A SEMANTIC BASED FRAMEWORK FOR SOFTWARE PRIVACY BY DESIGN

FATEMEH ZARRABI JORSHARI

A thesis submitted in partial fulfilment of the requirements of the

University of East London for the degree of

Doctor of Philosophy

School of Architecture, Computing & Engineering

January 2016

ABSTRACT

Software development market is currently witnessing an increasing demand for software applications conformance with the international regime of GRC for Governance, Risk and Compliance. In this thesis, we propose a compliance requirement analysis method for early stages of software development based on a semantically-rich model, where a mapping can be established from legal and regulatory requirements relevant to system context to software system goals and contexts. This research is an attempt to address the requirement of General Data Protection Regulation (GDPR, Article 25) (European Commission) for implementation of a "privacy by design” approach as part of organizational IT-systems and processes. It requires design of data protection requirements in the development of business processes for products and services. The proposed semantic model consists of a number of ontologies each corresponding to a knowledge component within the developed framework of our approach. Each ontology is a thesaurus of concepts in the compliance and risk assessment domain related to system development along with relationships and rules between concepts that compromise the domain knowledge. The main contribution of the work presented in this paper is a novel ontology-based framework that demonstrates how description-logic reasoning techniques can be used to simulate legal reasoning requirements employed by legal professions against the description of each ontology. The semantic modelling of each component of framework can highly influence the compliance of developing software system and enables the reusability, adaptability and maintainability of these components. Through the discrete modelling of these components, the flexibility and extensibility of compliance systems will be improved.

Additionally, enriching ontologies with semantic rules increases the reasoning power and helps to represent rules of laws, regulations and guidelines for compliance, also mapping, refinement and inheriting of different components from each other. This novel approach offers a pedagogically effective and satisfactory learning experience for developers and compliance officers to be trained in area of compliance and query for knowledge in this domain. This thesis offers the theoretical models, design and implementation of a compliance system in accordance with this approach.

ACKNOWLEDGEMENT

I have no words for thanking my director of studies, Professor Allan Brimicombe for his continued support and encouragement throughout delivering of this thesis to the end since working with him was a different and very useful experience for me. My Special thanks are for Dr. Abdel-Rahman Tawil for his supervisory during final stages of my PhD, also for all his guides, helps and leadership during my PhD. Also I am thankful to my previous team of supervisory for their introductory to this area of research, help and advices, especially to Professor David Preston.

Thanks to everyone in the University for helping to make a sufficient working environment for me. I'd particularly like to thank Professor Hassan Abdollah, Doctor Rabih Bashroush and Dr Hossein Saeidpour for their helpful feedback and comments on my work.

As importantly I would also like to thank my mother and father for their unflagging love, prayers and for the support I have received from them throughout has been overwhelming. I will be forever indebted with them.

At the end I would like to thank anyone mentioned here or not for supporting me for a long or short time during my PhD, since I believe this was not only an academic achievement, but also a life experience for me.

Contents

List of Tables

List of Tables

List of Figures

List of Figures

Abbreviations

NIST: National Institute of Standards and Technology

EU: European Union

ICO: Information Commissioner’s Office

GDPR: General Data Protection Regulation

OCEG: Open Compliance and Ethic Group

ITechLAW: International Technology Law Association

TTFL: Transatlantic Technology Law Forum

UN: United Nation

EDPS: European Data Protection Supervisor

UNCITRAL: Commissions of International Law, International Trade Law

UNICTTF: United Nation Information and Communication Technology Taskforce

APEC: Asian Pacific Economic Cooperation

OECD: Organisation of Economic Co-operation and Development

GRC: Governance, Risk & Compliance

ENISA: European Network and Information Security Agency

ML: Modelling Language

ISO: International Organization for Standardization

PCI DSS: Payment Card Industry Data Security Standard

DPA: Data Protection Act

HIPAA: The Health Insurance Portability and Accountability Act

PIPA: British Columbia Personal Information Privacy Act

COBIT: Control Objectives for Information and Related Technologies

KAOS: Keep All Objectives Satisfied

GRL: Goal Oriented Requirement Language

1. INTRODUCTION

1.1 Background and Motivation

Software systems are now widely used for applications including financial services, industrial management, and medical information management. Such systems collect and process sensitive information including personal and financial data (Breaux et al., 2008)

Therefore, safeguarding privacy and security of these data and also applications processing them, is one of the most critical consideration of the system developers and system users. Beside the technical safeguards and solutions for security and privacy, these subjects have also been considered in higher level of governments where laws and general policies are established. Governmental regulations that impact software systems are becoming ever-more prevalent in current legislative scenarios around the world. Therefore, it is now necessary that software for critical applications must comply with the relevant legislation. Particularly after the financial crisis of 2007-2008 (Kirpatrick, 2009) and considering the latest regulating climate, industries recognised the need to develop clear processes in order to improve their legal compliance process.

From another point of view, looking at software engineering and different activities of that, one of the initial stages is feasibility study or to be said system procurement. This is the place where decisions are made on the scope, budget and timescale and on whether the system should be procured. One of the main factors that is said to influence the decisions in this stage is “the need to comply with external regulations”. The reason behind this is the speed and completion of businesses through getting regulated with defined regulations. This has caused to a demand to replace noncompliant systems with the ones which make the compliance happen or monitor the compliance. ICT legal compliance has also been called as the marriage between business process management and information management (Rahmouni et al., 2009, Rifaut & Dubois, 2008, Roebuck & Dresner, 2005). It is where regulators preside, the organisation’s legal officers are witnesses and a guest list of middle managers, lawyers and other interested parties ensure that the couple’s brings up no nasty surprise!

In a look at the history of compliance in general, the collapse of an American energy company called Enron during 2001 with $15bn in debts and 20000 workers losing their jobs certainly woke regulators up to the subject of compliance. It also had consequences in UK to introduce wider powers to investigate companies under the Companies Act 2004. A consequence of non-compliance had been estimated by the British Chambers of Commerce costs about £4.625bn to implement the Data Protection Act in the UK for 2004. Department for Business, Innovation and Skills in UK publishes a survey conducted by PWC Institute and Infosecurity Europe every year. Based on the” 2013 Information Security Breaches Survey” (Department for Business Innovation & Skills, 2013), 93% of large organisations and 87% of smaller organisations had a security breach experience in 2012/2013 and the average cost of these breaches was between

£450k to £850k for large and £35k to £65k for small organisations which was almost tripled of the previous year rate. It is necessary to mention that also 85% of large organisations and 61% of smaller ones had been asked by their customers to comply with security standards such as the ISO 270001. According to the report 52% of organisations had a few experience of breach of data protection laws incidents during 2013, 25% had one incident during the year, 8% had about once a month, 12% once a day and 6% had several experiences of the incident during a day. These statistics also show that organisation had contingency plan for 50% of Infringement of laws or regulation incidents which were successful. But the legal actions that they took against the worst security breached only include 5% compared to their other security actions. These are proof on importance of legal compliance which is still being implemented. It also shows the importance of legal compliance as an integrated reference and a non-ignoring solution for security incidents.

Calling the new regime of Legal Governance, Risk Management and Compliance (LGRC) is a response to compliance requirement and has become a key issue in information Technology market (Open Compliance & Ethics Group (OCEG), 2009). Based on OCEG compliance has been defined as the process to ensure that information systems and relevant organisations follow existing laws, regulations, business rules and standards in their functions and adhere to ethical codes within their profession. Among the different approaches of compliance in information systems, Data Protection plays a key role in both industry and research in order to safeguard the privacy of personal data kept in information systems. This importance has been taken in different national and international legal frameworks in around the world such as EU Database Directive, Data Protection Directive 1995 and directive on Privacy and Electronic Communication. UK Data Protection act 1998 and Federal Data Protection of Germany are also some examples of implementation of Data Protection Directive in EU member states. New challenges of information technology have redounded to reformation of directives. For example, EU has proposed a reformation on Data Protection Directive in 2012 known as General Data Protection Regulation (European Commission Justice, 2012) and member states are instructed to apply it to their national laws by 2015. A role is issued to an institution called EU Commission in order to ensure the loyalty of member states to the adoption and application of EU directives. One of the most important aspects of compliance is considered in Article 25 of General Data Protection framework for implementation of a "privacy by design" approach as part of organizational IT-systems and processes. It requires that data protection is designed into the development of business processes for products and services. The importance of this matter has been also addressed by ICO (Information Commission Office, 2008). **Privacy by Design** is an approach to system engineering, which takes privacy into account throughout the whole engineering process in which human values should be considered in a well-defined manner throughout the whole process. On the other hand, technical compliance tools, are designed to be used to check the conformance of systems and application to laws, regulation and standards. Here we propose a framework which consider compliance as an early requirement of software systems to address Privacy by Design, but not compliance as something to be considered after production. The main purpose is to address Privacy by Design in software system development, but the framework is designed in a way that can also be used for PRD in business process.

In recent years, a large body of works have approached compliance as an early requirement of system and have aligned requirement engineering with compliance techniques. They mostly used goal-oriented methodologies of requirement engineering, taking law's rights as one of the main goal for the systems to be satisfied (Mouratidis et al., 2006; Houmb et al., 2010; Giorgini et al., 2005; Gangemi et al., 2003; Garzotto et al., 1999; Genesereth et al., 2014; Ghanavati et al., 2007; Gerber et al., 2008; Shamsaei et al., 2011). Various techniques to analyse and extract rights from legal texts have been researched by Breaux & Antón (2008) and Islam et al. (2010). The third type of works is those focusing on ontology techniques within the legal domain. Using semantic webs and developing ontology of legal concepts is also a well-known approach in the field of artificial intelligence. Authors in some surveys (Benjamin et al., 2005; Brekeur et al., 2003) have delivered a series of works providing legal ontology solutions for legal specialists. They have identified rich legal concepts in their taxonomies. Fenz et al. (2007), Gangemi et al. (2003), Ponoela et al. (2005) and Schmidt (2008) also proposed ontology and semantic web as solution for compliance. All mentioned works in requirement engineering have provided good efforts to address Privacy by Design. Ontology also was a great solution to provide knowledge repository for compliance. But still there are some points in compliance that should had been covered in future researches as being discussed in following.

First of all, governments and industries follow instruments from regulatory bodies and standardisation institutions to ensure information security. Thus, companies need to address compliance from two perspectives: IT compliance to industry best practice and guidelines and, on the other hand, compliance to laws. As discussed in previous paragraph, and also based on industry of compliance, standards such as ISO and Common Criteria and regulations such as Data Protection Act (Information Commission Office, 2012) and PCI DSS (PCI Security Standard Concil, 2016) play key role in compliance. This is a situation where an integrated and comprehensive solution for compliance is lacking that can cover different elements of compliance instead of providing isolated solution to one compliance element. Also According to OCEG a well-defined compliance is also augmented by an assessment of risk in order to safeguard the objectives of laws and policies (Open Compliance & Ethics Group (OCEG), 2009). In some situations, where a few of the elements of compliance are being overlooked or researched in isolation, new research is required to study compliance as an integrated concept in the area of software development.

Secondly, IT and legal compliance are verified mostly by experts at the moment. They are usually auditors or consultants, and this it is still a manual task to be performed by them. This compliance assessment process can be extraordinarily expensive. In the Information Era, one can think of an automated process that perform some compliance assessment steps automatically, thus reducing associated costs. Semantic web technologies in particular ontologies provide opportunities for developing modern automated compliance tools (Gangemi et al., 2003). For our work, ontologies are considered as the most appropriate platform being able to provide a number of advantages to our proposed framework in same time. Ontology provides the necessary domain knowledge of compliance in information technology in a repository of concept and their relationship. Accordingly, the components of our compliance framework can be defined separately using separate ontologies with concepts from domain of laws, guidelines and standards which are linked together using ontological relationships. The result is a united and integrated compliance solution to different resources in compliance from laws to standards and also guidelines and best practices. The query-based system of semantic approach also provides a user friendly and automated environment for users who want to be informed about knowledge of compliance. Our approach enables machines to use conceptual semantic models and apply reasoning techniques to infer compliance. Rule-based reasoning technique in ontology, especially the platform which we are using, protégé, provides ability to perform legal reasoning task automatically. This is the task performed by legally specialise and compliance officer in order to apply a rule of law to scenarios of real world. The correlation between different concepts and components of the compliance framework with ontology also provide the ability for user to trace a refined compliance requirement to its base requirement from laws, regulation or system context. Tracing requirements is one of the sought factors in compliance. Also, mapping between corresponding concepts from different ontologies of synonym terminology between different components of compliance framework is an advantage here which makes the compliance to different resources easier. The ontology also provides formalisation to the context of law, regulation and generally official document rules and texts. Therefore, this thesis focuses on designing a suitable architecture for compliance in software development and also business process to address Privacy by Design by using ontology and semantic rule technologies.

1.2 Aims and Objectives

The aim of this thesis is to propose an ontology based approach for supporting compliance of a developing information system to its related domain of laws, standard and policies. To achieve this goal, our work proposes a framework which delivers number of objectives to the area of information system development compliance based on Table1.1:

Objective	comments
Provide a repository of compliance knowledge using Ontology-Semantic web	• Implement a compliance framework as a knowledge repository to automatically retrieve, add or change information on compliance knowledge and system requirements • Categorize and interrelate different components of the framework as well as their concepts and objects • Perform legal reasoning to apply laws, regulations and policies to the scope of the

	developing system using semantic ontology reasoning infrastructures
Consider compliance as a critical requirement in Requirement Engineering stage of software development in order to answer to GDPR demand of Privacy by Design	• Start compliance from early stages of system development • Extract requirements from laws, regulations and policies • Categorize requirements using ontology taxonomy • Check requirement consistency by analysing requirements from different stakeholders • Trace requirements by identifying requirement dependencies, refining high-level requirements to application level
Perform an easy process of Law Analysis	• Resolve the ambiguity of legal language for software developers • Perform a legal reasoning task following similar procedures to legal professions
Perform a Compliance process including different elements of compliance	• Apply relevant laws, regulation and internal and external policies to the scope of developing system • Coverage and integration of different resources of compliance such as laws, guidelines and standards and the ability to refine them together in a hierarchical order
Perform Risk analysis against legal and security objectives of system	• Address constraint and risk against compliance objectives
Address system Design	• Perform early stages of system design using design patterns

Table1.1 . Objectives of Ontology-based Compliance Framework

To achieve the objectives above, separate ontological components are designed addressing each of the objectives in isolate. Each ontology describes the structure of knowledge domain of each objective whether it is Compliance Ontology, Risk Ontology, Requirement engineering Ontology or Design Ontology.

Each ontology consists of concepts and their relationship in a domain area. The connections and interactions between components of our framework has been implemented using of defined description-logic operations on ontologies such as *merge, mapping, integration, alignment, refinement, unification* and *inheritance* (Ontology & Semantic Web Online Tutorials). The separation and interaction of ontologies enables users to start compliance from early stages of software development, also to refine and reason facts of system context in a heretically order to high level demand of legal text and later to more application level requirements. The mapping between different components also benefit the user in order to find out about same concepts that has been defined in different terminology in our compliance components. Legal reasoning task has been possible in this framework using the semantic and rule based reasoning technique in protégé (Ontology & Semantic Web Online Tutorials). Extendibility in this context can be realised by allowing new ontologies to be added to this framework, also by adding new concepts to each of available ontologies, without having any significant impact on the architecture of system or a little to be changed. The proposed approach allows the user to start modelling of systems, find and apply related laws to the context of system and refine law's requirement by application level requirements from authority guidelines, standards and design patterns and perform risk analysis against system and its legal requirements, also to retrieve knowledge regarding each discussed steps.

1.3 Research Contribution

This research proposes a semantic rule-based approach to develop a compliance framework for software development in order to fulfil the requirement of General Data Protection Regulation known as "Privacy by Design". Our approach proposes an ontological architecture featuring a compliance engine which gets all its knowledge from ontologies implemented in our approach.

- The main contribution of this work is the separation, also the integration and refinement of the components of proposed framework using different ontologies. The coverage of most elements of compliance from laws to standards and guidelines and the method in which they are integrated together is the base novelty of the framework itself which has been possible by using the proposed knowledge-based approach.

- Simulating legal reasoning task of legal professions and being able to automate it using rule-based reasoning technique in semantic web is another contribution. Being able to conclude and refine from a simple fact from system context to legal requirements of system is a great advantage which fascinate the complex task of compliance for system developer who are not familiar with legal tasks. This will also benefit user of our system to deal with the complex task of law analysis and ambiguity of legal texts.

- The conceptual model of ontologies and the taxonomy of each provides a great knowledge repository from both legal and compliance domain and also requirement and design engineering for the user. The knowledge can be modified, extended or deleted in any time.

- Flexibility to change of laws and regulations is another innovation of current work which is one of the most on demand in the compliance area to deal with changes of compliance laws. Moreover, the ontology based approach addresses problem of maintenance and reusability of the framework components.

- Being able to represent and formulise rules of law by a same titled facility in ontology called *Rule*, and the unique syntax and format used to formalise them, makes this work different from other similar works.

- Having some early stages of system design in the proposed framework and its corresponding ontological model, helps non-professional developers to have some primitive ideas regarding the way in which the high-level legal requirements can be designed and implemented in following stage of system development.

1.4 Thesis Overview

The rest of this thesis is organised as following:

- Chapter 2 reviews the necessary literature on legal aspect of information system and the compliance specifically in area of Privacy by Design. Also it provides some literature regarding the components of our framework from laws, standards related to information system such as Data Protection and standards such as ISO. The literature review covers seven types of previous works. First are background on IT legislation. A survey on research in information technology laws are provided in this section. This helps the reader to have background regarding different IT laws and also makes reason for the selection of Data Protection Regulation as a compliance law in this research. Second and third categories present a background on previous works which had proposed after-the-fact compliance approaches information technology and before-the –fact approaches. The last three parts provide background knowledge on ontology-based compliance approaches, advanced software engineering and technical aspects of ontology and semantic web. The weak and strength points of previous works are discussed in conclusions and grants to this research are concluded at the end.

- Chapter 3 introduces the design of a novel framework and supporting approach to the compliance of information system development with related laws and regulations. Firstly, it describes the research methodology used in this research and also the research approach. The methods of data collection from areas of laws and regulation are being discussed in detail. The way the data for this research has been analysed will be explained and concluded. This will be followed by introduction of the framework and its components and their implementation by ontology. After all, it will discuss the ontological implementation of each framework's component in separate and will highlight the importance of semantic rules used in each ontology and also to connect and interrelate different ontologies together. Required technology to implement KN-SoPD, the ontological implementation of our framework is discussed later.

- Chapter 4 presents the result of the evaluation of our approach, proposed in this thesis.
- Chapter 5 concludes the thesis. It outlines the objectives achieved and the key contributions made in this work. Finally, it discusses the potential directions for future works.

