ή εφαρμογή κάποιου οργανισμού, εκείνος έχει συμφωνήσει σε πολιτικές ασφάλειας και ιδιωτικότητας που προσφέρει η εταιρεία για το μέλλον των δεδομένων του. Παρόλα αυτά οι ψηφιακές υπηρεσίες της εταιρείας μπορεί να επικοινωνούν και με τρίτους στους οποίους μπορεί να διαρρέουν τα δεδομένα των υποκειμένων των δεδομένων.

Μέσω των sticky πολιτικών, υπάρχει η Identity-Based Encryption (IBE) που επιτρέπει στα υποκείμενα των δεδομένων να ελέγξουν το πως τα δεδομένα τους χρησιμοποιούνται σε διαφορετικές πλατφόρμες της κάθε υπηρεσίας.

Με την IBE το υποκείμενο των δεδομένων κρυπτογραφεί το περιεχόμενο τους και τις sticky πολιτικές με την IBE ταυτότητα του παραλήπτη των δεδομένων. Η συγκεκριμένη ταυτότητα στην ουσία, δρα ως ένα δημόσιο κλειδί. Τα IBE κλειδιά αποκρυπτογράφησης του παραλήπτη δημιουργούνται από κάποια έμπιστη τρίτη αρχή. Αν η IBE ταυτότητα τροποποιηθεί, η έμπιστη αρχή δεν θα μπορεί να δημιουργήσει τα αντίστοιχα κλειδιά αποκρυπτογράφησης και έτσι δεν θα υπάρξει πρόσβαση στα δεδομένα.

Η χρήση των sticky πολιτικών εδώ, επιτρέπει στο να επιλεχθούν τα δεδομένα που θα είναι ορατά με βάση τα IBE κλειδιά κρυπτογράφησης.

Η IBM έκανε γνωστή την Enterprise Privacy Architecture (EPA). Κύριο χαρακτηριστικό της είναι ότι οι πολιτικές ασφάλειας και ιδιωτικότητας της εταιρείας ρυθμίζονται ανάλογα με τις ανάγκες της. Αποτελείται από τέσσερα τμήματα:

- Τον αναλυτή των κανονισμών ασφάλειας και ιδιωτικότητας που αναγνωρίζει τους τρέχοντες κανονισμούς.
- Το μοντέλο διαχείρισης των αναφορών που επιτρέπει στην εταιρεία να δημιουργήσει μία συγκεκριμένη στρατηγική προστασίας.
- Την δομή συμφωνιών ασφάλειας και ιδιωτικότητας που είναι υπεύθυνη στο να εντοπίζει τις συνδέσεις των υποκειμένων των δεδομένων με τμήματα της εταιρείας ή και με τρίτους.
- Την αρχιτεκτονική της τεχνικής αναφοράς, που ορίζει την τεχνολογία για την διαχείριση των ορισμένων πολιτικών. Η Platform for Enterprise Privacy Practices (E-P3P) αποτελεί μία βελτίωση αυτής της αρχιτεκτονικής όπου διαχωρίζει την ανάπτυξη των πολιτικών μέσα στην εταιρεία από τους μηχανισμούς που στην ουσία ελέγχουν όλα τα δεδομένα.

Γλώσσες Πολιτικών:

Η IBM επίσης έκανε γνωστή και την Enterprise Privacy Authorization Language (EPAL), η οποία είναι γλώσσα που βελτιώνει την δημιουργία πολιτικών με το να επιτρέπει τον έλεγχο των επιχειρήσεων εάν αυτές τηρούν τους κανονισμούς που ορίζουν οι σχετικοί νόμοι και τις προτιμήσεις ιδιωτικότητας των υποκείμενων των δεδομένων .

Μέσω αυτής, θα μπορούσαν να εφαρμοστούν και οι sticky πολιτικές. Μία πολιτική που ορίζεται μέσω της EPAL αποτελείται από ένα λεξιλόγιο, μία λίστα με κανόνες πιστοποίησης, προεπιλεγμένους κανόνες καθώς επίσης και από μία οικουμενική συνθήκη. Προεπιλεγμένα, η EPAL έχει αδυναμίες κυρίως στη μεταφορά δεδομένων σε διαφορετικές πλατφόρμες με ορισμένες πολιτικές ιδιωτικότητας . Αυτό το πρόβλημα μπορούν να το λύσουν οι sticky πολιτικές όπου επιβάλλουν την εφαρμογή των απαραίτητων πολιτικών σε κάθε εμπλεκόμενο φορέα (εάν βέβαια κάθε φορέας τις υποστηρίζει). Επίσης, η χρήση της EPAL έχει το μειονέκτημα ότι οι πολιτικές που ορίζει περιορίζονται στα πλαίσια μία συγκεκριμένης εταιρείας και δεν είναι αρκετά διαλειτουργική σε τρίτους .

Ομοίως, και η γλώσσα που χρησιμοποιείται για την αρχιτεκτονική E-P3P, η P3P αντιμετωπίζει το ίδιο ζήτημα με την διαφορά ότι ορίζει τον εξυπηρετητή(server) της εταιρίας υπεύθυνο στο διαμοιρασμό των δεδομένων στους κατάλληλους τρίτους φορείς .

Τέλος, υπάρχουν προτάσεις για την χρήση των sticky πολιτικών και σε άλλες γλώσσες όπως η Symbol Intensive Master Programming Language (SIMPL) η οποία έχει ως κύριο στόχο να καλύψει ένα μεγαλύτερο πλήθος οντοτήτων στις πολιτικές κάνοντας όσο πιο απλό τον ορισμό τους από τα υποκείμενα των δεδομένων.

Έλεγχος Πρόσβασης (Access Control):

Οι sticky πολιτικές μπορούν να ενταχθούν σε συστήματα ελέγχου πρόσβασης. Για να επιτευχθεί η ασφάλεια και η ιδιωτικότητα μέσω ελέγχων πρόσβασης χρήσιμα είναι τα μοντέλα Role Based Access

Control (RBAC) δηλαδή Έλεγχος Πρόσβασης βάσει Ρόλου και το Purpose-aware RBAC (PuRBAC) δηλαδή Έλεγχος Πρόσβασης βάσει Ρόλου με επίγνωση στο σκοπό. Με αυτά, θα υπάρξει πρόσβαση στα δεδομένα με βάση συγκεκριμένους περιορισμούς, σκοπό για την απόκτηση της πρόσβασης σε αυτά και ρόλο.

Στα παραπάνω, οι sticky πολιτικές μπορούν να αποτελέσουν μία πρακτική λύση αφού διαφορετικοί κανόνες μπορούν να είναι προσκολλημένοι σε διαφορετικά τμήματα των δεδομένων ίδιου τύπου. Βέβαια, αυτή η υλοποίηση έχει το αρνητικό ότι η εταιρεία που τις διαχειρίζεται δεν θα έχει ένα κεντρικό έλεγχο στους ελέγχους πρόσβασης καθώς επίσης και το ότι απαιτεί αρκετούς υπολογιστικούς πόρους.

Υπολογιστικό Νέφος (Cloud Computing):

Το υπολογιστικό νέφος είναι ένα μέσο που μπορεί ο καθένας να μπορεί να μοιράζεται υπολογιστικούς πόρους και δεδομένα μεταξύ διαφορετικών συσκευών. Ουσιαστικά, η πληροφορία αποθηκεύεται και δέχεται διαχείριση από κέντρα δεδομένων που μπορεί να ανήκουν σε τρίτους. Οπότε μία sticky πολιτική μπορεί να εφαρμοστεί και στο υπολογιστικό νέφος όπου τα υποκείμενα των δεδομένων θα ορίζουν τους σχετικούς κανόνες σε ό,τι αφορά τα δεδομένα τους.

Με την χρήση της υπηρεσίας Sticky Policy and Access Control Engine (SPACE) τα υποκείμενα των δεδομένων μπορούν με την βοήθεια των κατάλληλων εργαλείων να ορίσουν τις προτιμήσεις ιδιωτικότητας τους. Η υπηρεσία αυτή, χρησιμοποιεί sticky πολιτικές για να προσφέρει λειτουργίες που επιτρέπουν την πρόσβαση και τον έλεγχο με κατανεμημένο τρόπο στο νέφος. Αυτό, επιτρέπει στα υποκείμενα των δεδομένων στο να έχουν επίγνωση του τρόπου διαχείρισης των δεδομένων τους οποιαδήποτε στιγμή.

Οι sticky πολιτικές μπορούν να εφαρμοστούν στο νέφος με τους εξής τρόπους:

είτε με υποδομή κρυπτογραφίας δημοσίου κλειδιού (PKE Infrastructure) όπου το υποκείμενο των δεδομένων κρυπτογραφεί το περιεχόμενο τους και τις sticky πολιτικές με το δημόσιο κλειδί του παραλήπτη, είτε με IBE, είτε με άλλες μυστικές τεχνικές διαμοιρασμού.

Ο τελευταίος τρόπος φαίνεται να είναι πιο αποδοτικός από πλευράς υπολογιστικής απόδοσης και ελέγχου και σε σύγκριση με τους δύο προηγούμενους αποφεύγεται η υποδομή που απαιτείται για την διαχείριση των κλειδιών από όλους τους εμπλεκόμενους φορείς.

Ενότητα 2.2.β Πλεονεκτήματα

Η χρήση των sticky πολιτικών έχει τα εξής πλεονεκτήματα:

- Τα υποκείμενα των δεδομένων ορίζουν τους κανόνες για την μεταχείριση των δεδομένων τους σε κάθε φορέα που μπορεί να αποκτήσει πρόσβαση σε αυτά.
- Είναι δυνατή η διαχείριση των δεδομένων καθόλη την διάρκεια της χρήσης τους.
- Με την χρήση έμπιστων τρίτων αρχών μειώνεται αρκετά το κόστος διαχείρισης των πολιτικών από κάθε οργανισμό που λαμβάνει μέρος.
- Από την στιγμή που οι sticky πολιτικές βρίσκονται προσκολλημένες στα δεδομένα, τα υποκείμενα των δεδομένων μπορούν να διαχειρίζονται τις πολιτικές και όταν εκείνα είναι εκτός σύνδεσης.
- Το να μην είναι διαθέσιμα τα δεδομένα σε μη εξουσιοδοτημένους τρίτους, βελτιώνει άμεσα την εμπιστευτικότητα του συστήματος.

