Information Security

Effects of the General Data Protection Regulation (GDPR) on Information Security

An Ontology of GDPR

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

eingereicht von

Melisa Geko
1610619510

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer/Betreuerin: FH-Prof. Mag. Dr. Tjoa Simon

Sankt Pölten,
09.08.2018

(Unterschrift Autor/Autorin) (Unterschrift Betreuer/Betreuerin)

Ehrenwörtliche Erklärung

Ich versichere, dass

ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.

ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter/einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

diese Arbeit mit der vom Begutachter/von der Begutachterin beurteilten Arbeit übereinstimmt.

Der Studierende/Absolvent räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehre- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei der Absolvent als Urheber zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen dem Studierenden/Absolventen und der FH St. Pölten.

St.Pölten,09.08.2018

(Unterschrift Autor/Autorin)

Acknowledgments

Firstly, I would like to express gratitude to my supervisor FH-Prof. Mag. Dr. Tjoa Simon of the University of applied Sciences St. Pölten for his expertise, support and guidance during the work on my master thesis. Mr Tjoa took time out of his busy schedule to give kind advises, warm encouragements and valuable comments. He steered me in the right the direction whenever he thought I needed it.

Also, I would like to express my sincere thanks to my family for their full and unconditional support providing encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them.

Thank you.

Zusammenfassung

Viele Unternehmen haben erkannt, dass der richtige Einsatz der Datenanalyse ein entscheidender Wettbewerbsvorteil ist. Dieser Umstand und geringe Strafen bei Nichteinhaltung führten dazu, dass der Schutz der Privatsphäre oft vernachlässigt wurde. Um dies zu ändern und den Datenschutz in der gesamten Europäischen Union zu harmonisieren, hat die EU-Kommission ein neues Gesetz beschlossen, das die Rechte des Betroffenen klärt und ein angemessener Schutz personenbezogener Daten ermöglicht.

Die neue EU-Datenschutzverordnung (DSGVO) hat die aus dem Jahr 1995 stammende Richtlinie 95/46/EG (Datenschutzrichtlinie) ersetzt und sich zum Ziel gemacht, vorhandene Probleme zu adressieren. Die DSGVO soll den Umgang und die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlichen. Nach der zweijährigen Übergangsfrist trat die DSGVO am 25. Mai 2018 in allen EU-Mitgliedstaaten in Kraft und musste nicht in nationales Recht umgesetzt werden. Dadurch hat die DSGVO das gültige österreichische Datenschutzgesetz 2000 ersetzt.

Durch hohe Strafen bei Nichteinhaltung (d.h. bis zu 2% - 4% des weltweiten Jahresumsatzes) übt die neue Datenschutzverordnung einen hohen Druck auf die Organisationen aus, sich den Anforderungen der DSGVO anzupassen. Studien haben jedoch gezeigt, dass Unternehmen oft von den tatsächlichen Anforderungen überfordert sind.

In dieser Arbeit wird eine auf die neue Verordnung zugeschnittene Ontologie des Datenschutzes vorgestellt, die die Interdependenz von DSGVO und Informationssicherheit aufzeigt, um Organisationen bei diesem komplexen Thema mit einer Wissensbasis zu unterstützen. Hauptziel dieser Arbeit ist es, eine Struktur zu schaffen, die die wichtigsten Anforderungen von DSGVO an die Informationssicherheit, die Datenschutzgrundsätze, die Pflichten des für die Verarbeitung Verantwortlichen und die Rechte der betroffenen Person festlegt. Die vorgeschlagene DSGVO Ontologie wird als Grundlage für zukünftige Forschungen zur Übereinstimmung der Organisation mit DSVO dienen.

Schlüsselwörter:
DSGVO, Datenschutz, Ontologie, EU, Compliance, Informationssicherheit, Audit

Abstract

Many organisations have recognized that the correct use of data analysis is a decisive competitive advantage. This circumstance and low penalties for non-compliance led to the fact that proper protection of privacy was often neglected. To change this and to harmonize data protection throughout the European Union, the EU-Commission has adopted a new law, clarifying the data subject rights and ensuring an appropriate level of personal data protection. The new EU General Data Protection Regulation (GDPR) has replaced Directive 95/46 (Data Protection Directive), which was adopted in 1995, and introduces new rules to harmonize handling and processing of personal data by private companies and public authorities throughout the EU. After the two-year transition period, the GDPR came into force on 25 Mai 2018 and has immediate effect in all EU Member States and does not have to be transposed into national law.

Through high penalties for non-compliance (i.e. up to 2% - 4% of the annual worldwide turnover), the new regulation of data protection puts high pressure on organisations to be in alignment with the requirements of GDPR. However, studies have shown that organisations are often overwhelmed by the actual requirements.

In this thesis an ontology of the data protection tailored to the new regulation is presented, which highlights the interdependence of GDPR and information security in order to support organisations with this complex topic by providing a knowledge base. The main purpose of this work is to provide a structure which will identify the main requirements of GDPR relevant for information security, privacy principles, obligations of the data controller and rights of the data subject. The proposed GDPR ontology will be used as a basis for future research in the compliance of organisation to GDPR.

Keywords:
GDPR, Data Protection, Legal Ontology, EU, Compliance, Information security, Audit

Table of contents

List of Figures

List of Tables

List of abbreviations

DPA	Data Protection Authority
DPA 2000	Data Protection Act 2000
DPD	Data Protection Directive
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
IT	Information Technology
OWL	Web Ontology Language

1 Introduction

In our current digital era devices are connected through the network, great amount of information is stored, and inevitably more and more personal data is collected and processed. According to [1], at least 2.5 quintillion bytes of data are produced daily. This carries the danger of the "mass surveillance", which is represented by the loss of privacy and the right to informational self-determination. Therefore, the issue of data protection has become considerably more important in recent years [2].

Despite the fact that technology has primarily supporting role, today it is being used to connect people with each other, to complete jobs, purchase goods and services, and to learn and create. Sun Microsystems [3] call this new era as a participation age, where participants are not just obtaining information but are also processing and sharing it. This participation age affects people who use information, but also IT systems and services that support users and deliver information. These IT systems and services must ensure widespread access while also protecting the security and privacy of personal and other data categories [4]. Every computer system, as well as data protection process, is subject to a large number of additional individual risks. These risks must be managed and mitigated by appropriate measures. Since these data are nowadays mostly stored on computer systems, rules for the information security under the data protection law must be applied.

The worry about data abuse was already present in the late 1990s, as computer systems became more accessible to corporations and the general user [4]. While some organisations began mining their collected data, other organisations collected and aggregated data from private and public sources to sell these as products. In order to ease this concern, governments worldwide decided to pass a number of laws across different industries to manage use and to prevent misuse and negligence of the collected data [4]. Some of these laws were:

- New Zealand Privacy Act (1993);
- Hong Kong Personal Data Ordinance (1995);
- US Health Insurance Portability and Accountability Act (1996);
- European Union Data Protection Directive (1995);
- US Gramm-Leach-Bliley Act (1999))

The law relevant for European Union was EU Data Protection Directive 95/46/EC (DPD) that has been in place since 1995 [5]. This directive has defined a minimum standard for the data protection law and how companies can collect, use and process personal information. It is important to notice that this directive came from a time when only a few households had computers and almost no one had access to Internet, there was neither social media nor online banking or cloud computing.

Since many countries have made significant progress in terms of adopting laws to protect a data, it was difficult for EU citizens to determine how their rights are protected in the EU, moreover it was difficult for organizations to determine which laws should be considered when processing personal data and transferring these across several Member States [6].
When a company, which has decided to collect, process or forward personal data, wants to operate across borders, it can be confronted with challenging reconciliation processes due to the different legal situations. The different implementations of the EU Data Protection Directive 95/46 have led to the situation that companies have repeatedly complained about problems of the freedom of EU data traffic. Therefore, it was necessary to define rules which will clarify the protection and usage of personal data EU-wide.

According to IT Governance Privacy Team [6] General Data Protection Regulation is defined as latest step in this participation age, which confirms the importance and value of personal information. Although the security of information and data were already known, organisations are recently becoming aware of the real value of personal data, since the EU Commission published new law [6]. A company, in which data protection is not relevant, does not exist in theory, since every company has at least personal data of employees. Employee data can be used, among other things, for the transfer of wages and salary or for the application of social insurance. Whenever personal data is collected, processed or forwarded to third parties a company must apply data protection law. Moreover, an organisation using different Big data analysis techniques can track and predict person's behaviour and deploy it in automated decision making. As a consequence, personal data remains exposed to significant personal risks and to cyber theft. Considering all these issues and the continual advance of technology, the EU decided to define new law to clarify the data subject rights and to ensure an appropriate level of EU-wide protection of personal data [6]. This new law has two key goals:

1. "Protecting the rights, privacy and freedoms of natural persons in the EU" [6] and
2. "Reducing barriers to business by facilitating the free movement of data through the EU". [6]

The proposed new EU General Data Protection Regulation has replaced Directive 95/46 (Data Protection Directive), which was adopted in 1995, and has been designed to address existing problems. The idea of new regulation was to regulate handling and processing of personal data in EU area [7]. The regulation is relevant for private companies, public authorities throughout the EU, but also for companies worldwide that use and process personal data [7]. The new GDPR has an immediate effect (after the two-year transition period) in all EU Member States and does not have to be transposed into national law. Therefore, this regulation will replace Austrian law, and every board, decision-maker, or manager has to deal with this topic.

As already mentioned, the new regulation will put a pressure on organisations EU-wide to be compliant with it. Many studies [9], [10] have shown that the organisations are not clear with regards to the actual requirements given in the regulation. To achieve GDPR compliance organisations need to have a structured process in place. Unfortunately, the researches show that this is not the case for many of the respondents: 39 percent of organisations have this process and will put in realization GDPR measures until the end of year 2018, almost 18 percent will achieve GDPR compliance after 2019, and 7 percent of the respondents, who have a process in place believe they will implement all measures and achieve GDPR deadline of May 2018. [10] The GDPR sets out different requirements on organisations in order to adequately protect personal data, accordingly this thesis deals with information security and requirements relevant for this domain.
The aim of this thesis is to provide a structure, which will identify and highlight the main requirements of GDPR in the context of information security. The research area of this work is summarized in a question that should be covered and answered through this study:

- What are the main requirements of the GDPR that are relevant for information security, furthermore how to visualise these requirements to help organisations to understand the legal text and the main obligations?

The answer of this question is an ontology of GDPR which presents five main areas that contain main requirements of GDPR for information security, privacy principles, obligations of the data controller, processors and rights of the data subject. Since the ontologies are generally used to describe different domains and to express different perspectives within these domains [10], they are suitable for this work. The results are visualised, in approx. 250 classes and 25 relations between these classes. For more detailed information about ontology metrics, see appendix 6.

1.1. Structure of thesis

This thesis consists of the following sections:

- Section 1 presents an introduction and importance of data protection nowadays. Also, in this section the most important terms and definitions used in this work are described.
- Section 2 introduces a histological background of privacy.
- Section 3 is concerned with theoretical fundamentals of information security and data protection laws, particularly data protection act in Austria (DSG 2000).
- Section 4 contains the GDPR fundamentals, general information and summary of content.
- Section 5 defines and discusses proposed GDPR ontology. Also, in this section requirements of GDPR on information security and recommendation of effective implementation of GDPR in company are discussed.
- Section 6 describes Protégé 5 software used for implementation of the GDPR ontology.
- Section 7 contains general description of Protege plugins for visualization and use case of ontology.
- Section 8 is conclusion of this thesis and it highlights some of the limitation and future work.

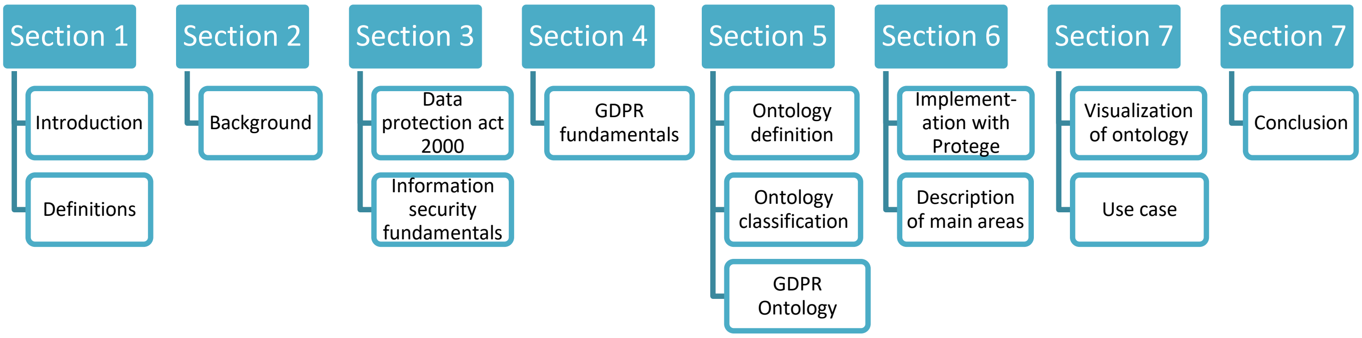


Figure 1: Thesis Structure

1.2. Important terms and definitions

- Compliance

“The process of adhering to policies and decisions. Policies can be derived from internal directives, procedures and requirements, or from external laws, regulations, standards and agreements.” [12]

- Personal Data

“Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.” [13]

- Data

“Information in a specific representation, usually as a sequence of symbols that have meaning.” [14]

- Information

“Facts and ideas, which can be represented (encoded) as various forms of data.” [14]

- Anonymity

“The condition of an identity being unknown or concealed.” [14]

- Sensitive Data

“Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms.” [7]

- Ontology – Information science

“An ontology is a formal explicit description of concepts in a domain of discourse (classes (sometimes called concepts)), properties of each concept describing various features and attributes of the concept (slots (sometimes called roles or properties)), and restrictions on slots (facets (sometimes called role restrictions)).” [15]

- Regulation

“A rule of order having the force of law, prescribed by a superior or competent authority, relating to the actions of those under the authority's control.” [16] Also called as executive order.

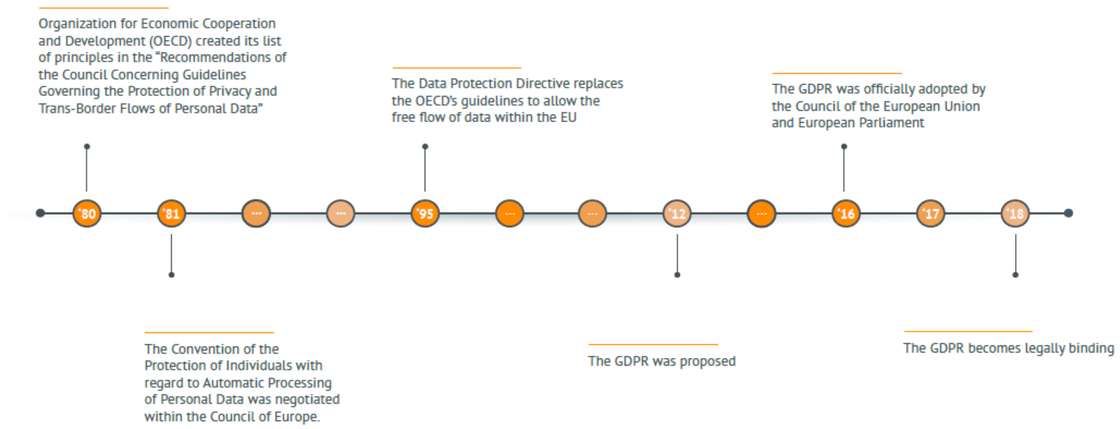
- Mass surveillance

“Far-reaching, complex and highly technologically advanced systems designed by US and some Member States intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner.” [17]

2 Historical background

One of the central issues of our time is data protection. Today, there are hundreds of laws that affect privacy: criminal law, the law of evidence, constitutional law, federal laws and numerous laws in other states around the world [18]. In order to better understand the law of data protection, it is necessary to pay attention to its origin and growth. Technology has played a major role in the history of the emergence of data protection law. According to [18] new laws are usually defined as a response to technological changes that have increased the collection and use of personal data.
The first grounds of individual`s right to privacy were Brandeis and Warren [18]. They defined right to privacy in their Harward Law Journal article [18]. Glancy in paper “The Invention of the Right to Privacy” comments the Warrens “Right to Privacy” and defined it as “the right of each individual to protects his or her psychological integrity by exercising control over information which both reflected and affected that individual’s personality” [19]. There are two important facts in privacy, first one is to understand that we have right to privacy and its importance and the second one is the importance of information security mechanisms or methods essential to achieve privacy [18]. As already mentioned, technology plays a major role, especially in this modern era, where the control over personal information is altered and influenced by technology.

In Europe the data protection awareness has arisen in 1980, when the Organization for Economic Cooperation and Development (OECD) published a list of principles with the purpose to protect people’s privacy [21]. These principles required from companies to notify people when and to what purposes their data was collected. However, these guidelines were nonbinding for organizations and had not any impact. Since the data privacy laws across EU countries were not unified and therefore caused various problems with the free flow of data within the EU, the European Commission decided to publish the Data Protection Directive in 1995 [13]. However, the implementation of this directive was differently from country to country and caused many problems in the EU. Therefore in 2012, the European Commission decided to propose new law, that will regulate processing of personal data across the EU. The new regulation is relevant for the EU organizations, but also for those who operate within its borders. Every company, that has or uses data of EU citizens, must comply with the new rules, regardless of where it is located [7]. This means that these rules will affect big technology companies such as Facebook and Google, but also, small US companies that have one or a few European clients [21].



Organization for Economic Cooperation and Development (OECD) created its list of principles in the “Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data”

The Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data was negotiated within the Council of Europe.

The Data Protection Directive replaces the OECD’s guidelines to allow the free flow of data within the EU

The GDPR was proposed

The GDPR was officially adopted by the Council of the European Union and European Parliament

The GDPR becomes legally binding

Figure 2: History of data protection [21]

3 Theoretical fundamentals

3.1. Data protection in Austrian Law

Every person has data, which can be discussed only with a selected group of people, such as his doctor, lawyer, friend or companion, and relies on the fact that these data will remain private and will not be made publicly available to everyone [22].
Even if a person has nothing to hide, it does not publish the password for his mail account or reveals the credit card PIN, because this data belongs to each individual and need to be protected.
Therefore, data protection is a fundamental right and is anchored in Article 1 of the Austrian Data Protection Act (DPA 2000) [23].

Article 1 provides:

(1) *“Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject.”* [23]

The right to data protection is not only present in Austria. Article 2 of the Austrian Data Protection Act (DPA 2000) refers to Article 5 of the Charter of Fundamental Rights of the European Convention, which assures the protection of personal data at European level.

Article 8 provides [24]:

(1) *Everyone has the right to the protection of personal data concerning him or her.*
(2) *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
(3) *Compliance with these rules shall be subject to control by an independent authority.*

3.1.1. What type of information is protected by the Data Protection Act?

In introduction was already been mentioned that whenever personal data are used, companies must deal with data protection. Austrian Data Protection Act defines the word “data”:

“Data (Personal Data): Information relating to data subjects (sub-para. 3) who are identified or identifiable; Data are “only indirectly personal” for a controller (sub-para. 4), a processor (subpara. 5) or recipient of a transmission (sub-para. 12) when the Data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means.” [23]

The special type of personal data is sensitive data. According to Data Protection Act this type of data is deserving special protection [23]. Sensitive data are racial or ethnic origin data, political opinion, religious or philosophical beliefs, health data and data concerning sex life [7].

3.1.2. Basic data protection principles and new DPA

The protection of personal data has been highly valued in Austria for a long time. Hence, the Austrian DPA of 1978 was one of the first of its kind in Europe [24]. Further, the DPA 2000 imposed many restrictions on controllers concerning collecting, processing and transferring personal data and it granted a number of rights to data subjects. It also describes principles relating to processing of personal data (including lawfulness, fairness, and purpose limitation) and the lawfulness of processing (requiring a legitimate purpose and a legal basis). Since the GDPR has introduced some additional rules for data processing and imposes significantly more obligations on controller of the data processing, Austrian Parliament has adopted the amendment of DPA 2000 and published Austrian Data Protection Amendment Act 2018 [26]. The main provisions of GDPR under the DPA 2018 specific to Austria are:

- **Application to legal persons**

As indicated in GDPR, the regulation covers the protection of natural persons. By contrast, according to DPA 2018, the fundamental right to data privacy will apply not only to natural persons, but also to legal entities [27].

- **Consent of children**

Based on the opening clause in Article 8 of the GDPR, the age of consent at which a child can express a valid consent to processing of their data is set to fourteen [27].

- **Processing of criminal convictions and offenses**

According to the GDPR Article 10 it is allowed to process data regarding criminal convictions and offenses only if it is authorized by Member State law. The new DPA 2018 provides detailed information for processing criminal data, e.g. statutory authorization or legitimate interests pursued by the controller [26].

- **Processing of images or video materials**

Since the processing of images is not permitted in case of monitoring employees and matching personal data obtained from image recordings with other personal data without the express consent of the data subject, the DPA 2018 sets out specific regulations on the permissibility of processing personal information contained in these materials. It also regulates the use of CCTV on public and private property, since the Austrian Data Protection Authority has not qualified the use of CCTV as processing of sensitive data [27]. However, it is necessary to examine legitimate interest of controller and / or to obtain consent from data subject.

- **Processing of employee information**

Processing employee data might require the conclusion of a contract between the controller and its employees. The DPA 2018 also point out that “the current privacy-related provisions of the Labor Relations Act will remain applicable to the processing of employee information” [28].

- **Fines imposed on legal entities**

Since the DPA 2018 relates, alongside natural persons, to the legal persons, it sets out specific rules to charge administrative fines on legal entities [28].

3.2. Information security

Across all organizations, information is a key driver for enterprise business value generation and can be foundation for competitive advantage. The full value of information can only be gained if it is kept accurate, complete and time precise. On the opposite, there will be weak business value generation if information is not well managed and maintained [29]. Cyber-breaches of the past highlight that if competitors or unauthorized persons get hold of critical information assets of an organization, the consequences can be catastrophic and corresponding organization may suffer great business losses.
The secure processing of information has therefore become one of the important things for the survival of many companies and government agencies. This information might be stored on paper, on computers, or inside people's heads.

According to the Committee on National Security Systems (CNSS) [30] information security refers to the practice and procedures implemented in order to protect information of unauthorized access, use, disclosure, disruption, modification, inspection and so on. Beside protection of information, information security includes also areas of information security management, data security and network security.

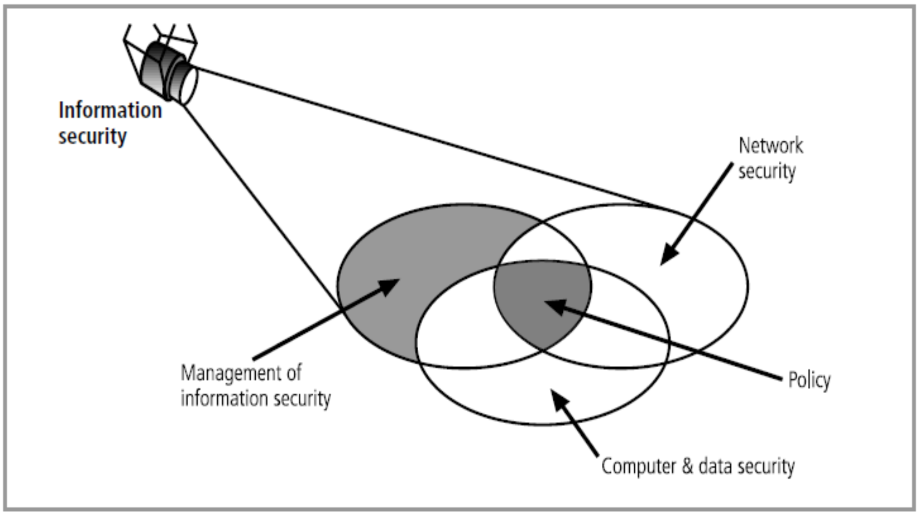


Figure 3: Components of information security [31]

One of the most asked question in the information security field is the difference between data protection and information security. Therefore, it is necessary to distinguish these two terms. Data protection deals exclusively with personal data whereas information security encompasses all data, both physical and digital and takes care of all sensitive information in organisation [32].