2. LITERATURE REVIEW

The literature review in compliance domain is generally divided to different categories. This is firstly due to different perspectives of compliance in general. At the beginning we are providing a survey on history of legislation in IT domain and international organisation participating in IT law assignment. This is to make ourselves and readers familiar with different laws and organisations related to IT legislation and specifically privacy laws. Then we will consider the traditional approaches of compliance where auditing happens after the production of final product known as After-the fact Compliance. In contrast to this, we also perform literature review on approaches in which compliance is considered through design and development of system called Before-the-fact Compliance. Each of these two main categories may include compliance solution as general, in IT domain or to a specific area except from IT. A separate literature review will also be considered to the different components employed in our framework and their isolated application in subject of compliance in previous works. Considerable number of previous researches had been afforded to analyse laws and extract requirements from them. Making organisational policies and implementing systems based on compliance requirements is an area of compliance in design which specifically will be discussed too. A main literature review is specified to ontology-based compliance approaches. They provide a knowledge repository of compliance concepts. Advanced software engineering. And using design patterns is discussed in another part. And finally technologies used for ontology and semantic web implementation is discussed at the end. We conclude this literature review with weak and strength points of current work with others. We should mention that there will be some overlaps between different areas of literature review here due to the fact that some previous works may have provided multi-objective compliance solutions.

2.1 International Organisation of Information Technology Laws

In light of the existing international and national laws and legal practices in information technology and computing, most of the international organisations such as ITechLaw (ITechLaw), TTLF (Transatlantic Technology Law Forum), and most of legal practitioners such as Kulesza (2012) and Lioyd (2011) has ranked information technology laws based on the jurisdictional powers of different territories where each state is obligated to restrict rules to its nations by approving national laws. Their main focus is on three areas of Europe, US and Asian Pacific. To overview the current IT related legal practices over national and international borders; the same geographical categorisation is being used here. The main reason of this choice is based on the potential technical capability of selected regions and their position and practices toward regulating cyber and computing spaces. The other key factor in differentiating laws here is the legal aspects of computing if they are Computer law, IT Law or Cyber Law. In order to represent the sustentative research to complicate international regulating attempts based on mentioned organisation, APPENDIX I has been provided. This information is designed in a hierarchy structure based on the territories of legal actions respectively in international, continental and national scopes. The second metric to categorise legal actions is based on the criteria of IT targeted by the legal practice. This is first generalised by legal aspects of IT (Computer Law, Cyber Law and IT Law) and later is narrowed by specific fields such as copyright, information security, privacy, e-commerce and others. Regulations in each category are categorised firstly from traditional legal frameworks which have considered the matter from a general point of view such as privacy regulations. After, those are listed which have special consideration on the matter in technology aspects such as Data Privacy regulations.

It is essential to mention that to look at the subject in international and continental scopes, expert groups are assigned in most cases who have especial activity and legal authority in a specific field of IT or a general matter such as UN Security Council. Following sections are provided to make ourselves familiar with international organisations and their working groups and committees in IT legislation.

2.1.1 United Nation and IT Legislation Regime

The unique international character of United Nation (United Nation (UN). Available at: http://www.un.org/en/index.html. (Accessed on March 2011).) as an international organisation who promotes and coordinates international peace and security, human rights and better living standard in every corner of globe through the membership of its 193 member states of countries, has made the organisation as a respected international authority who can take actions on a wide range of issues around the world. The strong authority tool of UN Charter which is signed by its members, is a constitute treaty which bounds all members to its articles. UN is organised on the base of number of main bodies as General Assembly, Security Council, Economic and Social Council, International Court of Justice, Trusteeship Council and others. General Assembly as the main deliberate and policy making organ of UN is consisted of representative of all UN member states who based on the unique forum of UN discuss, decide and vote on international issues covered by the charter. General Assembly also plays an important role in codification of international laws and standards through its assigned subsidiary commissions and committees and councils. Commissions of International Law, International Trade Law (UNCITRAL), Disarmament, peacebuilding commission and Human Right Council are some examples. The International Law Commission with the purpose of removing uncertainly areas of national laws, filling the gap of them in international circumstances such as protection of intellectual property, telecommunication and postal services, maritime and aerial navigation, was established in 1947 by General Assembly resolution of 174(II). The main goal of the commission has been introduced as “ the promotion of progressive development of international law” and “the preparation of draft conventions on subjects which have not yet been regulated by international law or in regard to which the law has not yet been sufficiently developed in the practice of States” (European Commission). UNCITRAL as the core body of UN in the field of international trade and commercial law has the responsibility to modernise, formalise and harmonise international conventions, model laws and rules, give legal guidelines and recommendation and update case laws and enact uniform commercial acts, worldwide on international business and new opportunities of commerce. UNCITRAL was first established by the United Nations General Assembly by resolution 2205(XXI) of 17 December 1966. It provides legislative and non-legislative instruments in areas such as international contract practices, electronic commerce, and international payment and secure transactions. The legislative instruments are conventions, model laws, legislative guides and model provisions

UN council of Human Right is another subsidiary organ of General Assembly (GA) established by resolution 60/251, which is specially mandated to promote and protect human rights for all by providing assistance and technical training to member states. Children rights, civil and political rights, cultural rights and privacy are some of the fundamental issues of human right covered by Human Right Council. Universal Declaration of Human Right is the key treaty of the council dealing with all aspects of human rights. Regarding rights in cyber space, HRC is one of the key organs which has taken serious actions to protect privacy of people in digital age. In December 2013, GA adopted resolution 68/167 expressing deep concerns of UN regarding the negative impact of surveillance and interception of electronic communications on human rights. In this way, GA called all states to review their procedures and legislations regarding the interception and surveillance of communication and protection of personal data by insuring their full compliance with international human right law and some other legal international instruments such as International Covenant on Civil and Political Rights.

Security Council is the main organ of UN which is responsible for the peace and security of the globe under the UN Charter. It consists of 15 members and decisions of the commissions are obligated to all member states of UN. Security Council also consists of some committees such as Counter-Terrorism Committee, specifically responsible to prevent terrorism actions around glob by making policies and giving technical assistance to states. It was established in the wake of 11 September attacks against United States in 2001.

Economic and Social Council (ECOSOC) is the principle organisation under the UN charter which coordinates the economic, social and related works of UN. It was established in 1946 under the charter of UN. One of the main achievements of ECOSOC regarding IT has been the establishment of "Information and Communication Technology Taskforce" (UNICTTF) in 2001.

2.1.2 European Union and IT Legislation Regime

The European Union was founded in 1950 after the Second World War by the aim of peace and neighbourhood and economic and political unity in Europe. The first founders were Belgium, France, Germany, Italy, Luxembourg and the Netherlands. Other countries such as Ireland, United Kingdom and Denmark joined the union later in 1973. It was by 2007 when 28 of Europe countries joined the unity and by the time the Union agreed on fundamental issues such as Schengen region, euro as the uniform currency of many European countries, Europe unison against terrorist after 11 September attacks and financial crisis in 2008. Some of the main bodies of EU can be mentioned as European Parliament, European Council, Council of EU, European Commission, Court of Justice, European Economic and Social Committee and European Data Protection Supervisor. Among them three main institutions of European Parliament, Council of EU and European Commission are involved in Europe legislation.

European Council sets the overall political directions of EU but has no power to pass law. It consists of head of states or governments of 28 European member states along with Commission president and Council of EU president.

European Parliament is directly voted by EU voters every five years and its member's present EU people. Along with the Council of EU, the European Parliament has a process called "Ordinary Legislative Procedure" to decide on the contents of EU laws and officially adopt them.

European Commission is also consisted of 28 commissioners from member states which each commissioner is responsible for a specific area of policy making assigned by the Commission president and approved by European Parliament. Their main responsibility with the "right of initiative" is to propose new EU laws and pass them to European Parliament and also enforce the approved laws to states as the body of "guardians of the Treaties". One of the main and recent activities of European Commission had been its proposing of Europe 2020 Strategy on March 2010, in order to improve the economy of European Union. The strategy is the following of another one in the period of 2000-2010 called Lisbon Strategy. In order to gain the goals, the strategy has targeted seven flagships initiative which the first one is called the Digital Agenda for Europe (DAE). DAE aims to improve digital technology and services to European citizens and businesses by taking 101 actions grouped under seven main areas. Regarding the IT legislation two of the action categories can be mentioned as to create a new and stable broadband regulatory environment and to propose EU cyber-security strategy and Directive. Under the defined actions European Commission has considered to update numbers of current directives and also propose new directives and rules.

Among different EU organs there is a position called the European Data Protection Supervisor (EDPC) assigned in 2001 which is subject to the special responsibly to advise, supervise and check EU's institutions and organizations compliance with data protection legislation and rights of the civil in relation with Data Protection Regulation (Regulation (EC) NO 45/2001). This is done with cooperation and works with Data Protection Officers across Europe's institutions and organizations which process personal data of people. The officers inform the EDPC about the information of their institution and type of personal data and processes they held on them. This is done through a registration to EDPC. It also monitors new techniques and also new legislation proposals which may affect the data protection. EDPS does this task through its instruments of planning tool, formal published comment and opinion and intervene to the cases of Court of Justice. One of the main cooperation of EDPS is through Article 29 Working Party which is composed of representatives of national authorities of data protection, EDPS and European Commission. Among the cooperation, expert advice and uniform application and interfere of Directive 95/46 is provided to nation authorities and the Commission. The tasks of Art29 WP are defined in Article 30 and Article 15 of Directives 95/46/EC and Directive 2002/58/EC.

2.1.3 Asian Pacific and IT Legislation Regime

APEC (APEC ELECTRONIC COMMERCE STREEING GROUP), established in 1989 and today composed of 21 of “member economies”, is the premier intergovernmental grouping in Asian Pacific region which aids to facilitate economic growth and cooperate trade and investment in the area. Unlike the other multilateral trade bodies, APEC operates based on non-binding commitments and has no treaty obligations required for its members. Indeed, each of member states has their own time and action plans to achieve APEC’s policies on a voluntary and non-binding basis and individual action plans and their results are submitted to APEC in regular basis and peer reviewed by APEC’s special teams.

APEC’s vision is to achieve number of predefined goals upon specified dates which have been introduced as “Bogor Goals” in a meeting of APEC’s leaders in Bogor, Indonesia, 1994. The Bogor goal was to have free *and open trade and investment in Asian Pacific by 2010 for industrial economies and 2020 for developing economies* (APEC ELECTRONIC COMMERCE STREEING GROUP). In order to meet the defined goals, APEC has considered three areas of works as *Trade and Investment Liberalization, Business Facilitation* and *Economic and Technical Cooperation*. APEC’s main policy making and duties are run based on number of meetings which on the top is the APEC’S economic leaders meeting held by 21 member’s representatives once a year. In lower level there is Ministerial meeting holding once a year prior to leader’s meeting to make recommendations for leaders and consider the year’s activity. Sectorial Ministerial meetings are held regularly in areas of education, technology and science, telecommunication, information industry and others and their recommendations will be provided to economic leaders. Also APEC Business Advisory Council (ABAC) provides recommendations to economic leaders through annual meetings and official reports. The policies made in the leader’s level are executed by number of committees and their sub-committees, expert groups, working groups and task forces. Committee on Trade and Investment (CTI) follows the goals of APEC for free and open trade and investment in the region and have expert groups of Intellectual Property, Electronic Commerce Steering Group (ECSG), Sub-Committee on Standards and Conformance and other groups. There are number of other working groups based on the Sectoral Ministerial meeting such as working groups of Counter-Terrorism and Telecommunication and Information. The main group working in the area of creating legal, regulatory and policy environment of e-commerce is ECSG whose activities are spread mainly on Data Protection and Paperless Trading by two specific sub-groups. ECSG was successful to achieve number of legal frameworks and strategies and individual member’s action plans as the answer to its activities. In order to obtain the goals, ECSG also has cooperation with international organizations in same category such as United Nation Centre for Trade Facilitation and Electronic Business and OECD, also with Internet Society. The Intellectual Property Right Expert Group was also established by CTI in 1996 in order to protect intellectual Property Right in Asian Pacific through legislative, administrative and enforcement mechanisms of APEC. The Sub-Committee on Standards and Conformance was also established in APEC in 1996 in order to harmonize standards and conformance in Asian Pacific and reduce the bad effect of standards diversity on trade in the area. The other working group of APEC which activity is focused on parts of information technology is the

Telecommunication and Information working group established in 1990 and consists of three steering groups of Liberalisation, ICT Development and Security and Prosperity (SPSG). Their aims of improvement in information and communication technology, safe and trustable ICT environment and cooperate in ICT activities in the region are being followed by the group implementing policies, task forces and strategies such as “Internet of Things”. SPSG as a steering group focusing on promoting security and trust in e-commerce and avoiding cybercrime in the area, has special cooperation with OECD and numbers of projects such as Cyber Security Policy Developments in the APEC Region led by USA.

2.1.4 OECD

The Organisation of Economic Co-operation and Development (Open Compliance & Ethics Group (OCEG) (2009) *GRC Capability Model “Red Book” 2.0.* OCEG Publication. composing of 34 members from different countries around the world from Europe to Asian Pacific and US along with the Europe Commission, gathers governments to share experiences and seek solutions to common economic, social and environmental problems and promote OECD’s established policies, standards, guidelines and recommendations across the members. The work is carried out by the contribution of OECD organs such as the Council, committees and Secretariat. OECD Council as the decision making power made up of one reprehensive per member country plus a representative of the European Commission. OECD Committees consisted of around 250 different committees and working groups, each focused on a specific area such as economic, trade, science, education and others. Representatives of the 34 members meet along the committees and working groups in order to advance ideas and review the progress in each mentioned specific policy area. The Secretariat chairs the commission, provides the links with national delegations and supports committees’ activities. OECD also has official relations and cooperation and extensive contacts with international organisations and bodies such as United Nation Council of Europe, Asian Pacific Economic Cooperation (APEC), also with civil societies such as ENISA (European Network and Information Security Agency), International Conference of Data Protection and Privacy Commissioners and GPEN (Global Privacy Enforcement Network) and indeed with some non-member countries in order to consult and conduct policy dialogues.

Among different departments of OECD, there is a one called “Directorate for Science, Technology and Industry” with specialized and assorted focus on matters such as Internet Economy, Science and Technology Policy, Broadband and Telecom, Innovation in Science, Industry and Technology and others not being mentioned here regarding their irrelatively to the subject. The Directorate supports the work of a committee called as Committee on Digital Economy Policy consisting of working parties of:

- Communication Infrastructure and Service Policy
- Measurement and Analysis of the Digital Economy

- Security and Privacy in the Digital economy

The working parties are established under the working area of Internet Economy and Broadband and Telecom and eventually develop recommendations and policy guidelines which express the consensus views of the entire OECD membership.

2.1.5 International Regime on Data Protection Legislation

Data protection or data privacy is a concept which expresses the relation between data or information collection and dissemination automatically or manually from one side, and the public, legal and political expectation of the privacy of that data stored, collected and processed from another side of issue. The classical definition of privacy legislation goes back to the introductory of a United States' judge to the concept of "to be left alone" (Kulesza, 2012; Brandies & Warrien, 2012). To have a vulgar definition of the term of data protection, it is an individual right to control the extent to which her personal information is disseminated to other people. As the concept of data protection has its roots in the essence of privacy as a human fundamental right, it is better to firstly proceed to history of privacy in legislation. The notion to privacy has been the feature of number of international and domestic for decade even centuries. It was aftermath of Second World War that there had been international recognition of consensus on the concept of Human Right although it is argued that Cyrus Cylinder is the world's first charter of human rights. The Universal Declaration of Human Rights was adopted in 1948 by General Assembly of the United Nation which indicates the privacy of people as a right which should be protected by law in Article 12 of the declaration. The Convention on Human Rights was also adopted by Council of Europe in 1950. The Article 8 of the convention is the particular relevance of the text to the subject of privacy of people. During the last third of twentieth century, simultaneous to the growth of computer use to store and process personal data, Western Europe was emerged by a trend to introduction of data protection laws especially concerned with personal data processing issues. This is when a linkage between general concept of privacy and personal data protection was drawn. It was in 1968 when Council of Europe addressed a request to Committee of Ministers to consider the extend to the Convention on Human Rights regarding the safeguard of personal data processed by computers since it was believed that the EU Convention and the UN Universal Convention on Human Rights both were devised before the wide usage of computers in processing personal data. Therefore, Council of Europe adopted data protection principles in its recommendations to member states to consider national legislation in the case, but never mentioned the means and methods to adoption at the time. In fact, the first legislative initiatives in the subject occurred in national level in German in 1970 and Swedish Data Protection Act in 1973. As more and more European countries adopted national data protection laws, problems raised regarding international trade of information regarding conflicts in national laws. Therefore, agreements and legal frameworks were adopted in Council of Europe as the "1981 Convention on Processing of Personal Data" and the EC Data Protection Directive in 1995 in order to avoid national laws' discrepancy. In addition to the convention and the directive, the Council of Europe also has provided number of recommendations and guidelines for member states in order to implement the directive and convention also in line of the data protection issues itself.

Data Protection Directive 1995 is one of the most important legal frameworks taken by European Parliament and Council to ensure and incorporate level of equal privacy legislation in Europe and its member state national law. Member states adopted their national laws to meet the goals defined by this directive. UK Data Protection act 1998 and Federal Data Protection of Germany are some samples of implementation of Data Protection Directive in EU member states. The models introduced in EU directives are also assimilated by some non-Europe states as described before in section 2.1.2. Technology progress and the new challenges of it has redounded to reformation of Data Protection Directive and to its following adopted national laws. As an instance, regarding the new methods of data collection, access and use in Internet and the challenges coming with that, EU has proposed a reformation on Data Protection Directive in 2012 known as General Data Protection Regulation and member states are instructed to apply their national laws. A role is issued to an institution called EU Commission in order to ensure the loyalty of member states to the adaptation and application of EU directives. Each member state has also some authorities responsible to adopt their national laws to directives and keeping the track of it by EU Commission. Information Commissioner's Office of UK (ICO) is an instance of the authority in UK (Information Commission Office, 2012)

In about the time when Council of Europe started its activity in the field of privacy and data protection, OECD also appointed an expert group in 1969 in order to analyse different aspects of privacy in relation to digital information, transformer data flow and policy generating in general. "Recommendations to Member States concerning Guidelines on the Protection of Privacy and Transformer Data Flows" is an OECD product in the field of data protection as the working result of another special group in 1980. As the group was remitted their work was carried out in close relation with Council of Europe and European Community. Although the mentioned guidelines did not have legal binding as the Convention of Council of Europe had and it should be seen as a common-law-based approach. OECD also adopted "Declaration on Data Flows" in 1985. Apart from the legal activities, OECD also has sponsored number of projects such as an online package referred to as a privacy generator which help web developers to use techniques and safeguards in compliance with OECD Guidelines on data protection.