Ενότητα 2.2.γ Μειονεκτήματα

Η χρήση των sticky πολιτικών έχει τα εξής μειονεκτήματα:

- Δυσκολία στο να συμφωνούν όλοι οι εμπλεκόμενοι φορείς σε κάποιο σύνολο πολιτικών.
- Από το προηγούμενο μειονέκτημα προκύπτει η ανάγκη για την ύπαρξη διαμεσολαβητών στο να ορίζουν επαρκώς το λεξικό της κάθε πολιτικής για όλους τους φορείς.
- Μείωση απόδοσης του δικτύου, αφού τα δεδομένα δεν βρίσκονται σε αποθηκευτικές μονάδες της εταιρείας που τα χρησιμοποιεί αλλά κάθε φορά μεταδίδονται μαζί με τις sticky πολιτικές τους.
- Εξάπλωση πολλαπλών ίδιων πολιτικών σε ένα σύστημα με αρκετούς υπολογιστικούς πόρους π.χ., υπολογιστικό νέφος.

ΚΕΦΑΛΑΙΟ 3 Τεχνολογίες Ψηφιακών Δικαιωμάτων

Υποκεφάλαιο 3.1 Open Digital Rights Language - ODRL

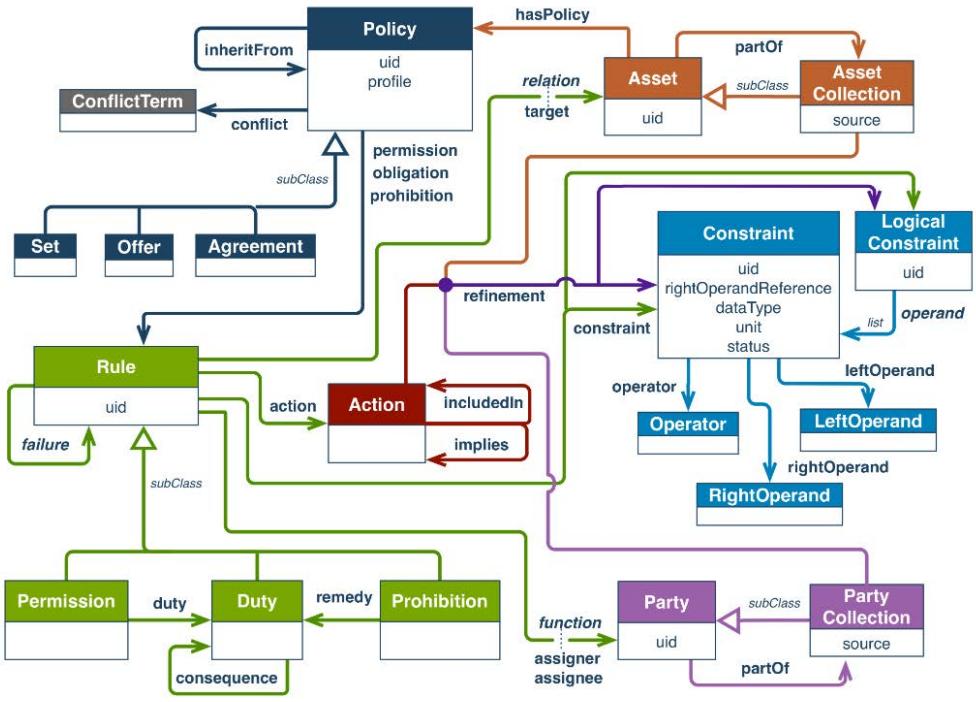
Η Open Digital Rights Language (ODRL) [9], είναι μία γλώσσα που εκφράζει πολιτικές για την επιβολή και διαχείριση ορισμένων ψηφιακών δικαιωμάτων πάνω σε διάφορες μορφές ψηφιακού περιεχομένου.

Για να ορίσει την κάθε πολιτική, η ODRL διαθέτει ένα διαλειτουργικό μοντέλο πληροφοριών και λεξιλόγιο, καθώς χρησιμοποιεί επίσης ευέλικτους μηχανισμούς κωδικοποίησης για την ανάλογη μεταχείριση του περιεχομένου.

Ενότητα 3.1.α Μοντέλο πληροφοριών της ODRL

Το μοντέλο πληροφοριών της ODRL περιγράφει τις θεμελιώδεις έννοιες, οντότητες και τις σχετικές σχέσεις που ορίζουν την σημασιολογία των ODRL πολιτικών .

Οι πολιτικές αυτές ορίζουν τις άδειες, απαγορεύσεις και καθήκοντα σχετικά με την χρήση του ψηφιακού περιεχομένου που στην γλώσσα θα αναφερόμαστε ως Asset. Μέσω του μοντέλου, δίνεται η δυνατότητα στο δημιουργό της πολιτικής να μπορεί να συμπεριλάβει όσες λεπτομέρειες θελήσει στην πολιτική με ευέλικτο τρόπο. Όπως φαίνεται στο Σχήμα 1,



Σχήμα 1: Μοντέλο πληροφοριών της ODRL – ODRL Information Model

Στο μοντέλο πληροφοριών υπάρχουν οι εξής κλάσεις:

Policy class: Μπορεί να περιέχει ένα σύνολο από Permissions(άδειες) ή/και Prohibitions(απαγορεύσεις) ή/και Duties(καθήκοντα). Αποτελεί την γονική κλάση της Set η οποία εκφράζει τους γενικούς κανόνες (Rules), της Offer η οποία εκφράζει τις προτάσεις (offerings) των κανόνων(Rules) από αναθέτοντα Parties και της Agreement που εκφράζει τις παραχωρήσεις των κανόνων (Rules) από αναθέτοντα Parties σε Parties που θα λάβουν αυτές τις παραχωρήσεις . Η Policy class δεν μπορεί να είναι κενή.

Έχει συγκεκριμένες ιδιότητες:

- Πρέπει να έχει μία uid τιμή ιδιότητας τύπου IRI[5] για να μπορεί να αναγνωρίζει την πολιτική.
- Πρέπει να έχει τουλάχιστον μία τιμή ιδιότητας Permission,Prohibition,Duty τύπου Rule.
- Μπορεί να έχει καμία, μία ή περισσότερες profile τιμές ιδιότητας τύπου IRI για να μπορεί να αναγνωρίζει το ODRL Profile όπου η συγκεκριμένη πολιτική ακολουθεί.
- Μπορεί να έχει καμία, μία ή περισσότερες inheritFrom[6] τιμές ιδιότητας τύπου IRI για να αναγνωρίζει την γονική πολιτική την οποία η συγκεκριμένη πολιτική θα κληρονομήσει.
- Μπορεί να έχει καμία ή μία conflict τιμή ιδιότητας τύπου ConlflictTerm για να μπορεί να διαχειριστεί σχετικά conflicts μέσα στην πολιτική.
- Μπορεί να δηλώνει ιδιότητες οι οποίες είναι κοινές στους κανόνες(Rules) της.

Asset class: Περιέχει ένα πόρο ή μία συλλογή πόρων που αποτελούν υποκείμενα ενός κανόνα (Rule). Αποτελεί γονική κλάση της AssetCollection κλάσης η οποία εκπροσωπεί μία συλλογή πόρων.

Μία asset κλάση έχει και τις ακόλουθες ιδιότητες:

- Θα ήταν χρήσιμο να έχει μία uid τιμή ιδιότητας για να αναγνωρίσει το Asset.
- Μπορεί να έχει καμία, μία ή περισσότερες partOf [7]τιμές ιδιότητας τύπου AssetCollection για να αναγνωρίσει το γεγονός ότι το συγκεκριμένο asset ανήκει σε μία συλλογή από assets.

Από την άλλη, η AssetCollection έχει τις εξής ιδιότητες:

- Μπορεί να έχει μία source τιμή ιδιότητας τύπου IRI για να παραθέσει το AssetCollection
- Μπορεί να έχει καμία, μία ή περισσότερες refinement τιμές ιδιότητας τύπου Constraint.

[5] Internationalized Resource Identifier (IRI).
[6] Ιδιότητα που χρησιμοποιείται από μία πολιτική για να κληρονομήσει τις ιδιότητες μίας γονικής πολιτικής .
[7] Ιδιότητα που χρησιμοποιείται για αναγνωρίσει ότι ένας πόρος (Asset) ανήκει σε μία AssetCollection.

Party class: Περιέχει μία οντότητα ή μια συλλογή οντοτήτων που αναλαμβάνουν ρόλους σε ένα κανόνα(Rule). Αποτελεί γονική κλάση της PartyCollection κλάσης η οποία εκπροσωπεί μία συλλογή οντοτήτων. Μία Party κλάση έχει τις συγκεκριμένες ιδιότητες:

- Θα ήταν χρήσιμο να έχει μία uid τιμή ιδιότητας τύπου IRI για να αναγνωρίσει το αντίστοιχο Party.
- Μπορεί να έχει καμία, μία ή περισσότερες partOf τιμές ιδιότητας τύπου PartyCollection για να αναγνωρίσει ότι το συγκεκριμένο Party αποτελεί μέρος μία συλλογής από Party.

Από την άλλη, η PartyCollection έχει τις συγκεκριμένες ιδιότητες:

- Μπορεί να έχει μία source τιμή ιδιότητας τύπου IRI για να παραθέσει το PartyCollection.
- Μπορεί να έχει καμία, μία ή περισσότερες refinement τιμές ιδιότητας τύπου Constraint.

Action class: Εκφράζει μία λειτουργία πάνω σε ένα Asset.

Μία action κλάση έχει τις συγκεκριμένες ιδιότητες:

- Μπορεί να έχει καμία, μία ή περισσότερες refinement τιμές ιδιότητας τύπου Constraint που κάνουν πιο ξεκάθαρη την σημασία της συγκεκριμένης Action λειτουργίας.
- Πρέπει να έχει μία includedIn [8] τιμή ιδιότητας τύπου Action όπου μεταβατικά θα διαβεβαιώσει πως η συγκεκριμένη Action λειτουργία περιλαμβάνει την λειτουργική της σημασία. Εξαιρούνται οι περιπτώσεις που η Action έχει ρόλο χρήσης και μεταφοράς (use[9] – transfer[10]).
- Μπορεί να έχει καμία, μία ή περισσότερες implies τιμές ιδιότητας τύπου Action που θα διαβεβαιώσουν ότι η συγκεκριμένη Action δεν απαγορεύεται να ενεργοποιήσει την λειτουργική της σημασία.