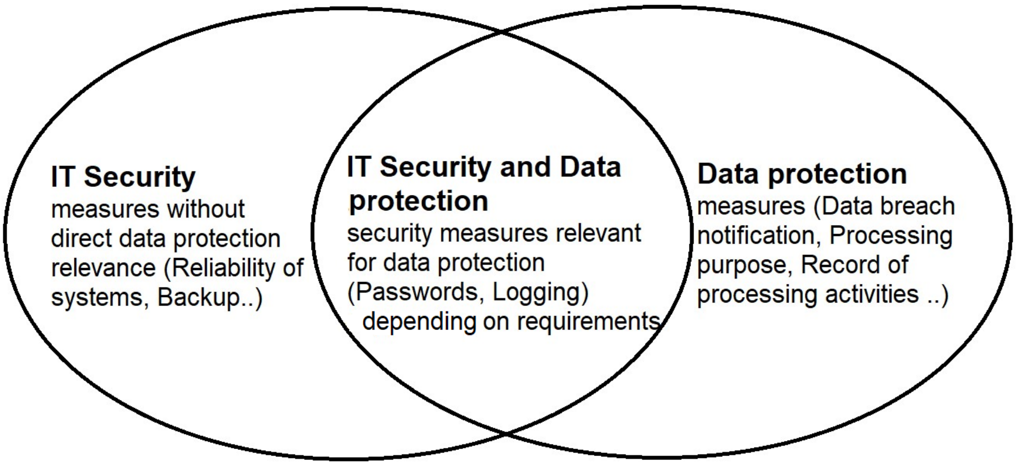

IT Security
measures without direct data protection relevance (Reliability of systems, Backup..)
IT Security and Data protection
security measures relevant for data protection (Passwords, Logging) depending on requirements
Data protection
measures (Data breach notification, Processing purpose, Record of processing activities ..)

Figure 4: Overlapping IT security and Data protection [33]

In the Figure 4 is overlapping of these two areas represented with two circles. Circle one represents the technical view IT Security and its security measures and circle two represents measures and principles which come from the data protection law. The intersection of these two circles contains all technical and organisational possibilities to secure data and to be compliant with the data protection law. However, one data protection principle or requirement cannot be fulfilled without information security.

3.2.1. Key concepts of information security and data protection

Information security as a discipline uses by the computer security industry called the C.I.A. triangle. This triangle is based on concepts of confidentiality, integrity, and availability as frameworks for thinking about how data should be protected [34]. For any given piece of data, we must ask: is it protected from being disclosed to those who should not access it? Is it protected from unauthorized persons? And is it available to those who need it?

§ 14. (1) "Measures to ensure data security shall be taken by all organisational units of a controller or processor that use data. Depending on the kind of data used as well as the extent and purpose of the use and considering the state of technical possibilities and economic justifiability it shall be ensured that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons." [23]

According to paragraph 14 of DSG 2000, level of data security depends on the kind of data used. Also, measures are based on the level of protection of the data.
In most of the literature, information is defined as processed data. In [4] information is defined in a more technical sense as set data facts and data are understood as all the facts that are processed into information.

As mentioned above, main purpose of information security is to protect information. Therefore, the C.I.A principles represent a basis of IT and should be guaranteed in any kind of secure system.

- **Confidentiality**

Confidentiality of information is achieved, when information is not made available or disclosed to unauthorized individuals, entities, or processes [34]. To access information, it is necessary to have rights and privileges.

Michael E. Whitman [34] describes in his book what is meant by confidentiality and what measures can be used to protect the confidentiality of information. Some of measures used to achieve confidentiality are [34]:

- Classification of information

According to ISO 27001:2016, main aim of this measure is to ensure that every information in organisation is classified and has an appropriate level of protection in accordance with its importance to that organization [35]. The levels of protection are not prescribed in standard, but in most cases, there are three levels: public (information accessible to everyone), internal (information accessible to employees) and confidential (information accessible only to specific persons). However, the levels of classification are influenced by the size of the organisation. [36]

- Application of general security policies

Security policy should be developed in organisation to address corporate philosophy, mission statements, culture, security objectives, or attitude to risk [35]. This policy contains rules and procedures for all individuals, who are accessing and using IT assets and resources of an organisation. [37]

- Education of information custodians and end users

Through appropriate awareness educations and trainings, all employees of the organisation and contractors will receive regular updates relevant for their jobs and correspondingly achieve appropriate level of confidentiality in organisation [35].

- **Integrity**

Integrity is maintaining and assuring the completeness and accuracy of data [34]. Data must stay correct, complete and up to date in its entire life-cycle. To protect information or data of corruption many methods have been introduced. For example, methods for detecting viruses that are designed for purposes of corrupting data or method of hashing file with the special algorithm. [34].

- **Availability**

Every information must be available to authorized users, persons or computer systems when it is needed [34]. Information availability is affected when a system is regularly non-functioning. Very common attacks nowadays are concentrating on denying access to information. Other factors that are affecting availability are time, power outages or natural disasters such as floods. Moreover, if a computer system cannot deliver information at the point of time, then this property is affected [34].

Beside the C.I.A triangle there are other principles also very important in certain scenarios, such as non-repudiation and authentication. Principle of non-repudiation is a technology-supported method, that supports secure message transmission between parties using digital signature [38]. On the other side, authentication refers to the ability of a system to confirm the identity of the sender [39]. These two principles, together with C.I.A represent the pillars of information security.

In addition to the protection concepts known from information security, the Standard Data Protection Model (SDM) [39] introduce three further protection goals derived from new regulation. Compared to the protection concepts of information security, these data protection goals are aimed to protect organisations from risks arising from the activities for the data subjects within and outside of business processes [39]. However, considering the protection goals of information security and data protection goals from SDM, organisation can achieve appropriate scalability in the selection and effectiveness of technical and organisational protection measures.

- **Unlinkability**

Considering the possibility of data abuse when using and processing data in larger sets, this protection goal refers to the requirement from GDPR to process and analyse data “only for the purpose for which they were collected” [39].

- **Transparency**

The data protection goal transparency is related to the “Transparency, lawfulness and fairness” principle of GDPR that makes possible to relevant entities, such as data subject and supervisory authorities, to understand “which data are collected and processed for a particular purpose, which systems and processes are used for this purpose, where the data flow for which purpose, and who is legally responsible for the data and systems in the various phases of data processing” [39].

- **Intervenability**

According to the GDPR, data subjects have rights that can be exercised at any time [7]. Considering this requirement, the intervenability protection goal refers to the obligation of controller to implement appropriate technical and organisational measures to be able to support these data subject’s rights [39].

4 EU General Data Protection Regulation

4.1. Basic information

The European General Data Protection Regulation was adopted in April 2016 by EU Commission and will go into effect on May 25, 2018. The GDPR consist of 99 Articles defining rights of individuals and obligations for organisations. This regulation also defines 173 recitals, which are essential for understanding how the Articles will be interpreted by the Data Protection Authorities [7].

4.2. Objectives of GDPR

According to Article 8 (1) of the Charter of Fundamental Rights of the European Union and GDPR every EU resident has the right to the protection of personal data and "has right to know and decide how his or her personal data is being used, stored, protected, transferred and deleted" [40].
The primary purpose of GDPR is to define new law and to set guidelines for the protection of personal data on the EU level but also applies globally for companies that work with the personal data of EU residents [7].
The objectives of GDPR can be achieved through the principles of personal data processing as set out in Art. 5 GDPR: transparency, lawfulness and fairness, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability [7].
In order to be compliant with the GDPR, organisations need to make review of their measures, practices and processes regarding the collection, use and protection of personal data.

4.3. Scope of GDPR

The scope of the GDPR is extended to all processing modes of personal data of EU residents (for fully or partially automated as well as non-automated processing) [7]. For example, the GDPR also applies in cases where an employee lives in Austria (EU) but works for a company in USA. Or a customer from Germany doing an online transaction with an USA -based retailer.

Some areas of data processing are excluded from the scope of GDPR. These are processing operations within the scope of an activity that falls outside the scope of Union law (e.g. national security activities, activities relating to the common foreign and security policy of the EU Member States, personal or family activities, professional or economic activity, use of social networks). [7].

4.4. Key components of GDPR

In the following table are represented all key components of GDPR. The table is divided in three parts: content of 11 chapters of GDPR, related articles and short description of content.

Content	Articles in GDPR	Description
General provisions	Art. 1 - 4	Aim of the regulation, scope and essential definitions.
Principles	Art. 5 - 11	Rules for processing and protecting personal data.
Rights of data subject	Art.12 - 23	Rights of the data subject, including the right to be forgotten, right to rectification, and right to restriction of processing.

Controller and processor	Art. 24 - 43	General obligations and necessary security measures of data controllers and processors, as well as data protection impact assessments, the role of the data protection officer, codes of conduct, and certifications.
Transfer of personal data to third countries of international organisations	Art. 44 - 50	Rules for transferring personal data outside of the Union.
Independent supervisory authorities	Art. 51 - 59	Description of supervisory authority with certain tasks and powers.
Cooperation and Consistency	Art. 60 - 76	Cooperation of supervisory authorities and ways they can remain consistent when applying this regulation.
Remedies, Liability, and Sanctions	Art. 77 - 84	Rights of data subjects to judicial remedies and the penalties for controllers and processors.
Provisions relating to specific data processing situations	Art. 85 - 91	Exceptions of the regulation and opening clauses for Member States to create their own specific rules.
Delegated Acts and Implementing Acts	Art. 92 - 93	Power of Commission to adopt delegated acts.
Final provisions	Art. 94 - 99	Relationship to past Directives and Agreements and review of other union legal acts on data protection.

Table 1: Content of GDPR

5 Ontology

5.1. Definition of ontology

Etymologically the term ontology comes from Greek (*ὄντος, ontos*) and means essentially existence, reality or theory of being and their relations [41]. The first known written use of the ontology comes from the Artificial Intelligence (AI) research in 1970s and 1980s, where ontology is presented as something what exists and what can be represented [41]. Tomas Gruber, a researcher in field of AI, has defined ontology as “a formal specification of a conceptualisation of a domain of interest” [42]. The conceptualisation itself is an abstract or simplified view of the world, based on objects, entities and relationships between them [42]. According to the Grubers definition, the ontologies are designed for a purpose, some particular domain of interest. More precisely it is a system for the formal organisation of information.

Over the past decade, the use of ontology in modern computing [43] and in the legal domain has become very common. Ontologies help researchers to share information, as without a shared terminology, communication, especially in a complicated domain like information security, cannot be successful [44]. Ontologies are designed to express concepts related to and between domains, and provide perfect solution for information management and knowledge sharing [43].

Usually, ontology consists of different components such as classes, relations (properties), instances, functions and axioms ordered hierarchically [45]:

- **Individuals:** Instances or objects
- **Classes:** Sets or collections of objects
- **Attributes:** Properties, features, characteristics that objects can have
- **Relations:** Ways in which classes and individuals can be related to one another
- **Restrictions:** Constraints describing individuals or classes
- **Axioms:** Assertions (rules) that are always assumed to be true and constrain the use of concept (e.g. one main / specific class must have at least one subclass).

5.2. Common use of ontology

While the ontology has been related to the philosophy in the past, it has now a specific role in computer science community (Artificial Intelligence, Database design, Computational Linguistics) [46]. Researchers recognize a potential importance of ontologies in fields such as knowledge management, information retrieval and extraction [47].

According to [15] the usage and development of ontology has following benefits:

- Sharing common understanding of the structure of information among people or software agents

One of the most common uses of ontologies is sharing common understanding of information. For example, when different Websites contain or provide same or similar content, then these Websites can share and use the same ontology [15].

- Enabling reuse of domain knowledge

Another important benefit of developing ontologies is that ontologies enable reuse of domain. For example, if researchers develop an ontology in one domain, other researches can reuse it for other purposes [15]. Additionally, it is possible to combine existing ontologies in other ontologies, in order to get description and representation of the large domain.

- Separating domain knowledge from the operational knowledge

Another use of ontologies is separating the domain knowledge from the operational knowledge [15]. Operational knowledge is based on experience and competence in different domains [48], while domain knowledge represents a knowledge of a particular domain.

- To analyse domain knowledge

Analysing domain knowledge and developing of ontology is possible once a specification of the terms is available [15]. Developing an ontology of one domain is same to defining a set of data and their structure of that specific domain. The structure of ontology can be use in other programs. For example, in this thesis is an ontology of GDPR and its requirements on information security presented. This ontology can then be used as a basis for some applications for analysing Obligations of Controller or Processor, or it can be used in some tools to audit organization and its compliance with all requirements.

5.3. Classification of ontology

Today, ontologies have found their applicability in various domains and fields (medical research, software engineering, banking and so forth) [43]. The differentiation between ontologies based on their generality level is presented in Figure 5.

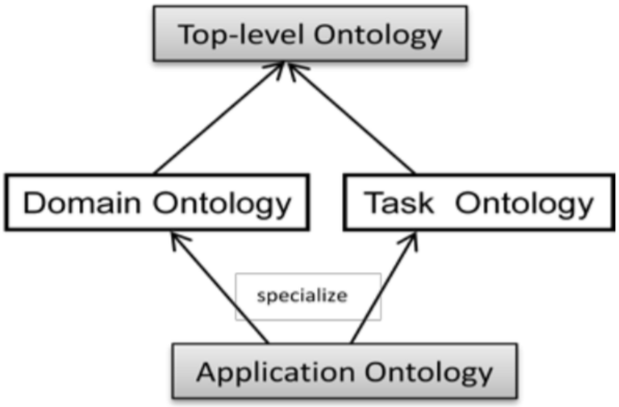


Figure 5: Guarino’s ontology classification [46]

According to Guarino’s classification [46] ontologies can be divided in 4 categories, based on its scope of the ontology:

- Top-level ontology: it describes general concept (i.e. space, time, matter, object, etc) and is useful for large communities of users

- Domain ontology: it describes the domain (security domain, medical domain, engineering domain and so on) and the vocabulary related to that domain to specialize terms introduced in the top-level ontology

- Task ontology: it is suitable for a specific activities or tasks (situation recognition, assembling parts together)

- Application ontology: it is developed for a specific application depending on particular domain and task.

Ontologies can be also classified according to the content, to the ontology language of representation or to the ontology components (concepts, instances, properties, axioms) [43].

Additionally, ontologies can be classified, according the type of structure and the amount of their use, in four categories [43]: terminological (lexical), axiomatized (formal), information ontology and software ontologies. For purposes of this thesis are terminological ontologies relevant. Terminological ontology is good for concept clarification and knowledge sharing. This kind of ontology contains two main artefacts, namely objects and relations, which are not fully followed by axioms and definitions [43]. The language used to describe this kind of ontology is SKOS (Simple Knowledge Organisation System) [48]. SKOS is a Semantic Web initiative proposed by W3C and its main purpose is to develop specifications and standards based on XML in order to support the use of knowledge organisation system. It also provides an easy conceptual modelling language for developing and sharing new KOSs and can be used on its own [48], or in combination with more-formal languages such as the Web Ontology Language (OWL) or Visualization Web Ontology Language (VOWL). VOWL is a visual notation for the user-oriented representation of ontologies and representation of elements of Web Ontology Language (OWL) [49].

5.4. Related work

Understanding and interpretation of requirements from legal text can be complex because of ambiguity and traceability contained in regulations [50]. Because of using sub-classes and specialization of relationships, ontologies have found a great application in the representation of knowledge in these fields [51].
Travis D. Breaux and Annie I. Antón have introduced in their work [50] a systematic method, called FBRAM (Frame-Based Requirements Analysis Method), for acquiring regulatory requirements [50]. In this method analysts need to manually identify and document requirements of regulations and at the end to use a tool that parses the annotations to extract regulatory requirements. Using upper ontology and the context-free mark-up language, analysts assign an interpretation to a regulation text [50]. As already described in Section 5.3, an upper ontology describes the most abstract terms that are shared across multiple domains [51]. The upper ontology used in this method describes knowledge about the semantic structure of regulatory requirements using three types of concepts [50]:

- Statement-level concept used to classify individual regulatory statements (Exclusion, Fact, Permission, Obligation, Refrainment);
- Phrase-level concept used to classify individual phrases in a regulatory statement (Exception, Condition, Subject, Act, Purpose, Term, Synonym...); and
- Abstract placeholder concept that classify statement and phrase-level concepts for analysts

While acquiring requirements form regulation, the FBRAM method is addressing two challenges: traceability and ambiguity. The possible types of ambiguity are also presented in Semantic Parameterization process [51] that engineers use to map natural domain descriptions to formal models expressed in Description Logic (logic used to express and reason about knowledge). According to [51] there are four types of ambiguity: *synonymy* (terms have same-meaning), *polysemy* (terms have multiple meaning), *anaphora* (backward references) or *cataphora* (forward references) and *under-specifications* or o*missions*. The Semantic Parameterization process can be used by engineers to describe defined sources of knowledge and to distinguish concepts and roles from individuals and interactions in the domain [51].

The main purpose of this process is to provide a system, that is similar to natural language and that makes possible to users to make statements about systems and to perform inquiries across collections of requirements [51].

The information from regulations often cannot be easily represented and queried. Using semantic web technologies, researchers presented in their work Queryable Provenance Metadata for GDPR Compliance [52]. This metadata can assist in the representation and querying of information related to compliance towards General Data Protection Regulation (GDPR). Reusing of previously published ontologies, this work focuses on obligations involving provenance metadata for consent and personal data [52].
In order to create questions for queries, authors used GDPR-readiness checklist published by Ireland's Data Protection Commissioner [53]. At the end, these questions have been represented using semantic query language SPARQL.

The use and application of ontologies in various fields is uncontested. As described in this section, ontologies are used not only for the representation of information, but also for performing various inquiries and knowledge acquiring from different information sources.

5.5. Ontology of GDPR

5.5.1. Methodology

In recent years information retrieval has become more difficult, because of use of various Big data tools that collect unstructured data [47]. Ontology-based information retrieval can help researches to easy understand a certain problem within particular domain. A legal topic which is currently the most discussed at European level is data protection. The herein proposed ontology is exclusively based on the European regulation for a data protection GDPR. It does not refer to data protection principles that may locally exist in EU member states but could be extended and tailored by experts of the corresponding member states. The development of GDPR ontology consists of three parts:

1) preparatory phase (definition of ontology scope, competency questions and requirements);
2) development phase (definition of classes, relations, properties, attributes); and
3) evaluation phase (evaluation by experts).

In the preparatory phase were different books and papers examined [54], [6], [40], [55], [56], [57], [58] in order to define GDPR requirements on information security. According to paper [58] there are 11 Articles of GDPR that are relevant for IT Security. These articles describe, among other things, principles for processing of personal data, responsibilities of data controller and processor, security of data, data breach reports as well as recording of processing activities and privacy impact assessment. Additionally, European Privacy Seal [54] has published criteria and requirements for the certification of IT products and services. This document contains main requirements of GDPR, as well as special requirements to the various phases of the processing, technical and organisational measures for protection of personal data [54]. Other papers and books [6], [40], [56], [57], [55] contain description of general requirements of GDPR and some best practices.

Considering all these papers and books, the results of preparatory phase were represented in an excel table. The main aim of this excel table was to get an overview of the GDPR articles and requirements relevant for information security and to understand which parts need to be covered in the ontology. Additionally, restrictions and exceptions as well as best practices and templates were added to the specific articles in this table.

After relevant parts of GDPR for ontology were detected, it was necessary to define main classes, subclasses and relationship between these classes. Based on results of the preparatory phase, in the second phase all components were defined, and ontology was developed and modelled using Protégé 5 Software. The GDPR ontology consists almost completely of classes and they are about knowledge. Finally, the ontology will be evaluated by experts. Graphic representation of methodology is shown at Figure 5.

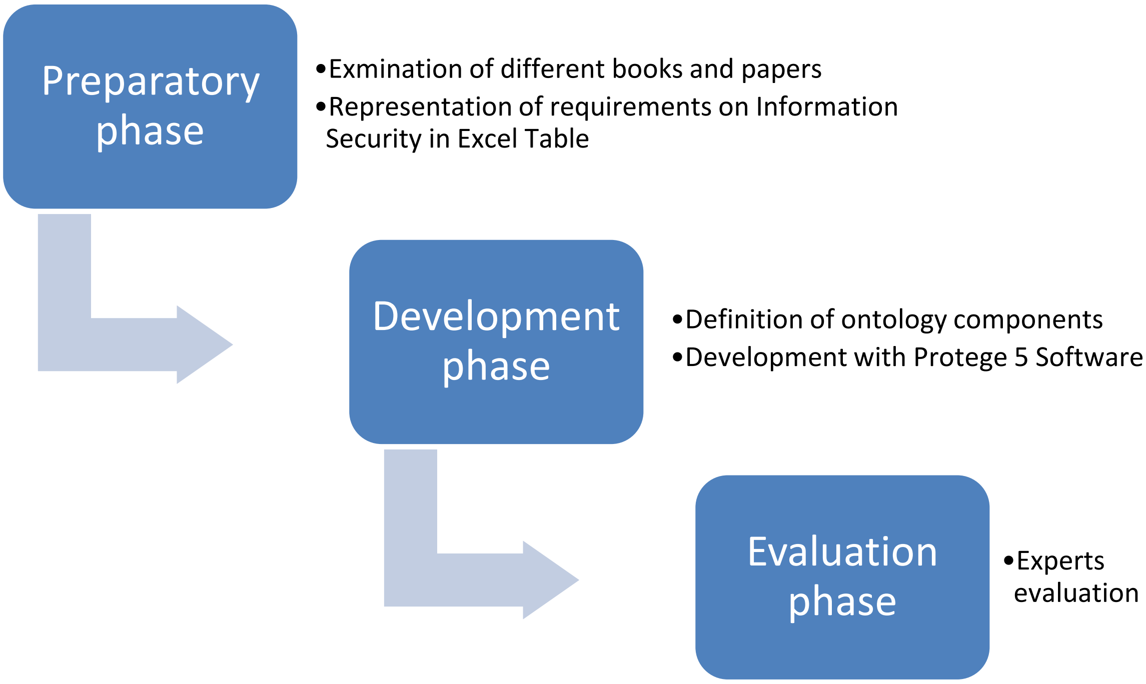

Preparatory phase
•Exmination of different books and papers
•Representation of requirements on Information Security in Excel Table
Development phase
•Definition of ontology components
•Development with Protege 5 Software
Evaluation phase
•Experts evaluation

Figure 6: Methodology of GDPR ontology

5.5.2. Design criteria

Considering the evaluation phase of GDPR ontology, it was necessary to define design criteria that should be taken into account when creating ontology, but also that will help later to evaluate design of this ontology. The possible evaluation of ontology is discussed in section 7.3. Design criteria that are possibly relevant for the evaluation of GDPR ontology development include:

1. **Accuracy:** All terms of ontology should be accurate and correctly represent aspects of GDPR. The evaluation based on this criterion involves review of ontology classes with GDPR legal text.
2. **Clarity:** All components and terms of ontology should be clearly and easy to understand defined. At the least, the defining terms should be logically consistent.
3. **Extendibility:** An ontology should be designed that one can extend ontology and to be able to define new terms for special uses,
4. **Easy to follow**: The representation of ontology has to be easy to understand for all users, with and without IT and ontology knowledge.

5.5.3. Scope of ontology

As recommended in [15], the development of ontology should begin with the domain and scope definition. As indicated in introduction, the scope of ontology will cover the GDPR requirements relevant for information security.