In same category of activity, APEC also established "Asia Pacific Privacy Charter Council" hosted in Cyberspace Law & Policy Community of University of New South Wales in 2003 which is drawn on APEC Privacy Framework. Its aim has been introduced to develop independent standards for privacy protection in accordance with privacy laws in the Asia Pacific region.

At the international level of United Nation, the UN Economic and Social Council agreed on "Guidelines concerning Computerised Personal Data Files" in 1990 which identifies 10 principles which are indicated as the minimum guarantees of data protection that nations should provide in their national legislation regarding data protection. The guideline also envisages the establishment of national agencies authorized to meet and observe the implementation and requirements of the guidelines. In a meeting of data and privacy protection commissioners in 2009, UN also considered a demand for global and international standardization in the field of data protection allowing for the development of a universal legal document with cooperation of national authorities and organizations in the field. It was followed by UN rapporteur on human right call in 2010 for establishment of a global privacy standard which still has not been proceed on.

In national legislation level, there is a gulf between countries which see the data protection essentially rooted in notion of human rights and those which believe data protection has economic bases. Banisar & Davies (1999) has provided a survey on the development and establishment of data protection law in about fifty countries around the world.

2.1.6 Future of Data Protection Legislation

The rapid development of technology which has observed its consequences in modern and global methods of trade in location-based services and smart cards, remote data sharing and storage in cloud computing, communications in social networks and other new generation of technology has changed the way personal data are collected, shared and used and consequently has brought new challenges in data protection. Also it is believed that the flexibility of international data protection legislation and guidelines in the implementation methods of data protection rules in national level, has made an uneven level of data protection in case of international services of technology. Therefore, international authorities such as European Commission have come to the term of reform in data protection rules. The Commission has proposed a complementary reform on Directive 95/46/EC on January 2012. The goal is to update and modernize the principles enshrined in 1995 directive in order to guarantee and strength data protection in future. In fact, the proposal is a reflection of the change in Lisbon Treaty and Article 16 TFEU, to create a new legal basis for a modernised and comprehensive approach to data protection and the free movement of personal data, also covering police and judicial cooperation in criminal matters (European Commission Justice, 2012). The Commission has been in public consultation and intensive dialogs with EU national data protection authorities and EU stakeholders and international organisations such as ENISA from 2009 and finally has come to united opinion on the demand for the reform on data protection rules in Europe. In 2012 the Commission proposed new framework consisting of:

- A Regulation (replacing Directive 95/46/EC) setting out a general EU framework for data protection

- A Directive (replacing Framework Decision 2008/977/JHA) setting out rules on the protection of personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities

In order to reduce legal fragmentation of national laws in data protection and have a stronger legal instrument with a direct applicably in the union, this general regulation framework has been adopted to replace the current directive and a harmonized set of core rules has been introduced. Some articles are repeated from Directive 95/46/EC, some new articles have been added and some are the extension of current articles. General Data Protection Regulation has been adopted in this research as a reference legislative framework for compliance to privacy by design. Compliance approaches in general are divided to two categories of After-the-fact and before-the fact solutions. To have a literature review on these two categories, we have following sections and listed relevant works both for compliance to data-protection or any other laws, regulation or industry. This is to have a review on any compliance methodologies as well.

2.2 After-the-fact- Compliance

Compliance in running businesses is a traditional and industrial solution in which compliance is audited when the final product is working and running in application area. These woks are also categorised to two main branches of *Retrospective Reporting* approaches where compliance auditing are performed manually (often through some consultation and guidelines) or by Automated Detection. Regarding the big number of almost commercial works in this area, we have selected the most known and famous ones in following lines to be reviewed. We will briefly review these works as after-the-fact solutions although they are not the concentrate of compliance in our work. Therefore, we don’t go further in details of them. Regarding the bunches of commercials approaches in this area, our aim is to have a brief review on their technical aspects.

Manual solution is provided through some consultation and guidelines. International organisations such as OCEG (Open Compliance & Ethics Group (OCEG)), provide manuals, guidelines and consultation service for compliance. OCEG Redbook is a general compliance roadmap provided by OCEG. Huge numbers of trading companies such as PriceWaterhouseCoppers also provide consulting services to their consumers regarding implementing compliance and policies in their businesses. OCEG provides general solutions for compliance as whole. Although the provisions are through prepared guidelines and consultancy to organisations and companies, but OCEG recommends using of automated tools for compliance as well. One can say that OCEG guidelines are both for after-the fact and before-the-fact compliance. GRC Red Book Capability Model (OCEG, 2012) provided by OCEG is a global and easy to be used reference model to guides through compliance process and also to evaluate developed compliance approaches. As an example the general GRC (Governance, Risk & Compliance) conceptual model provided by Vicent & Silva (2011) has been evaluated by OCEG GRC model. The evaluated works aims to provide GRC solution for businesses and organisations of any types. The conceptual model consists of number of components for elemental factors of GRC. Each component is related to other components through some defined relationships and finally an integrated solution for GRC is provided.

The work done by Roebuck & Dresner (2005) is also one of the most known works in compliance in running business which believes compliance should always be based upon an assessment of legal risk in an IT system. Roebuck’s and Dresner’s approach breakdowns the business into its ICT activities among main types of commercial participants considering their assets and place the law and performs and analyses legal risks in the context of processes of each group. The work adopts the PDCA cycle model for risk management in ICT project lifecycle.

The second category covers the bulk of existing software solutions for compliance. Following list are some of Software approaches provided for compliance.

IBM Lotus workplace for Business Controls & Reporting (International Business Machine Corporation, 2004) provided an open controls-management platform that enables to address challenges in managing internal business controls. The open, standards-based platform of Workplace for Business Controls and Reporting supports documentation and reporting of internal controls based on the Integrated Internal Control Framework from Committee of Sponsoring Organizations (COSO) of the Tredway Commission and the Control Objectives for Information Technology, COBIT, IT Governance Institute, as well as other international organizations. Consequently, it reduces the complexity of using a single tool to meet multiple requirements.

Microsoft Office Solutions Accelerator for Sarbanes-Oxley (Rochelle, 2003) is an automated approach for compliance to Sarbanes-Oxley Act of 2002. This is a solution to handle the amount of information generated in compliance process and automate reporting processes, making them an integral component of conducting business instead of an afterthought.

SAP GRC (Governance, Risk and Compliance) Solution (Scholer & Zink, 2008) enables users to manage GRC (Governance, Risk & Compliance) processes efficiently while investing minimum possible effort in documentation and controls. In addition, it allows users to monitor authorization and access.

Quality management programs and ISO 9000 certification efforts accomplished by organisations are typically based on group work and generate large amounts of written documentation. Groupware (Cirulli et al. 1997) technology can improve group work and process documentation.

The work done by Sadiq 2006 also is an example of automated solutions for compliance to Sarbanes-Oxley Act based on process-mining techniques. The approach uses a LTL Checker and verifies whether the observed behaviours discovered from process event logs matches the (un)expected/(un)desirable behaviours.

Among the works which have tried to accompany compliance in other fields rather than information technology, (Finley et al 2014) is also a formal information infrastructure for regulatory information management and compliance assistance built upon XML. It provides primary compliance knowledge for small businesses and producer of hazardous by-products to comply with US federal and state regulations.

The mentioned solutions hook into variety of enterprise system components and generate audit reports against hard-coded checks performed on the requisite system. These solutions often specialize in certain class of checks, for example the widely supported checks that relate to Segregation of Duty violations in role management systems. However, these approaches still reside in the space of “after-the-fact” detection. The advantage of these works is the reduction of time compared to the manual compliance approaches. But there are still gaps regarding compliance in these approaches. The main gap is in the sustainability of these approaches against changes in compliance laws, regulations and policies. Even with automated detection facility, the hard coded check repositories can quickly grow out of control making it extremely difficult to evolve and maintain them for changing legislatures and compliance requirements. The critical issues are that considering compliance from early stages of product design is always more efficient that after production. Therefore, we have concentrated on a solution for before-the-fact-compliance to generate compliance requirement as soon as possible in design stage of software development.

2.3 Before-the-Fact-Compliance

Since it is proved that considering compliance in design time specially in privacy matters, benefits system designers and owners to avoid relevant risks, eases implementation process, and makes sustainability to changes of the laws and regulations compared to before-the-fact approaches, (Scholer & Zink, 2008; Rubenstein & Good, 2013; Ruopeng et al., 2007; Islam et al., 2011), we have opted to design a before-the-fact approach for privacy compliance and therefore our concentration is on the works that adopts compliance techniques in design and development of information system, also business processes.

Before-the -fact approaches can be further categorized as either (a) compliance-aware design or (b) post design verification.

A large body of works in before-the-fact-compliance approaches are specified to compliance in business processes. These group of works ensure that business processes, practices and operations are in set of norms. The most application area of these approaches are in financial and banking industries (Basel Committee on Banking Supervision, 2004). Compliance in business processes are recognised both as compliance-aware-design and post-design verification approaches based on the nature of their work. For instance, authors Sadiq et al. (2005) investigated an approach that provides the capability to capture compliance requirements through a generic requirement modelling framework and subsequently fascinate the propagation of these requirements through business process models and enterprise application, thus achieving compliance by design in business process. Authors believe that compliance is the relationship between two formal specifications of business process and legal rules. The compliance modelling in this work takes advantage of a formal modelling language called FCL Formal Contract Modelling Language. They used a Model-driven business process execution technology in order to enforce compliance requirements into the business process goals and tasks.

Schumm et al. (2010), use a BPMS (Business Process Management System) (Panagacos, 2012) in order to model the business process and then integrate compliance requirements into the business processes using fragments and textual annotations. This work mostly is able to handle the frequency changes of laws and regulations in financial and banking industry. This is an area in compliance which needs more adaptability to the changes of compliance domain as it changes rapidly in financial and banking industry. It handles this importance by storing fragment processes in a data base repository and reusing them in changing circumstances. The repository assigns a Universal Unique Identifier (UUID) to each process fragment being stored which are used to query fragments and also to link compliance process fragments to their sources. Therefore, reusable fragments are being used as patterns here. This work covers both application of compliance in design and running time. A process called gluing is also used to physically apply a compliance requirement to the original business fragment. The authors believe gluing process comes with some shortcomings such as platooning the original business processes which has disadvantages. In a later work (Schumm et al. 2010), same authors use temporal logic to formalise elicited fragments in order to make an automated verification tool for the compliance fragments. Temporal logic is a modal logic for reasoning about dynamic scenarios, in which processes are formalised in format of states and their transitions over the time (Seshia, 2014). In compare of our work to this one, compliance to data protection and related regulations suffers less from the changes to the legal domain rather than in financial domain. Although we are still using an infrastructure for our proposed framework (ontology) which can store legal and regulatory requirements for any future adaptability to changes.

Ruopeng et al. (2007) extended the first version of Sadique's work with an approach for compliance-aware-design which allows the process designer to quantitatively measure the compliance degree of a given process model against a set of control objectives. Since the approach presented so far is focused on assessing compliance of a process model through execution sequences, it can also be considered as a post-design compliance verification approach.

Authors Goedertier & Vanthienen (2006) investigate the use of temporal deontic assignments (e.g. Liu et al. (2007)) on activities as a mean to declaratively capture the control- flow semantics that reside in business regulations and business policies. They introduced a language to express temporal rules about the obligations and permissions in a business interaction and also and an algorithm to generate compliant sequence-flow-based process models that can be used in business process design. The language is called PENELOPE. Most consideration of this work and the designed language is on the impact of sequence and timing constraints on business process design. This is due to the fact that the sequence and timing constraints on the activities in business processes are an important aspect of business process compliance. This may not be a first priority in software development compliance or may have limited application area.

In contrast to previous work, authors Schmidt et al. (2007) provided solution for compliance of service processes to relevant quality standards such as ISO 20000. Authors in this work are considering compliance as a very essential task in service production process since service produced, cannot be measured in advance. Therefore, the compliance of the service process with quality standards plays an important role in convincing the customer that the services rendered will result in the quality specified. However, the check for compliance is still a tedious task. Compliance checking is run through definition of two specific ontologies for compliance rules and service process.

Bons et al. (1995) identify this need to incorporate the legal state into the model of a trade procedure. To this end, the authors propose to annotate the states in Petri nets with a description of the logic deontic state. Deontic logic is the field of philosophical logic that is concerned with obligation, permission, and related concepts. Alternatively, a deontic logic is a formal system that attempts to capture the essential logical features of these concepts (Åqvist, 1994).

The contribution of the work by Goedertier & Vanthienen, (2006) is a framework for business process modelling based on business rules, called EM-BRACE: Enterprise Modelling using Business Rules, Agents, Activities, Concepts and Events. Business policy and regulation are internalized and made explicit in terms of the BRACE building blocks.

Business rules are also presented in the Business Collaboration Development Framework (BCDF) of Orriens et al. (2005). This framework strives for adaptability in business collaboration through web services using development rules – which include business rules – for domain analysis, management rules for validation and verification and derivation rules for model transformation.

Using patterns is another approach to compliance in business process (Turetken et al. 2011). Patterns are used to facilitate the specification of formal compliance rules to be used for automated compliance verification and monitoring. This work also introduced a compliance conceptual model to capture and manage compliance requirements and to relate them to business processes in a transparent and verifiable manner. The approach encompasses two logical repositories: the business process repository and the compliance repository, which may reside in a same shared physical environment supported by database technology.

Awad et al. (2008) introduces an approach to post-Design-Compliance verification using an automated checker. In this work, Compliance rules are translated into temporal logic formulae that serve as input to model checkers which in turn verify whether a process model satisfies the requested compliance rule.

Mentioned works are specified to compliance in business process. Thus the modelling languages being used there are Business Process Management Systems (Panagacos, 2012). Since our focus is on compliance in software development, we needed a modelling language which had concepts from software development. Although some previous works (Decreus et al. 2009; Betz & Reimer, 2016) have used BPMS for both business processes and software development early stages, but also researches such as done by (Selioukova, 2001) showed that BPMS can not be used for big size IT projects. Regarding the main aim of our work, "Privacy-by-Design", our selection would be narrowed down to information system analysis methodologies and in specific Requirement Engineering. The selected ML is a methodology in Requirement Engineering (System Analysis) and also has application in business process (Decreus & Poels, 2010). In contrast requirement engineering modelling languages are used both for business process management and software requirement engineering.

Regarding the objective of our work, privacy by design, we have done literature review on compliance to data protection and privacy by design. Later, previous works related to components of PRD will be discussed.

2.3.1 Compliance to Data Protection

There are number of works which specifically are considered for compliance to Data Protection and privacy laws in around the world. Compliance to EU Data Protection Directive and its implementations in national member such as Federal Data Protection Law in Germany, Data Protection Act (1998) in UK and Data Protection Code of Italy (2003) have been mostly practiced and also mentioned in previous sections.

PRIME (Privacy & Identity Management Of Europe) project (Hanson & Leenes, 2005), was a research project founded by the European Commission's 7th Framework Programme in 2004 to demonstrate the validity of privacy-enhancing identity management. PRIME project concentration was to put individuals in control of their personal-data by features of using consent, privacy negotiation, identity management, spectrum of anonymity and accountability. By these they mean using of online tools which help to manage the privacy and put the individuals in control to actively protect their personal data. PRIME could specify case-based legal requirements for domains such as e-learning, e-Health and some other applications. The requirements elicited for these cases had their roots in Data Protection Directive, OECD Privacy Guidelines, the Council of Europe Conviction NO.108, and the Fair Information Practice. To accomplish this, the PRIME project has designed and implemented a practical system-level solution (Human-Computer Interface system) which incorporates novel cryptographic protocols, sophisticated security protocols, and anti- facial intelligence algorithms. Centralizing all privacy decisions and controls to the user creates a single point of failure for accessing services, a single point of access for malicious users to steal credentials, and a single point of vulnerability to innocent mistakes (Josang & Pope, 2005). PRIME has considered identity management as the key component and solution for compliance to data protection. There are bulk of other works which also have provided technical or policy-making identity management approaches with or without link to data protection laws (Camenisch et al., 2010; Bonatti & Samarati, 2002; Cassasa,2004; Backes et al., 2005); Olsen & Mahler, 2007). It shall be mentioned that user identity management is one of the key requirements to comply with Data Protection and there are other requirements that need to be fulfilled as well. As said by the researchers of PRIME "But surely user-controlled privacy only addresses one aspect of privacy, the individual's interest in privacy." (Camenisch et al., 2010). Finally, the main point is the difference between the aim of our research with PRIME and other mentioned researches in this paragraph. To have privacy in design is a goal for system developers to know where and how to comply with privacy laws in which mentioned works has come with a solution for it. In other word, we are a step behind these researches.

Since electronic health record (EHR) systems increasingly become core applications in hospital information systems and health networks and regarding the sensitivity of stored information in these systems, compliance to privacy has become mandatory in healthcare organisations and consequently has attracted huge number of researches in this area. It requires compliance to

Data Protection laws or HIPPA (USA Government Congressional Reports, 1996) and related laws to health organisations depending on the area domain of application. PRIMA (Privacy Management Architecture) (Bhatti & Grandison, 2007) invented by IBM Almaden research lab, attempted to gradually embed privacy controls into workflow of Clinics using a Privacy Refinement technique. Several techniques based on the actual practices of healthcare organisations are used in this project to refine organizational policies to the level of patient. This work also leverages data mining and Hippocratic Database technology. Same as the previous work, PRIMA's concentration is on access control technologies which based on our work is not the only requirement of compliance to data protection law. In order to represent the real state of the system and map and compare it with ideal system (laws), this work has used logs of systems. Using system logs are about what already has happened and not everything or the things that may happen in future. It can be mentioned as an after-the-fact compliance solution. In other word "PRIMA helps administrators to refine the implemented policy so that it expands to include exceptions that are consistent with the intended policy" (Garris, 2008). In contrast our work plans the design of required technology based on intended policy extracted from law. Researchers in PRIMA also have used a method in order to formalise rules of HIPAA. The formal language uses a tuple of two literal-valued elements for each vocabulary and its attribute in the rule. The formalised rule is finally constructed of series of tuples. In contrast our work advantages of a triple of elements and their relationship in the format of ontological statement. This method of formalisation represents elements and sentences of law in a better format. Same as Data Protection, huge number of works in health record protection also had been specified to assess access rules and identity management as a key requirement of compliance. for example Blobel, (2004) tried to establish models, methods and tools to allow formal and structured policy definition, policy agreements, role definition by realising rights and duties, authorisation and access control. At the end UML and XML were used to practically implement the principles as well as some examples for analysis, design, implementation and maintenance of policy and authorisation management as well as access control.