Rule class: Αποτελεί γονική κλάση των Permission, Prohibition, Duty υποκλάσεων. Η Permission υποκλάση περιγράφει την δυνατότητα για να εκτελεστεί κάποιο Action πάνω στο Asset.Είναι δυνατόν να περιέχει κάποια ιδιότητα τύπου Duty. Η Prohibition υποκλάση αποκλείει την δυνατότητα να εκτελεστεί κάποιο Action πάνω στο Asset. Η Duty υποκλάση ορίζει την υποχρέωση να εκτελεστεί κάποιο Action πάνω στο Asset.

[8] Ιδιότητα με σκοπό την διαβεβαίωση ότι η σημασία του αναφερόμενου στιγμιότυπου κάποιας Action περιλαμβάνει την σημασία του στιγμιότυπου της Action.

[9] Use: Action υψηλού επιπέδου που περιλαμβάνει το μοντέλο και επιτρέπει την γενική χρήση από Parties.

[10] Transfer: Action υψηλού επιπέδου που περιλαμβάνει το μοντέλο και επιτρέπει την μεταφορά ιδιοκτησίας σε τρίτους.

Μία rule κλάση έχει τις ακόλουθες ιδιότητες:

- Πρέπει να έχει μία action τιμή ιδιότητας τύπου Action.
- Μπορεί να έχει καμία ή μία relation τιμές υπο-ιδιότητας τύπου Asset.
- Μπορεί να έχει καμία, μία ή περισσότερες function[11] τιμές υπο-ιδιότητας τύπου Party.
- Μπορεί να έχει καμία, μία ή περισσότερες failure[12] τιμές υπο-ιδιότητας τύπου Rule.
- Μπορεί να έχει καμία, μία ή περισσότερες constraint τιμές ιδιότητας τύπου Constraint.
- Μπορεί να έχει καμία ή μία uid τιμές ιδιότητας τύπου IRI για να αναγνωρίσει το Rule και να έχει την δυνατότητα να μπορεί να αναφερθεί από άλλα Rules.

Στην ουσία, αφού οι Permission, Prohibition, Duty είναι υποκλάσεις της Rule κλάσης, αυτές κληρονομούν όλες τις ιδιότητες της Rule. Παρόλα αυτά υπάρχουν και κάποιες πρόσθετες ιδιότητες.

Ξεκινώντας με την Permission :

- Πρέπει να έχει μία target τιμή ιδιότητας τύπου Asset .
- Μπορεί να έχει καμία ή μία assigner ή/και assignee τιμές ιδιότητας τύπου Party.
- Μπορεί να έχει καμία, μία ή περισσότερες duty τιμές ιδιότητας τύπου Duty.

Για την Prohibition:

- Πρέπει να έχει μία target τιμή ιδιότητας τύπου Asset.
- Μπορεί να έχει καμία ή μία assigner ή/και assignee τιμές ιδιότητας τύπου Party.
- Μπορεί να έχει καμία, μία ή και περισσότερες remedy τιμές ιδιότητας τύπου Duty.

Για την Duty:

- Μπορεί να έχει καμία ή μία target τιμή ιδιότητας τύπου Asset για να δείξει ότι το Asset είναι το κύριο υποκείμενο που θα εφαρμοστεί το Duty.
- Μπορεί να έχει καμία ή μία assigner ή/και assignee τιμές ιδιότητας τύπου Party.
- Μπορεί να έχει καμία, μία ή περισσότερες consequence τιμές ιδιότητας τύπου Duty μόνο όταν το Duty αναφέρεται από ένα Rule μαζί με τις ιδιότητες του duty.
- Το Party που είναι υποχρεωμένο να ασκήσει το Duty πρέπει να έχει την δυνατότητα να ασκήσει το Duty Action.

[11] Function: Αφηρημένη ιδιότητα που χρησιμοποιείται για να συνδέσει ένα Rule σε ένα Party.

[12] Failure: Αφηρημένη ιδιότητα που εκφράζει τις συνέπειες από την αποτυχία εκπλήρωσης ενός καθήκοντος (Duty) σε μία άδεια (Permission).

- Το Party που είναι υποχρεωμένο να ασκήσει το Duty πρέπει να ικανοποιεί τις συνθήκες του Duty.

Constraint class: Αποτελεί μία λογική (Boolean) έκφραση που βοηθάει στο να κάνει πιο ξεκάθαρη την σημασιολογία ενός Action ή μίας Party/Asset collection. Στην λογική αυτή έκφραση, γίνεται σύγκριση δύο τελεστών μέσω ενός σχεσιακού τελεστή. Αν η συνθήκη είναι αληθής τότε το Constraint ικανοποιείται. Έχει τις ακόλουθες ιδιότητες:

- Μπορεί να έχει καμία ή μία uid τιμή ιδιότητας τύπου IRI για να αναγνωρίσει το Constraint.
- Πρέπει να έχει μία leftOperand τιμή ιδιότητας τύπου LeftOperand.
- Πρέπει να έχει μία operator τιμή ιδιότητας τύπου Operator.
- Πρέπει να έχει είτε μία rightOperand τιμή ιδιότητας τύπου literal(σταθερά) ή IRI ή RightOperand για βασισμένους σε σύνολα τελεστές τύπου λίστες από literals, λίστες από IRIs ή λίστες από RightOperands, είτε μία rightOperandReference τιμή ιδιότητας τύπου IRI ή για βασισμένους σε σύνολα τελεστές τύπου λίστες από IRIs.
- Μπορεί να έχει καμία ή μία datatype τιμή ιδιότητας για τον τύπο δεδομένων του rightOperand/Reference.
- Μπορεί να έχει καμία ή μία unit τιμή ιδιότητας τύπου IRI για να ορίσει τον τύπο του unit που θα χρησιμοποιηθεί για την τιμή του rightOperand/Reference.
- Μπορεί να έχει καμία ή μία status τιμή ιδιότητας για τιμή που έχει δημιουργηθεί από το leftOperand action ή μία τιμή σχετική με το leftOperand για να ορισθεί ως αναφορά για την σύγκριση.

Οι τιμές ιδιότητας leftOperand ορίζονται ως στιγμιότυπα από την leftOperand κλάση. Τα στιγμιότυπα αυτά πρέπει να είναι αυστηρώς καθορισμένα για να ξεκαθαρίσουν την σημασία του leftOperand.

Οι τιμές ιδιότητας Operator ορίζονται ως στιγμιότυπα από την Operator κλάση. Αυτές ορίζουν την σχέση μεταξύ του leftOperand και του rightOperand.

Οι τιμές ιδιότητας rightOperand ορίζονται ως στιγμιότυπα από την rightOperand κλάση ή ως IRIs ή ως απλές τιμές. Αυτές θα συγκριθούν με το leftOperand.

Η rightOperandReference τιμή είναι ένα IRI το οποίο θα χρειαστεί να ‘‘χάσει’’ την αναφορά του για να λάβει την τιμή του rightOperand.

Η datatype δείχνει το τύπο του rightOperand/Reference και η unit δείχνει την τιμή unit του rightOperand/Reference. Για παράδειγμα datatype: xsd:decimal και unit: EU Currency, όπου εδώ ο

τύπος του rightOperand/Reference είναι δεκαδικός και το unit αναφέρεται στο Ευρώ (Νόμισμα Ευρωπαϊκής Ένωσης).

Ενότητα 3.1.β Παραδείγματα

Τα παρακάτω αποτελούν παραδείγματα ODRL πολιτικών που έχουν παραχθεί σε JSON-LD [10]. Παρόλα αυτά, είναι δυνατόν να παραχθούν πολιτικές ODRL σε RDF και XML επίσης.

Για το σχήμα 2, έχουμε έναν assigner:"http://example.com/org:xyz" ο οποίος αναθέτει το δικαίωμα αναπαραγωγής("play") του πόρου Asset : http://example.com/game:9090 μέχρι το τέλος του έτους 2017. Οπότε έχουμε μία πολιτική Offer που παραχωρεί άδεια("Permission").

Για το σχήμα 3, έχουμε έναν assigner: http://example.com/MyPix:55 ο οποίος αναθέτει το δικαίωμα προβολής("display") του Asset : http://example.com/photoAlbum:55 και ταυτόχρονα απαγορεύει στον assignee: http://example.com/assignee:55 την αρχειοθέτηση του. Άρα εδώ έχουμε μία Agreement που παραχωρεί μία άδεια("Permission") αλλά και απαγόρευση("Prohibition") ταυτόχρονα.

Για το σχήμα 4, έχουμε έναν assigner: http://example.com/org:43 ο οποίος αναθέτει την υποχρέωση στο assignee: http://example.com/person:44 της αποζημίωσης του με το ποσό των 500 ευρώ. Οπότε έχουμε μία πολιτική Agreement που επιβάλλει μία υποχρέωση("Duty").

```
{
   "@context": "http://www.w3.org/ns/odrl.jsonld",
   "@type": "Offer",
   "uid": "http://example.com/policy:9090",
   "profile": "http://example.com/odrl:profile:07",
   "permission": [{
       "target": "http://example.com/game:9090",
       "assigner": "http://example.com/org:xyz",
       "action": "play",
       "constraint": [{
           "leftOperand": "dateTime",
           "operator": "lteq",
           "rightOperand": { "@value": "2017-12-31", "@type": "xsd:date" }
       }]
   }]
}
```

Σχήμα 2: Παράδειγμα μίας άδειας(permission).

```
{
    "@context": "http://www.w3.org/ns/odrl.jsonld",
    "@type": "Agreement",
    "uid": "http://example.com/policy:5555",
    "profile": "http://example.com/odrl:profile:08",
    "conflict": "perm",
    "permission": [{
        "target": "http://example.com/photoAlbum:55",
        "action": "display",
        "assigner": "http://example.com/MyPix:55",
        "assignee": "http://example.com/assignee:55"
    }],
    "prohibition": [{
        "target": "http://example.com/photoAlbum:55",
        "action": "archive",
        "assigner": "http://example.com/MyPix:55",
        "assignee": "http://example.com/assignee:55"
    }]
}
```

Σχήμα 3: Παράδειγμα μίας απαγόρευσης(prohibition).

```
{
  "@context": "http://www.w3.org/ns/odrl.jsonld",
  "@type": "Agreement",
  "uid": "http://example.com/policy:42",
  "profile": "http://example.com/odrl:profile:09",
  "obligation": [{
      "assigner": "http://example.com/org:43",
      "assignee": "http://example.com/person:44",
      "action": [{
          "rdf:value": {
            "@id": "odrl:compensate"
          },
          "refinement": [
            {
              "leftOperand": "payAmount",
              "operator": "eq",
              "rightOperand": { "@value": "500.00", "@type": "xsd:decimal" },
              "unit": "http://dbpedia.org/resource/Euro"
            }]
        }]
    }]
}
```

Σχήμα 4: Παράδειγμα ενός καθήκοντος(duty).