Therefore, as a second step were so-called competency questions defined which determine the scope of the ontology [15] and also at the end serve as test whether the ontology contains enough details to answer these questions or not:

- What are the principles of processing and what need to be considered?
- What are the rights of data subject?
- What are the main obligations of a data controller?
- What are functions of a data processor?
- What are the main obligations of a data protection officer?

- *What are the exceptions?*
- *What are necessary documents?*
- *Which standards are included?*

Note: The exceptions, necessary documents and standards are added in class description of specific classes and are not part of automated answering of this ontology.

5.5.4. Main areas

The proposed GDPR ontology consists of five areas, which are representing a basis for ontology development:

- **Data** which is collected for processing;
- **Organisation** which is processing personal data;
- **Data protection principles** described in GDPR;
- **Data subject's rights** described in GDPR;
- **Obligations** of controller and processor including compliance to GDPR.

5.5.5. Definition of ontology components and relations

Every of five GDPR ontology areas have their subclasses, respectively sub-subclasses and data properties. In the following table are represented all classes and 2nd level subclasses including their relations.

Areas	Description	Subclasses	
Data	This area covers which types of data can exist in organisation and what is meant by sensitive data in GDPR.	Personal data	Sensitive data
		Pseudoanonymous data	
		Anonymous data	
Organisation	The organisation area is containing a general information such as personal, state, size, sector and department of organisation. Therewith, the activity which is performed by organisation.	Person	Data Subject
			Controller
			Processor
			Authority
			DP Officer
		State	EU
			Non-EU
			EEA
		Size	Small and medium sized
			Large sized

		Sector	Technology
			Healthcare
			Education
			Financial
			Insurance
			Manufacturing
		Department	Marketing
			IT
			Human Resources
			Sales
			Finance
		Activity	Data activity
			Processing
			Consent
			Code of conduct
			Impact assessment
			Marketing
Principles	These principles are defined in GDPR and need to be considered by organisations when processing personal data.	Lawfulness, fairness and transparency	
		Purpose limitation	
		Data minimization	
		Accuracy	
		Storage limitation	
		Integrity and confidentiality	
Rights	This area is presenting the data subject rights given in GDPR.	Right to information	
		Right to access	
		Right to rectification	
		Right to be forgotten	
		Right to restriction of processing	
		Right to notification	
		Right to data portability	
		Right to objection	
		Right to automate appropriate decision making	
Obligations	This area consists of obligations of controller, processor and DPO including security measures, records of processing, data breach notification and so on.	Controller	
		Processor	
		DPO	
		Certification	
		Compliance	

Table 2: Ontology classes and main subclasses

Before implementing all classes with Protégé 5 software, it was essential to define relations between main areas and ontology classes. Relations help to better understand meaning of classes and their connections. Following table shows the main areas, which individuals are responsible for these areas and what are relations between them.

Main areas	Individuals	Relations
Data	Data subject	Has Data
Organisation	Controller, Processor	Is Part Of
Principles	Controller	Must Fulfil
Data Subject's Rights	Data subject	Has Right
Obligations	Controller, Processor, DPO	Has Obligation

Table 3: Main areas relations

As shown in table 3, individuals and relations between them are assigned to each of these main areas. For example, data subject is owner of its data. Moreover, data subject has some rights. Since data protection principles are underlying controller's obligations and data subject's rights, we define relation "hasObligation" that is relevant for controller, processor or DPO. In ontology every organisation activity, obligation, or data subject's right is a subclass of some principles. As an example of such approach, the controller "mustFulfil" principles when collecting, processing and managing personal information data of all European citizens.

In addition to basic relations between main areas, the high-level relations between ontology classes have been defined. These high-level relations will be used later in object properties while defining classes in Protégé 5 software.

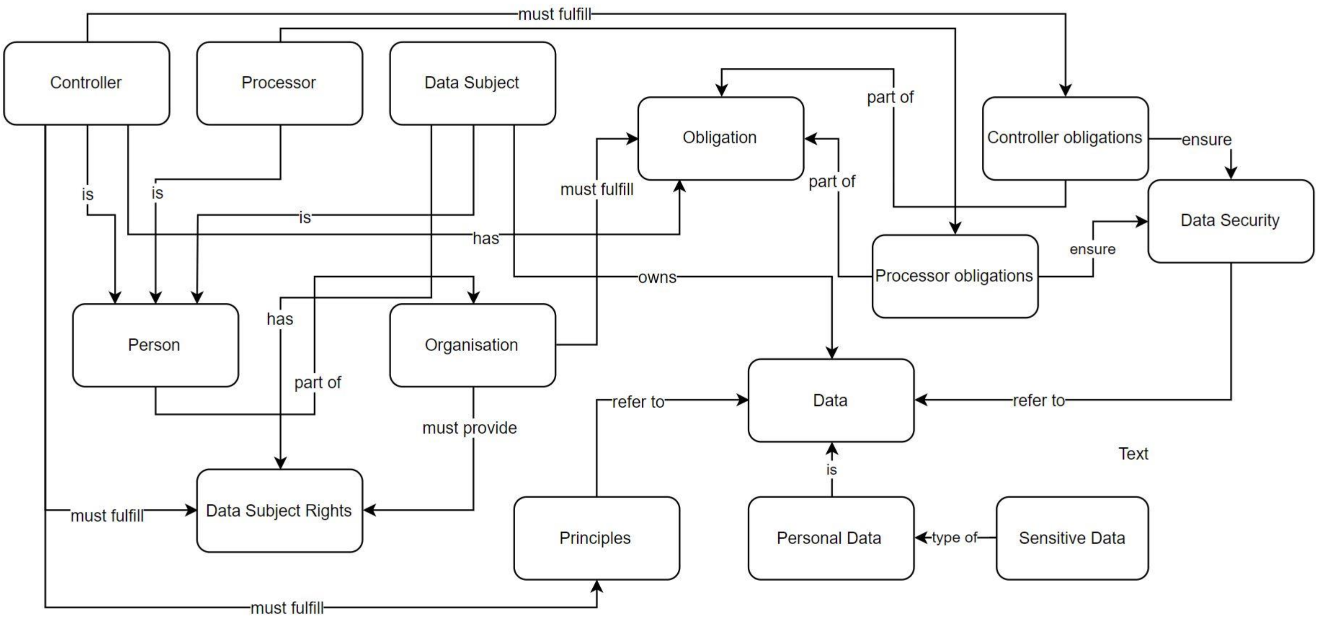


Figure 7: High-level ontology classes and relations between them

6 Implementation with Protégé 5 Software

6.1. General information about software

Protégé [54] is an open source editor for modelling and developing ontologies in computer science. This ontology editor was developed at the Institute of Medical Informatics at Stanford University in California and is now freely available as an open source application under the Mozilla Public License [55]. Protégé was originally developed to create knowledge databases or ontologies for medical research purposes. These ontologies in an informatic sense are formal, machine-readable representations of knowledge in a certain subject area (so-called domain), which is represented by so-called concepts and relations [54]. With Protégé, such knowledge databases can be created, filled with information and retrieved. The development and runtime environment are programmed in Java and therefore platform-independent.

Knowledge modelling with formal description languages is possible in Protégé in two ways:

- **Protégé-frames** works with the frame-based approach of knowledge representation, which provides information about specific domain knowledge in a hierarchical structure of concepts, attributes of concepts (slots) and concept instances (individuals) [54].

- **Protégé-OWL** is based on the Web Ontology Language (OWL) [56], the standard for ontology creation within the Semantic Web. In contrast to the frame-based approach, there are also logical mechanisms and explicit formal semantics through which implicit knowledge can be inferred from the modelled data structure - even across several ontologies and can be used to capture knowledge in a machine interpretable way. It also supports the latest OWL 2 Web Ontology Language and RDF [57] specifications from the World Wide Web Consortium.

Web Ontology Language has different sets of operators such as intersection, union and negation and is based on a logical model which makes it easier to define as well as to describe concepts [58]. It is especially applicable in domains, where complex concepts must be built up in definitions out of simpler concepts. Additionally, with help of a “reasoner” it is possible to check the consistency of classes and all statements and definitions in the ontology, but also to recognise which concepts fit under which definitions [58].

The main components used to model and develop ontology in Protégé are: classes, individuals, properties, and classes. In Protégé (OWL) classes are set of individuals, individuals represent objects in the domain and properties represent binary relations on individuals [58].

Classes are defined using formal descriptions that apply to all members of the class. For example, in the GDPR ontology the class “Personal data" would contain all the individuals that are seen as “Personal data” in this domain of interest. The classes are organised into a “superclass-subclass hierarchy” [58]. To explain this hierarchy, we will continue to consider the classes “Data” and “Personal data” – “Personal data” might be a subclass of “Data” (so “Data is the superclass of “Personal data). This says that, all “Personal data” are some kind of “Data”, and all members of the class “Personal data” are members of the class “Data”. The initial class hierarchy tree in Protégé contains one main class called “Thing”. As mentioned previously, classes are sets of objects. The class “Thing” is the superclass that contains all other classes, individuals or objects of one ontology. Because of this rule, all classes in ontology are subclasses of class “Thing” [58].

Individuals are an object in the domain and can be referred to as being “instances of classes” [58].

Properties, like already mentioned, represent relations and link two individuals together. For example, the property “isTypeOf” might link the individual “Sensitive data” to the individual “Personal data”. The relations between individual can have inverses. For example, the inverse of “hasObligation” is “isObligationOf”.
If “hasObligation” property links individual A to individual B then its inverse property “isObligationOf” will link individual B to individual A [58].

6.2. Ontology Properties

Protégé (OWL) distinct two main types of properties: Object properties and Datatype properties [58]. Object properties are relationships between two individuals and Datatype properties are linking the individual to the data literal. There is also a third type of property, which is not oft used, Annotation properties. The Annotation properties are used to add annotations to ontology classes, individuals and other properties. [58]
In guideline for developing ontologies [58] is recommended that property names “start with a lower-case letter, have no spaces and have the remaining words capitalised” [58]. This makes the property clearer and easy to understand to humans e.g. “hasObligation”, “isPartOf”, “isObligationOf”, “hasGrounds”, etc.

Most properties created in GDPR ontology are object properties.

6.2.1. Object Property Characteristics

The meaning of properties can be explained using property characteristics. The property characteristics can be: Functional, Inverse functional, Transitive, Symmetric, Antisymmetric, Reflexive and Irreflexive properties [58].

Functional Properties means that “for a given individual (object), there can be at most one individual that is related to the individual via the property” [58]. For example, individual Controller “appoint” Data protection officer and also the individual Controller “appoint” Processor, then the “appoint” property will be functional.

Inverse Functional Properties means that the inverse property of a given object is functional [58]. For example, inverse functional property can be property “isAppointedBy”. This is the inverse property of “appoint” — since “appoint” property is functional, “isAppointedBy” will be inverse functional.

Transitive Properties means that “one property relates individual A to individual B, and also individual B to individual C, then as a result individual A will be related to individual C” [58]. It is important to notice, if one property is transitive then its inverse property should also be transitive and cannot be functional [58].

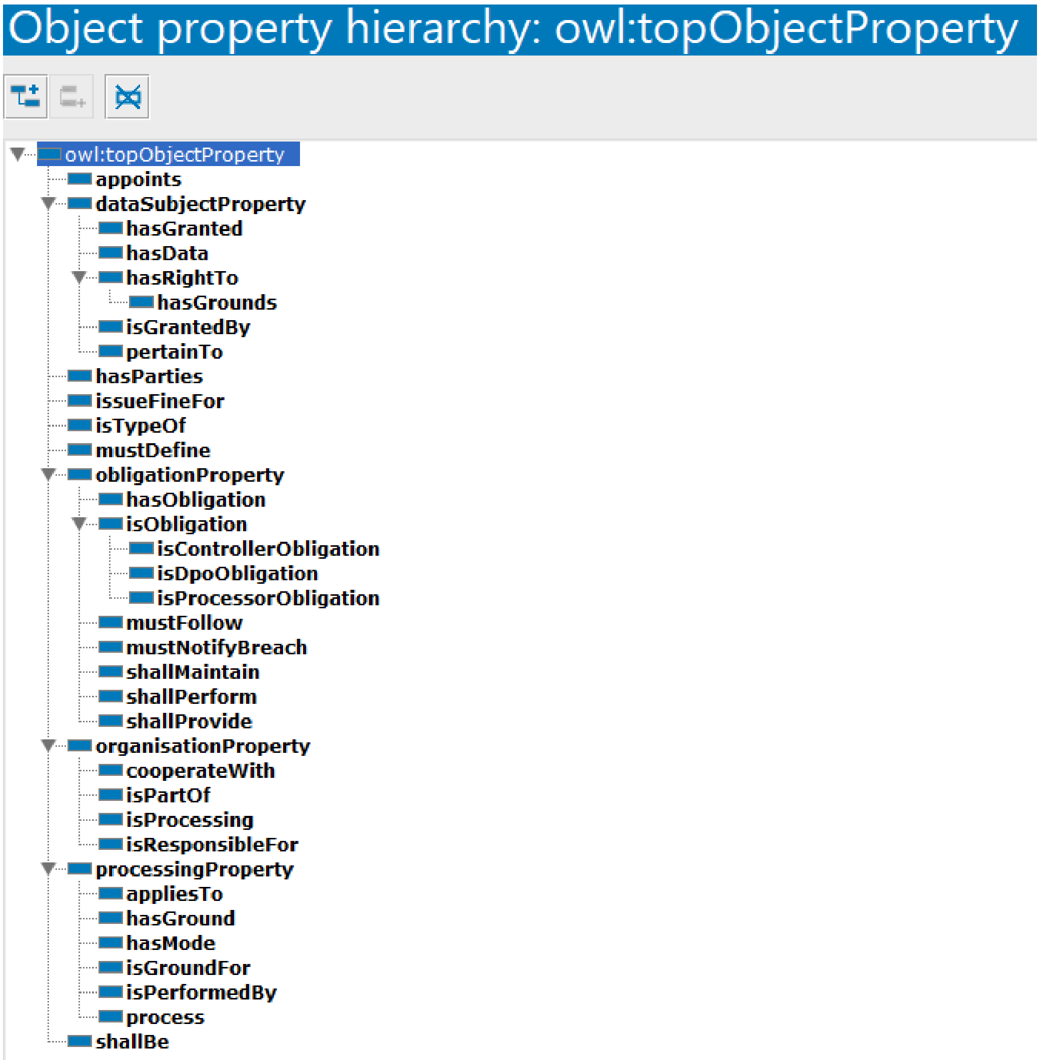
Symmetric Properties relate individual A to individual B and because of this property the individual B is also related to individual A. [58]

Antisymmetric properties relate individual A to individual B but the individual B cannot be related to individual A. [58]

Reflexive properties relate individual A to itself. [58]

Irreflexive properties can be explained as “a property that relate an individual A to individual B, where individual A and individual B are not the same” [58].

When creating Object properties, it should be noted that it is possible to form hierarchies of properties by adding some sub properties [58]. In case of GDPR ontology four main properties have been created: Data subject property, Obligation property, Organisation property, Processing property. These properties have their sub properties that specialise their super properties (just like in case of subclasses and their superclasses) [58]. For example, the property “isControllerObligation” and “isProcessorObligation” should be created as sub properties of the “Obligation property”.



Object property hierarchy: owl:topObjectProperty

- owl:topObjectProperty
  - appoints
  - dataSubjectProperty
    - hasGranted
    - hasData
    - hasRightTo
      - hasGrounds
    - isGrantedBy
    - pertainTo
  - hasParties
  - issueFineFor
  - isTypeOf
  - mustDefine
  - obligationProperty
    - hasObligation
    - isObligation
      - isControllerObligation
      - isDpoObligation
      - isProcessorObligation
    - mustFollow
    - mustNotifyBreach
    - shallMaintain
    - shallPerform
    - shallProvide
  - organisationProperty
    - cooperateWith
    - isPartOf
    - isProcessing
    - isResponsibleFor
  - processingProperty
    - appliesTo
    - hasGround
    - hasMode
    - isGroundFor
    - isPerformedBy
    - process
  - shallBe

Figure 8: Object properties hierarchy from Protégé Software

6.2.2. Property Domains and Ranges

In addition to characteristics, the properties specify a domain and range that link individuals from the domain to individuals from the range. [58] In the following table are represented all object properties, their domains and ranges as well as their characteristics used in GDPR ontology. Note, if object property has characteristic "None" means that it was not necessary to restrict or to define this property.

Object property		Domain	Range	Characteristics
Data Subject property	hasData	Data Subject	Data	Inverse functional Inverse of: pertainTo
	hasGranted	Data Subject	Consent	Inverse functional Inverse of: isGrantedBy
	hasRight	Data Subject	Data Subject Rights	Functional
	hasGrounds	Data Subject	Notification-Erasure-Restriction Grounds	Functional
	pertainTo	Person and Personal data	Data Subject	Inverse functional Inverse of: hasData
	isGrantedBy	Child consent or Consent	Data Subject	Inverse functional Inverse of: hasGranted
Obligation property	hasObligation	Controller and Processor and Data Protection Officer	Obligation	Inverse functional Inverse of: isObligationOf
	isObligationOf	Controller obligation	Controller	Inverse functional Inverse of: hasObligation
	isObligationOf	Processor obligation	Processor	Inverse functional Inverse of: hasObligation
	isObligationOf	DPO obligation	Data Protection Officer	Inverse functional Inverse of: hasObligation
	mustFollow	Controller and Processor	Principles	Functional
	mustNotifyBreach	Controller	Data Subject, Authority	Functional and inverse functional
	shallMaintain	Controller and Processor	Record of processing activities	Functional
	shallPerform	Healthcare and (Controller and Processor and ('Sensitive Data Processing'))	Impact assessment	Functional and inverse functional
	shallProvide	Controller and Processor	Transparent information, copy of data	Inverse functional
Organisation property	cooperateWith	Controller	Authority, Processor, Data Protection Officer	Functional, Inverse functional
	isPartOf	Organisation	Sector	None

	isProcessing	Healthcare	Sensitive data	None
	isResponsibleFor	Marketing	Direct marketing	None
Processing property	appliesTo	Processing	Personal data	None
	hasGround	Processing	Consent or Contract or 'Explicit purpose' or Legitimate or 'Specified purpose'	Inverse functional Inverse of: isGroundFor
	hasMode	Processing	Automated processing or Manual	Functional
	isGroundFor	Consent or Contract	Processing	Inverse functional Inverse of: hasGround
	isPerformedBy	Processing	Controller and Processor	Transitive
	processes	Controller and Processor	Data	Transitive
General property	appoints	Controller	DPO	Functional
	hasParties	Contract	(Controller and 'Data Subject') or (Controller and Processor) or (Controller and 'Data Protection Officer')	None
	issueFineFor	Authority	Controller and not (Consent or Contract or (Processing and (not ('Lawfulness, fairness and transparency'))))	None
	isTypeOf	Sensitive Data	Personal data	Functional
	mustDefine	Controller and Processor	Measures	Functional
	shallBe	Copy of data	Structured copy, machine readable, commonly used format	Functional

Table 4: Object properties of GDPR ontology

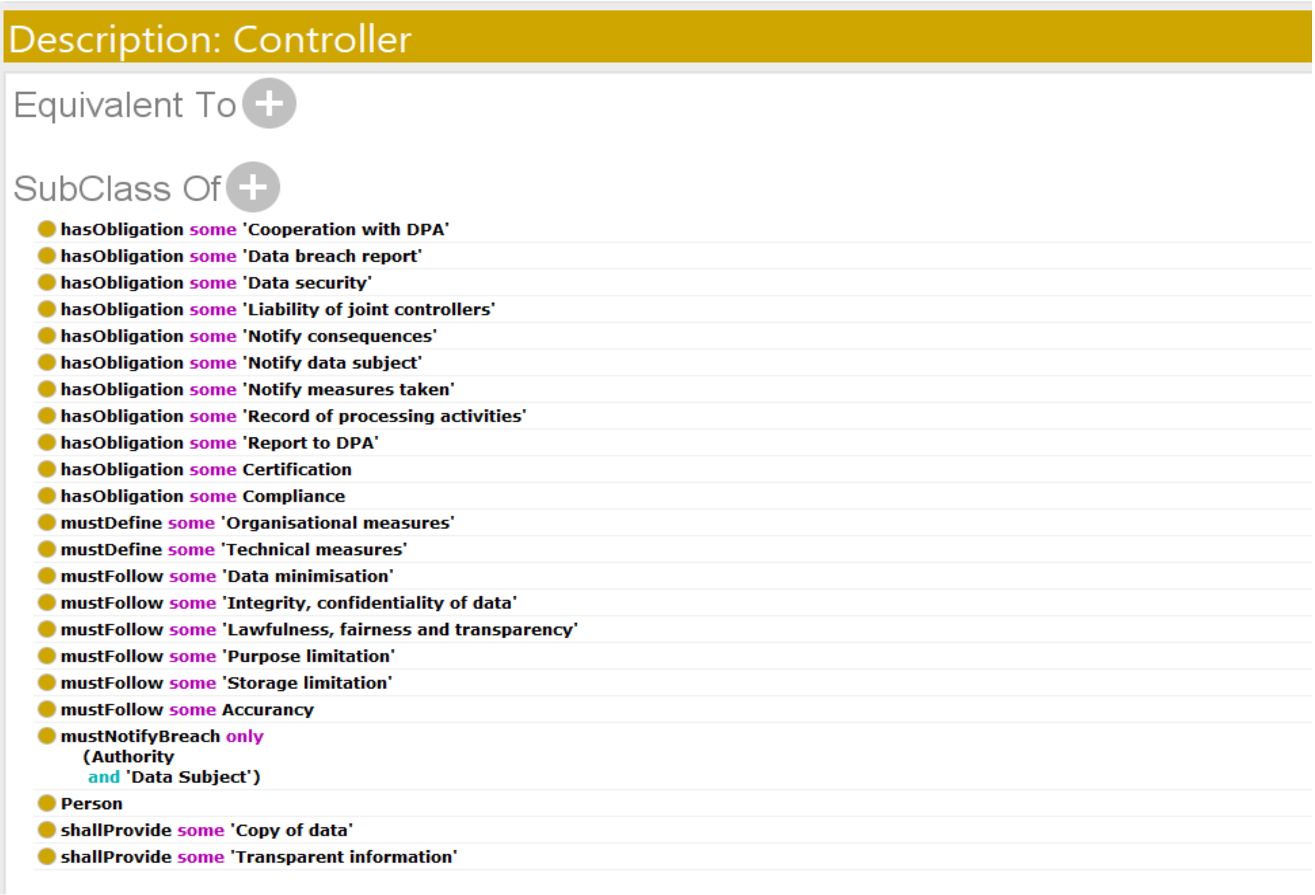
6.2.3. Restrictions

In order to describe classes of individual, it is necessary to use restrictions. OWL restrictions have three main categories: Quantifier Restrictions, Cardinality Restrictions, hasValue Restrictions [58]. In case of GDPPR ontology quantifier restrictions are used, which can be further categorised into “existential restrictions” and “universal restrictions” [58].

Existential restrictions are the most used restrictions in OWL and describe class of individuals that have “at least one relationship along a specified property to individuals that are members of a specified class” [58]. For example, the class of individuals that have at least one (some) property relationship to members of another individual. To denote these restrictions, Protégé software uses the keyword ‘**some**’ [58].

Universal restrictions describe, opposite to Existential restriction, classes of individuals that “for a given property only have relationships along this property to individuals that are members of a specified class” [58]. In Protégé the keyword ‘**only**’ is used.

Beside these two types of quantifier restrictions, there are also other restrictions in Protégé like ‘**max**’ or **‘min**’, which indicate that one individual has maximal / minimal one property relationship to another individual.