Creating policy for clinical organisations is a popular approach in compliance to HIPAA and any other laws. Works such as done by Anderson, (1996) and Bhatti & Grandison, (2007) are some examples of policy-making approaches for health organisations. The first work was based on a BMA (British Medical Association (BMI). Available at: https://www.bma.org.uk/. (Accesed on January 2017).) request from the author to study the threats to personal health information, and then to draw up a security policy model and interim guidelines for prudent practice. In other words, the basic of research is on a scenario-based risk assessment methodology and rules set out by General Medical Council and the British Medical Association (Sommerville, 1993) constructed policy has a model similar to Bell-LaPadula model for military systems (Bell & LaPadula, 1973) and the Clark-Wilson model for banking systems (Wilson, 1987). Similar work has been done by Kwon & Johnson (2012) in which a survey on 250 US healthcare organizations had been performed to find out security risks and then security patterns were clustered and examined to avoid identified risks. These relationships between the clustered security patterns and perceived regulatory compliance were analysed using t tests. Their results provide security practice benchmarks for healthcare administrators and can help policy makers in developing strategic and practical guidelines for practice adoption.

NEMA (National Electrical Manufacturers Association-USA) made a policy generally known as *break-the-glass* to resolve the problem of access control policy conflict in case of emergency unauthorised access to health records or non-working authorised access. Huge number of technical solutions to implement this policy in access control models have been investigated (Brucker & Petritsch, 2009; Byun et al. 2005).

Regarding the main objective of current research, Privacy by Design, policy-making is one of the important activity to consider when designing any approach and framework for compliance. For a PRD approach, we don't limit the work to only policy-making but also we have components for early stages of system design in our approach. Compared to the works which only took technical solutions for policies, we take high-level technical mechanisms using policy refinement by controls from standards and design patterns.

2.3.2 Privacy by Design

One of the most important aspects of compliance is considered in General Data Protection framework (GDPR, Article 25) (European Commission Justice, 2012) for implementation of a "privacy by design" approach as part of organisational IT-systems and processes. It requires that data protection is designed into the development of IT systems and business processes for products and services. The importance of this matter has been also addressed by ICO (Information Commission Office). **Privacy by Design (PRD)** is an approach to system engineering, which takes privacy into account throughout the whole engineering process in which human values should be considered in a well-defined manner throughout the whole process. However, privacy by design in software systems means making software under development to operate according to data protection law and any related policy and standard such as ISO 27000 and thus privacy plays an increased role in any company that produces software. GDPR ensures that companies are liable for any data protection breach related to using the developed software. As the coverage of system engineering for also enterprise system indicates, the liability to comply with privacy is also applicable to any organisation that uses software systems or manually keeps and process personal data. The compliance to privacy should be taken in their all activities including their management plan, policy making and also in their daily business workflow.

Same as other compliance solutions, privacy by design approaches are provided both as manual guidelines and automated tools. One of the main manuals approaches is provided by Microsoft (International Business Machine Corporation, 2007). The SDL aims to integrate privacy and security principles into each of the five stages of the software development lifecycle (requirements, design, implementation, verification, and release). These guidelines are based on FIPs (Fair Information Principles) and related U.S. privacy laws and is provided in a fifty-one-page document known as "Privacy Guidelines for Developing Software and Services," which discusses different types of privacy controls and special considerations raised by shared computers, third parties, and other situations; and then enumerates nine specific software product and web site development scenarios. This document is as a general guideline which helps system developers in design of a privacy-controlled system. It does not help designers in applying laws in applicable areas of a specific system which our approach is able to do this. International Business Machine Corporation, Microsoft Trust Center (2014) is also the recent attempt of IBM to offer privacy and security information and guidelines to service providers. They have also provided a general guideline to privacy by design in Building Global Trust Online, Microsoft Perspective for Policymakers.

Different information commissions around the world, have provided frameworks and guidelines for PRD. ICO in UK commissioned an expert report, entitled 'Privacy by Design" in 2008 (Information Commission Office, 2008). The purpose of this report was to find out the reasons behind poor adoption of privacy controls in UK organisation after 20 years' establishment of data protection law. The conclusion of this report was a number of barriers which needed to be overcome, including the need for a clear articulation of the business case for proactive privacy protection. This resulted to another work by ICO which provided a business case for investing in proactive privacy protection (Information Commission Office, 2010) in order to help organisations to understand business rationales and benefits of privacy by designs in their organisations when they are setting up a new business process or reviewing the current business process. This report is in two volumes in which the first introduces a business case to describe the benefits of taking privacy controls in an organisation. The second volume helps organisations to build a business case for themselves. The basis of the second volume is almost on privacy risk assessment methods to evaluate the value of privacy assets and identify risks and relevant controls against them. In contrast our work relies on privacy risk assessment as one of the components of compliance and benefits from other components as well, in addition to providing an automated tool for compliance. A work conducted by (Cavoukian, 2011), the Information Commissioner of Ontario, Canada, also published a document of guidelines on implementation of seven most important principles of privacy by design in organisations. This guidance is intended to serve as a reference framework and may be used for developing more detailed criteria for application and audit/verification purposes. The concept of Privacy by Design was actually originated in a joint report on "Privacy-enhancing technologies" by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research in 1995. German Federal Commissioner for Data Protection and Freedom of Information, Schaar, (2010) also called using of electronic health cards, electronic id card, and electronic proof of earning card in order to strength data protection.

IBM also has provided an obligation management solution for privacy by design which enables enterprises to configure information lifecycle and identity management solutions to deal with the preferences and constraints dictated by privacy obligations in an automated and integrated fashion (Ashley & Moore, 2002).

May et al. (2006) has used Access control techniques to analyse and verify legal privacy policies. In other word he only has analysed access and deny access rights of system stakeholders and other legal requirements are not discussed in this work.

Researchers Rubenstein & Good (2013) believe that privacy by design is not only "build in" privacy— in the form of Fair Information Practices or ("FIPs: FIPs define the rights of data subjects and the obligations of data controllers;") when producing software products, but it is also to translate FIPs into engineering and usability principles and practices. They presented some design principles for PRD, analysed the prerequisites for undertaking a counterfactual analysis of ten privacy incidents in Facebook, google and some other applications and then argue how these incidents could be avoided if their principles were implemented in mentioned applications. In this work, researchers argue that Cavoukian's seven principles (Cavoukian, (2011) are more aspirational than practical or operational which Cvoukian disagrees in (Cavoukian, 2011) saying the first four principles of *PRD* are not reflected in FIPs and provide much greater protection. Both Cavoukian and Rubenstein & Good agree that privacy should be analysed using two complementary perspectives; privacy engineering, which refers to design and implementation, while the second is useable privacy design, which focuses on technical approaches such as human computer interaction (HCI) research. Also the founders of PRD define "Design" in *Privacy by Design* as a broad approach to expressions of privacy, in a variety of settings – information technology, accountable business practices, operational processes, physical design and networked infrastructure (Cavoukian, 2011). Hoepman (2013) has defined eight strategies for PRD. His proposed strategies mostly are same as principles of privacy by design extracted from GDPR, OECD Data Protection principles and ISO 29100 concepts. He also discusses the advantage of using design patterns in rapid software development life cycle and propose usage of privacy patterns in design of systems.

Privacy by design has been specifically considered in design of specific information systems such as cloud computing and web designing as well. For instance Pearson (2009), Quah & R¨ohm (2013) and Ruiter & Warnier (2011) provided a guideline to take privacy in design of cloud application. The authors did not provide any specific or systematic framework or approach, but they only recommended a manual of guidelines and technologies for privacy in design of cloud applications. Privacy risks to web application and their countermeasures which should be considered in design of web applications have also been studies in OWASP Project (Open Web Application Security Projects) and have been provided as guidelines for developers. Privacy by design in Ubiquitous systems also had been practiced by Langheinrich, (2001). In same manner the researcher only provided some principles and guidelines for privacy-aware design of Ubiquitous systems. Kobsa (2002) also practiced effect of Data Protection laws on the personal data collected by web sites and prepared a list of technical controls that can be taken in design of web applications in order to safe guard privacy of web visitors. Bonneau & Preibusch (2009) investigated through number of social networks in order to find their privacy risks and presented a novel model consisting of technical controls to come over the shortages. Later in another work (Bonneau et al. 2009) same authors invented a user-centric technology to pass the control of privacy to individuals.

Concluded from mentioned researches and accordingly our own vision, various commentators have taken different approaches to privacy by design and data protection in general. Some have only focused on providing manual guidelines for PRD and data protection and some tried to extract policies from legal text. Privacy policies were refined by technical controls and guidelines in other works. Life cycle approaches have been practiced in some works in order to take privacy in all stages of system development. Some works only concentrated on privacy risk assessment as a solution for PRD and some others only concentrated to provide technical approaches such as user-centric systems (Human-interaction systems) or identity management approaches. As discussed before, there is a general idea between most of PRD researchers that requirements engineering, formal languages, and related tools and techniques are precisely what software developers need in order to transform privacy by design from a vague admonition into a planned and structured design process. Therefore, the main desire of our research was to focus on designing an approach which can integrate privacy compliance with requirement engineering methodologies in software development. In addition, our attempt was to implement an automated solution for this importance instead of a guideline manual. Our approach is a knowledge repository of requirement engineering and privacy compliance concepts which can automatically apply relevant rules of privacy laws and regulations on context of a designing software system. It also automatically refines applied rules to lower-level organisational and technical controls using standards, guidelines and design patterns. Therefore, fulfil both objectives of PRD, as Privacy engineering and FIPs. It also advantages from a privacy risk assessment component.

There are number of works with concentration on requirement engineering for privacy compliance or has used combination of privacy engineering and FIPs as an umbrella approach which are discussed in detail in coming sections.

2.3.3 Compliance Requirement Analysis

One of the most effective factors to software failure has been reported to be the non-existence of efficient and professional culture of software development process. Although the history of software engineering goes back to 60 decade when it was first introduced in a conference (Glass 2003), there are still believes and businesses that consider the software development process simplified to only the procedure of computer programming. But in fact a professional software development is much more and waster than a single computer program and include processes of software specification, software design and implementation, software evaluation and software validation. Software engineering adopts much organised, systematic and discipline engineering approaches which include and manage all processes involved in software production. Software specification is the activity of defining the system to be developed and the constraints on the system development. It normally happens through conversations between customers and system developers. Software Specification or Requirement Engineering is one the most critical phases of software engineering since the success of the software depends on how well the requirements are extracted and system criteria is defined (Robertson & Robertson ,2012). As one of the first and main activities of software development, Requirement

Engineering (RE) involves practices of discovering, gathering, analysing, documenting and maintaining the requirements and goals and constraints of the system to be designed. To express the importance of the matter, it is worth to mention that the success of a software system is evaluated based on the content of it satisfying the desired goals and purposes. The term requirement engineering first time came to general in 1992 when International conferences series of RE were established (Mead, 2013).

During different activities of RE, three different types of requirements will be proceeding; Functional, non-Functional and Domain Requirements. Functional requirements are the main and operational services that the system should provide and generally to be said, what exactly the system should do for its stakeholders. Non-Functional requirements only concern the quality and performance of the system such as standards or to be generally said, the constraints on the development of system. Domain requirements which can actually be functional or non-functional are those needed based on the application domain of the system or to be said, the type of system to be designed. Requirements are also categorised based on the demanded audiences of them into two sets of user requirements and system requirements. User requirements are high-level and abstract requirements which mostly describe external behaviour of system and concern the demands of stakeholders such as client manager, system end-user, client engineer, contractor managers and system architects. Inverse are system requirement which response to more detailed and technical requirements of stakeholders such as system end-users, client engineers, system architect and system developers. System requirements are actually analysed and expanded version of user requirements (Sommerville, 2006). Also, during different stages of system development from requirement engineering to design process and even after system implementation, software engineers may benefit the usage of some models to develop the abstract perspective of the system. As mentioned, the models can be used to drive, explain, clarify or document requirements or the system design of developing or existed system to other system stakeholders. Models can be represented using graphical or mathematical notations. The most common system modelling approach nowadays which has become the standard of object-oriented modelling language is called UML (United Modelling Language). Systems can be modelled from different perspective such as what UML does using number of diagrams such as activity, use cases, sequence, class and state diagrams.

In recent years, a large body of works have approached compliance as an early and non-functional requirement of system and, therefore, align requirement engineering with compliance techniques (Otto & Antón, 2007). They mostly used goal -oriented modelling language methodologies of requirement engineering, taking law's rights as one of the main goal for the systems to be satisfied. Goal-oriented requirement engineering has been defined as one of the most appropriate approaches to compliance (Yu et al. 2014). We are critiquing here the requirement engineering methodologies used by previous works in order to highlight the advantages of our selected requirement engineering component.

Gurses et al. (2011) tried to enforce data minimisation policies and requirements as one of the main attributes of privacy in engineering of information systems using four activities of their proposed framework. The activities include functional requirements analysis, data minimisation, modelling attacks, risks and threats and Multilateral Security Requirements Analysis. In other word, he has firstly found out system requirements, embed data minimisation as a non-functional requirement in system requirements, perform risk analysis and then took security controls for risks. No specific methodology to perform the four activities has been mentioned and the matters had been discussed generally.

Diriment & Lemoyne (2006) describe an approach where one of the main goal-oriented requirements engineering methodologies known as KAOS (Keep All Objectives Satisfied) is used to model regulations. They explain how to incrementally transform regulation documents into four models for goals, objects, agent and operation. KAOS has been successfully used in many industrial or service contexts mainly to produce requirements documents, to define strategies and refine them into IT plans and to reengineer requirements on top of existing systems. These authors used a case study from Civil Aviation industry called SAFEE project (Security of Aircraft in the Future European Environment) in order to validate their framework. They have modelled the system and ICAO Security Regulation for Civil Aviation by KAOS and its supporting tool "Objective". However, in KAOS refinements of goals ends when a sub-goal is performed by an agent. Thus we can conclude that the KAOS agents as defined in the Goal Model and the Model Responsibilities do not directly show the relationships between the actors. For a context such as laws, a modelling methodology which could represent social relationship between actors more clear was required. There is a history of works in requirement engineering also to improve communication and collaboration among safety engineers and software engineers in the context of RTCA DO-178B, the de-facto safety-related standard for developing software in civil and military airborne systems. DO-178B provides guidance on how to achieve assurance levels that the software will not impact the continued safe flight of the aircraft (Ferrel. T.K., Ferrel. U.D. (2000) *RTCA DO-178B/EUROCAE ED-12B.* Available at: http://www.davi.ws/avionics/TheAvionicsHandbook_Cap_27.pdf. (Accessed on June 2016). It is almost like a risk assessment document which categories risks to aviation and then address them in software development life cycle. NASA performed a survey to identify the challenges in developing software for safety-critical airborne systems (Hayhurst, K. J. & Holloway C. M. (2001) 'Challenges in Software Aspects of Aerospace Systems', *Proc. Annual NASA Goddard Software Engineering Workshop*.). The authors claimed that correctly communicating requirements between different groups of people is the key in developing a safe system. Consequently, number of works in IT industry attempted to address this requirement. Zoughbi. G., Briand. L., Labiche. Y. (), 'Modeling Safety and Airworthiness (RTCA DO- 178B) Information – Conceptual Model and UML Profile', *Journal of Software and Systems Modeling,* 10(3). Pp.337-367 proposed a Unified Modelling Language (UML) profile that allows software engineers to model safety-related concepts and properties in UML. A conceptual meta-model is defined based on RTCA DO-178B, and then a corresponding UML profile, which they call SafeUML, is defined to enable its precise modelling. These types of works, analyse D0-178B, extract key concepts and requirements and embed safety and security requirement from DO-178B into requirement engineering methodologies. UML has been used in other works also to model safety of aircraft systems (Hansen K. T. & Gullesen I., (2002) 'Utilizing UML and Patterns for Safety Critical Systems' *Proc. Workshop on Critical Systems Development with UML, in conjunction with the International Conference on the*

UML.Jürjens J. (2003) 'Developing Safety-Critical Systems with UML', *Proc. International Conference on the UML*, pp. 360-372.). These works are also similar to the ones for compliance to privacy and also for compliance to standards in other industries such as railway (CENELEC EN 50128. (1997) *Railway Applications: Software for Railway Control and Protection Systems*, Version 1997). This can prove the general acceptance of using requirement engineering methodologies in compliance.

Kalloniatis & Kavakli (2008) Introduced PriS for PRD. PriS models privacy requirements in terms of organisational goals and uses the concept of privacy-process pattern for describing the impact of privacy goals onto the organisational processes and the associated software systems supporting these processes. PriS is based on the Enterprise Knowledge Development (EKD) framework (Rolland et al. 1999), which is a systematic approach for developing and documenting organisational knowledge. EKD is a goal-oriented approach to requirement engineering. This work has categorised privacy requirements to eight basic categories of identification, authentication, authorisation, data protection, anonymity, pseudonymity, unlinkability and unobservability in which the first three are security requirements and the rest are related to data protection. for more privacy requirements author suggests using threat trees, attack trees, abuse cases, misuse cases, security use cases and abuse frames. Although data protection has been taken as a requirement of privacy but there is no direct link and tracing to any data protection law or any other privacy compliance resource in this work. Privacy requirements are later refined by seven process patterns and further with technical implementations.

Massey et al. (2010) has used a manual methodology which generates traceability links from software requirements to specific subsections of the legal texts. He also invented a methodology to rank and prioritise extracted legal requirements in order to find out which one is ready for implementation or for refinement. The methodology works based on the calculation of number of cross-references from a legal text to other materials and helps software developers to estimate the level of legal text ambiguity and decide to consult a legal professional. The proposed framework mostly is designed for graduate software development unfamiliar with legal text. But in our opinion the manual methodology used in this work is not an easy task and using a well-known requirement engineering methodology and an automated solution would help more. In addition, practising the level of legal text ambiguity in its alone does not help developers to solve the origin of problem and may only look as a time consuming task. In contrast we tied to solve the problem of ambiguity by a methodology to analyse and make an easy format of legal rules which can be used by developers.

Regarding compliance in health organisations, some works also have taken advantage from requirement engineering. For example, Weiss & Amyot (2005) introduced a framework based on the User Requirements Notation that models the business processes of a hospital and links them with legislation such as Personal Health Information Privacy Act (PHIPA). Supporting tool (jUCMNav) (Roy et al. 2006) has been used to model both the business processes of a health information custodian and the applicable privacy legislation. In URN The concepts of non-functional requirements and actors are borrowed from Non-Functional Requirements

(NFR) (Myloupolos et al. 1999) and i* (Yu, 2009). This work uses GRL (Goal Oriented Requirement Language) to capture the policies of a health information custodian and also usesUCM (Use Case Map) separately to represent the business processes that implement them. Further links connect two models together to track the custodian's compliance to the law.