Υποκεφάλαιο 3.2 MPEG REL

Η MPEG-21 Rights Expression Language [11] ή εν συντομία η MPEG REL είναι μία δηλωτική[13] γλώσσα βασισμένη κυρίως στην XML(eXtensible Markup Language) η οποία αποσκοπεί στην παροχή μηχανισμών για την χρήση και κατανάλωση ψηφιακού περιεχομένου προστατεύοντας ταυτόχρονα το περιεχόμενο, τα δικαιώματα των δημιουργών και λοιπές συνθήκες που συμπεριλαμβάνονται στο περιεχόμενο. Το περιεχόμενο μπορεί να είναι κάθε είδους δημιουργία σε ψηφιακή μορφή. Η συγκεκριμένη γλώσσα έχει ξεκάθαρη σημασιολογία και αυστηρά καθορισμένο συντακτικό, γεγονός που την καθιστά κατάλληλη στην υποστήριξη λειτουργιών χρήσης, διαμοιρασμού ευαίσθητων πληροφοριών ή και στην επιβολή χρέωσης για την χρήση του περιεχομένου.

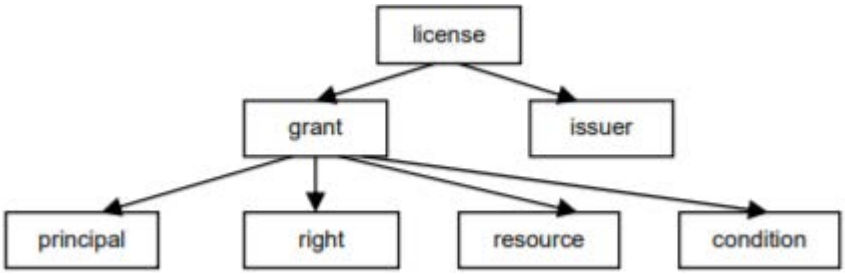
Ταυτόχρονα, η γλώσσα πέραν της βιομηχανίας, μπορεί να εφαρμοστεί επίσης και σε ιδιώτες οι οποίοι μέσω των ιδιοτήτων της MPEG REL μπορούν να καθορίσουν το μέλλον των προσωπικών τους δεδομένων, δηλαδή εάν τα δεδομένα τους θα υποστούν χρήση, επεξεργασία, διαμοιρασμό. Οπότε, με αυτό το τρόπο μπορεί να εξασφαλιστεί και η ιδιωτικότητα των καταναλωτών.

Ουσιαστικά, με την MPEG REL ένας δημιουργός ή ιδιοκτήτης ψηφιακού περιεχομένου μπορεί για το περιεχόμενο του να εξουσιοδοτεί συγκεκριμένα δικαιώματα σε κάποιο εντολέα. Αυτό επιτυγχάνεται με το μοντέλο δεδομένων της γλώσσας το οποίο δείχνει τις σχέσεις μεταξύ των στοιχείων που το αποτελούν με σκοπό να παραχθεί μία άδεια. Ένα τέτοιο βασικό μοντέλο αποτελείται από τα εξής στοιχεία: **license, grant, issuer, principal, right, resource, condition.**

- **license**: Περιέχει όλα τα παραπάνω τα οποία τα ορίζει ένας ή περισσότεροι εκδότες(issuers).
- **issuer**: Το στοιχείο που αναγνωρίζει ένα εντολέα ο οποίος εκδίδει μία άδεια. Είναι δυνατόν ο εκδότης(issuer) να διαθέτει μία ψηφιακή υπογραφή της άδειας υπογεγραμμένη από τον εντολέα για να τεκμηριώσει την εμπιστοσύνη μεταξύ εκδότη και εντολέα για την παροχή δικαιωμάτων της άδειας.
- **grant**: Στοιχείο το οποίο παρέχει συγκεκριμένα δικαιώματα σε ένα εντολέα.
- **principal**: Στοιχείο που βρίσκεται μέσα στο grant και εγκιβωτίζει την ταυτότητα όσων έχουν λάβει δικαιώματα.
- **right**: Στοιχείο που λαμβάνει ο εντολέας το οποίο συνεπάγεται με το δικαίωμα του να πράξει συγκεκριμένες ενέργειες κάτω από προϋποθέσεις.
- **resource:** Στοιχείο που αποτελεί τον πόρο στο οποίο ο εντολέας αποκτά δικαιώματα.

[13] Δηλωτική γλώσσα προγραμματισμού: Η γλώσσα όπου ο προγραμματιστής καθορίζει το στόχο που θέλει να επιτευχθεί και όχι το πως αυτός θα επιτευχθεί. [20]

- **condition**: Ορίζει του όρους, προϋποθέσεις και τις υποχρεώσεις με τους οποίους θα εκτελεστεί το κάθε δικαίωμα(right).



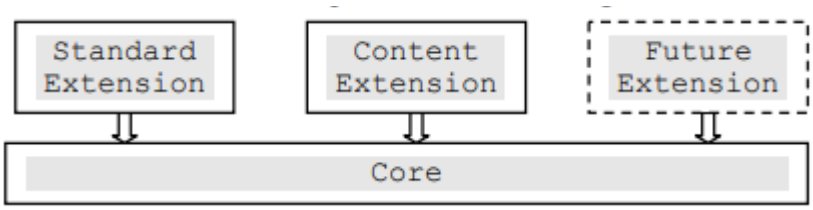
Σχήμα 5: Βασικό μοντέλο δεδομένων αδειών της MPEG REL.

Ενότητα 3.2.α Επεκτάσεις

Η δομή των επεκτάσεων της MPEG REL οργανώνεται στα εξής μέρη: **core, standard, content-multimedia .** Είναι σημαντικό να αναφερθεί πως αυτή η δυνατότητα για επέκταση οφείλεται στο ότι η γλώσσα συντακτικά βασίζεται στο XML Schema [12] και στους XML Namespaces [13] μηχανισμούς.

- **core επέκταση:** Διαμορφώνει την αρχιτεκτονική βάση της γλώσσας ορίζοντας τις γενικές δομές της.
- **standard επέκταση**: Ορίζει τις βασικές δομές της γλώσσας για την επίτευξη της διαχείρισης ψηφιακών δικαιωμάτων.
- **content-multimedia επέκταση**: Ορίζει τις δομές της γλώσσας για την επίτευξη της διαχείρισης ψηφιακών δικαιωμάτων που σχετίζονται με κάποιο ψηφιακό περιεχόμενο.

Ταυτόχρονα, στην γλώσσα υποστηρίζεται η προσθήκη μελλοντικών επεκτάσεων, όπου οι ιδιώτες ή οι επιχειρήσεις, με τους κατάλληλους προσδιορισμούς θα μπορούν να ορίζουν κάποιον διαφορετικό τύπο αδειών που θα παράγει η MPEG REL χωρίς να χρησιμοποιούν τις βασικές επεκτάσεις της γλώσσας .



Σχήμα 6: Δομή επεκτάσεων της MPEG REL.

Ενότητα 3.2.β Τύποι αδειών

Οι πιο συχνοί τύποι αδειών για την ανάλογη μεταχείριση του ψηφιακού περιεχομένου που παράγει η MPEG REL είναι οι: **usage, distribution, offer, certificate, revocation**.

Αναλυτικότερα,
η **usage** άδεια δηλώνει ότι ο εκδότης(issuer) πιστοποιεί σε κάποιον εντολέα(principal) συγκεκριμένα δικαιώματα χρήσης του ψηφιακού περιεχομένου.

η **distribution** άδεια δηλώνει ότι κάποιος εντολέας ικανοποιώντας συγκεκριμένες συνθήκες, μπορεί να ορίσει δικαιώματα στο περιεχόμενο και σε άλλους εντολείς.

η **offer** άδεια δηλώνει την απόκτηση ορισμένων δικαιωμάτων στο περιεχόμενο από τον εντολέα εάν εκείνος πληροί συγκεκριμένες προϋποθέσεις .

η **certificate** άδεια δηλώνει τον ισχυρισμό ενός εκδότη ότι κάποιος εντολέας έχει ως ‘’ιδιοκτησία’’ του ορισμένες ιδιότητες σχετικά με το περιεχόμενο.

η **revocation** άδεια δηλώνει το δικαίωμα του εκδότη να ακυρώσει την άδεια που έχει εκδώσει οποιαδήποτε στιγμή.

Ενότητα 3.3.γ Παραδείγματα αδειών MPEG REL

Παρατηρώντας τα παρακάτω παραδείγματα από μερικές από τις κατηγορίες αδειών της MPEG REL, στο σχήμα 7, έχουμε μία Distribution άδεια όπου φαίνεται ότι στο οργανισμό ACMEmusicwarehouse έχει παραχωρηθεί η άδεια να μπορεί να εκδίδει σε άλλους εντολείς το δικαίωμα για αναπαραγωγή του τραγουδιού whenTheThistleBlooms.mp3 για τρεις εβδομάδες εφόσον η ACMwarehouse πληρώνει το τέλος των 3$ για κάθε παραχώρηση δικαιώματος που εκτελεί.

Στο σχήμα 8, έχουμε μία Offer άδεια όπου γίνεται μία ‘’πρόταση’’ στην Alice για το δικαίωμα για αναπαραγωγή του τραγουδιού whenTheThistleBlooms.mp3 για τρεις εβδομάδες εάν εκείνη πληρώσει το τέλος των 3$.

Τέλος, στο σχήμα 9 έχουμε μία Certificate άδεια όπου ο εκδότης της άδειας πιστοποιεί πως η Alice είναι μέλος ενός music club.

Στα παρακάτω παραδείγματα ο εκδότης των αδειών είναι ο PDQ Records.

```
license
    grant
        ACMEmusicwarehouse
        issue
        grant
            anyone
            play
            whenTheThistleBlooms.mp3
            for 3 weeks
        fee $3
    issuer
        PDQ Records
```

Σχήμα 7: Distribution άδεια.

```
license
    grant
        Alice
        obtain
        grant
            Alice
            play
            whenTheThistleBlooms.mp3
            for 3 weeks
        fee $4
    issuer
        PDQ Records
```

Σχήμα 8: Offer άδεια.

```
license
    grant
        Alice
        possesProperty
        musicClubMembership
    issuer
        PDQ Records
```

Σχήμα 9: Certificate άδεια.