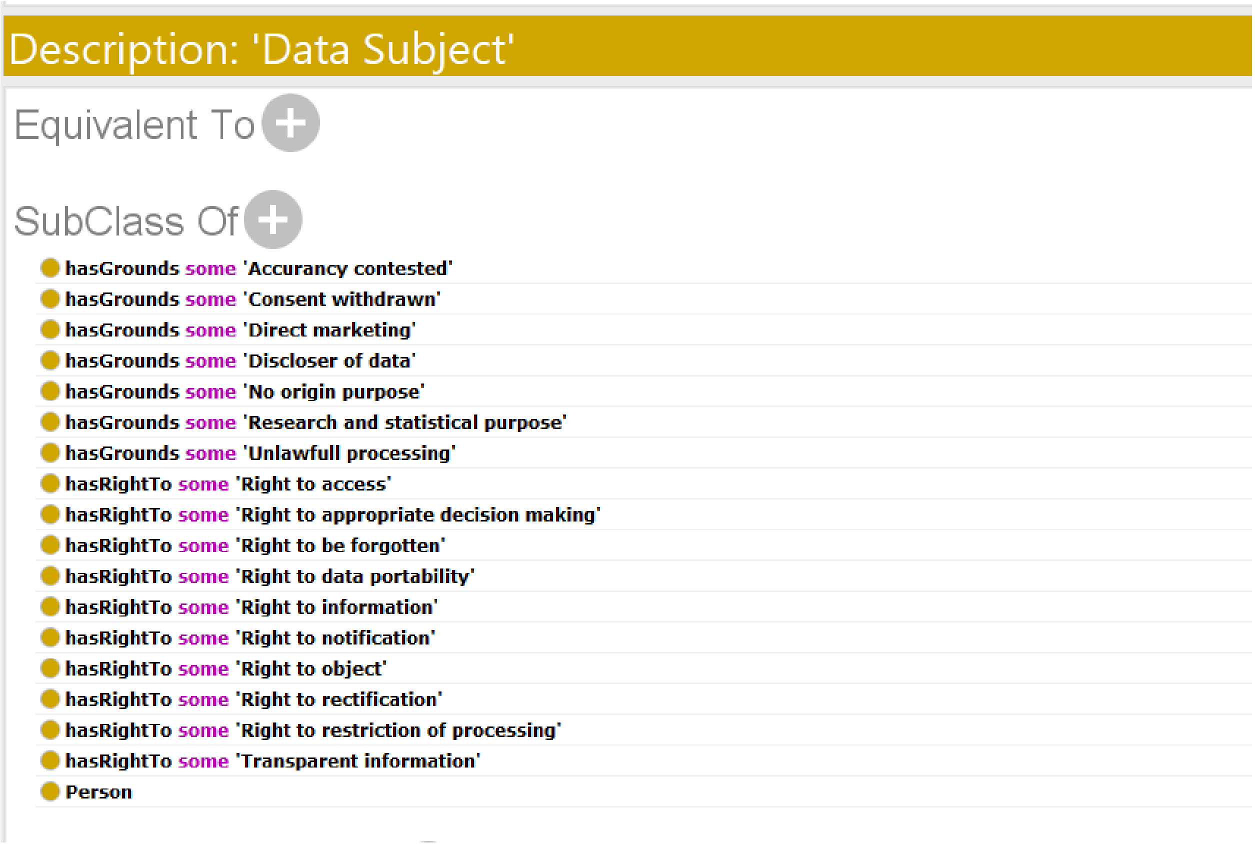
Description: Controller

Equivalent To

SubClass Of

● hasObligation some 'Cooperation with DPA'
● hasObligation some 'Data breach report'
● hasObligation some 'Data security'
● hasObligation some 'Liability of joint controllers'
● hasObligation some 'Notify consequences'
● hasObligation some 'Notify data subject'
● hasObligation some 'Notify measures taken'
● hasObligation some 'Record of processing activities'
● hasObligation some 'Report to DPA'
● hasObligation some Certification
● hasObligation some Compliance
● mustDefine some 'Organisational measures'
● mustDefine some 'Technical measures'
● mustFollow some 'Data minimisation'
● mustFollow some 'Integrity, confidentiality of data'
● mustFollow some 'Lawfulness, fairness and transparency'
● mustFollow some 'Purpose limitation'
● mustFollow some 'Storage limitation'
● mustFollow some Accurancy
● mustNotifyBreach only
(Authority
and 'Data Subject')
● Person
● shallProvide some 'Copy of data'
● shallProvide some 'Transparent information'

Figure 9: Example of Controller restrictions in GDPR ontology



Description: 'Data Subject'

Equivalent To

SubClass Of

- hasGrounds some 'Accurancy contested'
- hasGrounds some 'Consent withdrawn'
- hasGrounds some 'Direct marketing'
- hasGrounds some 'Discloser of data'
- hasGrounds some 'No origin purpose'
- hasGrounds some 'Research and statistical purpose'
- hasGrounds some 'Unlawfull processing'
- hasRightTo some 'Right to access'
- hasRightTo some 'Right to appropriate decision making'
- hasRightTo some 'Right to be forgotten'
- hasRightTo some 'Right to data portability'
- hasRightTo some 'Right to information'
- hasRightTo some 'Right to notification'
- hasRightTo some 'Right to object'
- hasRightTo some 'Right to rectification'
- hasRightTo some 'Right to restriction of processing'
- hasRightTo some 'Transparent information'
- Person

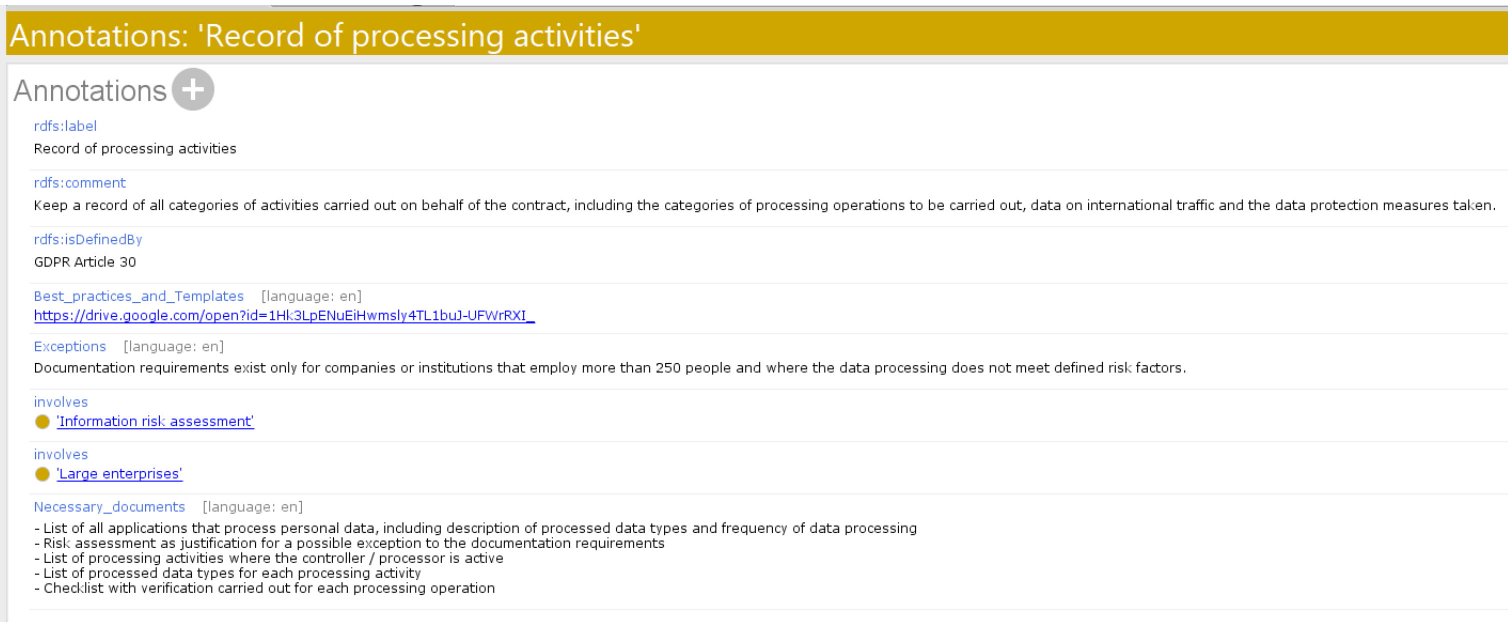
Figure 10: Example of Data Subject restrictions in GDPR ontology

6.2.4. Annotations

All classes in the GDPR ontology contain various pieces of information in their description field. For example, comments, label, defined article in GDPR and other references to resources such as web pages, books etc.

In GDPR ontology are used following annotations that annotate classes:

1. **rdfs:label** - names of ontology elements such as classes, properties and individuals
2. **rdfs:comment** - include definition of class
3. **rdfs:isDefinedBy** - reference in GDPR official document and other relevant standards
4. **rdfs:necessaryDocuments** - include what documents are necessary to be compliant with GDPR
5. **Best practices and Templates** - link with useful information, templates and other related documents



Annotations: 'Record of processing activities'

Annotations

rdfs:label
Record of processing activities

rdfs:comment
Keep a record of all categories of activities carried out on behalf of the contract, including the categories of processing operations to be carried out, data on international traffic and the data protection measures taken.

rdfs:isDefinedBy
GDPR Article 30

Best_practices_and_Templates [language: en]
https://drive.google.com/open?id=1Hk3LpENuEiHwmsly4TL1buJ-UFWrRXI_

Exceptions [language: en]
Documentation requirements exist only for companies or institutions that employ more than 250 people and where the data processing does not meet defined risk factors.

involves
● 'Information risk assessment'

involves
● 'Large enterprises'

Necessary_documents [language: en]
- List of all applications that process personal data, including description of processed data types and frequency of data processing
- Risk assessment as justification for a possible exception to the documentation requirements
- List of processing activities where the controller / processor is active
- List of processed data types for each processing activity
- Checklist with verification carried out for each processing operation

Figure 11: Example of annotations on ‘Record of processing activites’

The following diagrams (displayed in two parts for clarity) were generated using this software and display the main areas in ontology. The class hierarchy represents an "is-a" relation which means that a “class A is a subclass of B if every instance of A is also an instance of B” [15]. The detailed description of classes is provided in section 6.3.

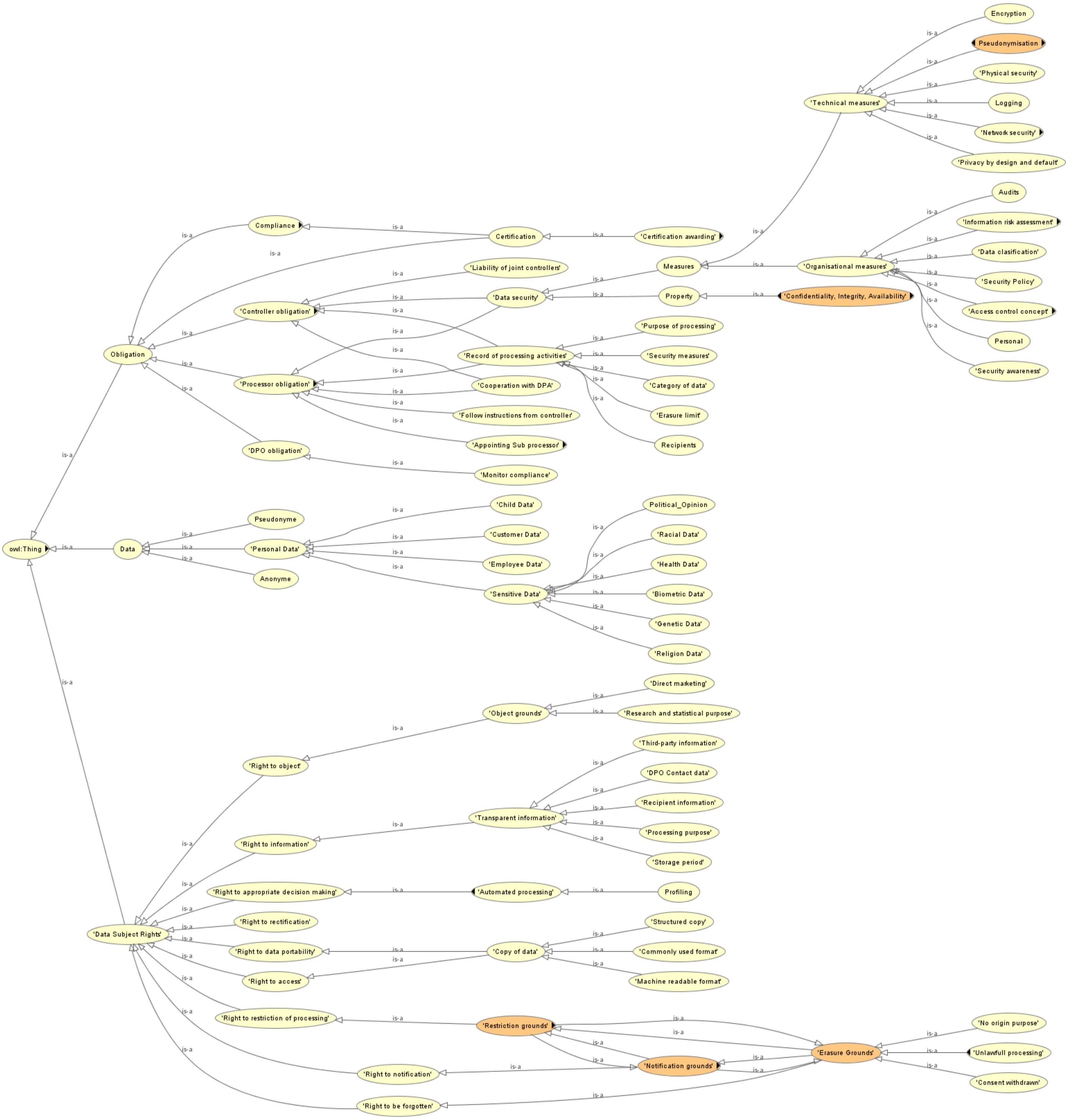


Figure 12: GDPR Ontology Part 1

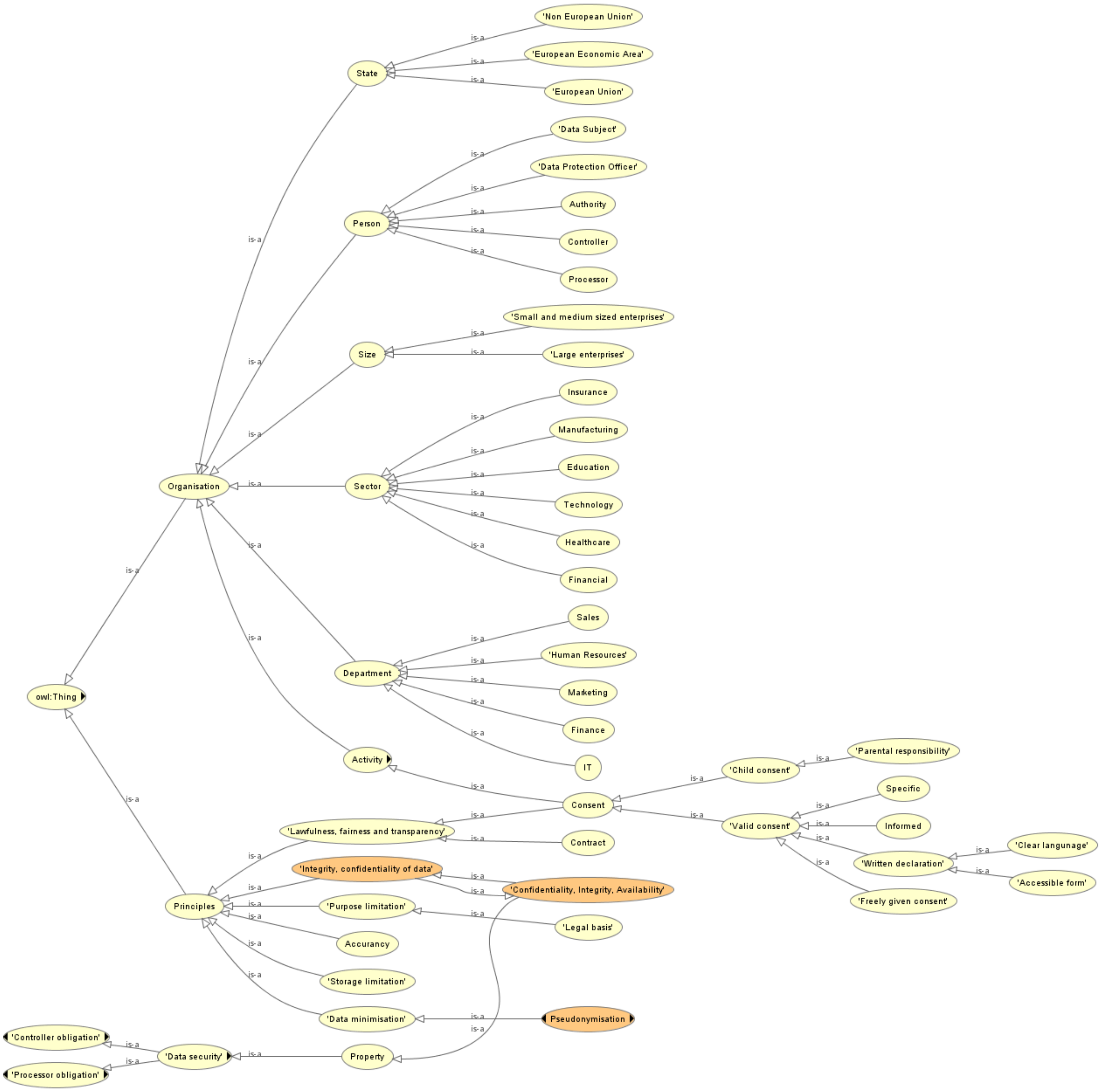


Figure 13: GDPR Ontology Part 2

6.3. Description of main areas

In this section are described main areas of GDPR ontology. The description contains all important information for specific area that need to be considered. Moreover, for every area are specified some recommendations and exceptions. For detailed description of classes see Appendices.

Note: Some parts in following sections (6.3.1 – 6.3.5) are marked by *italic writing.* These parts represent text stated in GDPR.

6.3.1. Main area: Data

Data area (Figure 12: GDPR ontology part 1) refers to the generic usage of the term 'data' and contains subclasses defining personal data along with the various specific types of sensitive personal data mentioned in the GDPR text. This also contains concepts related to representing anonymised and pseudonymised data. The provisions of the GDPR apply to the processing of personal data of natural persons. By definition, "personal data" means “*any information relating to an identified or identifiable natural person* ("data subject")” [7] .The types of personal or personal data are numerous. A final summary is hardly manageable. However, the following is a list of values to give a first impression of what is covered by personal data [59]:

- general personal data (name, date and age of birth, place of birth, address, e-mail address, telephone number, etc.)
- identification numbers (social security number, tax identification number, health insurance number, identity card number, matriculation number, etc.)
- bank data (account numbers, credit information, account balances, etc.)
- online data (IP address, location data, etc.)
- physical characteristics (sex, skin, hair and eye colour, stature, dress size, etc.)
- ownership characteristics (vehicle and real estate ownership, land registry entries, license plates, registration data, etc.)
- customer data (orders, address data, account data, etc.) and much more.

According to the GDPR, the *principles of data protection do not apply to "anonymous information"* [7], i.e. information that does not relate to an identified or identifiable natural person, or personal data that has been made anonymous in such a way that the person concerned cannot or can no longer be identified [60]. The regulation does not concern the processing of such anonymous data, nor does it apply to statistical or research purposes. [7] Therefore, the sub class anonymous data is considered as part of superclass data.

In addition, there are also special personal data that require increased protection. The rules for collecting and processing such data are much stricter. This kind of personal data are called sensitive data. Sensitive data include “personal data revealing racial and ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as the processing of genetic data, biometric data to uniquely identify a natural person, health data or data relating to a natural person's sex life or sexual orientation” [66], [7].

Another type of data mentioned in GDPR is child data. The GDPR sets an age limit of 16 years for the legality of a child's consent to the provision of information society services. This requirement is an open clause for EU Member States, so they can provide lower age limits, but not below the age of 13 [7]. The Austrian Data Protection Act (DSG) in the version of the Data Protection Adaptation Act 2018 sets this age limit at the age of 14. [27]

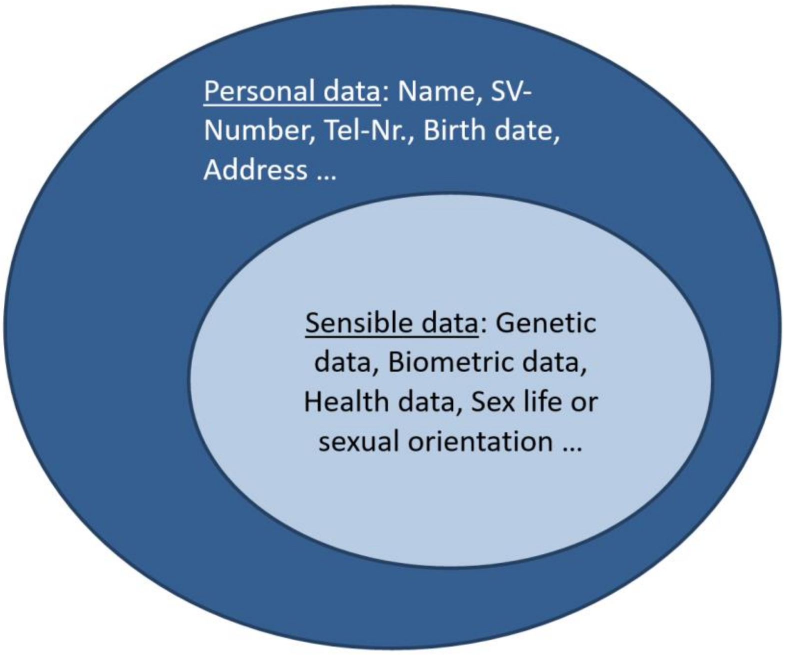

Personal data: Name, SV-Number, Tel-Nr., Birth date, Address …
Sensible data: Genetic data, Biometric data, Health data, Sex life or sexual orientation …

Figure 14: Graphical representation of personal data

Even today, many people are still too reckless in their handling of personal data - often out of ignorance of how valuable it can be for individual companies and authorities. Global data octopuses such as Google and Facebook collect data on the activities of users on the World Wide Web.
This master data (from location data to information on purchasing behaviour and contacts) is usually used for the placement of individualised advertising for the respective user. And above that, they ultimately generate annual profits in the millions. Personal data is therefore worth its weight in cash.

6.3.2. Main area: Organisation

The area Organisation (Figure 13: GDPR ontology part 2) consists of six main classes: Person, State, Sector, Size, Department and Activity.

Person

The main area “Organisation“ contains all relevant information for organisation which is processing personal data. Every organisation has persons involved in organisation processes. These persons can be

- a data subject, person who owns data,
- controller who processes data,
- processor who supports controller in processing of data,
- data protection officer who ensures that organisation is compliant with the regulation, and
- authority who supervises the whole process.

For example, the entrepreneur who records customer data (from natural persons) to create an invoice to the customer is controller. The external accountant who receives and processes the invoice data for the preparation of the balance sheet from this entrepreneur is a contract processor. Further examples for the contract processor are: cloud services providers, newsletter management providers, IT data maintenance providers. According to a recent decision by the data protection authority, tax consultants are not contract processors. [60]

Not every company is free to collect all the data it can get its hands on. [7] If it is permissible for public or non-public body to collect and process data, it must guarantee data protection. That means, persons or preciously employees who work in data processing must be instructed about data secrecy and require data protection training in the handling of the data records [33].

Size

The size of organisation also has a role in GDPR. The GDPR ontology distinct two types of organisation size. Some requirements of regulation are only addressed to Large sized organisations (more than 250 employees), on the other hand we have small and medium sized organisation with <250 employees. More preciously requirements depending of organisation size are discussed in Obligations area.