The work in (Shamsaei, 2011) is an effort in compliance for Business process management as an important part of corporate governance. Authors believe goal-oriented compliance management using Key Performance Indicators (KPIs) to measure the compliance level of organizations is a key in compliance of business process. They propose a novel method to model the context and measure compliance using the User Requirements Notation (URN). Key Performance Indicator (KPI) is an extensions of URN. Therefore same citation points of Weiss & Amyot (2005) are applicable here too.This work ensures compliance to four levels of laws, policies and regulation listed as internal organisational policies, regulations and laws, and service level agreements between companies and standards. They also have implemented an algorithm to calculate level of compliance in goals.

Siena et al. (2008), depict a systematic process in order to transform legal concepts into stakeholder goals so that if the goals are fulfilled through a particular system design, then the law is upheld. This work relies on the assumption that why choices about an information system is successfully captured by the analysis of the goals of stakeholders through i* modelling language. Intentional compliance in this work plays a crucial role in guiding the development of the system, and keeping it compliant through all the phases of the development, so that the running system will also result compliance.

Common Criteria as an important reference for information security of systems also has been analysed by requirement engineering processes in number of works such as the one done by Mellado et al. (2007). This researcher proposed SREP (Security Requirements Engineering Process), which is a standard-centred process and a reuse-based approach dealing with the security requirements at the earlier stages of software development in a systematic and intuitive way by providing a security resources repository and by integrating the Common Criteria into the software development lifecycle. SPER relies on Unified Process (UP) (Booch & Rumbaugh, 1999) to model and represent software development process life cycle, and embed SPER activities and Common Criteria components in iterative stages of UP. (SREP) is an asset-based and risk-driven method for the establishment of security requirements in the development of secure Information Systems.

Islam et al. (2010) take laws and regulations as one of the main resources for security requirements of developing systems. Regarding the different terminology between two areas of software development and laws, researchers have proposed a framework for compliance which is able to elicit security requirements from laws and integrate them to system requirements. The framework takes advantage from SecureTropos, an agent-oriented requirement analysis methodology in which goals of agents are drown through their dependencies together. Legal rights are also mapped to system requirements as dependencies between legal stakeholders) and UMLsec to design system based on elicited requirements. SecureTropos is a methodology based on i* with extra consideration for security requirements.

Secure Tropos has also been used in some other works to model system requirements and legal context. Massacci et al. (2004) have presented a comprehensive case study of the application of the Secure Tropos RE methodology for the compliance to the Italian legislation on Privacy and Data Protection leading to compliance to ISO-17799. ISO-17799 is a code of practice for information security management. A modelling language for evaluation of compliance in requirement engineering called Nomos was represented by Ingolfo et al. (2014). Nomos 3 is an updated version of Nomos2 made by same authors which was used to model laws and had a reasoning mechanism for compliance. it represented law's norms (duty, right, etce) using Hohfeld theory and perform reasoning to apply norms to specific situations. System context is modelled in Nomos using a security oriented version of i* called SecureTropos. Two models are integrated together using a process and it has made extension to visual representation of i*. Nomos3 has concepts of roles and responsibilities in order to perform compliance in a specific domain. We do not believe on limiting privacy requirement only to security requirements. Therefore, our work considers both security and non-security requirements extracted from Data Protection law.

To summarise, all works to embed compliance in requirement engineering are using a ready methodology of RE to model system and legal context or have invented a modelling approach. we are not agreeing with some of the requirement engineering methodologies used in previous works as they lack to model social relationship between law's stakeholders. In contrast we have used i* which model systems using dependencies between actors. I* is a goal-oriented requirement engineering methodology which has concepts of goal and actors and their dependency relationship together and had been used both for software development and business process modelling. Triple of two objects and their dependency has a form similar to the ontological framework which we are using in this research. We are not agreeing with the usage of other versions of i* with special attributes for security as we are not aiming on only security requirements of system and believe that data protection and privacy requirements are not limited to security. Indeed, some of these works have extended current RE frameworks with legal concepts. Other mentioned works mostly are using different methods to models systems and laws separately and manually linking and mapping two models together. In our conceptual model we are doing the same at first, but since we are using a unique ontological framework to formalise both models, thus we have similar formats of both model and can easily and automatically map the models together. Less number of above approaches have considered technical solutions for elicited requirements (Kalloniatis & Kavakli, 2008)) which in contrast we are taking design patterns which also includes security and privacy patterns for technical refinement.

2.4 Law Analysis

In order to understand the vague language of laws and make an easier format of them, major number of IT works in the field of legal systems, are specified to analysis, legal reasoning and application of laws, such as (Bruninghaus & Ashley, 1999) and (Aleven, 1999). By analysing laws, we mean any approach that can perform following tasks (Benjamin, 2005):

- Creation of regulatory metadata, formalisation and content standardization (e.g. LegalXML/LeXML/MetaLEX, ADR/ODR-XML, RDF, OWL, etc.)
- Information extraction from legal documents
- case matching against existing jurisprudence
- legal reasoning

In the subject of case matching and legal reasoning, most of works are concentrated on analysis of case laws in which the subject is in interest of legal systems in countries such as United States and United Kingdom with common law where case law plays a critical role in legal reasoning and decision making. In such a system, the lawyer consults a corpus of previous decisions of judges and identifies the facts which support their current case. Researchers Bruninghaus & Ashley (1999), worked toward automatically indexing case texts to factors in order to help the construction and maintenance of case-based reasoning. The technique called *SMILE* integrates a legal thesaurus and linguistic information with a machine learning algorithm to automatically assign number of abstract fact patterns to legal cases from CATO's (Case-based Tutoring with Concept Maps) case Database (Aleven, 1999). Also number of works had been dedicated to rule-based reasoning. Among them PROSA (PROblem Situations in Administrative law) proposed by researcher Montjeweff (1999) is a model-based computer system for teaching legal case solving. PROSA has gained advantage of a general coaching framework to construct a legal-case solving model consisting of sequence of subtasks. Part of PROSA is a tracer tool that makes the regulation structure explicit. The tracer is based on predefined referencing graph to help law students understand the rule and its concepts, definitions and references by hyperlinks as a ready to use tool. PROSA has taken advantages of other works such as (Scholten, 1931) in order to perform its model's subtasks. Schelton has provided a general explanation of methods of private law in which they are analysed and applied. His work was a significant effort to teach law students and jurists about methods of private law and a major help here in order to determine the most appropriate analysing methods in current research. Schelton believes that legal reasoning needs both the knowledge of rules and knowledge of facts in order to apply them together and conclude to a decision. But also he believes that science of law finding is not only to apply facts to available rule's element and sometimes rules are not immediately available in law and are needed to be discovered from ready rules by methods of interception. He has mentioned some interception methods such as grammatical, historical, traditions, analogy and legal refinement. One of his main concentrations had been the competence of the authority of law analyser who extrapolate hidden rules from available one since he believes it make no sense to put the application of laws in the hands of any authority although he accepts the fact that individuals contribute to the development of law in their relationships with community.

In theatrical and classical approaches to legal reasoning, Van Eemerence (2004) presents a philosophical and theoretical framework to argumentation as a means of resolving differences of opinion by testing the acceptability of the disputed positions. It also proposes a practical code of behaviour for discussants who want to resolve their differences in reasonable way. Such theories can be used in matching and arguing the case facts with element of law mostly in the argumentation of common laws and is a good conceptual model to be simulated in IT. In the field of legal reasoning and fact matching most of mentioned works in compliance are using manual processes for this activity. In contrast we are using an automated approach for legal reasoning which will be discussed in following lines.

The other contribution of IT researches in subject of law analysis is to automatically profile and extract arguments (information) from legal texts expressed in complex natural language. In context of compliance, PRD and requirement engineering, some works also tried to firstly analyse legal context in order to overcome the problem of ambiguity in the language of legal texts. Various techniques to analyse and extract rights from legal texts in order to be considered in requirement engineering and representing legal rules in a formal language, also have been researched by Breaux & Antón (2008). In these works, permitted actions by laws, are called rights and mandatory actions are called obligations. In this work (Breaux & Antón, 2008) Rights, obligations, their constraints and exceptions, and their elements such as stakeholder were depicted from law texts by using extensively validated natural language patterns. From stakeholder rights and obligations, system requirements can be inferred and implemented. This work helps system developers and compliance officers to analyse laws. The work later was automated with a supporting tool (Kiyavitskaya et al. 2007) , (Bhatia et al. 2016). The author also later introduced reasoning and refinement technique which would map extracted legal requirements to matching IT controls from standards such as ISO27K (Breaux et al. 2013) by using a technique called *analysis pooling* (Gangemi et al. 2002). This work was also extended by a specification language which uses a simple SQL-like syntax to express whether an action is permitted or prohibited, and to restrict those statements to particular data subjects and purposes (Smullen & Breaux, 2016) (mapping). No more information for the work was available.

Giorgini et al. (2005) also extracted information in formats of *ownership, delegation* and *permission* from legal texts. Siena et al. (2008) and Islam et al. (2011) also adopt a fundamental legal taxonomy grounded on 8 elementary concepts classified by Hohfeld (1913) as privilege, claim, power, immunity, and their correlatives no-claim, duty, liability, disability. We do not believe on using Hohfeld theory and its different types of rights in this application area. In our point of view, the legal analysis technique employed in this work and different discussed types of rights of Hohfeld is not easy task for system developers. Hohfeld is a fundamental theory in law being thought to law students and even is not being used by lawyers nowadays. To extract rights and other elements of legal texts and make an easier format of law rules, most works use language patterns or Natural Language Processing methodologies. In contrast we are simulating classical textual analysis approaches using by legal professionals and lawyers.

Formalisation is a key stage of automation of legal approaches in IT, and different formalisation methods have been used in related works. As expressed in previous sections compliance and other legal approaches in IT mostly have used Deontic and Temporal logics in order to formalise legal texts and extracted information (Schumm et al. 2010; Goedertier & Vanthienen, 2006; Bons et al. 1995). Generally speaking, there are also some automated and graphical formalisation tools known as Computer-aided Verification tools which are used to formalise requirements automatically (Busboom et al. 2017; Frehse et al. 2011; Wagner et al. 2016). One of the other satisfactory solution for legal knowledge formlisation also had been usage of metadata such XML and ontology and semantic web in recent years. “The ontology is therefore both a description model and a source of metadata for semantic tagging, providing at the same time a tool for conceptual retrieval and a model of content which maintains references to legal texts” (Gangemi et al. 2003). Regarding the ready platform of semantic web, its recent adequate usage in legal knowledge representation and compliance, close structure of knowledge construction of it to the format of analysed laws in our framework, its built-in reasoning methodology which can be used for legal reasoning task and other reasons which will be discussed later in this chapter, we decided to use semantic web ontology in order to formalise legal and other contexts in our framework, thus achieving all these objectives simultanancy. Ontology also helped our framework’s components to be represented in a common language instead of separately.

2.5 Ontology-based Compliance Approaches

Generally, ontology is about gathering concepts in a specific domain and making relationship between them to construct a knowledge. Making ontology in information security, privacy and legal domain has a strong history. Constructed ontologies might have been implemented using database, semantic web or other technologies. In this category we are providing a literature review on related works to ontology-based compliance approaches.

Gharib et al. (2016) provided a survey on current literature on privacy by design compliance works in order to identify the main concepts/relations for capturing privacy requirements. In addition, the identified concepts/relations are further analysed to propose a novel privacy ontology to be used by software engineers when dealing with privacy requirements. Privacy concepts are initially divided to four groups of Organisational, Risk, Treatment and Privacy dimension. The result of survey shows that no work yet has used all mentioned types of concepts in a unique approach. Thus proposing a novel approach to do this importance. This work is a very good resource to have a literature review on the subject of privacy and PRD. In contrast using different components as resources of PRD, we have all the categories of mentioned concepts in our approach. The categories of privacy concepts can be used to evaluate our work.

Using semantic webs and developing ontology of legal concepts is also a well-known approach in the field of artificial intelligence. Brekeur & Winkel (2003) in a survey have delivered a study on works providing legal ontology solutions for legal specialists. They have identified rich legal concepts in their taxonomies. This work helped us to find and match and also evaluate our ontological concepts of law.

Gangemi et al. (2003) describes some ontology-based tools that enable legal knowledge formalisation. Jurwordnet is an extension to the legal domain of the Italian version of EuroWordNet (ItalWordNet (IWN)). EuroWordNet was a project to establish a lexicon database aimed at providing a knowledge base for the multilingual access to sources of legal information (Vossen, 1997). Therefore, it includes numerous ontologies from EU Directives and National level legislations. It is a content description model for legal information and a lexical resource for accessing multilingual and heterogeneous information sources. Its concepts are organised according to a "Core Legal Ontology" (CLO), based on DOLCE+, an extension of the DOLCE foundational ontology. A foundational ontology is an upper-level ontology as a candidate for a “universal” standard ontology (Gangemi et al. 2002). Regarding growing number of ontologies in this project, and possible links between them, there should be a resistance and compatibility between their structure. Rather, it is intended to act as starting point for comparing and elucidating the relationships with other future modules of the library, and also for clarifying the hidden assumptions underlying existing ontologies or linguistic resources such as WordNet. Jurwordnet and CLO are also used to represent the assessment of legal regulatory compliance across different legal systems or between norms and cases. It can also be used to link between domain ontologies and legislative texts. Jurwordnet is a general approach for compliance to European laws.

Ryan et al. (2003) also designed an Ontology-Based Platform for Trusted Regulatory Compliance Services. The goal of this research was to validate application conformance with existing regulations using derived multi-lingual regulatory ontologies. The proposed approach can be used both for PRD compliance and compliance auditing in running applications. The initial regulations examined in this work are data privacy and digital rights management. Ontology is decomposed to two layers, first a Lexan based consisting of conceptualisation of the domain, and the other a layer of ontological commitments representing domain rules. The underlying technology to store the ontologies is RDBMS databases. Authors believe that other people can learn how to apply and reuse the result of this research by applying the ontological modelling techniques in this work to any close methods such as semantic web ontology.

Casellas et al. (2010) describes the knowledge acquisition process devoted to the analysis of Data Protection requirements in the Spanish legal system towards the development of a legal ontology for the representation of data protection knowledge in the framework of the NEURONA project. The design of this modular ontological system is based on a central Data Protection Knowledge Ontology, which contains the core concepts of Data Protection, and a Data Protection Reasoning Ontology, which structures the required classification reasoning towards assessing Data Protection compliance. Compliance results to the classification of files containing personal data into different categories regarding their compliance with, within others, the required measures of protection. This work cannot be mentioned as a PRD approach as it does not contain elements of RE and it only focused on security and compliance of data protection files.

Schmidt et al. (2008) address compliance in service process using an ontology-based approach for representing service processes and checking their compliance. This work is based on two ontologies: one to represent the service processes and the other to store the compliance requirements. The process representation ontology uses three so-called views to appropriately represent the service processes. It is based on predefined patterns of interactions between service provider, customer and other third party service providers. The compliance of service processes is checked against standards such as ISO 20000. The ontology for storing the compliance requirements differentiates syntactic, semantic and pragmatic requirements. Ontological rules of mentioned groups make relationships and links between these two ontologies. The work has knowledge not only from Data Protection law, but also from case law interpretations, guidelines from independent authorities, and international or professional standardization bodies such as COBIT. The legal domain is from Spain. In contrast we have opted GDPR to have an international view on data protection. from other point of view this work has gathered all the knowledge from different data protection regulation under one ontology. In contrast we have different ontologies for each resource, thus our work is able to trace any refinement to its source. Indeed, the level of refinement of different resources in mentioned work is not clear to us.

Fenz et al. (2007) introduced an ontology-based framework to improve the preparation of ISO/IEC 27001 audits, and to strengthen the security state of the company respectively. In combination with a Security Ontology approach, researchers aim at an automatic partial audit preparation by extracting IT infrastructure knowledge from an established Security Ontology. Besides the automation, the ontological mapping of the ISO/IEC 27001 standard provides a foundation for an electronic tool, supporting the actual certification process by providing a central platform for all participating actors. Furthermore, they introduce the generic OntoWorks framework to access, visualize, and reason on ontological databases and provide an overview on its usage for the ISO/IEC 27001 Ontology and the Security Ontology.

Beach et al. *(*2015) designed A rule-based semantic approach for automated regulatory compliance in the construction sectorExpert Systems with Applications.

Humberg et al. (2014), also used Ontologies to Analyse Compliance Requirements of Cloud-Based Processes. This ontology represents knowledge from different legal resources relevant to cloud computing such as data protection laws or the European directive Solvency II and standards such as ISO 27k series (International Organisation of Standardization) or the IT-Grundschutz Catalogues (German Federal Office for Information Security (BSI)). Two types of classes are used to represent concepts in mentioned regulations: Those that contain the actual content, and others that represent the structure the content is organised in. concepts of Situation and Constraints also are used in order to represent the context of regulation rules. Constrain is the condition for rule to be applied and should be mapped to system context and the Situation is the result of constraint's application based on legal rule. Rule elements and consequently constraints are personalised using business processes related to cloud system modelled by BPMN or UML. In contrast to our work and in our opinion, the types of classes and their relationships that we have introduced in our platform are easier to be understood. For example, Humberg ‘ontology include class of Activity to represent actions in legal texts. In contrast we have modelled them by object properties, thus having less triples of knowledge’s. The other difference between our work and this one is the modelling of a goal-oriented requirement engineering methodology by ontology in ours. It has number of benefits; first we have an element of PRD in our approach. Although Humerg’s work is using BPMN or UML, but as mentioned in Section2.3 a goal-oriented RE methodology is more appropriate for compliance, plus that modelling in Humberg’s approach is done separately. secondly, since we have modelled RE methodology in our ontology and have liked this ontology to regulation ontologies, we have integrated compliance and RE together and we do both RE and compliance in same platform. Indeed, the level of matching and equalisation between classes of different legal ontologies was not clear for us as it was also mentioned by Humberg; “improvement of existing heuristics for the detection of matchings” as a future work. In contrast we have an integrated process of equalisation between similar classes in our work, thus mapping between ontologies is much easier.

Rahmouni et al. (2009) also proposed an ontology-based framework to comply privacy laws to healthcare systems. The ontology only included legal concepts from European and national data protection laws. A rule was decomposed to its element such as subject, action, resource and purpose and data protection concepts such as consent and notice. No element of RE is existed and in order to enforce policies at the system level they are specified in a way that conforms to a widely adopted policy language that has proven efficiency in the enforcement of privacy policies called extensible access control mark-up language (XACML). This framework was later implemented in cloud domain (Rahmouni et al. 2015).