Υποκεφάλαιο 3.3 ccREL

Η Creative Commons Rights Expression Language (ccREL) [14], αποτελεί ένα πρότυπο που συνιστά ο οργανισμός Creative Commons (CC) για την παραγωγή αδειών πνευματικής ιδιοκτησίας σε μορφή αναγνώσιμη από την μηχανή. Πριν αναλυθεί η ccREL, σημαντικό θα ήταν να γίνει μία αναδρομή στο παρελθόν, στις αρχές του 21ου αιώνα όπου και ιδρύθηκε ο CC με κύριο στόχο την προώθηση και προστασία των πνευματικών δικαιωμάτων στο Διαδίκτυο που εκείνη την εποχή δεν υπήρχε τρόπος διαχείρισής τους. Ο CC για να δώσει λύση στο συγκεκριμένο πρόβλημα κλήθηκε να αντιμετωπίσει ένα κοινωνικό και νομικό ζήτημα, την δημιουργία αδειών πνευματικής ιδιοκτησίας για χρήση και διαμοιρασμό με συγκεκριμένους περιορισμούς σε αναγνώσιμη μορφή για τους ανθρώπους αλλά και το ζήτημα της χρήσης δικτύων τα οποία θα δημιουργούσαν επαναχρησιμοποιούμενες και εύκολες στην εύρεση τους άδειες. Τα παραπάνω θα έπρεπε να αυτοματοποιηθούν με την χρήση σχετικών προγραμμάτων η οποία θα γεφύρωνε αποδοτικά την αλληλεπίδραση ανθρώπου-μηχανής πάνω στο ζήτημα της αναγνώρισης και έκδοσης αδειών πνευματικής ιδιοκτησίας.

Ενότητα 3.3.α RDF

Η ccREL βασίζεται στο World-Wide Web Consortium's Resource Description Framework (RDF) [15] που αποτελεί μέρος της W3C Semantic Web Activity.

Ο βασικός λόγος που επιλέγεται το RDF είναι η διαλειτουργικότητα που προσφέρει, η οποία κάνει πιο εύκολη την συνεργασία, επιτυγχάνοντας έτσι τον κύριο στόχο του CC, δηλαδή την επίτευξη της συνεργασίας μεταξύ των δημιουργών στην προώθηση και στο διαμοιρασμό των έργων τους . Ο όρος διαλειτουργικότητα αφορά το επίπεδο μηχανής, στο οποίο η πληροφορία, η σημασία των δεδομένων και οι ιδιότητες τους θα πρέπει να λειτουργούν διαλειτουργικά καθώς και τα σύνολα των σχετικών ιδιοτήτων να μπορούν να εξελίσσονται. Η RDF, επιτρέπει την προσθήκη επεκτάσεων, όπως την προσθήκη νέων ιδιοτήτων χωρίς να επηρεαστεί η λειτουργία του υπάρχοντος προγράμματος .

Η RDF χρησιμοποιείται στην περιγραφή οντοτήτων στο παγκόσμιο Ιστό. Κάθε οντότητα παίρνει ονομασία με το URL(Universal Resource Locator) και την γενίκευση του, το URI(Universal Resource Identifier).

Κάθε ατομική περιγραφή οντότητας RDF στη ccREL ονομάζεται τριπλέτα(triples) η οποία αποτελείται από ένα υποκείμενο(subject), μία ιδιότητα(property) και μία τιμή(value). Ουσιαστικά, κάθε τριπλέτα περιγράφει την σχετική άδεια που έχει παραχθεί. Το υποκείμενο είναι ένα URL που αντιστοιχεί στην ιστοσελίδα για την οποία έχει δημιουργηθεί άδεια. Η τιμή είναι το URL της άδειας και η ιδιότητα είναι το URL της σημασίας της άδειας. Είναι σημαντικό να αναφερθεί πως στην RDF, μία τριπλέτα μπορεί να αναπαρασταθεί με μορφή γράφων όπου είναι δυνατόν να φανούν οι σχέσεις μεταξύ των στοιχείων που τους αποτελούν. Κάθε ακμή και κορυφή του γράφου αντιστοιχεί σε URI's.

Ενότητα 3.3.β Αφηρημένο μοντέλο ccREL

Το αφηρημένο μοντέλο ccREL αποτελεί ένα αφηρημένο προσδιορισμό της ccREL, δηλαδή χωρίς κάποιο συγκεκριμένο συντακτικό. Κάθε αντικείμενο στο οποίο έχει δοθεί άδεια περιέχει ένα μικρό σύνολο επεκτάσιμων ιδιοτήτων RDF. Οι ιδιότητες αυτές χωρίζονται σε δύο κατηγορίες:

- τις ιδιότητες έργου (work properties) που περιγράφουν τις πτυχές από συγκεκριμένα έργα(works).
- τις ιδιότητες άδειας (license properties) που περιγράφουν τις πτυχές των αδειών(licenses).

Αναλυτικότερα, κάποιος ο οποίος θέλει να εκδώσει μία άδεια για κάποιο έργο θα πρέπει να παρέχει τουλάχιστον μία RDF τριπλέτα.

```
<http://lessig.org/blog/>
      xhtml:license
      <http://creativecommons.org/licenses/by/3.0/> .
```

Σχήμα 10: Βασική RDF τριπλέτα.

Η παραπάνω τριπλέτα αποτελείται από το URL του προσωπικού blog του Lawrence Lessig : http://lessig.org/blog που αποτελεί το υποκείμενο(subject) της άδειας, το xhtml:license είναι μία συντομογραφία του http://www.w3.org/1999/ xhtml/vocab# που αποτελεί το URL της άδειας που πρόκειται να εκδοθεί και τέλος το http://creativecommons.org/licenses/by/3.0 που είναι το URL το οποίο περιγράφει τη σημασία της άδειας που πρόκειται να εκδοθεί.

Όπως προαναφέρθηκε, αυτή η τριπλέτα είναι η ελάχιστη πληροφορία που πρέπει να παρέχει ο εκδότης για να ορίσει την work ιδιότητα(property).Παρόλα αυτά, ο CC προτείνει στους εκδότες να παρέχουν επιπλέον τριπλέτες. Το παρακάτω είναι ένα σχετικό παράδειγμα:

```
<http://lessig.org/blog/> dc:title "The Lessig Blog" .
<http://lessig.org/blog/> cc:attributionName "Larry Lessig" .
<http://lessig.org/blog/> cc:attributionURL <http://lessig.org/> .
<http://lessig.org/blog/> dc:type dcmitype:Text .
```

Σχήμα 11: Λεπτομερής RDF τριπλέτα.

Οι συγκεκριμένες ιδιότητες έργου ορίζονται ως:

- **dc[14]: title** που αφορά τον τίτλο του εγγράφου για το οποίο θα εκδοθεί άδεια.
- **cc[15]: attributeName** που αφορά το όνομα στο οποίο θα γίνει παράθεση όταν το έργο τροποποιηθεί ή διαμοιρασθεί.
- **cc: attributionURL** που αφορά το URL στο σύνδεσμο(link) όταν υπάρξει σχετική τροποποίηση ή διαμοιρασμός του έργου.
- **dc:type** που αφορά τον τύπο του αδειοδοτημένου εγγράφου.

Επίσης, υπάρχουν ακόμα δύο ιδιότητες έργου όπως η dc:source η οποία παρέχει ένα URI που δείχνει την αρχική πηγή του έργου που πρόκειται να τροποποιηθεί και η cc:morePermissions που παρέχει ένα URL με πληροφορίες σχετικά με επιπρόσθετες αποδοχές(Permissions) πέρα από εκείνες που επιτρέπει η CC άδεια, αφορά δηλαδή επιπλέον άδειες που μπορεί να ορίσει ο δημιουργός του έργου και να τις παραχωρήσει σε όποιον θέλει να τροποποιήσει ή να διαμοιραστεί το έργο του.

[14] dc: Συντομογραφία για το λεξιλόγιο Dublin Core που συντηρείται από την Dublin Core Metadata Initiative.

[15] cc: Συντομογραφία για το οργανισμό Creative Commons, όπου ορίζει τους όρους της σχετικής άδειας.

Στην ουσία, οι παραπάνω ιδιότητες έργου αφορούν τους εκδότες οι οποίοι περιγράφουν τους όρους αδειοδότησης του έργου.

Όσον αφορά τις ιδιότητες άδειας, αυτές ορίζονται από τον CC και δεν αναμένεται κάποια αντιμετώπιση από τους εκδότες. Επίσης, ο CC δεν επιτρέπει σε τρίτους να τροποποιούν τις συγκεκριμένες ιδιότητες οπότε οι εκδότες θα χρειαστεί να δημιουργούν δικές τους άδειες βασιζόμενοι σε αυτές τις ιδιότητες που ορίζει ο CC.

Οι συγκεκριμένες ιδιότητες άδειας είναι οι εξής:

- **cc:permits,** η οποία επιτρέπει την χρήση του συγκεκριμένου έργου πέρα από τι ορίζει η σχετική νομοθεσία πνευματικών δικαιωμάτων . Οι πιθανές τιμές που μπορεί να χορηγήσει μία CC άδεια στην cc:permits είναι η cc:Reproduction που επιτρέπει την αντιγραφή του έργου σε ποικίλες μορφές, η cc:Distribution που επιτρέπει την διανομή του έργου και η cc:DerivativeWorks που επιτρέπει την δημιουργία παράγωγων έργων από το αρχικό έργο.
- **cc:prohibits**, η οποία απαγορεύει την χρήση του συγκεκριμένου έργου χωρίς να επηρεάζεται η σχετική νομοθεσία πνευματικών δικαιωμάτων. Η πιθανή τιμή που μπορεί να χορηγήσει μία CC άδεια στην cc:prohibits είναι η cc:CommercialUse που απαγορεύει την εμπορική χρήση του έργου.
- **cc:requires**, η οποία απαιτεί από τον χρήστη συγκεκριμένες δράσεις ακολουθώντας το τι επιτρέπεται από την cc:permits. Οι πιθανές τιμές που μπορεί να χορηγήσει μία CC άδεια στην cc:requires είναι η cc:Notice που παρέχει την ένδειξη της άδειας του έργου, η cc:Attribution η οποία αποδίδει τα εύσημα στο δημιουργό, η cc:ShareAlike η οποία μοιράζει την ίδια άδεια σε παράγωγα έργα του αρχικού κατά την αναδιανομή τους και η cc:SourceCode που παρέχει τον πηγαίο κώδικα κατά την αναδιανομή του έργου.