Sector

Every organisation can be part of some sector. In GDPR ontology are listed some possible sectors. The main idea of sector class is that some requirements of GDPR are refer to specific sector. For example, if an organisation is part of Healthcare sector it is more likely that the core activity of this organisation is processing special category of personal data (sensitive data). According to GDPR, every organisation or more preciously controller whose core activity is processing sensitive data, must perform impact assessment [7].

State

Another relevant fact for the organisation is its location. The organisation can be located in or outside the European Union or be a part of European Economic Area. The GDPR applies to the processing of personal data in so far as it takes place in the context of the activities of a controller or contract processor in the EU, irrespective of whether the processing takes place in the EU[66].
While data traffic within the EU is not restricted by the same level of data protection guaranteed by the GDPR, data traffic with third countries (or international organisations) is only permitted under the following conditions [60]:

- first, data processing within the EU must comply with the requirements of the GDPR,
- the level of protection for individuals, guaranteed throughout the Union, must not be undermined in the transfer of personal data in third countries or international organisations [40].

For the transmission of "non-sensitive data" to (additional or joint) persons responsible, it must be checked whether one of the following legal bases exists in the specific individual case [40], [7]:

- *the data subject has given his/her consent to the processing of his/her personal data for one or more specific purposes*;
- *data processing is necessary for the fulfilment of a contract or for the implementation of pre-contractual measures*;
- *processing is necessary to fulfil a legal obligation;*
- *data processing is necessary to protect the vital interests of the data subject or another natural person*;
- *data processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority conferred on the controller;*
- *processing is necessary to safeguard the legitimate interests of the data controller or a third party, unless the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.*

For special categories of personal data ("sensitive data"), the following grounds of legality may be considered [7]:

- *consent;*
- *the existence of a legal basis (including collective agreements) for exercising rights under law, social security and social protection law;*
- *protection of the vital interests of the data subject or another natural person (and the data subject is unable to give his/her consent for physical or legal reasons);*
- *data processing by a political, philosophical, religious or trade union foundation, association or other non-profit organisation within the framework of its legitimate activities on the basis of appropriate guarantees;*
- *personal data have obviously been made public by the data subject;*
- *for the assertion, exercise or defence of legal claims or proceedings of the courts during their judicial activity;*
- *for reasons of public interest in the field of public health, for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes (on the basis of Union law or the law of a Member State).*

In case of transferring data to contractors, no legal basis is required if an order processor contract has been concluded with the necessary content required by law [7]. If the data is transmitted within the EEA area (i.e. the EU states and the EEA states Liechtenstein, Iceland, Norway), no legal basis other than the general legal obligations, such as checking compliance with the required legal basis, need to be examined [60].

In case of transferring data to managers or processor in third countries or international organisation, in addition to the general legal obligations (e.g. the existence of legal bases for the transmission, compliance with the basic principles, fulfilment of the rights of the persons concerned, etc.), further legal bases must be examined [60].

Departments

Every organisation is made of several departments, which are performing some activity. For example, we have Marketing department which is responsible for direct marketing. By the definition, direct marketing includes addressed and unaddressed (advertising) messages addressed to selected persons or groups of persons [7]. The aim is to establish an interactive relationship with the target persons in order to induce them to an individual, measurable reaction. Both the sending out by companies themselves (e.g. sending out a direct advertisement by a hotel business) and the sending out by the advertising agency on behalf of their customer would be included [61].

It should be mentioned in particular that the GDPR itself provides *processing of personal data for the purpose of direct marketing as a possible legitimate interest* [7]. I.e. the processing of personal data for the purpose of direct marketing measures to existing customers for own products or services would be legal without consent, legal authorization or on the basis of a legitimate interest of the advertiser [67].

The right of objection of the persons concerned is to be emphasised. According to the GDPR, the ”*data subject has the right to object free of charge at any time to the processing of personal data concerning him/her for the purpose of direct marketing”* [7]. The same applies to profiling as far as it is connected with such direct advertising. If such a contradiction occurs, the data may no longer be used for these purposes. The person concerned must be expressly informed of this right in a comprehensible form that is separate from other information [60].

Activity

The activity within GDPR ontology can be data activity, impact assessment and consent relevant for GDPR. Data activity contains all activities related to data (collection, processing, archive, store, transfer). By collecting of data, it is necessary to take into account that data is accurate, that collection is needed for explicit or specified purpose and have a legal basis. Related to processing of data, GDPR ontology distinct two types of processing mode: automated and manual processing [7]. Part of automated processing is profiling.
The GDPR defines this as "*any type of automated processing of personal data consisting in the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects relating to the work performance, economic situation, health, personal preferences, interests, reliability, behaviour, whereabouts or relocation of that natural person*" [7].

One part of activity class is a consent. The data subject shall give his/her consent to the *processing of his/her personal data for one or more specific purposes* [7]. "*Consent must be given by a clear affirmative act voluntarily, in the specific case, stating in an informed and unequivocal manner that the data subject agrees to the processing of his/her personal data"* [7]. This consent may be given in writing form, electronically or orally, for example by ticking a box on a website, by selecting technical settings for information society services or other declarations or behaviours that clearly indicate the consent of the data subject to processing in the respective context [68]. If the processing serves several purposes, separate consent is required for each purpose of the processing. In case of processing of sensitive data an "explicit" consent is required [7].

Another relevant part of organisation activity is impact assessment. An adequate risk management should precede a data protection impact assessment. If the risk assessment of the individual data processing comes to the conclusion that it "*represents a high risk for the rights and freedoms of the data subject, a data protection impact assessment must be carried out"* [7] - especially if an automated decision is to be made for the data subject, masses of sensitive data are processed, or publicly accessible areas are systematically observed on a massive scale [40].

Moreover, after completion of an impact assessment, the person responsible must also independently assess whether an identified risk can be prevented (if not it is recommended to consult with the supervisory authority) [40]. A data protection impact assessment should be carried out in particular for processing operations using new technologies, as the effects of these new technologies are not yet known in practice [7]. The following cases are listed in which data protection impact assessments must be carried out [7], [40]:

- *the systematic and comprehensive automation-supported evaluation of personal aspects, e.g.: profiling;*
- *the extensive processing of special categories of personal data or personal data relating to criminal convictions and criminal offences;*
- *the systematic monitoring of publicly accessible places property of private individuals, i.e. natural persons, but also legal entities.*

An impact assessment shall be carried out before starting processing operations [40]. According to GDPR, minimum content of a data protection impact assessment is [7]:

- *a systematic description of the planned processing operations and the purposes of the processing, including, where appropriate, the legitimate interests pursued by the controller;*
- *an assessment of the necessity and proportionality of the processing operations in relation to the purpose;*
- *an assessment of the risks to the rights and freedoms of the data subjects;*

- *the remedial measures planned to address the risks, including guarantees, safeguards and procedures to ensure the protection of personal data and to demonstrate compliance with the regulation [7].*

6.3.3. Main area: Principles

Principle area (Figure 13: GDPR ontology part 3) gives an overview of general data protection principles provided in GDPR but also in Data protection Handbook [25]. Key principles of European Data Protection Law are:

- Lawfulness, fairness and transparency,
- Purpose specification and limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity, confidentiality of data

Lawfulness, fairness and transparency

This principle refers to the responsibilities of the person responsible under Article 12 of GDPR [7] including the provision of accurate, easily accessible and comprehensible information to the data subject about the data collection, its scope and its continued use (Recital 39) [7].

Purpose specification and limitation

In the regulation is laid down, that data may be collected (only) for “*specified, explicit and legitimate purposes”* [7]. Processing for purposes other than the original purposes is regulated differently. While the GDPR permits further processing only if it is "compatible with the original purpose", the transfer and use is permitted for another purpose if it is necessary for the "responsible interests" of the responsible body and "a reason for the assumption that the legitimate interest of the interested party in excluding the processing or use is outweighed " [7].

Exception for this principle are *further processing for scientific, historical (research) purposes or statistical purposes* [7].

Data minimisation

This principle states that “data collected and processed should not be held or further used unless this is essential for reasons that were clearly stated in advance to support data privacy” [70]. An organisation should identify the minimum amount of personal data which is needed to fulfil purposes of processing [60]. Therefore, according to GDPR organization is allowed to hold that much information, but no more.

Accuracy

Accuracy principle means that organisation must ensure the accuracy of all personal data used for processing while taking reasonable measures to achieve this principle, ensuring that the source and status of personal data is clear and considering any challenges to the accuracy of information [7]. Besides that, all technical and organisational measures must be taken to ensure that inaccurate personal data is deleted or corrected [40].

Storage limitation

“Personal data must be stored in a form which permits identification of the data subject for no longer than is necessary for the purposes for which it is processed” [71]. In particular, this requires that the storage period for personal data be limited to the absolutely necessary minimum [40].

Integrity and confidentiality

Personal data must be processed in such a way *as to ensure adequate security of personal data* [7]. Appropriate technical and organisational measures are also intended in particular to ensure that unauthorised persons have no access to the data and cannot use either the data or the equipment with which they are processed. The content of this principle is not a completely new fact, but a highlight of the, in the everyday life constantly increasing use of IT, importance of security and confidentiality of personal data [60].

6.3.4. Main area: Rights

The Rights area (Figure 12: GDPR ontology part 1) presents the data subject rights which are, as the name suggests, rights of the person affected by an application of data (data subject) against the person responsible [6]. For example, it can defend itself against incorrect or incomplete data records or request that data be deleted again. According to GDPR, following rights are assign to data subject [7]:

- Right to transparent information
- Right to be forgotten
- Right to notification
- Right to rectification
- Right to restriction of processing
- Right to data portability
- Right to appropriate decision making
- Right to objection
- Right to access

Right to transparent information

The controller shall take appropriate measures to provide the person (data subject) concerned with all information and communications in “*a concise, transparent, intelligible and easily accessible form, using clear and plain language”* [7]. The information shall be transmitted in writing, electronically, orally or in any other form, depending on request of data subject [72]. In GDPR ontology under the term “Transparent information” is to understand information about processing purpose, storage period, recipient information, DPO contact data and third-party information.

Right to be forgotten (Right to erasure)

According to the regulation every data subject has right to obtain from the controller the erasure of personal data concerning [7]. In the GDPR ontology this class contains subclass “Erasure grounds” which represents precondition for this right. A precondition for the right of deletion is that one of the following reasons applies [7]:

- *the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;*
- *the data subject has withdrawn his/her consent to data processing (and there is no other legal basis), in particular data of a child collected in connection with an information society service offered to him/her or*

- *the personal data have been processed unlawfully.*

If any of these reasons apply, data subject can exercise right to erasure and controller must delete personal data without undue delay [60].

Right to notification

This right is associated with the controller obligation to notify recipients about erasure of personal data or restriction of processing [7]. If data have been rectified, deleted or restricted at the request of a data subject, the data controller shall inform any other party to whom the data have been disclosed of the assertion of such claims [40]. An exception exists only if this notification obligation would be impossible or would involve disproportionately high costs. According to GDPR, data subject has right to information about these recipients. [7]

Right to rectification

The data subject has a right to rectify their personal data [7]. A precondition for the claim is that the data is incorrect, i.e. does not correspond to reality (e.g. incorrect date of birth) or that the data is incomplete taking into account the purpose of processing [72].

Right to restriction

The data subject has right to restrict the processing of his/her personal data. A condition for the right of restriction is that one of the following reasons applies [7]:

- *the data subject has disputed the accuracy of the personal data;*
- *the data subject has objected processing;*
- *the processing is unlawful, and the data subject has refused to delete the personal data and has instead requested that the use of the personal data be restricted;*
- *the data controller no longer needs the personal data for the purposes of the processing, but the data subject for the assertion, exercise or defence of legal claims.*

Right to data portability

The right to data transferability enables the data subjects to obtain his /her personal data and to reuse them for their own purposes and for various services [7]. In GDPR ontology a controller should provide structured copy of data in commonly used and machine-readable format.

Right to appropriate decision making

Data subject has "*right to not to be subject to a decision based solely on automated processing*" [7]. Appropriate decision making is related to the automated processing where a decision is decision made automatically, without any human involvement [73].

This automated processing includes especially profiling [60]. This kind of processing can lead to quicker and more consistent decisions, but also represents significant risks for individuals [62]. Therefore, data subject has right to not to be subject of automated processing.

Right to object

The data subject has the "*right to object to processing of their personal data"* [7]. If data subject has exercised this right, the controller is not allowed to continue processing the data of that person [72]. In GDPR ontology this class has some “objection grounds” that are known from regulation and can be asserted in various situations [7]:

- *personal data are processed for direct marketing purposes;*
- *personal data are processed for scientific or historical research purposes or statistical purposes;*

6.3.5. Main area: Obligations

The main area “Obligations” (Figure 12: GDPR ontology part 1) outlines obligations relevant for controller, processor and data protection officer. Moreover, this area includes some compliance suggestions, necessary to prove that these obligations are compliant with GDPR.

Controller obligations

Data controllers are one of the most important persons involved in the processing and, under the GDPR, have responsibilities and obligations regarding the protection of personal data and data subject’s rights [7]. The main responsibility of data controller is to be compliant with the GDPR. Therefore, class “Controller obligations” contains duties and tasks necessary to demonstrate compliance with the GDPR. These obligations are privacy impact assessment, data breach notification, data security, cooperation with Data Protection Authority, record of processing activities and liability of joint controllers.

One of the controller obligations is to keep a record of processing activity. Article 30 of GDPR [7] regulates the obligation that the controller, but also a processor, must “*keep a list in which all processing activities which are subject to their responsibility are included”* (until now in Austria there was only the obligation to report internal data processing procedures in the Austrian data processing register, but not to keep an internal company list) [27].
This obligation has an exception, namely size of organisation. Only large size organisations (more than 250 employees) have obligation to record their processing activities [7]. Once this first hurdle in the number of employees has been overcome, three additional prerequisites must be met for the exception to take effect: [40]

- processing does not pose a risk to rights and freedoms - GDPR generally speaks of risk and not of special or significant risks, therefore all risks should be taken into account. Since any processing of personal data carries risks, this criterion has no value;

- not only occasionally processing - this condition refers to a processing in the singular: if exactly this does not only occur occasionally, then the exception does not apply either and a directory of processing activities has to be created. What is meant by "not only occasionally" is not clear defined in the regulation [40]. This may mean processing that takes place only sporadically, such as taking photographs at a company event;

- no special categories of data, e.g. - when controller is processing the special categories of data, it is necessary to keep a record of processing activities, due to the special risks (e.g. when a pharmacy processes the health data).

An exception always refers only to special processes that may be exempt from the obligation. A company with fewer than 250 employees should check whether and for which special processing the exception applies. In case of uncertainty, it is better to include the processing in a directory as a precautionary measure than to take a risk [40].

The form of the record is left on controllers and processors. It can be in writing or in an electronic format [7]. The requirement is that the directory must be "somehow" represented in order to be made available and easy to follow for the authority.

According to some sources [6], [40] [2] a record of processing activities should contain following information:

- name and contact details of the controller, representative and a data protection officer,
- description of purposes,
- categories of data subjects and personal data concerned,
- categories of recipients to whom the personal data have been disclosed, including recipients in third countries or international organisations,
- transfer of personal data to a third country or to an international organisation,
- time limits for deletion and
- general description of technical and organisational measures.

Data Security

The controller must implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Art 32 of GDPR contains the provisions on "security of processing" (ensuring data security, taking into account the state of the art and implementation costs, as well as the probability and level of risk to rights and freedoms [7]. Organisations should not assume that the current measures they have taken in accordance with the provisions of the DPA 2000 in the area of data security are already sufficient [60]. Article 32 of the GDPR requires a number of more specific safety measures than the provisions currently in force in order to achieve a level of protection appropriate to the risk, including GDPR’s Data Protection by Design and by Default principles [7].

Measures which controller must implement are divided into technical and organisational measures. The GDPR ontology contains some measures that are already known from the Article 32 of GDPR and controls from Information Security Management Systems (ISMS) [40]:

- performing a risk analysis;
- pseudonymization and encryption of personal data;
- ensuring confidentiality, integrity, availability and resilience of the systems. Resilience is the new criterion mentioned in the regulation and is closely related to "availability". IT systems and applications should offer a response time behaviour (performance) that is appropriate for the respective data application, which is influenced by the number of users and their requests, as well as the hardware and software used;
- restoring systems in case of a physical or technical incident;
- review, evaluation and evaluation of the effectiveness of the measures - Audit process.

According to [40] it is recommended to set up an ISMS, as well as to follow the international requirements of the ISO /IEC 27000 series of standards (in particular ISO 27001 and ISO 27002). Additionally, the newly revised and restructured "Austrian Information Security Manual" (version 4.0.1) [63] is also based not only on the BSI basic protection catalogues, but also on these two standards [40].

Data Breach Report

Another obligation of the controller is to *report data breaches to the supervisory authority and to notify data subject affected by a violation of the protection of personal data* [7]. Data breach is defined as a loss of complete control over the data itself and therefore also over what happens to this data (data breakdown) [40]. Article 33 of GDPR deals with the reporting of violations of the protection of personal data to the supervisory authority and Article 34 with the notification of the affected person. In many cases, the new system will ensure that data subjects are actually informed about a data outflow affecting them and can act accordingly.

According to Article 34 of GDPR " *When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*" [7].

What is meant by high risk is not defined in regulation, but it is possible to interpret it on the basis of Recital 85 [40]:

- *loss of control over personal data: unauthorised publication of data;*
- *risk of restricting rights;*
- *identity theft: a login to a harmless website, access to a chargeable service, access to sensitive data;*
- *financial losses: published trade secrets, loss of orders;*
- *unauthorized removal of pseudonymization: names of participants in medical studies become known;*
- *damage to reputation: make a negative assertion under a false name;*
- *loss of confidentiality: data subject to professional secrecy (doctor, lawyer);*
- *other significant economic or social disadvantages.*

Controller has obligation to report the breach to the supervisory authority within 72 hours [7]. According to GDPR this report should at least contain [7]:

- *a description of the nature of the breach, where possible indicating the categories and approximate number of persons and records concerned;*
- *the name and contact details of the data protection officer or another contact point for further information;*
- *description of the probable consequences;*
- *description of the measures taken or proposed by the person responsible to remedy the breach and, where appropriate, measures to mitigate its possible adverse effects.*

Cooperation with authority

Among other obligations and responsibility, data controller shall cooperate, on request, with the supervisory authority in the performance of its tasks [7].

Liability of joint controllers

Article 26 of the GDPR regulates the joint controllers responsible for processing. Pursuant to Article 26(1), several entities are "joint controllers" when they jointly / together determine the purposes of and the means of processing. This definition is consistently based on Article 4, according to which one controller *is the body that alone or together with others decides on the purposes and means of processing personal data*. [7]

Therefore, in cases where more than one controller shares the responsibility, controller has obligation to clarify who has to fulfil which tasks from the [7]. Because of this, joint controller must conclude an agreement in which they determine in a transparent manner which of them fulfils which obligations for compliance with the obligations under the GDPR, in particular the rights of the data subjects and the duties to provide information pursuant to Articles 13 and 14 of the GDPR [7].

Processor obligations

The processing of data on behalf of the processor entails a number of obligations. The obligations of processor do not differ much from those of the controller. First of all, it is important to conclude a contract for order processing in accordance with Article 28 of the GDPR [7]. Without such a written contract, there is no legal basis for order processing.

Record of processing activities

Alongside of controller, a processor has also obligation to ensure a security of data and keep a directory of processing activities. The only difference between these directories is its content. The processors directory shall at least contain following [7]:

- *name and contact details of the order processor and each person responsible, as well as, if applicable, the representative of the person responsible or the order processor and a data protection officer;*
- *categories of processing carried out on behalf of each responsible person;*
- *information about transfer of personal data to a third country or to an international organisation;*
- *for each processing category, a general description of the technical and organisational measures - these details are in any case part of the contract with the processor.*

Appointing sub processor

In cases where a processor engages another processor for carrying out specific processing activities on behalf of the controller, it is necessary to conclude processing contract between the processor and the other contract processors, which satisfies the requirements of GDPR and does not fall below the data protection obligations of the contract between the controller and the primary processor [7].

Cooperation with DPA

Beside controller, also the processor and shall cooperate with the supervisory authority in the performance of its tasks [7]. However, this obligation only applies to clarifications of facts which can only be obtained with the help of the processor.

Data breach notification

In case of data breach, the processor has obligation to contact controller [7]. This class in GDPR ontology is equal to Data breach report class.

Data security

The processor has also obligation to take all technical and organisational measures necessary for data security in accordance with Article 32 of GDPR [7]. The exact measures to be taken must be described as precisely as possible, as they are intended in particular to provide information as to whether there may be a violation of duty.

In addition to the actual implementation of technical and organisational measures, the processor must offer appropriate guarantees to the controller in accordance with GDPR [60]. Related to Recital 83, these guarantees should enable the processor to demonstrate that these technical and organisational measures result in lawful data processing and that the rights of the data subject are sufficiently taken into account [7].

Follow instructions from controller

The agreed contract between controller and processor must provide obligations of the processor to "*process personal data only on documented instructions from the controller"* [7]. In this case, processor must follow instructions from controller such as out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects. The processor is also contractually obliged to support the responsible person in complying with his obligations. These obligations include the adoption of technical and organisational measures reporting data protection violations to supervisory authorities, notification of persons affected by data protection violations, support in a data protection impact assessment and consultation of the supervisory authority in the case of high-risk processing [7], [66].

DPO obligation

The main obligation of data protection officer is to monitor compliance of implementation of GDPR [7]. The GDPR sees the data protection officer as an instrument of control for the controller prior to the official procedure. In the following cases, data protection officers must be appointed [7]:

- *authorities or public authorities* - examples: a federal minister, a state government, ASFINAG AG, a state court (for purposes of justice administration), the data protection authority itself, ORF...
- *undertakings - where the core activity is to carry out processing operations which require extensive regular and systematic monitoring of data subjects [40].* Examples: Credit agencies, banks, insurance companies - operating valuation platforms and comparison portals, big data analysts, IT service providers...
- *companies must also appoint a data protection officer if their core activity is the processing of specific categories of data or data relating to criminal convictions and offences.* Examples: Hospital owner, provider of DNA sample testing.

In order to fulfil its tasks, the Data Protection Officer must have a certain professional qualification and practice in data protection domain. All tasks and duties of a company data protection officer are regulated and comprise in Article 39 of the GDPR [7]:

- *information and advice for the controllers, contractors and employees,*
- *monitoring compliance with the GDPR and special national regulations sensitisation and training,*
- *consulting and monitoring in connection with the supervisory authority.*

Certification and Compliance

Every company that offers goods or services in the European Union (EU) must comply with the GDPR [7]. Understanding the data protection regulations of the GDPR and implementing them correctly in the company is a great challenge. Therefore, GDPR introduces certification mechanisms and data protection marks, in order to enhance transparency and compliance with this regulation. [40]

For larger companies it is relevant to provide evidence of an adequate level of security through recognised certificates. These may include ISO 270xx certificates and the European Privacy Seal (EuroPrise) [64], which is geared to data protection compliance.

These classes in GDPR ontology contain also some information of certification awarding such as adherence and validity of a certificate.

7 Visualization and use case of ontology

7.1. Visualization with Protégé Plugins

This section provides some existing approaches and tools for visualizing ontology. In order to visualize the ontology in different ways, it is necessary to install some plugins for the ontology editor Protégé 5.

Over the years different visualisation techniques aiming to analyse and understand complex information structures have been described. Visualisation models and techniques vary according to user's need. However, for better understanding using a combination of various types of visualization is recommended [65].

- **OntoGraf**

OntoGraf [66] is a plugin for visualizing OWL ontologies for Protégé and is already included in the normal installation of the ontology editor from version 4.1. Classes and instances are displayed with OntoGraf as rounded rectangles with different symbols and relations are mapped to these edges.