Each of above ontology-based compliance approaches used one or two ontologies in order to represent compliance knowledge from a domain such as standards or laws and another ontology for the domain where compliance should be satisfied. In contrast we are covering knowledge representation from more number of compliance resources in our work. The quantity and quality of ontological properties and rules that we are representing, also the methods we used to merge and map different ontologies together is unique.

2.6 Compliance to Standards

The term quality assurance (QA) or quality control is widely used in manufacturing industry and it is about processes and standards which lead to product of high quality. We can translate it to software engineering as processes which are applied to software development activities in order to ensure the achievement of software quality. Also it refers to activities such as verification and validation of the application of quality processes after a product is released. One of the most important and key factors in QA are the standards and the identification and selection of the appropriate standards to the scope of the system and its requirements, since standards are methods by which the quality of products and their production processing are accomplished. SQA encompasses the entire software development process from requirement engineering, design, coding, testing and release management and also can be general or specified to a narrow area of the product quality as security. As a result, standards such as ISO 9000 which are specially used for product quality management are aligned with ISO 27000 series which are specially designed and used for information security management. The alignment is in a way that one suitably designed management system can thus satisfy the requirements of all these standards (International Organisation of Standardisation-Information technology, 2013). Number of works have been specified to the compliance of systems either IT systems or others, to relevant quality assurance standards. Regarding the subject matter of this research, we have collected a literature review on compliance to mostly ISO 27000 and other standards as the following list.

Fenz et al. (2007) introduced an ontology-based framework to improve the preparation of ISO/IEC 27001 audits, and to strengthen the security state of the company respectively. By ontology they provide an easy access database of standard knowledge which is also merged by security knowledge.

Saleh (2005) provided compliance solution to international information security management standards in order to establish a common and safe environment for e- services. The authors have developed a mathematical model that enables the investigation of compliance of organizations with the widely acknowledged international information security management standard ISO 17799-2005. The model is based on the strategy, technology, organization, people and environment – STOPE – framework that provides an integrated well-structured view of the various factors involved in compliance to ISO 17799.

Susanto et al. (2012) research is concerned with the assessment of the application of ISO 27000 controls to organizations. They provide this assessment through a STOPE (Strategy, Technology, Organization, People and Environment) methodologies. The controls are mapped on these domains and subsequently refined into "246 simple and easily comprehended elements" which can be used by any organisation to comply with ISO 27000.

Within the context of business processes design and deployment Rifaut & Dubois (2008) introduced and illustrated the use of goal models for capturing compliance requirements applicable over business processes configurations. In fact, they used a goal-oriented approach together with the ISO/IEC 15504 standard in order to provide a formal framework according to which the compliance of business processes against regulations and their associated requirements can be assessed and measured.

The research by Massacci et al. (2004) as discussed in previous section is also an effort through the compliance to ISO 17799.

Except from the last two works, the rest are providing compliance to running business (after-the-fact) and can also be categorised on this categorisation. The compliance solutions provided in this section are considered and can be used for any organisation who is looking to achieve ISO certificate or wants to audit the issued certificate. Our aim of compliance is to perform compliance process on design of IT systems also to have an integrated compliance to most possible resources of compliance from laws and regulations to standards and others. However, as discussed before we do not believe on refinement of Data Protection law requirements only to security requirements. Therefore, an isolated compliance solution only to standards is not our objective, thus we have considered other compliance components in our framework as well.

2.7 Advanced Software Engineering by Design Patterns:

The growing usage of information system and the huge number of software implemented in similar domains and industries, has lead software developers to reuse-based software engineering strategies where existing applications or components of them or even objects and functions are being tailored, adapted and reused to new systems. The main purpose of reuse strategy is to reduce the costs and time except from condition where the cost and time of modifications and adoptions are more than development from scratch. The complementary form of reuse strategy is being used where an idea of work is being reused and it is being represented in an abstract notation such as a system model. In other word the reusing concept does not hold any implementation detail and can be adapted in range of different other situations. The design process in most software engineering discipline is based on reuse of available conceptual components (Sommerville, 2006). Design patterns, architectural patterns, and model-driven software engineering are some examples of reuse-based engineering approaches. Reusing of abstract designs which do not have implementation details, known as design patterns, we can design the system in a way that fit the requirements of system. The main concern regarding reuse strategy is to have a systematic reuse strategy which is planned and introduced in an organisation wide reuse program. To have such a strategy, the best practice has been to introduce and also reuse of standardised patterns. Some standards, such as user-interface standards, are well known in software development and web design industries. It is important to mention that most software developers think of design patterns as a way of supporting object-oriented programming (Sommerville, 2006).

Christopher Alexander says, “Each pattern describes a problem which occurs over and over again in our environment, and then describes the core of the solution to that problem, in such a way that you can use this solution a million times over, without ever doing it the same way twice” (Sommerville, 2006). In other words, design patterns are reusable and general solutions to repeatable problem occurring in software engineering. A software developer can use design patterns as fundamental solution in related systems and change the margins based on situations. In short, software developers can leverage the experience of other skills by using patterns. The idea of design pattern was first introduced by Christopher Alexander and his colleagues and later took the root in object-oriented software community. It also gained popularity by the publication of their book; *Design Patterns: Elements of Reusable Object-Oriented Software*, in 1994 (Gamma et al. 2012).

Using security and privacy patterns also have been introduced recently in domain of compliance. These are to ensure technical solutions and implementations are considered for elicited requirements. Some of these works have been discussed in previous sections and we are just pointing to them here (Kalloniatis & Kavakli, 2008; Turetken et al., 2011; Schmidt et al. 2008). Some works also participate to introduction of security and privacy patterns (Dritsas et al. 2006; Compagna et al. 2007). We have used the term, design pattern as general for any implementation for system functional requirements and non-functional requirements such as security and privacy. We have used the current catalogues of patterns for this aim. Our future aim is to introduce privacy requirements based on types of developing systems.

2.8 Technical Aspects of Ontology & Semantic Web

2.8.1 Introduction

A Compliance framework in software development is proposed here in order to ensure developed systems will adhere to the requirements of laws, regulations and external and internal policies related to the system context. We have chosen the notion of a framework as the optimal model through which to address these issues. A framework is a layered structure consisting of a set of subsystems or components, each performing part of the entire intended process and interrelating components through the output of other components (Paradkar, 2011). During the entire framework process, links between the components perform the role of mapping and component integration. Each component also has a number of integrated concepts. In order to provide a platform representing both conceptual and application models of the proposed framework, we needed an approach that could provide both semantic and syntactic aspects of our model along with the relations between elements of the framework. This could all be found in the definition and application of ontology in computer science. Considering the philosophical connotation of the word “ontology”, it is being used here to indicate the categories and different components within the universe of the proposed framework, plus sufficient information regarding the concepts and relationships of each component and the components together.

This chapter presents an overview on the technical background of the building block of our proposed framework, which is Ontology and in specific Semantic Web.

2.8.2 Ontology and Semantic Web

The word “*ontology*” is a compound word composed of two parts, *onto,* a Greek word meaning “to be” and *logy* in the meaning of science. In philosophy ontology is the study of being, existence or reality and it concerns matters such as the entities which exist or can be existed along with their properties and relations and the way they can be grouped based on their similarities and differences (Smith et al., 2003). One of the most widely referred definition of ontology is introduced by Jakus et al. (2013). He believes Ontology is as a formal, explicit specification of a conceptualisation that represents an abstract model of a phenomenon in the world as it helps to identify appropriate domain concepts and semantic relationships among these concepts with formal definitions in terms of axioms. Another advantage of ontology representation of Knowledge is to organise the metadata of complex information resources. These metadata provide syntactic and semantic information about information resources which are encoded as instances in the ontology (Sheth et al., 2002). Using formal representation of ontologies and metadata created from them enables reasoning in order to retrieve inferred knowledge from ontology (Dolog, 2006).

Ontology also has made its branch in computer science in order to represent the knowledge of a hierarchy of concepts within a specific domain using taxonomic hierarchic classes of the concepts (Antonio & Harmelen, 2004). Ontology is being used in artificial intelligence as a structural framework organising information in a specific or a general field in order to capture knowledge and automate reasoning (Seng & Kong, 2009). There are two types of ontology available. Generic ontology contains knowledge that can be reused across various domains such as Cyc. The other type of ontology is Specific Ontology which is specific to a particular domain, task activity or method such as natural language processing ontology which a single instance can be mentioned as OntoLearn (Neri, 2006).

The main reason of the extension of ontology in information technology is the vast amount of information stored in different and separate resources which makes the task of knowledge extraction very difficult. Even the strong search engines these days fail to extract exact required knowledge since they hugely depend on keyword searches without considering the different meaning of single words and terms. This demand made the potential for a uniform technique assisting the automated knowledge extraction based on the theory of ontology. The fundamental of the solution is based on building block elements of concepts and the reality that every knowledge in this world is a combination of the triple of subject, predict and object. In fact the triple makes the relation between the elements of -the world (Antonio & Harmelen, 2004). One example in this case is the concept (class) of *person* as a subject and properties of *firstName, lastName, age, male* and *female* as objects. To make the relation or predict of "a person has lastName" or "a person is male" we have triples of (person, has, lastName) and (person, is, male). In this way we can construct different knowledge in the ontology of *family* and extract required information (Jakus et al., 2013). But to construct knowledge of concepts in a domain, the concepts and their relations should be linked together in an organized structure. This is being done by a meaningful association between concepts which is called a semantic relation. When all the associations are linked and represented in a formal and computer interpretable way idiomatically it makes a semantic network. One of the computerized techniques is called *Semantic Web*. "Semantic Web is the vision of web of the future with the structure of information that is understandable to computer, so the later can perform many tasks instead of humans" (Jakus et al., 2013, p.45). As described before, the essence of semantic web is the resources of information represented in triples and linked together. The representation is done by a language called Resource Description Framework (RDF) which describes the resources in form of triples. The triples of subject, relation and object include components of ontology as classes or concepts, objects or individuals and relations which are defined by properties. RDF triples are encoded by the facilities of XML marking language in order to be easily exchanged between applications and computers. The more advanced relationship between concepts is being constructed using Web Ontology Language (OWL). OWL extends the vocabulary of RDF by providing more meanings to the triples. Ontology can be constructed manually using dedicated software tools such as TERMINAE, PROTEGE, HOZO and others. The Semantic Web is considered as the next generation of the Web where information is given "a well-defined meaning", better enabling computers and people to work in cooperation (Berners-Lee, 2006). In order to process, transform and assemble information automatically, semantic webs help users to make smarter decisions. Several technologies have been developed for shaping, constructing and developing the semantic web. Such technologies are being applied in many practical applications to semantically model the knowledge in their respective domains. In the field of legal knowledge, ontologies are applied to model knowledge about domains of laws, case laws and also compliance. Figure 2.1 shows the semantic web stack, which illustrates the architecture of the Semantic Web. The functions and relationships of the components can be summarized as follows (Berners-Lee, 2006):

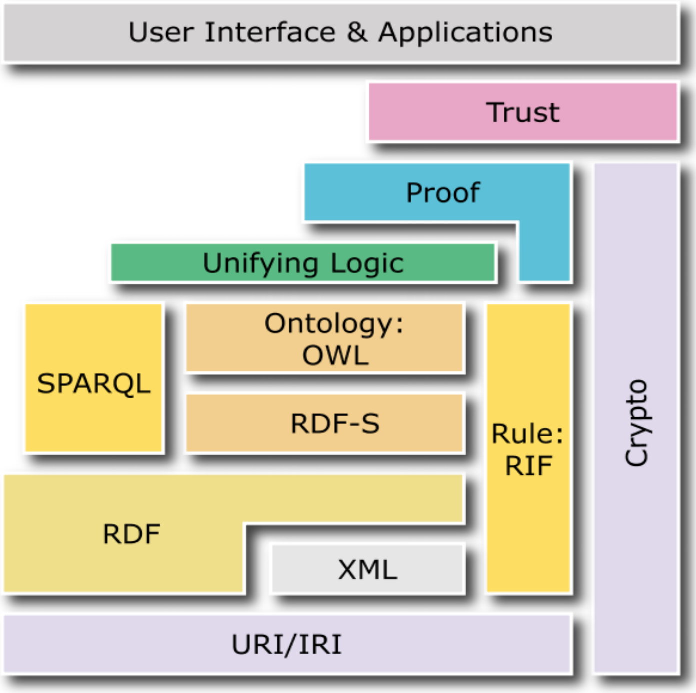


Figure2.1 : Semantic Web Stack (Berners-Lee 2006)

- The URI (Uniform Resource Identifier) as the global standard encoding system for computer character representation, provides a global standard to uniquely identify semantic web resources. (Medic & Golubovic, 2010)

- RDF is a simple language for expressing data models including objects (web resources) and their relationships. An RDF-based model can be represented in a variety of syntaxes, e.g., RDF/XML, N3, Turtle, and RDFa. RDF is a fundamental standard of the Semantic Web

- XML as a mark-up language provides an elemental syntax for content structure within documents, yet associates no semantics with the meaning of the content contained within.

- OWL as an extension on RDF, adds more vocabulary for describing properties and classes: relations of dis-jointers, cardinality, equality, richer typing of properties, characteristics of properties (e.g. symmetry), and enumerated classes are examples of OWL. It also provides reasoning power to the semantic web based on description logic.

- SPARQL is a protocol and query language for semantic web data sources in order to retrieve knowledge from ontology.

- RIF is the W3C Rule Interchange Format. It's an XML language for expressing Web rules that computers can execute. It is defining more relationship on OWL triples.

The other layers which has not been introduced here are not still standardised.

2.8.3 Ontology Language

An ontology language is a formal language for encoding an ontology. As the foundation and main structure of ontological systems, ontology languages allow construction of knowledge in a specific domains. They normally include reasoning rules in order to define and impose more knowledge.

There are different ontology languages available at the moment. Traditional and primitive languages can be mentioned such as Knowledge Interchange Format (KIF) (Genesereth & Fikes, 2014) , Cycl7 (Guha & Douglas, 1990), FLogic (Kifer et al., 1995) and LOOM8 (Macgregor & Robert, 1999) . The next generation of ontology languages are based on XML syntax such as Ontology Exchange Language (XOL) (Karp et al., 1999), SHOE9 (Haarslev & Moller, 2001), Resource Description Framework (RDF)10 and RDF Schema11 (DuCharme ,2011) . The last versions of ontology languages have been developed on top of RDF(S) and had been able to improve their application and extend them by some extra features: Ontology Inference Layer (OIL) (Fensel et al., 2000) and DAML+OIL (Horrocks, 2002) examples.

Most recent ontology developers have used graphical ontology editors for creating or manipulating ontologies. These editors provide an easier and more user friendly environment in which developers do not need to manipulate ontology language codes. The output of these editors will be in one of the web ontology languages supported by ontology editors. Some of the more popular ontology editors are Protégé (Noy & Musen, 2000), OWL-P (Desai et al., 2005) and OilEd (Bechhofer et al., 2003).

In the next section the most popular web languages for representing ontologies which are being used in current project will be reviewed. These languages are Resource Description Framework (RDF), RDF Schema (RDFS) and Ontology Web Language (OWL). They are based on the XML syntax have different terminologies and expressions.

2.8.4 Resource Description Framework/Schema(RDF/S)

RDF (McBride 2002) is a language recommended by the World Wide Web Consortium World Wide Web Consortium. Available at: https://www.w3.org/. (Accessed on Jnuary 2014). to describe web resources and their relationships. It was originally designed as a metadata data model. It is now being used as a general method for conceptual description or modeling of information that is implemented in web resources. It is also used in knowledge management applications.

RDF uses Internationalised Resource Identifiers (IRIs) to identify resources. An IRI is a long string of characters which allows RDF to directly refer to non-local resources. The building block of RDF is a triple of subject-predicate-object which makes statements about mentioned resources in order to make a knowledge in the domain. The subject indicates the resource, and the predicate expresses a relationship between the subject and the object. The simplest way to represent a statement is to use the definition and turn it into a triple. For example, the statement: “"there is a Person identified by http://www.w3.org/People/EM/contact#me, whose name is Eric Miller, whose email address is e. miller123(at)example (changed for security purposes), and whose title is Dr.” can be presented as follows:

<http://www.uel.ac.uk/People/EM/contact#me>

<http://www.uel.ac.uk/contact#fullName> "Eric Miller"

<http://www.uel.ac.uk/People/EM/contact#me>

<http://www.uel.ac.uk/contact#mailbox> <mailto: Emailer(at)uel.ac.uk>.

<*http://www.uel.ac.uk/People/EM/contact#me*>

<http://www.uel.ac.uk/contact#personalTitle> "Dr."

Subject: The Subject is the resource we want to make a statement about. In our example we want to make a statement about the person EM contact details. In order to express a statement about this content, the IRI “*<http://www.UEL.ac.uk/People/EM/contact#me>”* is used.

Predicate: The predicate describes the kind of information expressed about the subject. In our example we want to make a statement about the EM contact detail to express his full name, email address and title by IRIs *<http://www.w3.org/2000/10/swap/pim/contact#fullName> "Eric Miller", <http://www.w3.org/2000/10/swap/pim/contact#mailbox> <mailto:E.Miller(at)uel.ac.uk>* and *<http://www.w3.org/2000/10/swap/pim/contact#personalTitle> "Dr."*

Object: The object defines the value of the predicate. In our example we want to state that the full name of ED is “Eric Miller”, his email is “*Emailer(at)uel.ac.uk” and his title is “Dr”*. The object can be a literal, like in our example, or another resource represented with an IRI.

The code for the preceding statement can also be represented in XML as follows:

<rdf: Description about=" *http://www.UEL.ac.uk/People/EM/contact#me* "> <contact-FullName> Eric Miller </contact-FullName> </rdf:Description>

The domain in which RDF concepts are defined is depended to user and RDF is called a domain-independent resource of knowledge representation. Depended on the domain, we can define the vocabulary and specify the relationship between subjects and objects using properties.

The taxonomy of RDF is organised in terms of hierarchies of subclass and sub-property relationships, domain and range restrictions and instances of classes. However, it has limitations in describing resources including descriptions of existence, cardinality, localised range and domain constraints or transitive, inverse or symmetrical properties which has made Scientifics to overcome these limits by developing Ontology.

2.8.5 Ontology Web Language OWL

The Web Ontology Working Group of W3C identified a number of characteristics for semantic web that would require a more expressiveness than what RDF and RDF Shema could offer. Web ontology languages were proposed by the semantic web research community to overcome the weaknesses of RDF/S.