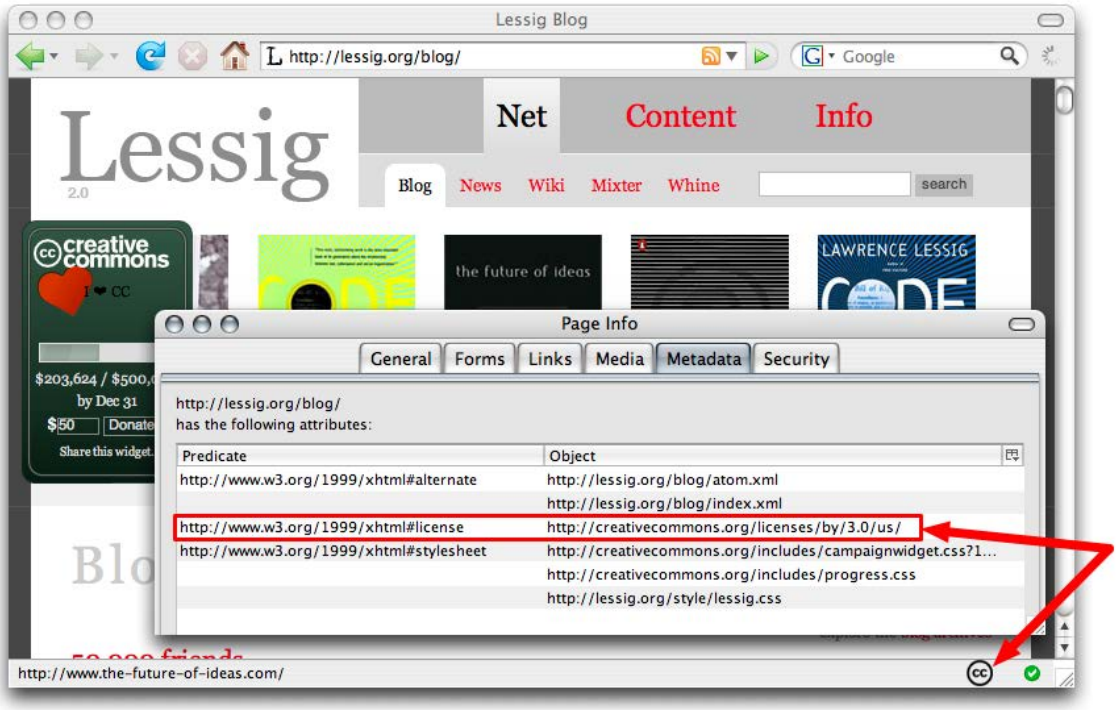
- **cc:jurisdiction**, η οποία συσχετίζει την άδεια με μία συγκεκριμένη νομική δικαιοδοσία.
- **cc:deprecatedOn**, η οποία δείχνει την ημερομηνία που η συγκεκριμένη άδεια αποσύρθηκε.
- **cc:legalCode**, η οποία παραθέτει το αντίστοιχο νομικό κείμενο της άδειας.

Ενότητα 3.3.γ Παραδείγματα

Παρακάτω φαίνονται κάποια παραδείγματα – πραγματικές υλοποιήσεις της ccREL.

Σχήμα 12: Σήμανση RDFa σε απόσπασμα από το άρθρο δημοσιευμένο στην Nature Proceedings, όπου φαίνεται η αντίστοιχη Creative Commons άδεια και οι RDF τριπλέτες.

Σχήμα 13: Σήμανση RDFa μίας ενημέρωσης για άδεια Creative Commons.



Σχήμα 14: MozCC Add-On-Επέκταση στο φυλλομετρητή(browser) Mozilla Firefox η οποία δείχνει εάν η ιστοσελίδα έχει αδειοδοτηθεί από την Creative Commons, όπου με το «κλικ» στο εικονίδιο «CC» ανοίγει νέο παράθυρο με τις σχετικές πληροφορίες για την άδεια.

Σημείωση: *Τα Σχήματα 1-4 πάρθηκαν από την ιστοσελίδα https://www.w3.org/TR/odrl-model/ .*
Τα Σχήματα 5-9 πάρθηκαν από το άρθρο των X. Wang, T. DeMartini, B. Wragg, M. Paramasivam και C. Barlas (2005).
Τα Σχήματα 10-14 πάρθηκαν από το άρθρο των H. Abelson, B. Adida, M. Linksvayer και N. Yergler (2008).
Για περισσότερες λεπτομέρειες ανατρέξτε στην βιβλιογραφία.

ΚΕΦΑΛΑΙΟ 4 Σύστημα

Ενότητα 4.1 Περίπτωση χρήσης και απαιτήσεις

Η βασικότερη **περίπτωση χρήσης** του συγκεκριμένου συστήματος είναι η μετατροπή προτιμήσεων ιδιωτικότητας των υποκειμένων των δεδομένων για μία ορισμένη οντότητα δεδομένων (data asset) σε ODRL προτιμήσεις ιδιωτικότητας.

Όπως ακριβώς ορίζει το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (National Institute of Standards and Technology, NIST) των Η.Π.Α [16] μία οντότητα δεδομένων μπορεί να είναι ένας φάκελος, μία βάση δεδομένων, ένα έγγραφο ή ακόμα και μία ιστοσελίδα.

Όσον αφορά τις προτιμήσεις ιδιωτικότητας, μία τέτοια προτίμηση εκφράζει τους όρους που θέτουν τα υποκείμενα των δεδομένων σε ό,τι αφορά την ιδιωτικότητα τους. Για παράδειγμα, εκείνοι μπορούν να επιτρέπουν ή να απαγορεύουν την χρήση, το διαμοιρασμό ή και την επεξεργασία των προσωπικών τους δεδομένων και με αυτόν τον τρόπο ορίζουν οι ίδιοι την ιδιωτικότητα τους μέσα στο σύστημα.

Πιο συγκεκριμένα, με βάση τις προτιμήσεις των υποκειμένων των δεδομένων γίνεται μία κατηγοριοποίηση σε Permission, Prohibition, Duty δηλαδή Άδεια, Απαγόρευση και Υποχρέωση όπως ορίζει η Open Digital Rights Language (ODRL).

Για την περίπτωση της άδειας(Permission), μπορούμε να ορίσουμε μία προτίμηση ιδιωτικότητας που δίνει το υποκείμενο δεδομένων όπως η : “Allow use of data if member : staff”, όπου το υποκείμενο δεδομένων επιτρέπει την χρήση των δεδομένων του εάν μέσα στο σύστημα, για το ορισμένο data asset οι members ανήκουν στην κατηγορία του προσωπικού(staff).

Ομοίως και για την περίπτωση της Prohibition(απαγόρευσης), μπορούμε να ορίσουμε μία προτίμηση ιδιωτικότητας όπως η : “Deny distribution of data if assignee : student”, όπου το υποκείμενο δεδομένων απαγορεύει τον διαμοιρασμό των δεδομένων του εάν ο assignee(εκδοχέας) ανήκει στην κατηγορία των φοιτητών(student).

Τέλος, για την περίπτωση της Duty(υποχρέωση), μπορούμε να ορίσουμε μία προτίμηση ιδιωτικότητας όπως η : “Must delete data if account : closed”, όπου το υποκείμενο δεδομένων υποχρεώνει την διαγραφή των δεδομένων του αν ο λογαριασμός του πλέον έχει κλείσει.

Με τα παραπάνω λοιπόν, γίνεται αντιληπτό ότι οι προτιμήσεις ιδιωτικότητας που ορίζει το κάθε υποκείμενο δεδομένων μπορεί να είναι εκατοντάδες και να καλύπτουν κάθε επιθυμία του υποκειμένου σε ό,τι αφορά την ιδιωτικότητα του.

Για το σύστημα, ορίζονται οι εξής **απαιτήσεις** :

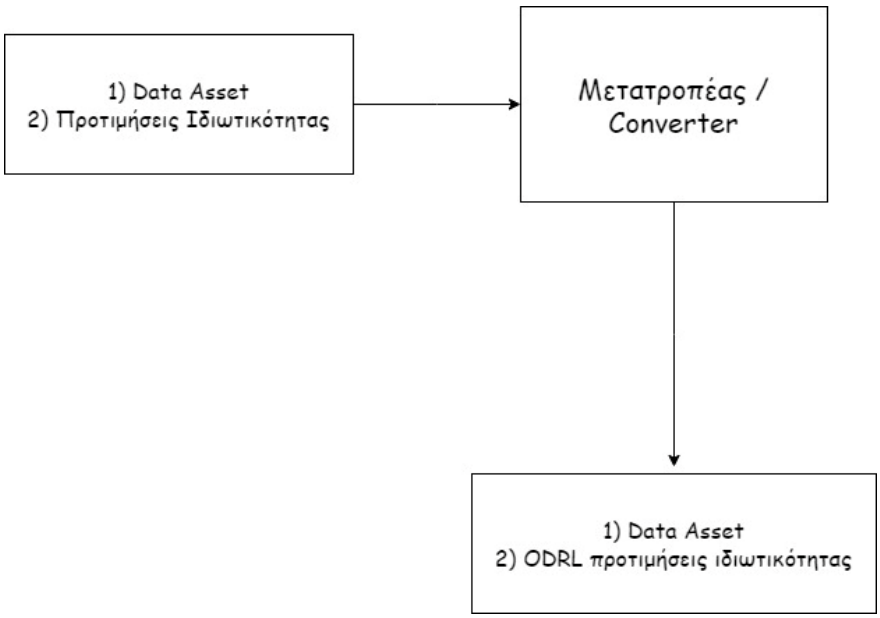
Το σύστημα πρέπει να επιτρέπει στα υποκείμενα δεδομένων να προδιαγράφουν το data asset και τις προτιμήσεις ιδιωτικότητας τους. Επειδή οι προτιμήσεις αυτές μπορεί να είναι ποικιλόμορφες, το σύστημα θα πρέπει να τις αναγνωρίζει και να τις αντιστοιχεί στην σχετική ODRL λειτουργία, όπου και αργότερα θα τις μετατρέψει σε ODRL προτιμήσεις. Σε αυτό το σημείο θα πρέπει να γίνει μία πρακτική υλοποίηση όπου θα επιτρέπει την προσθήκη μελλοντικών τροποποιήσεων ή και επεκτάσεων σε ό,τι αφορά την μετατροπή αυτή.

Επίσης, το σύστημα πρέπει να χρησιμοποιεί το XML Schema (XSD), το οποίο ορίζει την δομή, τους τύπους δεδομένων και τα στοιχεία που θα χρησιμοποιηθούν με βάση τα πρότυπα που ορίζει η ODRL.