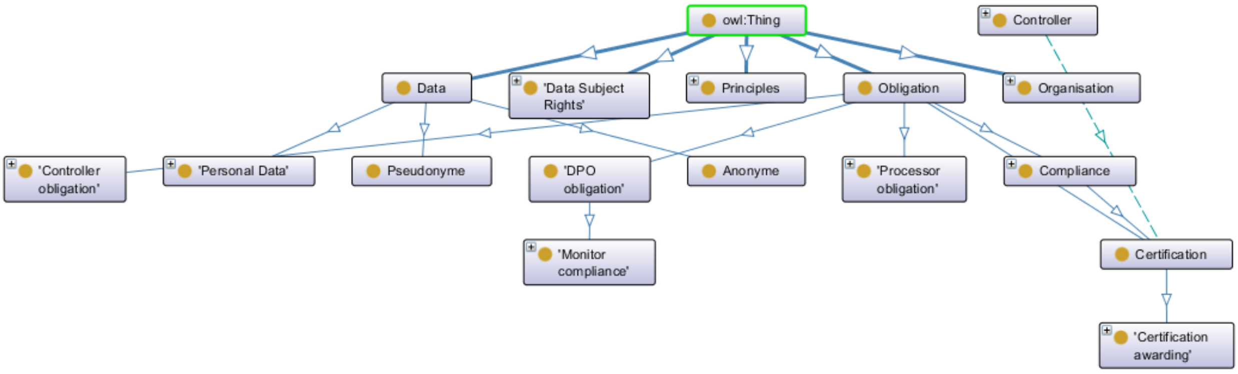


Figure 15: Representation of class hierarchy using OntoGraf

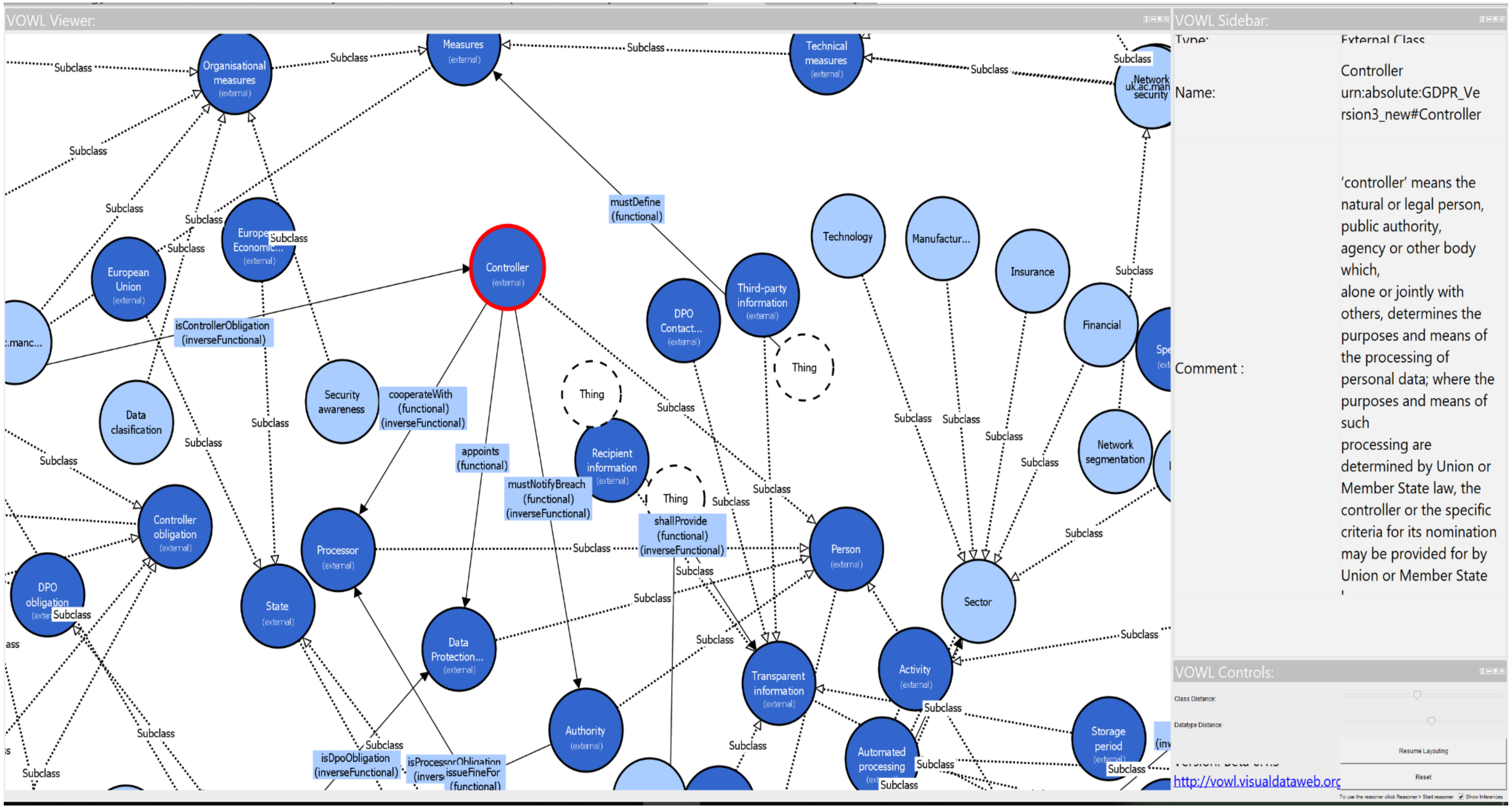
Figure 15 shows a part of class hierarchy created using OntoGraf Plugin in Protégé 5. OntoGraf offers several different layouts for the arrangement of nodes, including a grid, a radial, a force-based and in different directions-oriented tree representations. The plug-in supports subclass relationships and equivalence as well as object properties [66]. The view can be filtered by different types of relationships or nodes. The display can be enlarged or reduced (zooming) and the image section can be moved (panning). If the user moves his mouse over a node, further information is displayed in a tooltip. By double-clicking, subclasses of a parent class can be shown or hidden, and nodes can be fixed at a specific position using a pick and pin. OntoGraf also offers a search function for classes and instances.

- **Protégé VOWL**

VOWL is a visual notation specification for OWL ontologies. VOWL is primarily aimed at users who want to get an overview of an ontology but are not experts in the field of ontologies. In VOWL, OWL elements such as classes and properties are mapped to graphical elements and connected to a node edge graph. The most important components of VOWL are the graphical primitives, a color scheme, the force-based layout for the graph display and the rules for the multiple display of certain elements for a clearer display. In VOWL, classes are displayed as circles, data types and names for properties as rectangles and properties themselves as directed edges. The color of the circles and/or rectangles also indicates whether the respective element is deprecated or belongs to an external or the RDF namespace.

The ProtégéVOWL [67] presented is the first implementation of VOWL 2.0. ProtégéVOWL is a plugin written in Java for the ontology editor Protégé and uses the visualization toolkit "Prefuse" for graph representation.

This plugin consists of three parts: Besides the graph display on the left side, there is a sidebar for further information on the currently selected element (top right) and an area for adjusting and controlling the force-based graph layout (bottom right).



VOWL Sidebar:

Type: External Class

Name: Controller urn:absolute:GDPR_Version3_new#Controller

Comment : 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State

VOWL Controls:

http://vowl.visualdataweb.org

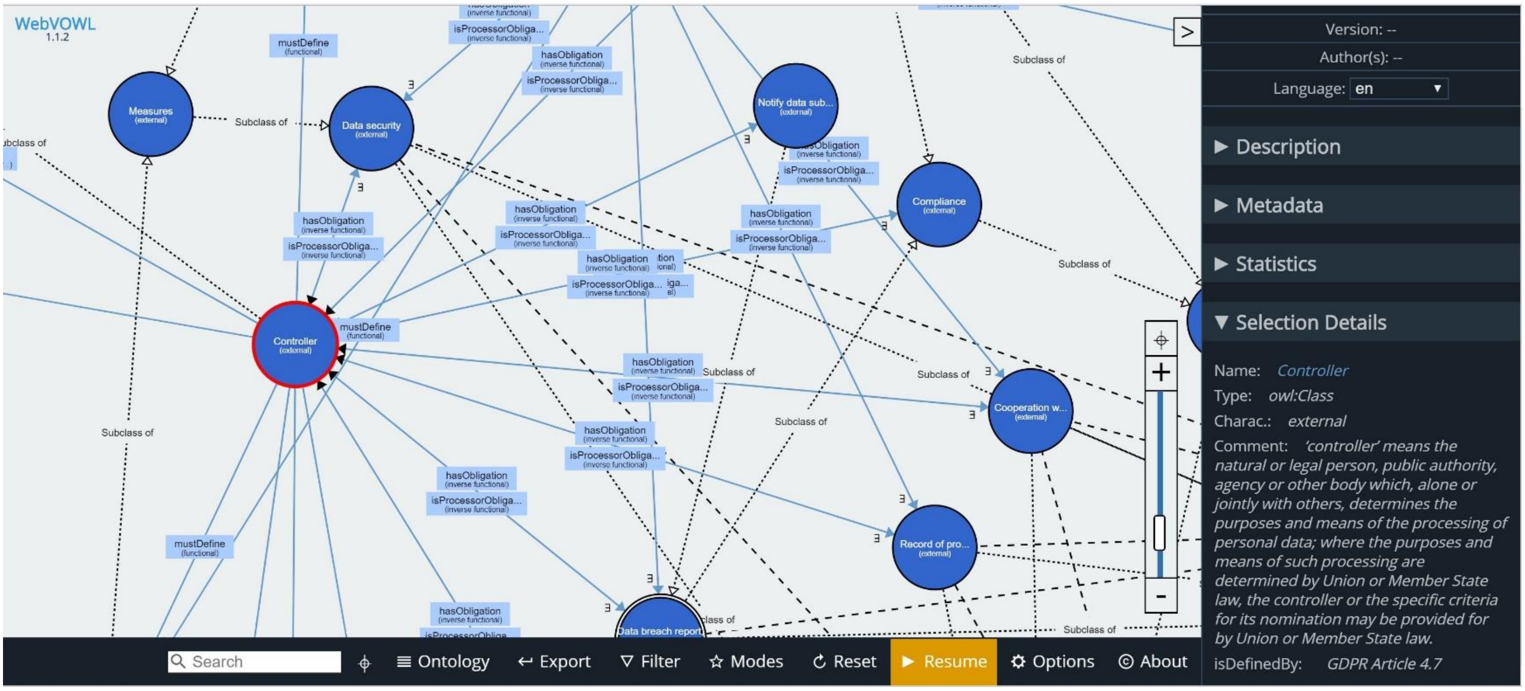
VOWL Viewer:
Organisational measures (external)
Measures (external)
Technical measures (external)
Network uk.ac.man security
Subclass
European Union (external)
Europe Economic... (external)
Controller (external)
mustDefine (functional)
Technology
Manufactur...
Insurance
Financial
Spe (ext
Third-party information (external)
DPO Contact... (external)
Thing
:manc...
isControllerObligation (inverseFunctional)
Data clasification
Security awareness
cooperateWith (functional) (inverseFunctional)
appoints (functional)
Recipient information (external)
mustNotifyBreach (functional) (inverseFunctional)
shallProvide (functional) (inverseFunctional)
Network segmentation
Controller obligation (external)
Processor (external)
Person (external)
Sector
DPO obligation (exter
State (external)
Data Protection... (external)
Transparent information (external)
Activity (external)
Authority (external)
Automated processing (ext
Storage period (external)
isDpoObligation (inverseFunctional)
isProcessorObligation (invers
issueFineFor (functional)
(inv
Class Distance:
Datatype Distance:
Resume Layouting
Reset
Version: Beta 0.1.5
To use the reasoner click Reasoner > Start reasoner ✓ Show Inferences

Figure 16: Visualization of ontology using Protégé VOWL

- **WebVOWL**

Unlike ProtégéVOWL, WebVOWL is a standalone application that displays VOWL2 ontologies and displays the graphical elements in the web browser using open web standards such as CSS and SVG. WebVOWL relies on the Javascript Toolkit D3 for the calculation of the force-based graph layout.

The information about the ontologies are displayed in WebVOWL from a JSON file at runtime. Followinf figure shows the WebVOWL user interface for displaying the GDPR ontology. The user of WebVOWL has the possibility to zoom in the visualization and to move the displayed image section. It is also possible to position nodes as required and fix them there. The force layout can also be influenced by pausing or adjusting the attraction forces.



Version: --

Author(s): --

Language: en

▶ Description

▶ Metadata

▶ Statistics

▼ Selection Details

Name: *Controller*

Type: *owl:Class*

Charac.: *external*

Comment: *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*

isDefinedBy: *GDPR Article 4.7*

Figure 17: Visualization of ontology using WebVOWL

In WebVOWL classes are available in the center of the graphical representation and are displayed as circular nodes in a force-based layout. The size of a circle represents the number of instances of the respective class. In order to to improve readability, the circles have a certain minimum radius rmin and are logarithmically scaled beyond this.
As in VOWL, the arrowheads of the lines between the classes represent the direction of the relation between the instances of the respective classes. For example, if a line points from class C1 to class C2, instances of class C1 are linked to instances of class C2 via the properties P involved. Relations via properties are displayed with a filled arrowhead. In the following figure are represented main notations for OWL ontology.

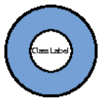
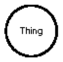
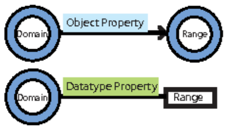
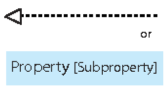
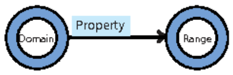
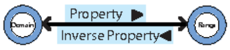
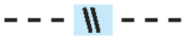
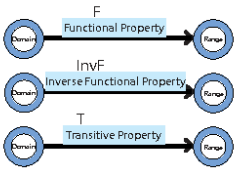
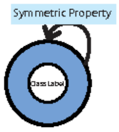
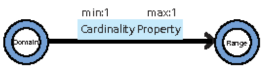
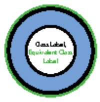
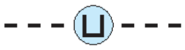
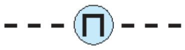
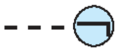
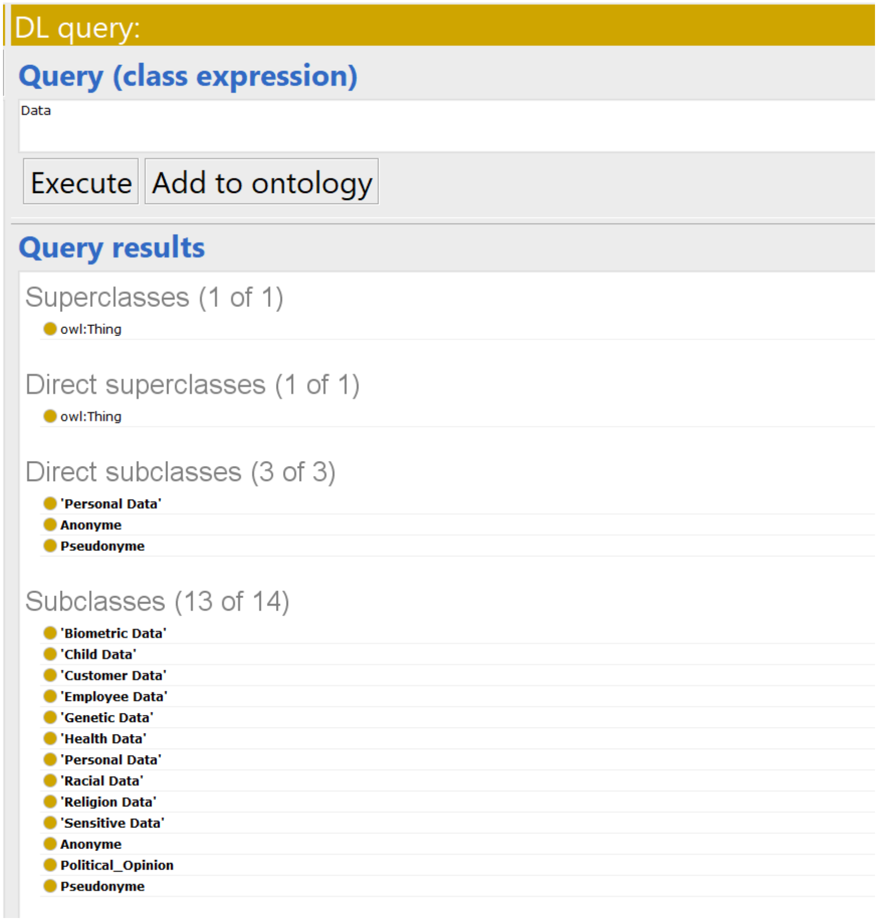
Element	Graphical representation	Description
owl:Class		Circle with round label (*rdfs:label*) in the middle. Classes from imported ontologies are displayed entirely in gray (incl. the label background).
owl:Thing		Simple circle with label *Thing*.
owl:ObjectProperty, *owl:DatatypeProperty*	 Domain Object Property Range Domain Datatype Property Range	Line or arc annotated with the label of the property. The label's background color indicates the type of the property (object or datatype property).
rdfs:subClassOf, *rdfs:subPropertyOf*		Dotted line/arc with an unfilled arrow head at the end pointing to the superclass or superproperty. Subproperties having the same domain and range as their superproperties can alternatively be listed in square brackets within the label of the superproperty.
rdfs:domain, *rdfs:range*		Arrow starting at the domain and pointing to the range. Datatype properties do not need an arrow, as they are always directed to the literal or data value.
owl:inverseOf		Line/arc with arrow heads at both ends and annotated with the label of the property and its inverse counterpart. Filled arrow heads at the end of the labels indicate the direction of the properties (i.e. their range).
owl:disjointWith		Dashed line/arc with \\ symbol as label.
owl:FunctionalProperty, *owl:InverseFunctionalProperty*, *owl:TransitiveProperty*	 F Functional Property Domain Range InvF Inverse Functional Property Domain Range T Transitive Property Domain Range	Object property representation with an *F* for functional properties, *InvF* for inverse functional properties, and *T* for transitive properties on top of the property label.
owl:SymmetricProperty		Object property representation with identical domain and range, i.e. start and end point of the arrow is the same class.
owl:cardinality, *owl:minCardinality*, *owl:maxCardinality*		Exact, minimal, and/or maximal cardinality constraints are written above the property label.
owl:equivalentClass		Colored ring around a class. The labels of all equivalent classes are shown as comma-separated list in the label, each colored in the same font as the corresponding ring.
owl:unionOf		Dashed line/arc with ⊔ symbol as label.
owl:intersectionOf		Dashed line/arc with ⊓ symbol as label.
owl:ComplementOf		Dashed line/arc with ¬ symbol as label.
Literals, data types and data values		Rectangle containing the literal or data value.

Figure 18: Meaning of primary OWL relations [49]

7.2. Use case of ontology

The GDPR ontology presented in this thesis can be used to get a first understanding of regulatory requirements and to help organisations in being compliant with GDPR. Additionally, controller and processor can get an overview of their obligations and data subjects can determine what their rights are. To use this ontology, it is necessary to install Protégé 5 software. As already described in Section 7.1 this software offers different visualization plugins that aid in understanding of ontology. Using Web-based visualization of ontologies, organisations get an overview of all classes and the relationships between them, as well as classes definitions from regulation and recommendations from different best practices. Beside visualization of ontology, Protégé 5 software has so-called "DL Query Tab" for querying and searching an ontology. DL Query allows posing simple ontological queries, e.g. direct superclasses, subclasses, instances etc. An example of simple query of GDPR ontology is when we type class label in query box and as a result we get all subclasses that are related to this class. Below is example of "Data" class. As we can see on Figure 19, "Data" class has some direct subclasses Personal Data, Anonyms and Pseudonyms. Besides that, there are other subclasses that are indirectly connected to "Data" class: Biometric data, Child data, Customer data and so on. These are all possible types of data mentioned in GDPR ontology.



DL query:

Query (class expression)

Data

Query results

Superclasses (1 of 1)
- owl:Thing

Direct superclasses (1 of 1)
- owl:Thing

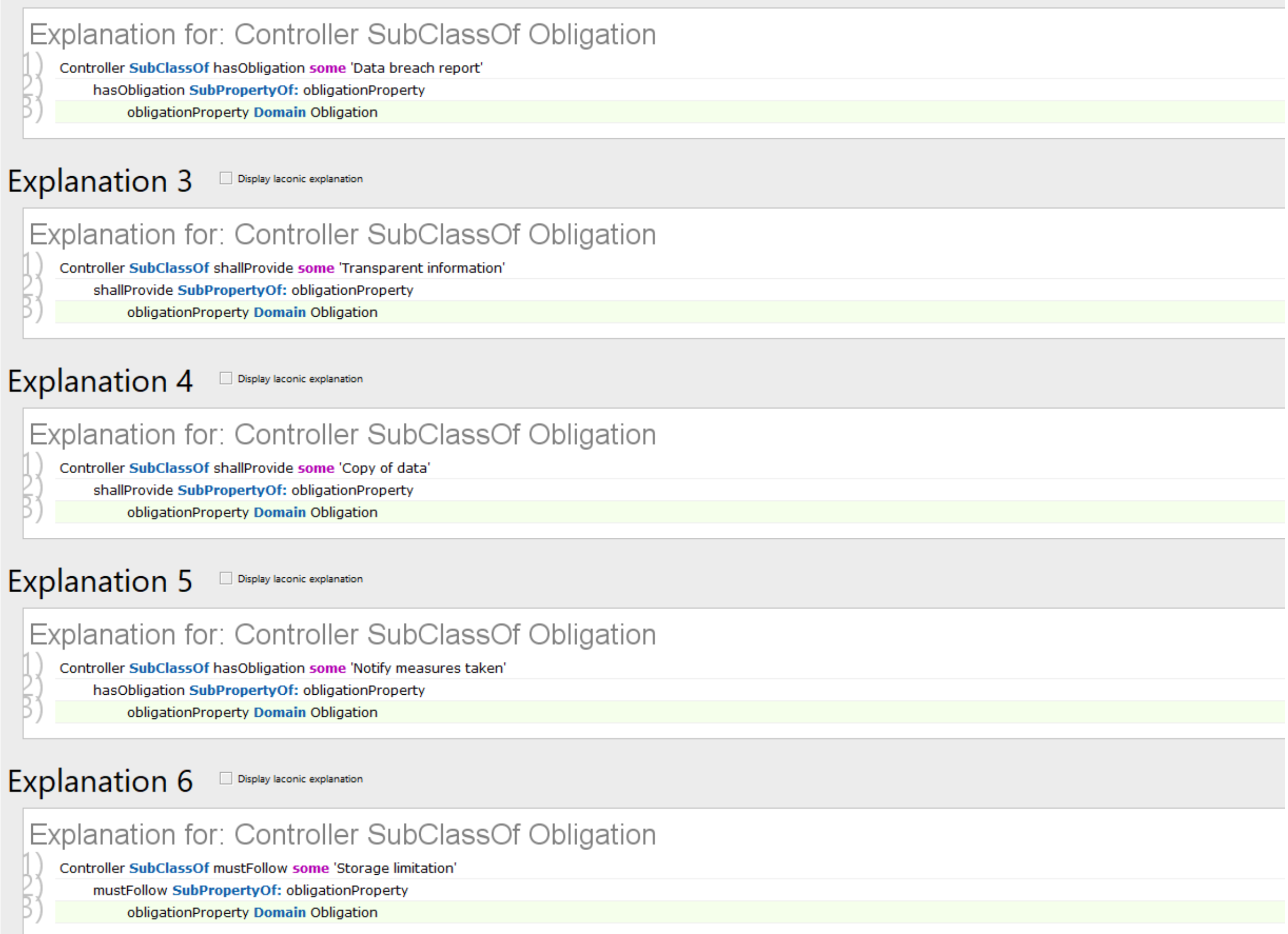
Direct subclasses (3 of 3)
- 'Personal Data'
- Anonyme
- Pseudonyme

Subclasses (13 of 14)
- 'Biometric Data'
- 'Child Data'
- 'Customer Data'
- 'Employee Data'
- 'Genetic Data'
- 'Health Data'
- 'Personal Data'
- 'Racial Data'
- 'Religion Data'
- 'Sensitive Data'
- Anonyme
- Political_Opinion
- Pseudonyme

Figure 19: Querying of Data class

7.2.1. Use case for Controller

A controller can also use this ontology by performing simple DL query for “Controller” class and viewing of explanations of assigned subclasses. On Figure 20 part of explanations for “Controller and hasObligation some” query is represented. As we can see, “DL Query” makes possible to combine classes, properties and restrictions while performing queries. The explanations contain some object properties relevant for this class such as “hasObligation”, “shallProvide”, “mustFollow” etc. Therefore, when we type “Controller” in query box, as a result we get a list of all controller relevant information (e.g. obligations, duties, definitions).