The integration of OIL, DAML+OIL and RDF results in OWL being based on RDF's syntax, thus the web-based applications can directly access OWL ontologies. Similar to RDF Schema, OWL can declare classes and properties, organise them in a "subclass" and "sub-property" hierarchy and assign the domain and range of these properties. It can also express which individuals belong to which classes, and what the property values of specific individuals are. Nonetheless, it should be noted that OWL is an extension of RDFS in a higher logical layer. Therefore, it offers the following for expressing meaning and semantics:

• Equivalent of classes: Defining equivalence or difference classes and properties, using properties like equivalentClass, sameAs, and disjointWith.

• Boolean combination of classes: OWL classes can be specified as logical combinations using Boolean "or", "and" and "not", which in OWL is called unionOf, intersectionOf and complementOf.

• Special characteristic of properties: Declaring logical properties of properties, like TransitiveProperty, SymetricProperty, FunctionalProperty and inverseOf.

• OWL constructors' class have more restrictive mechanisms on the kinds of values the property may take such as specific values, universal or existential quantification using hasValue, allValuesFrom or someValuesFrom respectively.

• Cardinality restrictions: OWL allows cardinality restriction using properties like minCardinality, maxCardinality.

- Local scope of properties: defining range restrictions on properties

OWL is based on Description Logic (DL) which enables for full formalisation of the meaning of the OWL language propositions. Description logic enables automated logical reasoning techniques. The reasoner allows logical conclusion and consistency checks on classes, individual instances and properties. There are different types of reasoner available such as FaCT++ (Tsarkov & Horrocks, 2006), Racer (Haarslev & Moller, 2001), and Pellet (Sirin & Parsia, 2004). Most modern automated and graphical ontology tools such as SWOOP12, Protégé, and TopBraidComposer have facilities to add and install all the mentioned reasoner prompt-ins in their application.

2.8.6 Semantic Web Rule Language (SWRL)

Although OWL is a strong ontology language to represent knowledge in a specific domain, it still lacks from some limitation, particularly in identifying semantic relationships between individuals which is a result of trying to retain the decidability of key inference problems (Fensel et al., 2000). OWL does not include a composition conductor in order to capture chain relationships. As an example, in family ontology designed by OWL, it is not possible to present a relation of has-UncleOf based upon on object-properties of has-brotherOf and has-childOf. This demand has been addressed by extending OWL with sematic Rules. Rules capture dynamic knowledge as a set of conditions that must be fulfilled in order to derive further information that cannot be achieved by ontology. Semantic Web Rule Language (SWRL) extends OWL with Horn-like rules based on the rule mark-up language RuleML. It enables automatic deduction of new knowledge from existing facts. Thus, SWRL rules ultimately increase the expressivity of OWL-DL.

SWRL rules are in following form:

Facts → consequent   Or A1,A2,A3,… -> B

There are two intuitive ways of reading this rules. Once is called Deductive rules which can be read as if facts are true then consequence is true too. The other way is called Reactive rules which implies if facts are true then carry out the actions in consequence (Haarslev & Moller, 2001).

Both the facts and consequent can include multiple atoms connected through logical conjunctions (written a1∧a2∧...∧an) or be empty. Atoms can be written in the following forms (Yarandi, 2011):

1. C(x) where C is an OWL description and x is an OWL individual variable or a data value.

2. P(x,y)where P is an OWL object property and x and y are OWL individual variables or data values.

3. Q(x,y) where Q is an OWL data property and x and y are OWL individual variables or data values.

4. B(x1,x2,...) where B is a built-in relation and x1,x2,... are OWL individual variables or data values.

5. sameAs(x, y), differentFrom(x, y) where x, y are OWL individual variables or data values.

Using mentioned rules, the Uncle relationship in family ontology can be represented as following:

$$\text{hasChildOf}(?x,?y) \land \text{hasBrother}\ (?x,?z) \rightarrow \text{hasUncle}(?y,?z)$$

Using OWL and SWRL, ontology has been used in order to represent the knowledge in domains which include policies, actions and conclusions on available facts of domain.

2.8.7 OWL Reasoning using Pellet

A semantic reasoner or rules engine is able to infer logical consequences from a set of asserted facts or axioms. Pellet (Sirin & Parsia, 2004) is an open source, Java reasoner for OWL ontologies. It provides standard and cutting-edge reasoning services and can be used with both Jena and OWL API libraries to provide reasoning. It provides functionalities to see the species validation, check consistency of ontologies, classify the taxonomy and check ontologies. Pellet is an OWL DL reasoner using the tableaux algorithms (a decision procedure that aims to determine the suitability of an input formula in a given logic) which is provably complete. Pellet supports reasoning with SWRL rules. Pellet interprets SWRL using DL-Safe Rules notion. There is no need for using any additional utility function to use SWRL in Pellet.

2.8.8 Data Representation using XHTML

XHTML1 is a family of XML Mark-up Languages that extend versions of Hypertext Mark-up Language (HTML), the language in which web pages are written. The structure of the different models used in the semantic rule-based approach is represented through OWL language. However, different models do not include actual IOs and assessments and only include their IDs. Consequently, when the Compliance model is ready to be delivered, the actual IOs and assessment are attached to the model. As Compliance model created by system are delivered via the web, their textual IOs and assessment are written in XHTML and may include image files, Flash animations and audio or video content that can be delivered via a web browser.

2.9 Conclusion

Here, we are discussing the differences and similarities of our work regarding its strength and weak points to above mentioned literature reviews. In above sections, approaches of compliance to after-the-fact and before-the fact have been investigated. In both categories we discussed manual and automated approaches. We represented argumentation of different works regarding the advantage of taking compliance as early as possible. Thus we also put the potentials of current work to the design of a before-the fact compliance approach. This is to ensure compliance requirements are taken in design and development of software systems. As discussed, although addressing all compliance issues at design time is impossible and compliance issues mostly come up in the operation of the business, but having only compliance auditing techniques in running application makes it costlier for organisations in case of breach. Bulk of commercial compliance auditing software and consulting organisations are available. Among compliance to different laws and regulations which we performed a survey on them, data protection plays a key role mostly in information system industry where huge amount of personal data is stored and consequently their privacy is very critical. In recent year a gap in before-the-fact compliance approaches for privacy was felt and consequently international calls for it were announced such as amendment on European Data Protection Directive.

There is a general acceptance regarding usage of the term "Privacy by Design" (PRD) for a category of before-the-fact approaches which we use here as well and therefore aim to propose a Privacy by Design approach. This term was used in Article 14 of General Data Protection Regulation. As called, PRD is about integrating privacy requirement elicitation in requirement engineering stage of software development or business process.

The current literature review on PRD approaches, categorise these works to two general categories of manual and automatic solution, plus three dimensions of policy making, taking technical and organisational controls for privacy requirements and developing technical approaches such as identity management approaches. In contrast We have provided a conceptual framework (KN-SoPD) for PRD and an automatic tool to support the conceptual framework (AU-SoPD) which is able to make compliance to a derived privacy policy from laws and regulations with supporting security and privacy technical controls.

Some of the works in first two mentioned dimensions uses RE methodologies as well. This is due to the definition of privacy by design which is to align compliance and requirement engineering. They have used different approaches to RE. We have opted a goal-oriented RE methodology in our framework which can represent social relationships between system stakeholders, thus is able to be aligned with laws. This is in situation which some previous works have used goal-oriented methodologies which lack in the concept of agent. The goal-oriented modelling components used in or framework for system development can also be used for business processes modelling. Some also have used the same methodology as us, but no systematic way have been proposed to automatically apply legal context to systems and they were performed manually. In contrast we performed a survey on classical and modern law analysis techniques and employed a legal reasoning method which simulates the same job of legal professional, also automated this method.   The works mentioned above mostly lack in a systematic process of law analysis. Some only participated in extracting rights from legal texts or using language patterns

Most of above mentioned works in this literature review, have separately targeted compliance to a specific law or regulations in a domain such as Sarbanes-Oxley Act, Business Contracts, HIPAA (The Health Insurance Portability and Accountability Act), PIPA (British Columbia Personal Information Privacy Act), ISO standards, COBIT (Control Objectives for Information and Related Technologies) or Data Protection. This is in a condition where a system may need compliance to different legal resources. Compliance to an act generates very high-level requirements which needs to be interfered and refined to more application level requirements from standards, guidelines and technical implementations. some previous works have provided such a facility by providing security and privacy controls to implement legal requirements. There is also lack of a systematic link and refinement process between compliance resources in most of previous works. They mostly perform this task manually or by conceptual frameworks. This requirement has been addressed in our work by taking into account numerous components of compliance, also by making semantic relationships between them using ontological methodologies and techniques. Ontology is about collecting a taxonomy of concepts in a domain and relating them through their semantic relations. We proposed a semantic approach which uses semantic web technology, also provides a query-based knowledge repository both for system analysis and design, compliance and risk analysis. This differs our work from the ones with normal ER databases for ontology in a way that it is to work on the Web, also provides interconnections between each two entities if defined. ER databases make relationship between tables, thus making complex queries is almost a difficult task in ER databases. We also discussed the technology aspects and the definitions of semantic web in this literature review. Few number of the aforementioned works also represented a knowledge-based compliance solution which can impose and integrate regulatory requirements into the modelling of software systems which is available in our work. The method to classify ontological concepts and relationship is also unique and different from other semantic based compliance solutions. Therefore, all the reasons mentioned in this paragraph makes this work as a contribution in the knowledge of compliance in software development

Also we believe that compliance is not an isolated matter and that the compliance and risk regime should be considered as a united and integrated concept. some of mentioned approaches above have taken risk assessment as an important issue in compliance. Less have provided a knowledge-based and automated solution for risk assessment. Also our risk assessment methods are aligned with our RE component and other compliance components.

Totally speaking, our literature review shows that although after-the-fact approaches (compliance auditing) are used hugely in industry and very beneficial, but why delay the risk too late! A huge number of before-the-fact compliance approaches are also specified to compliance in business process which takes a BPMS and embed legal requirements in it. Our main purpose here is privacy by design, theorem we need a specific RE component for it, which may also be used for business processing. And finally PRD approached are provided as a technical solution for privacy such as identity management or are mostly conceptual models consisting of compliance components. Regarding the first category, we believe that technical approaches such as user centric technologies only satisfy one part of privacy goal (which is security), but not all of them. The second category are almost through some guidelines which separately participate compliance to law, regulation or technical controls. We aim to provide comprehensive framework consisting of all these linked to each-other with a supporting automated tool. This is in a situation to possible compliance to all mentioned resources at once in addition to a privacy impact assessment component.

Finally, we propose a framework for privacy by design, which can be used by a software developer or compliance officer in order to get and obtain a full knowledge repository of compliance to data protection and its related standards (from privacy to security) in design and requirement engineering stage of system development. The extracted requirements from this approach, are both from data protection law (specifically GDPR), relevant ISO standards and organisational guidelines. This all is possible under the unique umbrella of KN-SoPD framework and also elicited requirements are able to be traced to their higher or lower level requirements from other compliance resources.

Compared to works with general legal ontologies, this work lack to be limited to data protection and specifically GDPR. But the framework and supporting tool both have been designed general and can be extended at any time. In this case, number of ontological rules will west and may make complication. Thus, the methodology to define and integrate rules should be improved. This also should be managed in a way to overcome the overlapping of laws. In contrast to the work with less number of components, this work looks complicated. Here the aim was to represent different compliance resources and their integration. Future work can combine all components in one ontology with less concepts and classes. Here we also only concentrated on compliance requirements and design. Post-design compliance auditing was an advantages of few number of previous works that can be considered in future.

3. RESEARCH DESIGN

3. 1 Introduction

In this chapter we will discuss the issues involved in designing a semantic-based compliance framework, called KN-SoPD (Knowledge-based Software Privacy by Design) and its supporting tool, Au-SoPD (Automated Software Privacy by Design) in software development toward fulfilling the objectives and goals of this research. After this introduction, Section 3.2 explains the methodology of this research. Right after, details on research approaches and methods for collecting and analysing data are highlighted. This section also introduces different types of data being used in this research and include a qualitative analysis in order to select the best data for this research. Section 3.5 introduces and justifies the semantic rule-based approach for producing the proposed compliance framework. In this section, we will explain the main features of this approach including the separation of the compliance models each representing different components of KN-SoPD, the representation of these models using ontology enriched taxonomy, the abstraction mechanisms employed through ontological modelling to facilitate this separation, defining ontological concepts in finer granularity levels for each component of framework and we finish this section by showing the architecture of our system. Section 3.6 explain how semantic web technologies has been used to develop Au-SoPD.

Section 3.7 conclude this chapter briefly describing whole chapter.

3. 2 Research Methodology

The purpose of this thesis is to propose a novel approach for supporting a software development regulatory compliance framework. This novel approach aims to improve flexibility, extensibility and reusability of such systems while offering a pedagogically effective and satisfactory compliance experience for software developers and compliance officers. This study is conducted in four phases:

The first phase was performing the library research which refers to the secondary data and its analysis. The goal of this phase was first to review current national and international IT laws, standards and guidelines in order to have a survey on them and select the most appropriate and most referred resources in the industry of information system compliance to subjects of security and privacy. This stage also includes an investigation through a number of diverse approaches in classical and traditional legal reasoning and compliance methods aimed to conclude to a law analysis approach in our work and a literature review on current compliance approach by other researchers both from general or domain specific compliance solutions. This was in order to present the differences between these systems and highlight the shortcomings of the existing models. In second phase of our work, an innovative law analysis and a semantic rule-based approach is proposed to overcome the deficiencies of the current approaches in designing and implementing a semantic based regulatory compliance approach. In order to achieve the aim of this research, which is mentioned above, the approach proposes a law analysis and compliance process and its implementation by an ontological architecture featuring a compliance engine. This engine does not include any knowledge about a particular domain or any adaptation strategy; it obtains all the necessary information from the respective ontologies. The approach also presents legal reasoning and compliance techniques with semantic rules for expressing the refinement, mapping, integration and inherency of the framework components. Finally, a semantic rule-based approach is designed and implemented using the semantic technology of protégé which is represented in the next stage of our research.

The last stage of our research concentrates on the evaluation of the proposed approach using following evaluation methodologies:

- **Case Study Evaluation:** OWASP TOP 10 Privacy Risks (Open Web Application Security Projects) and their countermeasures are used to evaluate extract privacy requirements of our approach

- **PRD Approach Comparison**: Current work is being evaluated by other similar approaches from our literature review based on PRD 7 principles (Cavoukian, 2011) and some other characteristics

3. 3 Research Approach

Inductive/Deductive research is "the foundation of modern research". An inductive/deductive reasoning can balance projects in computing science. Deductive approach is used for implementation and inductive is used to explain, interpret and provide protocols and theories for the project. In this research we are also using a selection of both deductive and inductive research approach. Deductive approach is used in the implementation stage of our research and inductive is used to conclude and provide the base theory for the development and design of the conceptual model of the proposed compliance framework.

3. 4 Methods of Data Collection and Analysis

Since our research includes data collection and categorisation, it is using both a quantitative and quantitative approach in this stage. The latest part of this thesis is specified to evaluation of this approach by examination of a real world scenario in which the update will be evaluated and compared to requirements of an equivalent standard from and also a comparison study on other similar approaches. The evaluation is based on numeric and non-numeric data obtained from the outputs and a qualitative and quantity approach has been used for this analysis.

We are performing data analysis in different stages of our research. The first stage concentrated on gathering and collecting data regarding different types of available information technology laws, regulation and standards and guidelines. The main goal of this analysis was to make ourselves more familiar with different regulatory frameworks that IT systems should comply with. To do so, we first collected IT laws and regulation from different territories and also categorised them based on a subjective categorisation of IT laws. The main resources to collect this information were online search engines and books in related subjects. The second stage of our data analysis regarding evaluation of our approach is conducted by a real world case study from web application development. The selection of this case study was regarding to the richness of legal issues involved in the processing of the project's data, also the sensibility of the processing data in web applications. As reported by Verizon Data Breach Investigation Report 2015, up to 61% of breaches involved attacks against web application (Kandek, 2015). The other reason of this selection is its huge usage to transfer business and also the high interest and involvement of IT industries in web application development business. Since recently there had been some initiatives by Open Web Application Security Projects (OWASP), trying to address the Privacy by Design issue in design of e-commerce applications, the case study selected here is taken from e-commerce application development area. The case study has been selected from a real business scenario from industry which is similar to a case study being used in another research. At the end a comparison analysis is performed on the output of the evaluation of our framework on the selected case study against the Top 10 priorities of privacy concerns in e-commerce application addressed by OWASP. This is to conclude how our approach has been successful to deliver compliance to the development of a web application. The second evaluation part includes comparing our work with 13 other similar based on 7 principles of PRD (Cavoukian, 2011).

3.4..1 Collecting IT Laws and Regulations

The initial study of this research as a part of our literature review has been concentrated on current information technology legislation frameworks. To do so we first cetegorised IT laws in to three main groups of Computer Laws, Internet Laws and Cyber Laws. The main and well known authorities in IT law establishment and regulations also had been researched on. This starts by an international body in the field which mostly plays the role of organising territory bodies and followed by introducing continental based authorities. In this way we were able to introduce international IT legal authorities and have a categorisation of international IT laws. The result of our literature review is summarised in APPENDIX I. This table has been designed in a way that laws in each territory are categorised based on their subjects.

Although it has been tried here to provide a comprehensive list of information technology laws, regulations and guidelines from international and national territories, but this project couldn't cover the compliance to every conceivable law. Therefore, IT legislations which already has a significant effort in compliance domain is being picked up here to be analysed and compiled to. Data Protection legislation as one of the oldest and strongest tools to safeguard the privacy of personal data has been selected here to be practiced. The cooperation between international organisations (Table3.1) and the similar structure of their data protection legislation is another reason of this choice. Table3.1 is providing a comprehensive study between different Data Protection legislation regulated internationally.