Τέλος, το σύστημα πρέπει να είναι πρακτικό, γρήγορο και να μην καταναλώνει αρκετούς υπολογιστικούς πόρους καθώς εκείνο αργότερα μπορεί να λειτουργήσει σε μεγαλύτερη κλίμακα αποτελώντας μέρος ενός άλλου συστήματος.

Ενότητα 4.2 Αρχιτεκτονική συστήματος

Το παρακάτω σχεδιάγραμμα φανερώνει την αρχιτεκτονική του συστήματος:



Σχήμα 15: Γενική δομή του συστήματος.

Στην ουσία, το σύστημα οργανώνεται σε ένα «μετατροπέα(converter)" ο οποίος λαμβάνει από το υποκείμενο των δεδομένων το data asset και τις προτιμήσεις ιδιωτικότητας του, με σκοπό την μετατροπή των προτιμήσεων εκείνων σε ODRL προτιμήσεις ιδιωτικότητας καθώς και την εξαγωγή τους σε XML μορφή. Τα παραπάνω υλοποιήθηκαν σε γλώσσα προγραμματισμού Java με την εξής διαδικασία:

Αρχικά, έγινε η εγκατάσταση και χρήση του JAXB (Java™ Architecture for XML Binding) [17] όπου η συγκεκριμένη αρχιτεκτονική μας επιτρέπει την αντιστοίχιση XML περιεχομένου σε κλάσεις Java αλλά και το αντίστροφο, δηλαδή την αντιστοίχιση Java κλάσεων σε XML περιεχόμενο.

Με την χρήση του JAXB είναι δυνατή η δημιουργία των αντίστοιχων κλάσεων σε Java που ορίζει η ODRL από το XML Schema (XSD) της.

Στην συνέχεια, πριν την δημιουργία των κατάλληλων αντικειμένων που εκπροσωπούν τα Permission, Prohibition, Duty γίνεται το λεγόμενο String Parsing ή αλλιώς Ανάλυση Αλφαριθμητικών που ορίζει ο το υποκείμενο των δεδομένων, όσον αφορά τις προτιμήσεις ιδιωτικότητας του. Δηλαδή, με βάση τις προτιμήσεις που εισάγει το υποκείμενο, το σύστημα θα πρέπει να αναγνωρίσει το είδος της πολιτικής και τα στοιχεία που την αποτελούν.

Στην συγκεκριμένη ανάλυση, ορίζουμε το “if” ως λέξη διαχωριστής. Ο τρόπος που θα ορίσει το υποκείμενο των δεδομένων τις προτιμήσεις του θα είναι τέτοιος έτσι ώστε μετά το “if” θα υπάρχει ο περιορισμός(constraint) που εκείνος ορίζει. Ο περιορισμός αυτός αποτελείται από το leftOperand, operator και rightOperand. Ταυτόχρονα, πριν το “if” ορίζουμε το ruleType το οποίο αποτελεί την κύρια δράση της προτίμησης αυτής.

Για παράδειγμα η προτίμηση του υποκειμένου: “Allow use of data if member : staff ”, δίνει με διαχωριστή το “if”, leftOperand: member, rightOperand : staff και operator “:” ενώ το ruleType είναι “use”.

Όσον αφορά το operator εκπροσωπεί τους τελεστές και στο σύστημα έχει προνοηθεί η εισαγωγή κάποιας προτίμησης ιδιωτικότητας που μπορεί να περιέχει τους τελεστές “:,=,<,>,!=”.

Τέλος, η πρώτη λέξη της προτίμησης που θα δοθεί, θα αφορά την κατηγορία πολιτικής που θα δημιουργηθεί. Έχουν ορισθεί συγκεκριμένες λέξεις-κλειδιά που παραπέμπουν στην ανάλογη πολιτική. Πχ Αν δοθεί η λέξη “allow”, ”permit” τότε έχουμε άδεια(Permission). Αν δοθεί η λέξη “prohibit”, ”deny”, ”restrict” τότε έχουμε απαγόρευση(Prohibition). Από την άλλη αν δοθεί η λέξη “do”, ”require”, ”must” τότε έχουμε υποχρέωση(Duty).

Για να παραχθεί η XML μορφή των πλέον ODRL προτιμήσεων ιδιωτικότητας θα πρέπει να γίνει το λεγόμενο XML Serialization με την βοήθεια του JAXB, ελέγχοντας ταυτόχρονα και την περίπτωση που υπάρξουν σφάλματα(exceptions) κατά την διάρκεια αυτής της μετατροπής.

Παρακάτω, στο Σχήμα 16: Διάγραμμα κλάσεων συστήματος, φαίνεται το διάγραμμα των κλάσεων που υλοποιούνται στο σύστημα. Σε αυτό διακρίνονται τα πεδία των κλάσεων, οι ειδικές μέθοδοι για την αρχικοποίηση των αντικειμένων των κλάσεων διαφορετικά γνωστοί ως constructors, οι ιδιότητες των κλάσεων, άλλες εσωτερικές κλάσεις και οι εξαρτήσεις των κλάσεων μεταξύ τους.

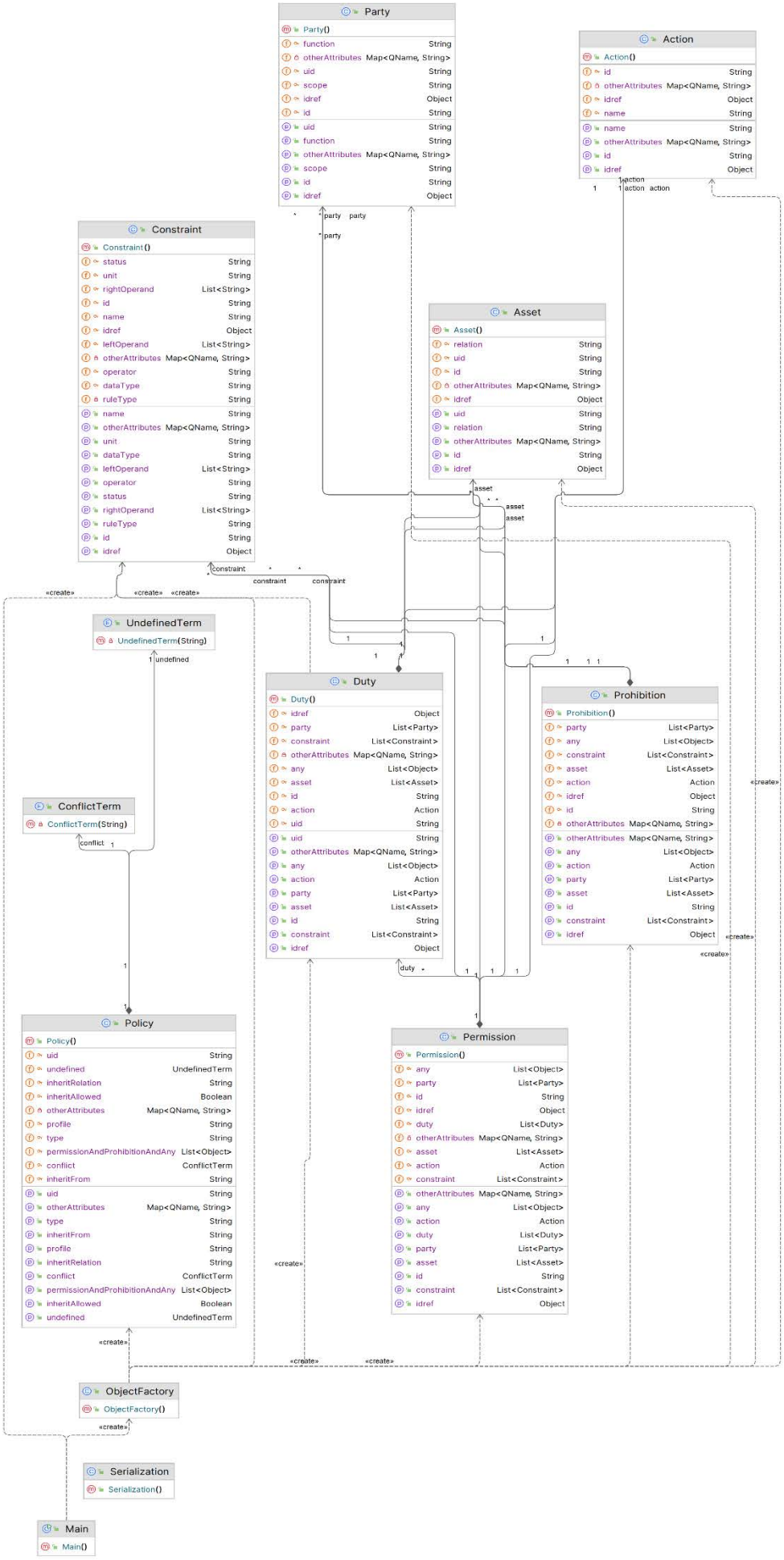
Το διάγραμμα αποτελείται από τις κλάσεις Permission, Prohibition, Duty, Constraint, Party, Action, Asset, UndefinedTerm, ConflictTerm, ObjectFactory, Serialization, Main.

Οι προαναφερθείσες κλάσεις πλην των ObjectFactory, Serialization, Main λειτουργούν όπως ακριβώς ορίζει το Μοντέλο Πληροφοριών της ODRL.

Η **ObjectFactory**, είναι κλάση που δημιουργείται από το JAXB και παρέχει τις κατάλληλες μεθόδους για την δημιουργία των αντικειμένων των κλάσεων.

Η **Serialization**, είναι κλάση που αναλαμβάνει την μετατροπή των αντικειμένων σε XML μορφότυπο και το αντίστροφο.

Η **Main**, είναι η κύρια κλάση που ρυθμίζει όλες τις λειτουργίες του συστήματος χρησιμοποιώντας κατάλληλα όλες τις άλλες κλάσεις.



Σχήμα 16: Διάγραμμα κλάσεων συστήματος.