Explanation for: Controller SubClassOf Obligation

1) Controller **SubClassOf** hasObligation **some** 'Data breach report'
2) hasObligation **SubPropertyOf:** obligationProperty
3) obligationProperty **Domain** Obligation

Explanation 3 □ Display laconic explanation

Explanation for: Controller SubClassOf Obligation

1) Controller **SubClassOf** shallProvide **some** 'Transparent information'
2) shallProvide **SubPropertyOf:** obligationProperty
3) obligationProperty **Domain** Obligation

Explanation 4 □ Display laconic explanation

Explanation for: Controller SubClassOf Obligation

1) Controller **SubClassOf** shallProvide **some** 'Copy of data'
2) shallProvide **SubPropertyOf:** obligationProperty
3) obligationProperty **Domain** Obligation

Explanation 5 □ Display laconic explanation

Explanation for: Controller SubClassOf Obligation

1) Controller **SubClassOf** hasObligation **some** 'Notify measures taken'
2) hasObligation **SubPropertyOf:** obligationProperty
3) obligationProperty **Domain** Obligation

Explanation 6 □ Display laconic explanation

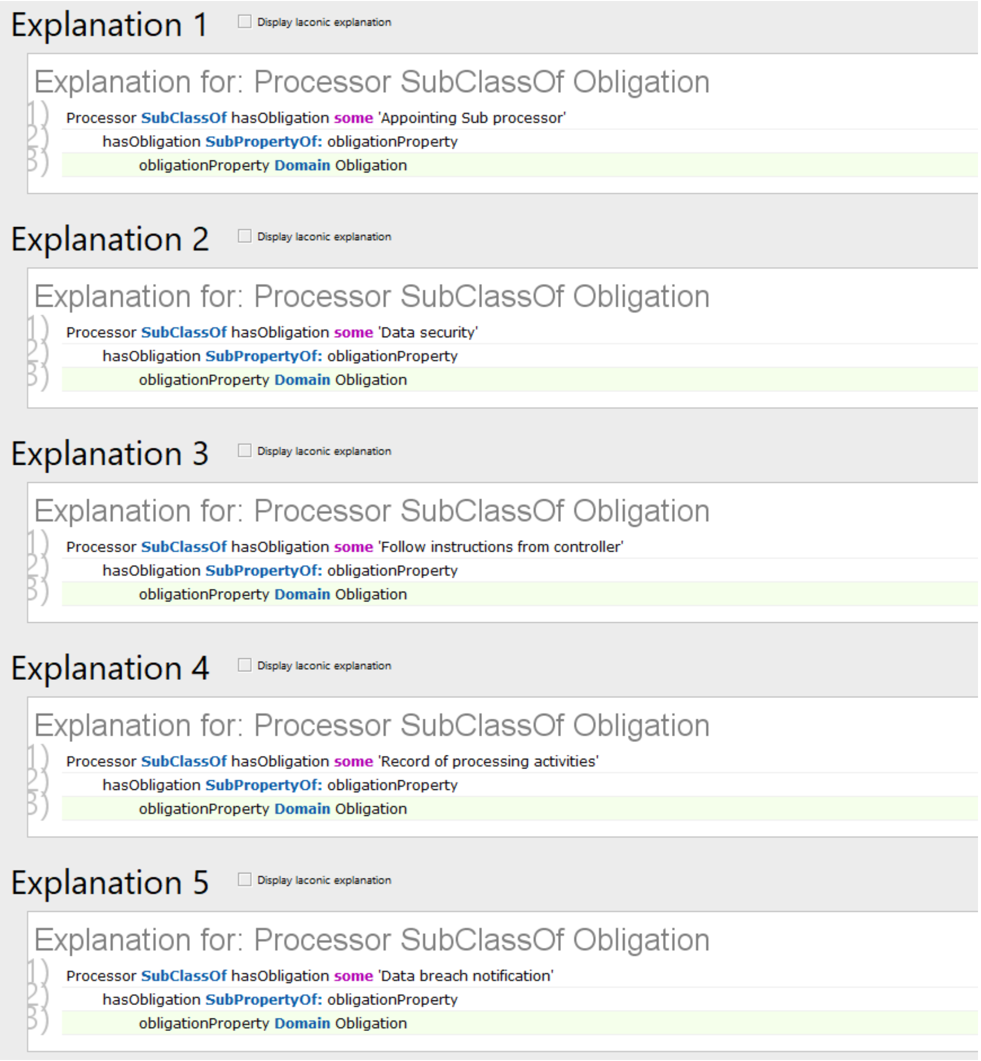
Explanation for: Controller SubClassOf Obligation

1) Controller **SubClassOf** mustFollow **some** 'Storage limitation'
2) mustFollow **SubPropertyOf:** obligationProperty
3) obligationProperty **Domain** Obligation

Figure 20: Some explanations for “Controller” query

7.2.2. Use case for Processor

Additional interesting use case of ontology is DL Query for “Processor” class. As represented in competency questions, the ontology should give an answer what the functions of processor are. Beside controller, processor is also relevant actor in GDPR, since he processes personal data on behalf of controller [7]. Therefore, controller and processor have some similar obligations and duties. Performing DL query in Protégé 5 software, it is possible to get an overview of all obligations relevant for processor. The processor is related to some object properties such as “hasObligation”, “isProcessorObligation”, “mustDefine”, “mustFollow”, and “shallProvide”.



Explanation 1 □ Display laconic explanation

Explanation for: Processor SubClassOf Obligation

```
1) Processor SubClassOf hasObligation some 'Appointing Sub processor'
2)     hasObligation SubPropertyOf: obligationProperty
3)         obligationProperty Domain Obligation
```

Explanation 2 □ Display laconic explanation

Explanation for: Processor SubClassOf Obligation

```
1) Processor SubClassOf hasObligation some 'Data security'
2)     hasObligation SubPropertyOf: obligationProperty
3)         obligationProperty Domain Obligation
```

Explanation 3 □ Display laconic explanation

Explanation for: Processor SubClassOf Obligation

```
1) Processor SubClassOf hasObligation some 'Follow instructions from controller'
2)     hasObligation SubPropertyOf: obligationProperty
3)         obligationProperty Domain Obligation
```

Explanation 4 □ Display laconic explanation

Explanation for: Processor SubClassOf Obligation

```
1) Processor SubClassOf hasObligation some 'Record of processing activities'
2)     hasObligation SubPropertyOf: obligationProperty
3)         obligationProperty Domain Obligation
```

Explanation 5 □ Display laconic explanation

Explanation for: Processor SubClassOf Obligation

```
1) Processor SubClassOf hasObligation some 'Data breach notification'
2)     hasObligation SubPropertyOf: obligationProperty
3)         obligationProperty Domain Obligation
```

Figure 21: Some explanations for "Processor" query

7.3. Evaluation

Based on competency questions defined in section 5.5.3 and based on defined design criteria it is possible to evaluate this proposed ontology. As shown in use cases, within this ontology is possible to perform some basic DL queries which help to answer competency questions: the principles of processing, the rights of data subject, the main obligations of a data controller, the functions of a data processor and the main obligations of a data protection officer.

In paper [72] author gives an overview of possible criteria and strategies to evaluate design and implementation of ontologies. The evaluation of ontology can be viewed from different perspectives [72], some of these are:

- application-based (plugging ontology into an application and evaluating results);
- data driven (comparing it to existing data, in this case to GDPR); and
- human-based (ontology will be used by users who try to evaluate how well an ontology meets its purpose).

Using these proposed evaluation strategies, it will be possible to evaluate GDPR ontology and how this ontology meets predefined Accuracy, Clarity, Extendibility and Easy to follow design criteria.

8 Conclusion

Over the past few years various Big Data products have been developed, meant to aid in the “structuring” of great amounts of unstructured data created from different sources [8]. Organisations worldwide use these products and try to collect, analyse, and translate as many as possible data in order to achieve a competitive edge in the marketplace. Unfortunately, many of these organisations are not considering the potential risks when working with personal data.

With the General Data Protection Regulation (GDPR) EU has implemented its vision of creating a common legal basis for all Member States. Personal data protection is one of the basic tasks that the GDPR puts before organizations, whether it's personal data of users, clients or employees. Organizations need to know at any time where the data are and for what purpose they can use. Likewise, if someone decides to withdraw the consent to use his personal data, organizations must be able to do so within the set time limit. Failure to comply with the provisions entails fines and high penalties - up to 4% of the total annual worldwide turnover or up to EUR 20 million, whichever value is higher. The regulation applies to all economic operators operating in the EU - including micro enterprises, small and medium-sized enterprises, public institutions, bodies and agencies that collect personal data. With the entry into force of the GDPR, many companies have an obligation to appoint Data Protection Officers (DPOs), or personal data protection officers.

The new regulation puts a pressure on organisations EU-wide to be compliant with it. Considering that actual requirements given in the regulation are not clear defined and they implementation also presents a challenge for organisations, this work attempts to identify and represent the main requirements relevant for information security, in order to support organisations in their way to GDPR compliance. At the beginning of this thesis the following research questions was proposed and during the research attempted to be answered:

- What are the main requirements of the GDPR that are relevant for information security, furthermore how to visualise these requirements to help organisations to understand the legal text and the main obligations?

This work represents an ontology, which identifies and highlights the main requirements of GDPR in the context of information security. The requirements for information security are identified from different papers and books and divided in five main areas, which include basic definitions, such as what is organisation, which sector, location or size, what kind of personal data will be collected, processed or stored on one side, and processing principles which are matched with corresponding rights for the data subject and obligations of controller on the other side. Additionally, best practices, standards and templates are added in description of ontology classes in Protégé software to facilitate the implementation of GDPR.

The presented approach can be used by organisations to get a first understanding of GDPR requirements and the legal text, for data subjects to determine their rights, for data controllers and processors to understand their obligations. Data controllers and their processors are able to determine what their duties against the data subject are, what they need to consider when processing personal or sensitive data.

In this ontology this is achieved by querying of ontology classes and viewing explanations for these classes using Protégé software. Moreover, ontology can be used as a basis for some applications for analysing obligations of controller or processor, or it can be used in some tools to audit organization and its compliance with all requirements.

8.1. Limitation of thesis

The ontology presented in this thesis is a starting point which has to be extended and refined until it produces the full benefit. In order to increase the usability for users, it is an easy-to understand ontology, leaving out many aspects of the legal text and concentrating on the relevant aspects for information security. However, the main purpose was not to express the GDPR, but to define key points that can support organisations of all sizes to identify requirements relevant for them.

A limitation of the ontology is that it was not yet assessed by legal experts in order to evaluate its correctness. The quality of GDPR ontology can be assessed by experts and by using the ontology in applications for which it is designed. However, after following all the rules and suggestions for developing ontology [15], an important aspect to notice is that there is no correct way to model a domain. Ontology development can be seen as an iterative process, and the methodology of its development depends on the application that is anticipated. Therefore, this work will proceed in several research and improvement directions to complete this ontology and to enable automated acquiring of information and performing detailed queries. Additionally, it will be meaningful to integrate this ontology with some existing approaches and security ontologies, in order to get a detailed describing portion of the GDPR and information security domain.

List of references

[1] IBM Marketing Cloud, “IBM - 10 Key Marketing Trends for 2017,” 2017. [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN. [Accessed 10 December 2017].

[2] Verimax, “EU-Datenschutz-Grundverordnung,” [Online]. Available: http://www.verimax.de/eu-datenschutz-grundverordnung. [Accessed 20 Februar 2018].

[3] “Sun Microsystems,” [Online]. Available: https://www.oracle.com/sun/index.html.

[4] C. Warren Axelrod, Jennifer L. Bayuk and Daniel Schutzer, Enterprise Information Security and Privacy, Artech House, 2009.

[5] EU Commission, “EU Data Protection Directive 95/46/EC,” 1995.

[6] IT Governance Privacy Team, EU GDPR: An Implementation and Compliance Guide, IT Governance Publishing, 2016.

[7] EU Commission, “EU General Data Protection Regulation 2016/679,” 2016. [Online]. Available: https://gdpr-info.eu/.

[8] Deloitte, “Umfrage EU-Datenschutzgrundverordnung,” Dezember 2017. [Online]. Available: https://www2.deloitte.com/at/de/seiten/risikomanagement/artikel/umfrage-eu-datenschutzgrundverordnung.html. [Accessed 20 January 2018].

[9] Carmao, “Computer Woche,” [Online]. Available: https://www.computerwoche.de/a/eu-dsgvo-unternehmen-muessen-sich-jetzt-vorbereiten,3330971. [Accessed 15 November 2017].

[10] Joost Breuker and Radboud Winkels, “Use and reuse of legal ontologies in knowledge engineering and information management,” ICAIL 2003 Workshop, April 2003.

[11] “Gartner - IT Glossary,” [Online]. [Accessed 07 August 2018].

[12] European Comission, [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. [Accessed 27 March 2018].

[13] IETF, “RFC 4949 Internet Security Glossary Version 2,” 2007.

[14] N. F. Noy, D. L. McGuinness, et al., “Ontology development 101: A guide to creating your first ontology,” 2001.

[15] “Regulation,” [Online]. Available: http://computer.yourdictionary.com/regulation. [Accessed 29 04 2018].

[16] European Union Agency for fundamental rights, “Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU,” 2014.

[17] Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy,” The Harvard Law Review Association Vol. 4, No.5 , 1890.

[18] C.Warren Axelrod, Jennifer L.Bayuk, Daniel Schutzer, “Enterprise Information Security and Privacy,” Artech House Publisher, 2009, pp. 21-22.

[19] Dorothy J. Glancy, “The invention of the Right to Privacy,” Arizona Law Review, Vol 21, No.1, 1979.

[20] “Clickz - From 1980 through next May: The evolution of GDPR,” [Online]. Available: https://www.clickz.com/1980-next-may-evolution-gdpr/203155/. [Accessed 03 Mai 2018].

[21] G. Greenwald, “Why privacy matters?,” 2016 .

[22] “Federal Act concerning the Protection of Personal Data (DSG 2000) - English Version,” *Article 1,* pp. 5-6, 2014.

[23] E. Commision, “Charter of fundamental rights of the European Union (2000/C 364/01),” p. 10.

[24] “European Law Institute,” [Online]. Available: https://www.europeanlawinstitute.eu/membership/institutional-observers/austrian-data-protection-

authority/. [Accessed 20 December 2017].

[25] Günther Leissler, Janos Böszörmenyi, Patrizia Reisinger , “Working Paper on the National Adaptations of the GDPR in,” E-conférence, National Adaptations of the GDPR, 2017.

[26] “Austrian Data Protection Act 2018 (Anpassungsesetz),” 2017.

[27] Morrison & Foerster LLP, “Austria’s GDPR Implementation Law,” Lexology, 2017.

[28] B. G. Raggad, Information Security Management, CRC Press, 2010.

[29] CNSS, “National Training Standard for Information Systems Security (Infosec) Professionals,” [Online]. Available: www.cnss.gov.

[30] C. Learning, Artist, *Course Technology.* [Art].

[31] R. Knyrim, Datenschutzrecht Praxishandbuch fuer richtiges Registrieren, Verarbeiten, Uebermitteln, Zustimmen, Outsourcen, Werben uvm., Wien: Manz Verlag, 2015.

[32] BSI - Bundesamt für Sicherheit in der Informationstechnik, “ IT-Grundschutz-Kataloge – B 1.5”.

[33] M. E. Whitman, Principles of Information security 4th edition, Cengage Learning, 2011.

[34] “ISO 27001 Information technology - Security techniques - Information security management systems - Requirements,” 2016.

[35] “Advisera - Information classification according to ISO 27001,” [Online]. Available: https://advisera.com/27001academy/blog/2014/05/12/information-classification-according-to-iso-27001/. [Accessed 07 August 2018].

[36] “Cyberpedia - What is and IT Security policy,” [Online]. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy. [Accessed 07 August 2018].

[37] Roberta Bragg, CISSP Security Management and Practices, 2002.

[38] “Computer Security Blog - The pillars of information security,” [Online]. Available: http://computersecurty.blogspot.com/2013/09/the-pillars-of-information-security.html. [Accessed 15 Mai 2018].

[39] ULD, “Standard Datenschutzmodell SDM,” in *Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder*, Düsseldorf, 2018.

[40] R. Knyrim, Datenschutz-Grundverordnung, Manz, 2016.

[41] C. Roe, “Dataversity: A short history of ontology,” [Online]. Available: http://www.dataversity.net/a-short-history-of-ontology-its-not-just-a-matter-of-philosophy-anymore/. [Accessed 20 March 2018].

[42] J.Davies, R.Studer,P.Warren, Semantic Web Technologies: Trends and REsearch in Ontologybased Systems, Wiley, 2006.

[43] T. Slimani, “A Study on Ontologies and their Classification,” Recent Advances in Electrical Engineering and Educational Technologies, 2014.

[44] A. Ekelhart, S. Fenz, M. D. Klemen, and E. R. Weippl., “Security ontology: Simulating threats to corporate assets,” in *International Conference on Information Systems Security*, 2006.

[45] Dr. Roman V Belavkin, "Ontologies," [Online]. Available: http://www.eis.mdx.ac.uk/staffpages/rvb/teaching/BIS4410/hand08.pdf. [Accessed 31 August 2017].

[46] Nicola Guarino, “Formal Ontology and Information Systems,” *Proceedings of FOIS’98,* pp. 3-15, 1998.

[47] Kamran Munira, M. Sheraz Anjum, “The use of ontologies for effective knowledge modelling and information retrieval,” *Applied Computing and Informatics 14,* pp. 116-126, 2018.

[48] Valente Giulio & Alessandro Rigallo, “Operational Knowledge Management: a way to manage competence.,” 2015.

[49] “SKOS (Simple Knowledge Organization System),” [Online]. Available: https://www.w3.org/TR/skos-primer/.

[50] Stefan Negru, Steffen Lohmann, “A Visual Notation for the Integrated Representation of OWL

Ontologies," WEBIST, 2013.

[51] Travis D. Breaux and Annie I. Antón , "A Systematic Method for Acquiring Regulatory Requirements: A Frame-based Approach," in *6th International Workshop on Requirements for High Assurance Systems (RHAS-6)* , Delhi, India, 2007.

[52] Travis D. Breaux, Annie I. Anton and Jon Doyle, "Semantic Parameterization: A Process for Modeling Domain Descriptions," in *ACM Transactions on Software Engineering and Methodologies*, 2007.

[53] Harshvardhan J. Pandit, Declan O'Sullivan, Dave Lewis, "Queryable Provenance Metadata For GDPR Compliance," in *Semantics 2018 – 14th International Conference on Semantic Systems*, 2018.

[54] "GDPR Readiness Checklist," [Online]. Available: http://openscience.adaptcentre.ie/GDPR-checklist-demo/demo/GDPR-readiness-checklist.html. [Accessed 07 August 2018].

[55] "EuroPrise Seal," [Online]. Available: https://www.european-privacy-seal.eu/EPS-en/Home. [Accessed 29 June 2018].

[56] Veriscan , "Information Security Management System (ISMS) and handling of personal data," Veriscan Security AB, 2017.

[57] BSI, "EU DSGVO Info6," Die Bundesbeauftragte für den Datenschutzund die Informationsfreiheit, 2017.

[58] Maria Virvou, Eirini Mougiakou, "Based on GDPR privacy in UML: case of e-learning programm," in *8th International Conference on Information, Intelligence, Systems & Applications (IISA)*, Cyprus, 2017.

[59] Heiko Behrendt, "Neue Anforderungen der DSGVO für die IT Sicherheit," ULD - Unabhängiges Landeszentrum für Datenschutz, Schleswig - Holstein, 2016.

[60] "Protege 5 Software," [Online]. Available: https://protege.stanford.edu/. [Accessed 10 Oktober 2017].

[61] "Mozilla Public License," [Online]. Available: https://www.mozilla.org/en-US/MPL/. [Accessed 10 Mai 2018].

[62] "Web Ontology Language," [Online]. Available: https://www.w3.org/OWL/.

[63] Semantic Web Standards, "Resource Description Framework," [Online]. Available: https://www.w3.org/RDF/. [Accessed 21 Mai 2018].

[64] Matthew Horridge, "A Practical Guide To Building OWL Ontologies Using Protege," The University Of Manchester, 2009.

[65] "Datenschutz - Information," [Online]. Available: https://www.datenschutz.org/personenbezogene-daten/. [Accessed 20 June 2018].

[66] "Wirtschaftskammer Österreich WKO - Informationen zur EU Datenschutz Grundverordnung," [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Informationen-zur-EU-Datenschutz-Grundverordnung.html. [Accessed 20 Mai 2018].

[67] WKO, "WKO - EU GDPR Datenschutz, Direktmarketing," [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-GDPR-datenschutz-direktmarketing.html. [Accessed 25 June 2018].

[68] WKO, " Wichtige Begriffsbestimmungen," [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Wichtige-Begriffsbestimmu.html#Einwilligung. [Accessed 14 June 2018].

[69] "Handbook on European Data Protection Law," *European Union Agency for Fundamental Rights,* pp. 61-75, 2014.

[70] [Online]. Available: https://www.edq.com/uk/glossary/data-minimisation/. [Accessed 29 July 2018].

[71] CAS Software, "CRM User guide data protection," [Online]. Available: https://www.meliorcras.ro/data/_editor/files/CAS%20xRM%20%20EU-GDPR_EN.pdf. [Accessed 29 July 2018].

[72] WKO , "DSGVO - Betroffenenrechte," [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Betroffenenrechte.html. [Accessed 29 July 2018].

[73] “Information Commissioners Office-Rights related to automated decision making including profiling,” [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/. [Accessed 29 July 2018].

[74] “ICO UK - Guide to general data protection regulation,” [Online]. Available: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/rights-related-to-automated-decision-making-including-profiling/. [Accessed 02 June 2018].

[75] “Österreichisches Informationssicherheitshandbuch v 4.0.1,” 2016.

[76] R. Sivakumar, P.V. Arivoli, “Ontology Visualization Protege Tools,” in *International Journal of Advanced Information Technology (IJAIT) Vol. 1, No. 4*, 2011.

[77] “Protegewiki - OntoGraf,” [Online]. Available: https://protegewiki.stanford.edu/wiki/OntoGraf. [Accessed 2018 Juli 20].

[78] “VOWL - Visual Data Web,” [Online]. Available: http://vowl.visualdataweb.org/protegevowl.html. [Accessed 2018 Juli 20].

[79] Auriol Degbelo, “A Snapshot of Ontology Evaluation Criteria and Strategies,” in *Proceedings of Semantics 2017*, Amsterdam, Netherlands, 2017.

[81] Committee on National Security Systems , “CNSSI 4009 Glossary,” 2015.

[82] “ATKearney - Bringing Structure to the Unstructured World of Big Data,” [Online]. Available: https://www.atkearney.com/analytics/article?/a/it-s-challenge-bringing-structure-to-the-unstructured-world-of-big-data. [Accessed 30 Juli 2018].

Appendices – Description of ontology classes

Appendix 1: Data area

Main area	Data
Label	Data
Defined by	GDPR Article 4
Superclass	GDPR
Subclasses	Personal, anonymous, pseudonymous

Main area	Data
Label	Personal data
Defined by	GDPR Article 4
Superclass	Data
Subclasses	Child data, sensitive data, customer data, employee data

Main area	Data
Label	Child data
Defined by	GDPR Article 8
Superclass	Personal data
Subclasses	-

Main area	Data
Label	Customer data
Defined by	-
Superclass	Personal data
Subclasses	-

Main area	Data
Label	Employee data
Defined by	-
Superclass	Personal data
Subclasses	-

Main area	Data
Label	Sensitive data
Defined by	GDPR Article 4
Superclass	Personal data
Subclasses	Genetic data, racial origin, biometric, health, political opinion, religion

Main area	Data
Label	Anonymous data
Defined by	GDPR Recital 26
Superclass	Data
Subclasses	-

Main area	Data
Label	Pseudonyme data

Defined by	GDPR Article 4.5
Superclass	Data
Subclasses	-

Appendix 2: Organisation area

Main area	Organisation
Label	Person
Defined by	-
Superclass	Organisation
Subclasses	Controller, Processor, Data protection officer, Data Subject, Authority

Main area	Organisation
Label	Controller
Defined by	GDPR Article 4.7
Superclass	Person
Subclasses	-

Main area	Organisation
Label	Processor
Defined by	GDPR Article 4.8
Superclass	Person
Subclasses	-

Main area	Organisation
Label	Data protection officer
Defined by	GDPR Article 38
Superclass	Person
Subclasses	-

Main area	Organisation
Label	Data subject
Defined by	GDPR Article 4
Superclass	Person
Subclasses	-

Main area	Organisation
Label	Authority
Defined by	GDPR Article 4
Superclass	Person
Subclasses	-

Main area	Organisation
Label	Activity
Defined by	-
Superclass	Organisation
Subclasses	Consent, Data activity, Data Breach report, Impact assessment

Main area	Organisation
Label	Consent
Defined by	GDPR Article 4

Superclass	Activity
Subclasses	Child consent, Valid consent

Main area	Organisation
Label	Child consent
Defined by	GDPR Article 8
Superclass	Consent
Subclasses	Parental responsibility

Main area	Organisation
Label	Valid consent
Defined by	GDPR Article 7, Recital 32
Superclass	Consent
Subclasses	Freely given consent, Informed, Specific, Written declaration

Main area	Organisation
Label	Written declaration
Defined by	GDPR Article 7
Superclass	Valid consent
Subclasses	Clear language, Accessible form

Main area	Organisation
Label	Data activity
Defined by	-
Superclass	Activity
Subclasses	Collection of data, Codes of conduct, Processing, Archive, Erase, Store, Transfer

Main area	Organisation
Label	Collection of data
Defined by	GDPR Article 13
Superclass	Data activity
Subclasses	Accurate, Explicit purpose, Legitimate, Specified purpose

Main area	Organisation
Label	Processing
Defined by	GDPR Article 4
Superclass	Data activity
Subclasses	Large scale processing, Sensitive data processing, Unlawful processing, Mode of processing

Main area	Organisation
Label	Mode of processing
Defined by	-
Superclass	Processing
Subclasses	Automated processing, Manual

Main area	Organisation
Label	Automated processing
Defined by	GDPR Article 22

Superclass	Mode of processing, Factors for PIA, Right to appropriate decision making
Subclasses	Profiling

Main area	Organisation
Label	Transfer data
Defined by	-
Superclass	Data activity
Subclasses	Cross-border transfer

Main area	Organisation
Label	Data Breach report
Defined by	GDPR Article 33
Superclass	Activity
Subclasses	Notify Data Subject, Report to PIA
Comment	Data Breach report = Data Breach notification

Main area	Organisation
Label	Notify Data Subject
Defined by	GDPR Article 34
Superclass	Data Breach report
Subclasses	Notify consequences, Notify measures taken

Main area	Organisation
Label	Impact assessment
Defined by	GDPR Article 35
Superclass	Activity
Subclasses	Factors for PIA, Key stages of PIA

Main area	Organisation
Label	Factors for PIA
Defined by	GDPR Article 35
Superclass	Impact assessment
Subclasses	Automated processing, Cross-border Transfer, Sensitive data processing, Systematic monitoring

Main area	Organisation
Label	Key stages of PIA
Defined by	GDPR Article 35
Superclass	Impact assessment
Subclasses	Identify need for PIA, Identify risks, Identify privacy solution, Information flow, Documentation

Main area	Organisation
Label	Department
Defined by	-
Superclass	Organisation
Subclasses	Finance, Human Resources, IT, Marketing, Sales

Main area	Organisation

Label	Sector
Defined by	-
Superclass	Organisation
Subclasses	Educational, Financial, Healthcare, Insurance, Manufacturing, Technology
Comment	These are instances of Sector class.

Main area	Organisation
Label	Size
Defined by	-
Superclass	Organisation
Subclasses	Large sized enterprises, Small and medium sized enterprises

Main area	Organisation
Label	State
Defined by	-
Superclass	Organisation
Subclasses	European Union, Non-European Union, European Economic Area
Comment	These are instances of State class.

Appendix 3: Data Subject's Rights

Main area	Data Subject's Rights
Label	Data Subject's Rights
Defined by	GDPR Chapter 3
Superclass	-
Subclasses	Right to access, Right to appropriate decision making, Right to be forgotten, Right to data portability, Right to information, Right to notification, Right to object, Right to rectification, Right to restriction of processing

Main area	Data Subject's Rights
Label	Right to access
Defined by	GDPR Article 15
Superclass	Data Subject's Rights
Subclasses	Copy of data

Main area	Data Subject's Rights
Label	Copy of data
Defined by	GDPR Article 15.3
Superclass	Right to access, Right to data portability
Subclasses	Commonly used format, Machine readable format, Structured copy

Main area	Data Subject's Rights
Label	Right to appropriate decision making
Defined by	GDPR Article 22
Superclass	Data Subject's Rights
Subclasses	Automated processing

Main area	Data Subject's Rights
Label	Right to be forgotten
Defined by	GDPR Article 17
Superclass	Data Subject's Rights
Subclasses	Erasure Grounds
Comment	Erasure Grounds = Notification Grounds = Restriction Grounds

Main area	Data Subject's Rights
Label	Erasure Grounds
Defined by	GDPR Article 17.1
Superclass	Right to be forgotten
Subclasses	Consent withdrawn, No origin purpose, Unlawful processing

Main area	Data Subject's Rights
Label	Right to data portability
Defined by	GDPR Article 20
Superclass	Data Subject's Rights
Subclasses	Copy of data

Main area	Data Subject's Rights
Label	Right to information
Defined by	GDPR Article 13
Superclass	Data Subject's Rights
Subclasses	Transparent information

Main area	Data Subject's Rights
Label	Transparent information
Defined by	GDPR Article 12
Superclass	Right to information
Subclasses	DPO Contact data, Processing purpose, Recipient information, Storage period, Third-party information

Main area	Data Subject's Rights
Label	Right to notification
Defined by	GDPR Article 19
Superclass	Data Subject's Rights
Subclasses	Notification Grounds
Comment	Notification Grounds = Erasure Grounds = Restriction Grounds

Main area	Data Subject's Rights
Label	Notification Grounds
Defined by	GDPR Article 19
Superclass	Right to notification
Subclasses	Discloser of data

Main area	Data Subject's Rights
Label	Right to object
Defined by	GDPR Article 21
Superclass	Data Subject's Rights
Subclasses	Objection grounds

Main area	Data Subject's Rights
Label	Objection grounds
Defined by	GDPR Article 21
Superclass	Right to objection
Subclasses	Direct marketing, Research and Statistical purpose

Main area	Data Subject's Rights
Label	Right to rectification
Defined by	GDPR Article 16
Superclass	Data Subject's Rights
Subclasses	-

Main area	Data Subject's Rights
Label	Right to restriction of processing
Defined by	GDPR Article 18
Superclass	Data Subject's Rights
Subclasses	Restriction Grounds

Main area	Data Subject’s Rights
Label	Restriction Grounds
Defined by	GDPR Article 18.1
Superclass	Right to restriction of processing
Subclasses	Accuracy contested

Appendix 4: Principles

Main area	Principles
Label	Principles
Defined by	GDPR Chapter 2, Article 5
Superclass	-
Subclasses	Lawfulness, fairness and transparency, Purpose of specification and limitation, Storage limitation, Accuracy, Data minimisation, Integrity and confidentiality of data

Main area	Principles
Label	Lawfulness, fairness and transparency
Defined by	GDPR Article 5 lit a
Superclass	Principles
Subclasses	Consent, Contract
Comment	Subclass consents contains valid consent and child consent as above described in Organisation area.

Main area	Principles
Label	Accuracy
Defined by	GDPR Article 5 .1 lit d
Superclass	Principles
Subclasses	-

Main area	Principles
Label	Data minimisation
Defined by	GDPR Article 5.1 lit c
Superclass	Principles
Subclasses	Pseudonymisation

Main area	Principles
Label	Pseudonymisation
Defined by	GDPR Recital 28
Superclass	Data minimisation
Subclasses	-

Main area	Principles
Label	Integrity, confidentiality of data
Defined by	GDPR Article 5.1 lit f
Superclass	Principles
Subclasses	-

Main area	Principles
Label	Purpose limitation
Defined by	GDPR Article 5.1 lit b
Superclass	Principles
Subclasses	Legal basis

Main area	Principles

Label	Legal basis
Defined by	GDPR Article 5.1 lit e
Superclass	Purpose limitation
Subclasses	-

Main area	Principles
Label	Storage limitation
Defined by	GDPR Article 5.1 lit e
Superclass	Principles
Subclasses	-

Appendix 5: Obligations

Main area	Obligations
Label	Obligations
Defined by	GDPR Chapter 4
Superclass	-
Subclasses	Certification, Compliance, Controller obligation, Processor obligation, DPO obligation

Main area	Obligations
Label	Certification
Defined by	GDPR Article 42
Superclass	Obligations, Compliance
Subclasses	Certification awarding

Main area	Obligations
Label	Certification awarding
Defined by	GDPR Article 42
Superclass	Certification
Subclasses	Adherence, Validity, Voluntary

Main area	Obligations
Label	Compliance
Defined by	-
Superclass	Obligations
Subclasses	Certification, Codes of conduct

Main area	Obligations
Label	Controller obligations
Defined by	GDPR Article 24
Superclass	Obligations
Subclasses	Cooperation with DPA, Data Breach Notification, Data security, Liability of joint controllers, Record of processing activities, Impact assessment

Main area	Obligations
Label	Cooperation with DPA
Defined by	GDPR Article 31
Superclass	Controller obligation
Subclasses	-

Main area	Obligations
Label	Data Breach Notification
Defined by	GDPR Article 33
Superclass	Controller obligation
Subclasses	Notify Data Subject, Report to DPA
Comment	Data Breach Notification = Data Breach Report

Main area	Obligations
Label	Data security

Defined by	GDPR Article 32
Superclass	Controller obligation
Subclasses	Measures, Property

Main area	Obligations
Label	Measures
Defined by	GDPR Article 32
Superclass	Data security
Subclasses	Organisational measures, Technical measures

Main area	Obligations
Label	Organisational measures
Defined by	-
Superclass	Measures
Subclasses	Access control concept, Audits, Data classification, Information risk assessment, Personal, Security awareness, Security policy

Main area	Obligations
Label	Access control concept
Defined by	ISO / IEC 27552:2017, 29151:2016
Superclass	Organisational measures
Subclasses	Administration of special rights, Documentation of access, Evaluation of required user groups, Evaluation of user access rights, Process for assigning passwords, Registration and De-Registration of users, Time limit of connection

Main area	Obligations
Label	Audits
Defined by	-
Superclass	Organisational measures
Subclasses	-

Main area	Obligations
Label	Data classification
Defined by	ISO / IEC 27552:2017
Superclass	Organisational measures
Subclasses	-

Main area	Obligations
Label	Information risk assessment
Defined by	ISO / IEC 27552:2017
Superclass	Organisational measures
Subclasses	Assets, Data Security risks, Documentation
Comment	Information risk assessment is also Impact assessment.

Main area	Obligations
Label	Security policy
Defined by	ISO / IEC 27001
Superclass	Organisational measures
Subclasses	-

Main area	Obligations
Label	Technical measures
Defined by	GDPR Article 32
Superclass	Measures
Subclasses	Encryption, Logging, Network security, Physical security, Privacy by design and default, Pseudonymisation

Main area	Obligations
Label	Network security
Defined by	-
Superclass	Technical measures
Subclasses	Network controls, External connection options, Network segmentation

Main area	Obligations
Label	Network controls
Defined by	-
Superclass	Network security
Subclasses	IEEE 802.1x

Main area	Obligations
Label	External connection options
Defined by	-
Superclass	Network security
Subclasses	-

Main area	Obligations
Label	Network segmentation
Defined by	-
Superclass	Network security
Subclasses	-

Main area	Obligations
Label	Physical security
Defined by	-
Superclass	Technical measures
Subclasses	-

Main area	Obligations
Label	Privacy by design and default
Defined by	-
Superclass	Technical measures
Subclasses	-

Main area	Obligations
Label	Pseudonymisation
Defined by	GDPR Recital 28
Superclass	Technical measures
Subclasses	-

Main area	Obligations
Label	Property
Defined by	GDPR Principle Integrity and confidentiality of data
Superclass	Data security
Subclasses	Confidentiality, integrity and availability

Main area	Obligations
Label	Confidentiality, integrity and availability
Defined by	GDPR Principle
Superclass	Property
Subclasses	-

Main area	Obligations
Label	Liability of joint controllers
Defined by	GDPR Article 26
Superclass	Controller obligation
Subclasses	-

Main area	Obligations
Label	Record of processing activities
Defined by	GDPR Article 30
Superclass	Controller obligation, Processor obligation
Subclasses	Category of data, Erasure limit, Purpose of processing, Recipients, Security measures

Main area	Obligations
Label	DPO obligation
Defined by	GDPR Article 39
Superclass	Obligations
Subclasses	Monitor compliance

Main area	Obligations
Label	Monitor compliance
Defined by	GDPR Article 39
Superclass	DPO Obligation
Subclasses	-

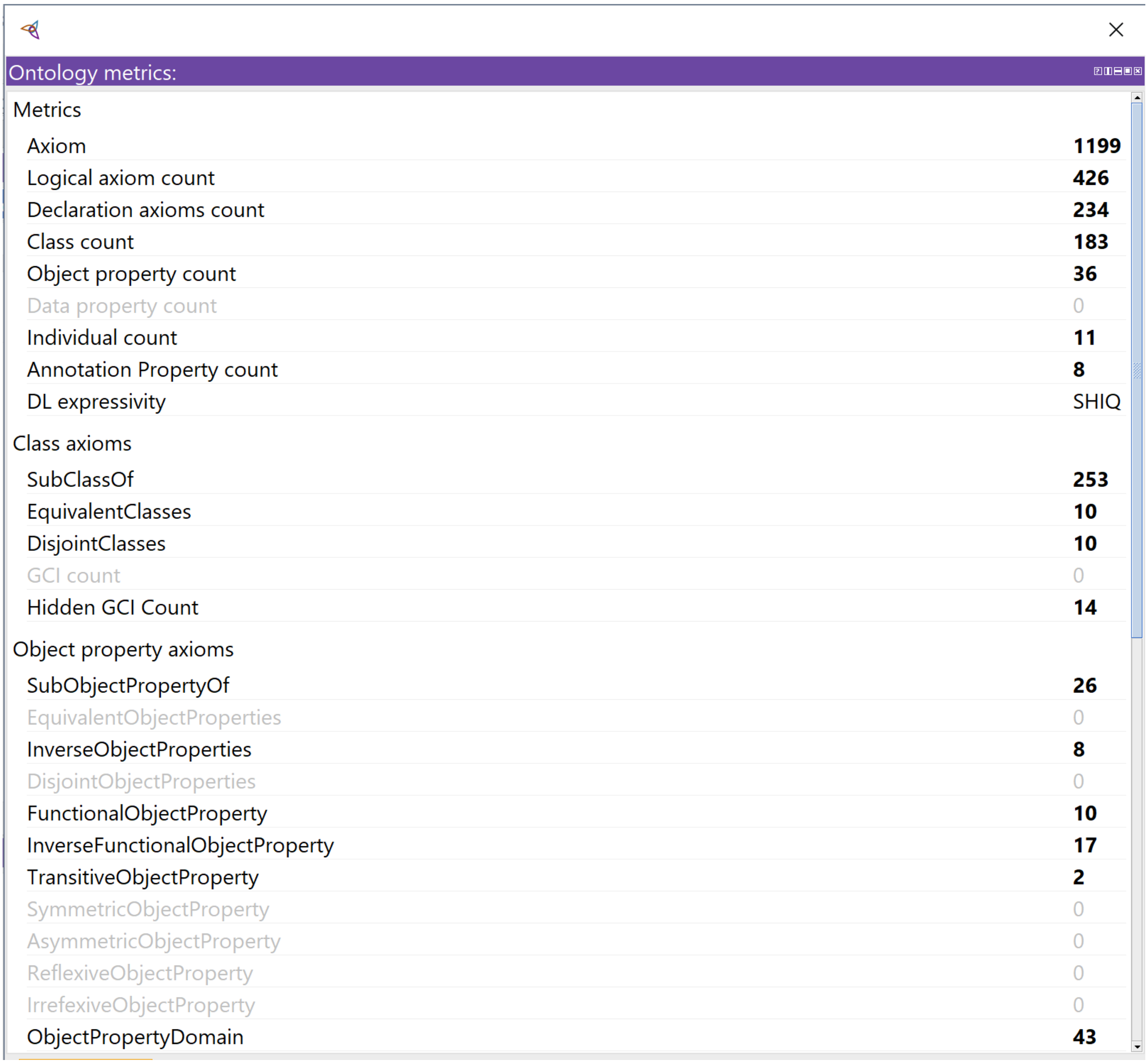
Main area	Obligations
Label	Processor obligation
Defined by	GDPR Article 28
Superclass	Obligations
Subclasses	Appointing Sub processor, Cooperation with DPA, Data Breach notification, Data security, Following instructions from controller, Record of processing activities

Main area	Obligations
Label	Appointing Sub processor
Defined by	GDPR Article 28.4
Superclass	Processor obligation

Subclasses	Contract, Follow same obligations

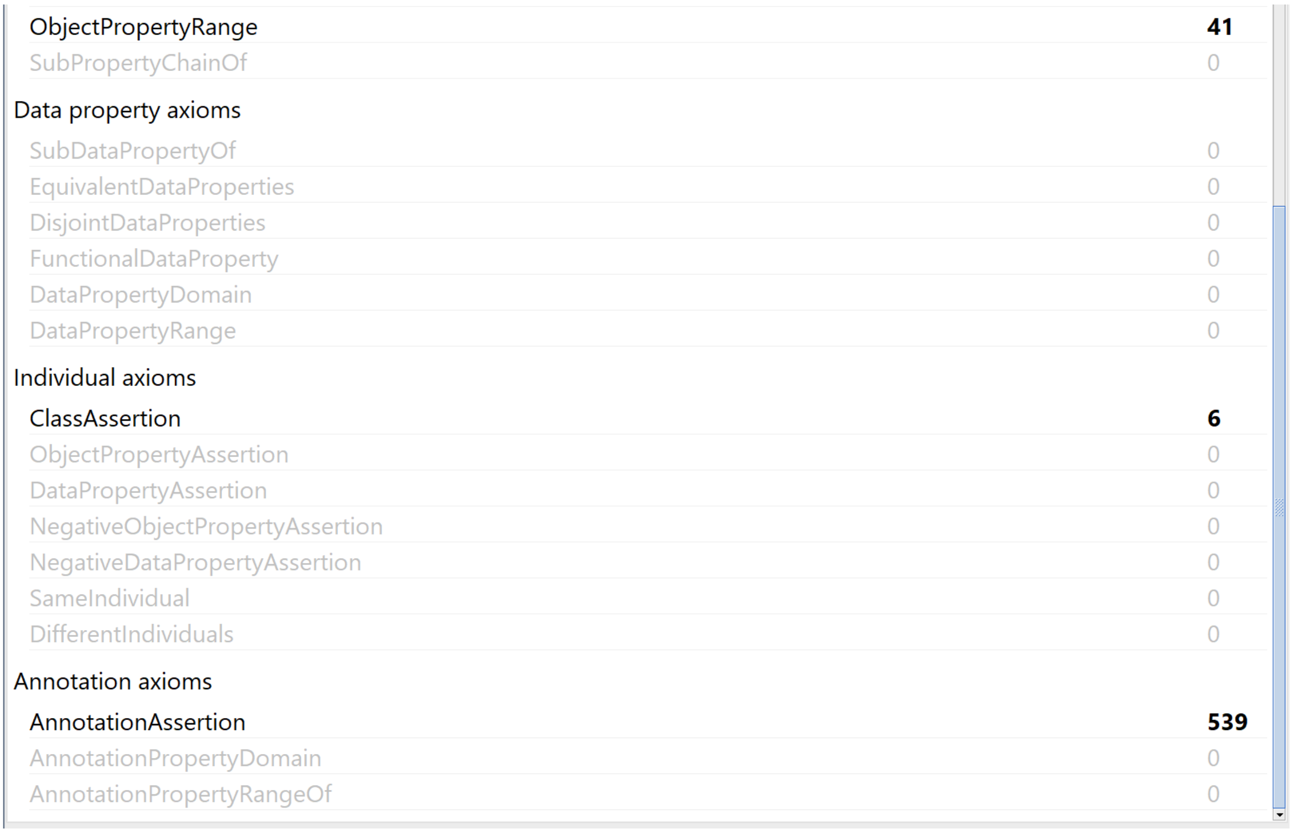
Main area	Obligations
Label	Follow instructions from controller
Defined by	GDPR Article 28
Superclass	Processor obligation
Subclasses	-

Appendix 6: General ontology metrics



Ontology metrics:

Metrics	
Axiom	**1199**
Logical axiom count	**426**
Declaration axioms count	**234**
Class count	**183**
Object property count	**36**
Data property count	0
Individual count	**11**
Annotation Property count	**8**
DL expressivity	SHIQ
Class axioms	
SubClassOf	**253**
EquivalentClasses	**10**
DisjointClasses	**10**
GCI count	0
Hidden GCI Count	**14**
Object property axioms	
SubObjectPropertyOf	**26**
EquivalentObjectProperties	0
InverseObjectProperties	**8**
DisjointObjectProperties	0
FunctionalObjectProperty	**10**
InverseFunctionalObjectProperty	**17**
TransitiveObjectProperty	**2**
SymmetricObjectProperty	0
AsymmetricObjectProperty	0
ReflexiveObjectProperty	0
IrrefexiveObjectProperty	0
ObjectPropertyDomain	**43**



ObjectPropertyRange	**41**
SubPropertyChainOf	0
Data property axioms	
SubDataPropertyOf	0
EquivalentDataProperties	0
DisjointDataProperties	0
FunctionalDataProperty	0
DataPropertyDomain	0
DataPropertyRange	0
Individual axioms	
ClassAssertion	**6**
ObjectPropertyAssertion	0
DataPropertyAssertion	0
NegativeObjectPropertyAssertion	0
NegativeDataPropertyAssertion	0
SameIndividual	0
DifferentIndividuals	0
Annotation axioms	
AnnotationAssertion	**539**
AnnotationPropertyDomain	0
AnnotationPropertyRangeOf	0

Figure 22: Ontology metrics

Information Security