Ενότητα 4.3 Παραδείγματα εκτέλεσης

Παρακάτω φαίνονται τα αντίστοιχα παραδείγματα εκτέλεσης που έχουν προαναφερθεί στην Ενότητα 4.1 από την εκτέλεση τους στο IntelliJ IDEA περιβάλλον.

```
Enter data asset:
https://example.com/45665
Enter privacy preferences
Allow use of data if member: staff

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns3:Permission xmlns:ns2="http://www.w3.org/ns/odrl/2/"
xmlns:ns3="use">
    <ns2:constraint operator=":" rightOperand="staff" leftOperand="
member">
        <ruleType>use</ruleType>
    </ns2:constraint>
</ns3:Permission>
Data asset:https://example.com/45665

Process finished with exit code 0
```

Σχήμα 17: Σχετικό παράδειγμα άδειας(Permission) σε μορφή XML με προτίμηση ιδιωτικότητας:"Allow use of data if member: staff".

```
   Enter data asset:
   https://example.com/45665
   Enter privacy preferences
   Deny distribution of data if assignee: student

   <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
   <ns3:Prohibition xmlns:ns2="http://www.w3.org/ns/odrl/2/"
xmlns:ns3="distribution">
       <ns2:constraint operator=":" rightOperand="student"
leftOperand=" assignee">
           <ruleType>distribution</ruleType>
       </ns2:constraint>
   </ns3:Prohibition>
   Data asset:https://example.com/45665

   Process finished with exit code 0
```

Σχήμα 18: Σχετικό παράδειγμα απαγόρευσης(Prohibition) σε μορφή XML με προτίμηση ιδιωτικότητας : "Deny distribution of data if assignee: student".

```
   Enter data asset:
   https://example.com/45665
   Enter privacy preferences
   Must delete data if account: closed

   <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
   <ns3:Duty xmlns:ns2="http://www.w3.org/ns/odrl/2/"
xmlns:ns3="delete">
       <ns2:constraint operator=":" rightOperand="closed"
leftOperand=" account">
           <ruleType>delete</ruleType>
       </ns2:constraint>
   </ns3:Duty>
   Data asset:https://example.com/45665

   Process finished with exit code 0
```

Σχήμα 19: Σχετικό παράδειγμα καθήκοντος(Duty) σε μορφή XML με προτίμηση ιδιωτικότητας:"Must delete data if account: closed".

Πρέπει να αναφερθεί πως και στα τρία παραδείγματα δόθηκε ως data asset το URL : https://example.com/45665 το οποίο χρησιμοποιείται συμβολικά και δεν παραπέμπει σε κάποια ιστοσελίδα για παράδειγμα. Αντιστοιχεί στην οντότητα δεδομένων για την οποία θα μετατραπούν και θα εφαρμοστούν οι προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων.

ΚΕΦΑΛΑΙΟ 5 Συμπεράσματα-Μελλοντική εργασία

Εν κατακλείδι, το περιεχόμενο της πτυχιακής εργασίας αποτέλεσε η εμβάθυνση στις προτιμήσεις ιδιωτικότητας, στις τεχνολογίες ψηφιακών δικαιωμάτων και στο σύστημα που αναπτύχθηκε στο πλαίσιο της. Όσον αφορά τις προτιμήσεις ιδιωτικότητας έγινε ανάλυση του νομικού ζητήματος προστασίας των προσωπικών δεδομένων με βάση αυτά που ορίζει ένας από τους σημαντικότερους κανονισμούς του 21ου αιώνα, ο Γενικός Κανονισμός Προστασίας Δεδομένων, ο γνωστός GDPR.

Επίσης αναφέρθηκαν οι “Sticky” πολιτικές που επιτρέπουν στους κατόχους των δεδομένων να ορίσουν τις προτιμήσεις ιδιωτικότητας τους σε αυτές τις πολιτικές και να τις «στείλουν» προσκολλημένες πάνω στα ίδια τα δεδομένα .

Από την άλλη, όσον αφορά τις τεχνολογίες ψηφιακών δικαιωμάτων, έγινε η παρουσίαση των πιο σημαντικών τεχνολογιών όπως η ODRL, MPEG-REL, ccREL.

Τέλος, έγινε η παρουσίαση του συστήματος που λαμβάνει ως είσοδο τις προτιμήσεις ιδιωτικότητας του υποκειμένου των δεδομένων και την οντότητα δεδομένων (data asset) την οποία αφορούν οι προτιμήσεις αυτές. Έπειτα, χρησιμοποιώντας τους κατάλληλους μηχανισμούς, τις μετατρέπει με βάση την ODRL τεχνολογία ψηφιακών δικαιωμάτων σε ODRL προτιμήσεις ιδιωτικότητας και τις εμφανίζει σε XML μορφότυπο.

Μελλοντικά, στο σύστημα κρίνεται απαραίτητη η δημιουργία ενός γραφικού περιβάλλοντος χρήστη (Graphical User Interface, GUI) το οποίο θα καταστήσει το σύστημα πιο προσβάσιμο και φιλικό προς τα υποκείμενα των δεδομένων. Θα πρέπει να σχεδιαστεί με τέτοιο τρόπο έτσι ώστε να είναι ευνόητο και τα υποκείμενα των δεδομένων να μπορούν με ευκολία να εισάγουν τις προτιμήσεις ιδιωτικότητας τους χωρίς να χρειάζεται να γνωρίζουν το τεχνικό μέρος της ODRL. Με αυτόν το τρόπο, τα υποκείμενα των δεδομένων ανεξάρτητα από τις γνώσεις τους σε ό,τι αφορά την ODRL θα μπορούν να μετατρέπουν τις προτιμήσεις ιδιωτικότητας τους. Σε αυτό το γραφικό περιβάλλον θα μπορούσε επίσης να ενσωματωθεί ένα περιβάλλον ανταπόκρισης πραγματικού χρόνου όπου τα υποκείμενα των δεδομένων θα μπορούν να δίνουν ενημέρωση για τεχνικά προβλήματα και ανακρίβειες στην μετατροπή των προτιμήσεων τους. Ακόμα, θα ήταν δυνατόν τα υποκείμενα δεδομένων να μπορούν να αποθηκεύουν τις ODRL προτιμήσεις ιδιωτικότητας τους και να τις διαχειρίζονται ανάλογα την περίπτωση μέσω τους προσωπικού τους προφίλ. Τέλος, χρήσιμη θα ήταν η ομαλή προσαρμογή του GUI σε διαφορετικές πλατφόρμες και εφαρμογές καθώς και η εξασφάλιση της διαλειτουργικότητας του σε διαφορετικές συσκευές.

Μία από τις σημαντικότερες μελλοντικές προσθήκες στο σύστημα είναι η χρήση τεχνικών επεξεργασίας φυσικής γλώσσας (Natural Language Processing, NLP). Αρχικά, για την καλύτερη αντιστοίχιση των προτιμήσεων ιδιωτικότητας που εισέρχονται από το πληκτρολόγιο θα μπορούσαν να χρησιμοποιηθούν οι τεχνικές αναγνώρισης οντοτήτων όπου το σύστημα θα αναγνωρίζει κάποιους όρους και οντότητες σχετικά με τις άδειες, απαγορεύσεις, καθήκοντα που ορίζει η ODRL και έτσι με μεγαλύτερη ακρίβεια θα δημιουργούνται οι κατάλληλες ODRL προτιμήσεις ιδιωτικότητας [18]. Η προσθήκη τεχνικών NLP θα μπορεί να διαχειριστεί και να μετατρέψει αρκετά σύνθετες για το σύστημα προτιμήσεις ιδιωτικότητας και έτσι αργότερα το σύστημα θα μπορεί να αποτελέσει μέρος ενός συστήματος μεγαλύτερης κλίμακας.

Μελλοντική μελέτη και έρευνα μπορεί να αποτελέσουν οι πιθανές εξελίξεις στο νομικό κόσμο της προστασίας προσωπικών δεδομένων καθώς επίσης και το πως η πρόσφατη εμφάνιση της τεχνητής νοημοσύνης θα μπορούσε να επηρεάσει θετικά ή αρνητικά την προστασία δεδομένων. Στο κομμάτι των τεχνολογιών ψηφιακών δικαιωμάτων μένουν τα ερωτήματα: «Θα υπάρξει κάποια νέα, καλύτερη και πιο πρακτική τεχνολογία που θα αντικαταστήσει τις παλαιότερες ;», «Κατά πόσο θα συνεχίζουν να χρησιμοποιούνται αυτές οι τεχνολογίες;» [19].

Βιβλιογραφία

[1] S. Warren και L. Brandeis , «The Right to Privacy,» *Harvard Law Review, 4,* pp. 193-220, 1890.

[2] J. Klosek, «Data Privacy in the Information Age,» 2000, pp. pp 1-2.

[3] B. Eberhard , B. Willms, G. Dirk και R. Niels, «Digital Rights Management-Technological, Economic, Legal, and Political Aspects,» *(Vol.2770) Springer,* 2003.

[4] https://www.w3.org/XML/.

[5] «https://gdpr-info.eu/».

[6] E. Politou, E. Alepis και C. Patsakis, «Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions,» *J.Cybersecur.,4,tyy001,* 2018.

[7] https://www.enforcementtracker.com/.

[8] D. Miorandi, A. Rizzardi, S. Sicari και A. Coen-Porisini, «"Sticky Policies: A Survey",» *IEEE Transactions on Knowledge and Data Engineering, vol.32, no.12, doi:10.1109/TKDE.2019.2936353,* pp. 2481-2499, 1 Dec 2020.

[9] «https://www.w3.org/TR/odrl-model/».

[10] https://www.w3.org/TR/json-ld/.

[11] X. Wang, T. DeMartini, B. Wragg, M. Paramasivam και C. Barlas, «"The MPEG-21 rights expression language and rights data dictionary",» *IEEE Transactions on Multimedia, vol.7, no.3, doi:10.1109/TMM.2005.846788,* pp. 408-417, June 2005.

[12] «https://www.w3.org/TR/xmlschema/».

[13] «https://www.w3.org/TR/xml-names/».

[14] H. Abelson, B. Adida, M. Linksvayer και N. Yergler , ccREL: The Creative Commons Rights Expression Language, 2008.

[15] «https://www.w3.org/RDF/».

[16] «https://csrc.nist.gov/glossary/term/data_asset».

[17] «https://javaee.github.io/jaxb-v2/».

[18] G. Chowdhury, «Natural language processing. Annual Review of Information Science and Technology, 37,» *ISSN 0066-4200,* pp. 51-89, 2003.

[19] Z. Ma, «Digital rights management: Model, technology and application,» *China Communications, vol.14, no.6,* pp. 156-167, 2017.

[20] A. Clare και M. Swain, «Declarative Language,» σε *In: Dubitzky, W., Wolkenhauer, O., Cho, KH., Yokota, H. (eds) Encyclopedia of Systems Biology*, New York, NY, Springer, https://doi.org/10.1007/978-1-4419-9863-7_1334, 2013.