United Nation	**OECD**	**Directive 95/46/EC**	**APEC privacy framework**
Principle.1 lawfulness and fairness	PART TWO.7. Collection Limitation Principle	Article 5,6	Part III.III Collection Limitation
Principle.2 **Accuracy**	PART TWO.8. Data Quality Principle	Article 6	Part III.VI Integrity of Personal Information
Principle.3 **Purpose-specification**	PART TWO.9, 10. Purpose Specification Principle, Use Limitation Principle	Article 7	Part III.II Notice Part III.III Collection Limitation Part III.IV Uses of Personal Information
Principle.4 **Interested-person access**	PART TWO.13.Individual Participation Principle	Article 10,12,14,22,23	Part III.VIII.23 Access and Correction Part III.V Choice
Principle.5Non-discrimination		Article 8	Part IV.A.II.33 Giving Effect to the APEC Privacy Framework
Principle.6 **Make exceptions**	PART ONE.4.Scope of Guidelines	Article 13	Part III.VIII.24 Access and Correction
Principle.7 **Security**	PART TWO.11. Security Safeguards Principle	Article 17	Part III.VII Security Safeguards Part III.I. Preventing Harm
Principle.8Supervision and sanctions	PART FIVE.19. NATIONAL IMPLEMENTATION	Article 28, 18,21,24	Part IV.A.II.31 Giving Effect to the APEC Privacy Framework

	PART THREE.15.IMPLEMENTING ACCOUNTABILITY		
Principle.9 **Trans border data flows**	PART FOUR.16,17,18. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION	Article 25,26	Part III.IX Accountability
Principle.10 **Field of application**	PART ONE.2. Scope of Guidelines	Article 3	Part II. Scope

Table3.1 . Data Protection Legislation's Principles Comparison

As it is visible from the obtained information of Table 3.1, there is almost a confederate system of legislation regarding the principles of data protection regulations in the spotted territories. Although the same structure of status is not followed in different legal texts, but the contents indicates the same meaning and instruct almost the same rules to similar stakeholders. As described before, the cooperation between different international organizations, e.g. OECD and Commission of Europe, APEC and OECD, United States and APEC and also the authority of United Nation above all territories has resulted to almost an integrated legal system in the case but not always synchronized. This along with the importance and effectiveness of Data Protection Law on compliance to privacy, which is the main purpose of this research, made us to select Data Protection as the main focus of compliance here. The most important logic behind this selection is the recent reconsideration of this legal tool regarding the new privacy legal challenges of developing technology.

3.4..2 Case study Selection

To understand the process of compliance in this work, also to practice the system requirement gathering task approach chosen in this framework, a case is being studied here to extract requirements regarding designing a web application and application of relevant laws. There are different types of web applications such as e-commerce, healthcare, educational, corporate and others. Considering the sensitivity of the financial and privacy aspect of the case, and also Since there had been some initiatives by OWASP (Top 10 Privacy Risks Project for web applications) (Open Web Application Security Projects (OWASP)) trying to address the Privacy by Design issue in design of e-commerce applications, the case study selected here is taken from e-commerce application development area. e-commerce application requirements have been selected to be analysed. In order to synchronize works and limit the processing time, we are using the same case which has been presented in (Bolchini & Paolini, 2004) with additional analysis and application of relating laws to the case and some major changes. The case is to design and analyse requirements for web site of an Italian supplier of silver-made artefacts briefly called B-Silver. In order to represent the different types of requirements, the categorization of requirements represented in the work of (Bolchini & Paolin, 2004) is also being used as the reference here. Researchers in this work, have represented web application requirements also using i* framework. Based on this work, web application requirements are categorised to groups of high-level communication requirements, hypermedia specific requirements, content, interaction, navigation and also presentation requirements of a web application. We use the same categorisation and apply any necessary legal demands to the application areas of these requirements.

3. 5 Ontology Based Compliance Framework Design and Specification

According to OCEG (Organisation of Economic Co-operation and Development), compliance has been defined to adhere to laws and policies. However, from a different perspective, well-defined compliance approaches should also be augmented by an assessment of risk management in order to safeguard the objectives of laws, regulations and best practices from aligned risks. Following the aim of this research which is to attain "Privacy by Design" as being defined by Article 25 of GDPR, this is necessary here to have an element for system design as well. Therefore, in our desired compliance process, firstly it is essential to have knowledge about laws, regulations and policies in context of the system, secondly to know how to design the system and apply the laws and policies to system context and finally how to perform risk analysis against compliance objectives. Based on this description, we have divided our compliance process and following to that this chapter is divided to following lists:

- Analysis of Laws & Regulation: This process is based on traditional and classical definitions and methods of law analysis. This will help to understand the meanings of each component in our framework, also the reasons behind their employment in our framework. Each of law analysis techniques and supporting framework components will be discussed in detail in separate sections. An ontology model supporting each component, along with its concepts, classes, object properties and data properties is described on following of the description of component's tradition approaches in further sections. Textual analysis method used in our approach is discussed in Section 3.5.2 along with number of articles from General Data Protection Regulation 2012 being analysed. Compliance ontology is being discussed in Section 3.5.6

- Application of law to system context: This process is discussed in Section 3.5.7. application of law is possible when the system is being modelled by a requirement engineering and specifically here system modelling methodology. I* Modelling Language has been selected here for this purpose which will be explained in this section. Section 3.5.8 provides ontology model of i* language which is generally categorised under Requirement Engineering Ontology. Applying laws to modelled system is provided using some ontological processes such as individualling and reasoning which will also be discussed in this chapter.

- Interfering and refinement of laws: In section 3.5.13 other elements of compliance are provided. Supporting ontology of standard and ICO are discussed in 3.5.14, 3.5.15 and 3.5.16.

- System Design: details regarding the different types of systems and design patterns related to each type of system which can help to design the system based on extracted legal requirements are depicted in section 3.5.10

- Risk assessment: general approach to risk assessment and its supporting ontology are explained in 3.5.17 1nd 3.5.18.

Our proposed approach to compliance is depicted based on each mentioned processes followed each after another. Each process is supported in our framework by one or more components. We have chosen the notion of a framework as the optimal model through which to address these issues. A framework is a layered structure consisting of a set of subsystems or components, each performing part of the entire intended process and interrelating components through the output of other components. During the entire framework process, links between the components perform the role of mapping and component integration. Each component also has a number of integrated concepts. In order to provide a platform representing both conceptual and application models of the proposed framework, we needed an approach that could provide both semantic and syntactic aspects of our model along with the relations between elements of the framework. This could all be found in the definition and application of ontology in computer science. Ontology, an explicit formal specification of a conceptualisation is the most suitable means for representing knowledge due to its flexibility and extensibility in designing concepts and their relationships. This definition emphasises that ontology allows defining formally and explicitly the concepts in a domain and their relationships. They also have potential to clarify the domain's structure of knowledge and to enable reasoning about knowledge domains (Chandrasekaran et al., 1999). Therefore, they have proven to be useful for representing knowledge in many domains particularly in legal environment (Brekeur & Winkel, 2003). An ontology-based semantic model provides high level modelling capabilities to represent major components of compliance in software systems development and also provides reasoning mechanisms to accomplish further semantic enrichment steps that can perform the compliance process. We have called our framework (conceptual model) as KN-SoPD which abbreviation for Knowledge-based Software Privacy by Design and its supporting tool as AU-SoPD for Automated Software Privacy by Design. In this chapter and following chapters we are using these names to refere to our proposed framework and its tool. Therefore, it is evident that laws, regulations, best practices, system context and compliance applying models are major components of our compliance framework. Each component is modelled by an ontology specified to it and each compliance process is supported by one or more components and following to that by one or more ontologies. Domain models can describe both the semantics and structure of mentioned components. Accordingly, the starting point in our approach was the classification of ontologies in the domain of our proposed framework of compliance which differentiates the following types of ontologies:

- Compliance Ontology consists of two main ontologies of Laws and regulations. This is to distinguish between legislative bills written by national or international legislators (laws) and rules and guidelines adopted by administrative agencies in order to control the implementation of laws in society.

1- Law Ontology: Law’s characteristics necessary for the compliance are retained in the Law ontology. This ontology consists of concepts, terms and relationships based on the definitions and articles of General Data Protection Regulation 2012. This ontology also provides a general platform for any laws which the system needs to be complied to and can be extended by other laws in future.

2- Regulation Ontology: Regulations, on the other hand, are standards and rules adopted by administrative agencies that govern how laws will be enforced. In our ontology we have covered this by two ontologies of standard as a more official statement and authority guidelines as some reference to interfere laws.

2.1- Standard Ontology: This ontology is considered for another element of compliance; such as standard. This ontology has been taken in order to refine law’s requirements to further applicable details. This ontology include categorisation of concepts based on ISO 27000 series and also ISO 29000.

2.2- Authority Guidelines Ontology (organisational): a specific ontology has been considered to refine and define laws requirements by governmental or organisational guidelines. Here we are taking the ontological concepts from ICO (Information Commission Office) as a UK based organisation which is in charge of compliance with GDPA.

- Risk Ontology: Risk assessment also is modelled by a unique ontology in our work. The concepts are based on definitions of ISO 27005 as an international standard for risk assessment.

- Requirement Engineering Ontology: I* Modelling Ontology: The above mentioned ontologies all perform the task of compliance to the context of system being represented by a requirement engineering and system modelling ontology. In fact, we have considered compliance as one of the primitive requirement of system. Requirements from above ontologies should be mapped to system context which is modelled by concepts from a goal and agent oriented modelling languages in ontology.

- Design Ontology: Compliance requirements are drawn to design level by sage of an ontology of design pattern knowledge. We have provided list of different design patterns based on types of developing systems.

Figure 3.1 depicts a top-level model of the proposed Compliance Framework along with its components and their relationships. Each component of the framework corresponds with one of the compliance ontologies as listed in this section and is accompanied by a number of sub-components which are going to be discussed in detail in coming sections. Figure3.1 will be referred in coming sections to describe the details of this framework.

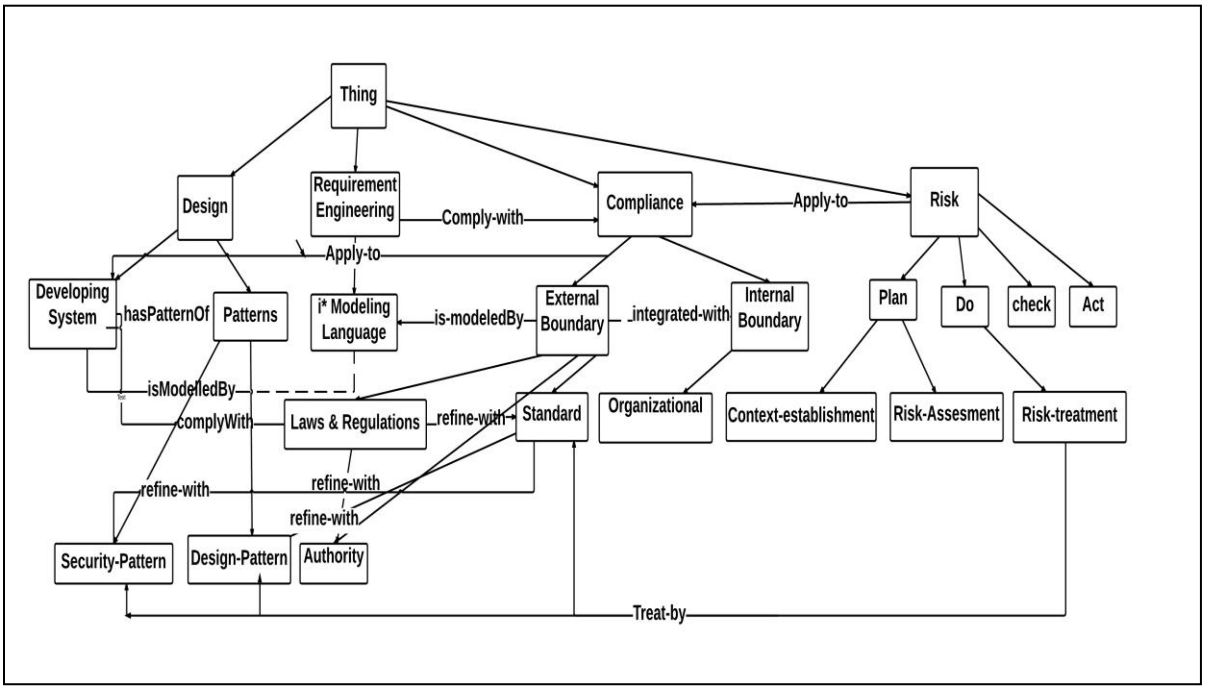


Fig 3.1 High Scheme of Ontology-based Compliance Framework

compliance processes as listed above, have been drawn in Fig 3.1 using number of links between the proposed framework's components. In ontology these links are provided using ontological logic operators such as *Mapping*, *Inheritance*, *Refinement* and *Integration* and using the ontological reasoner. Following sections are provided to discuss compliance process in general and also its supporting ontology in semantic web. Therefore, we have designed the structure of this chapter based on the compliance processes firstly. Each compliance process is supported by one or more of previously listed ontological components. Each ontology supporting a compliance process will be discussed in each section after a full description of its compliance process.

3.5.1 Analysis of Laws & Regulations

One of the most challengeable areas of legal compliance is understanding and analysing legal documents. This is due to ambiguity and complexity of legal texts and the fact that they are not written for ordinary people. As experience has shown, every law even the most carefully worded needs explanation (Scholten, 1931). Legal texts and statutes are normally constructed of complex sentences which need to be broken down to their constituent elements in order to make the understanding easy. Also they are written in very general and often vague language in order to proscribe or prohibit future conduct. Therefore, to make a precise and comprehensive compliance to the requirements of a law which are indicated into it, the text needs to be analysed and be interpreted to its meaning hidden in the text. When the case is the compliance in technical areas such as information technology, further analysis is required to extract the technical requirements from the law.

3.5.2 Classical Methods of Law Analysis

To have a classic review on the matter of analysing laws, first we have a look on traditional meaning of law analysis. As it is defined by legal professionals and researchers, analysis of law is about to find the application of a rule and any application to a set of relevant facts (Connelly, 2006). A rule of law is a constitutional provision or a statute which as an enforcement statement establishes a standard of conduct. In legal and judgment system a rule acts as a formula to make a decision in a case of judgement. Based on definition a case is “a civil or criminal processing, action, suit or controversy at law or equity” (Garner, B.A. (2014) *Black’s Law Dictionary.* 8th Edition, London: Thomsohn Ruiters,). In such situation lawyers and judges argue and try to find and match the rules of law which applies to a given set of facts of the occurred case in a logical process of syllogism. To do so a general formula called IRAC (Issue, Rule, Analysis, Conclusion) as the building block of the process of legal analysis is followed by lawyers. Issue deals with the facts and circumstances which brought the parties to court. Rule process finds the governing law for the issue. This rule can be the common law that was developed by court or the law that was passed by legislators. This process includes finding components of the rule as the proving elements, exceptions, also the underlying policies and social considerations. Analysis answers the question if the rule applies to the case facts comparing them together and also if the facts match the further underlying policies of the rule. And finally conclusion is the court’s decision in the case. As far as the meaning of the statutory is interpreted and applied to the case, it will become a precedent.

All the actions involved in process of law analysis in an occurred case are traditionally based on nature of an *argument.* Defined by theoretical definitions, argumentation is a “complex speech act aimed at justifying or refuting on proposition and getting a reasonable critic to accept the standpoint involved as a result” (Van Eemerence, 2004). To distinguish if compliance is actually a kind of argument, we need to identify and understand characteristics of an argument as described by professionals. Based on other resources (Besnard & Hunter, 2008) argumentation normally involves identifying relevant assumptions and conclusion for a given problem being analysed by performing one or more reasoning steps. The act of argumentation consists of following concepts:

- Proponent as the person or group of people putting forward the argument
- Audience who is the person intended as the recipient of the argument
- Fact which is an item of information specific to a given context.
- Warrant is part of the argument that relates facts to qualified claims. It captures a form of defeasible rule which is valid until some required facts are hold except to exceptional circumstances. Backing is kind of justification for a warrant such as belief, law, moral, authority, ethics and others.
- A rebuttal captures the circumstances that would be regarded as exceptions for a warrant.
- Qualified claim is the drawn conclusion when the warrant holds.

Considering both proponent and audiences of argument it also involves agent and entities of argumentation. An agent is an autonomous, proactive and intelligence system that has some role. Examples are lawyers or journalists. A composed set of agents with concerted roles are called entity such as board of directors in a company or a court. In such a circumstance where a single agent or entity has collated knowledge to construct an argument, the argumentation is oncological. In contrast there is a dialogical argument where a set of agents or entities construct the argument by collation knowledge for and against a particular conclusion (Besnard & Hunter, 2008).

To evaluate and contrast definition of an argument with compliance, first of all it should be noticed that although at the beginning the nature of two opposite opinions in dialogical arguments between compliance officer as the proponent and system developer as the audience doesn’t look to be valid in compliance, but to find the applicable area of compliance in developing system and reaching to law’s claim or conclusion is an argumental task in its nature. To match the other mentioned concepts of argument with compliance a running example is more helpful;

There are different methods of legal arguments and analysing as following:

1. Rule Based Analysis & Argument
2. Analogical Reasoning: Precedent Analysis & Argument
3. Textual Reasoning & Legislative Intent
4. Policy Based Reasoning & Argument
5. Tradition Reasoning & Argument

6. Legal Refinement Reasoning

In rule based analysis a rule of law is applied to a case in order to reach to a judgmental result. As it is defined by (Holdeman Edwards, 2010) in rule based analysis “X is the answer because the principle of law articulated by the governing authorities mandates it.” A rule based analysis can originate from a case or a statute. In order to perform the analysis, the rule is separated into its elements and the facts and circumstances of the case are matched and counter argued to the elements. In such cases the court normally performs a balancing test by identifying the factors to be tested. Analogical analysis is the direct and parallel match between the new problem’s facts and a previous case and concluded case law, saying precedent analysis. Based on (Holdeman Edwards, 2010), in such analysis “X is the answer because the facts of this case are just like the facts of A and X was the result there”. Policy based is the other type of analysis that appeals to future consequences that follow from adopting a certain rule. To run the analysis, the court first predicts the consequences of following the rule and then decides about the more consistent consequences with underlying values of law. In this case “X is the answer because that answer will encourage desirable results for our society and discourage undesirable results” (Holdeman Edwards, 2010). The last legal analysis being discussed here is Tradition reasoning which is based on tradition as a principal test for determining human’s fundamental rights. In here, “X is the answer because that is the way things have always been done” (Holdeman Edwards, 2010). In fact, the common law originally was the reflection of customs of the people in traditions of community and didn’t purport to incorporate the wisest or most enlightened social policies as today is. Some judges have afforded to author opinions that relies expressly on tradition to resolve constitutional issues. Tradition also helps in interpreting rules by providing meaning to some statutory words and phrases.

One of the most general approaches of analysis is textual reasoning and legislative intent. In this method, lawyers and judges read and reread the statute of law. In this method the concentration is the exact language of statue text. The process to perform textual analysis consists of number of orders that should be considered (Connelly, 2006):

1. In early stage of the analysis the reader should note the title of the statute and any preamble or statement of statutory purpose. These purposes mostly are mentioned as *objectives* in early parts of the law text.

2. Note the date when the statute became a law

3. Break the statute into the separate elements to be established

4. Understand and interpret the statutory words and texts of elements. One of the main tasks to do this is to read the section of law related to *definition*

5. Note and consider any authority words in the text to determine if the statute is mandatory (shall), prohibitory (shall not) or declaratory (may)

6. Interpret the meaning of the statute. This task is done to understand the vague, general and ambiguous language of legal texts. In such circumstances courts normally look for external evidences such as:

   6.1 . Legislative History: interpret is performed based on the path of information created by the statute's passage through the legislative process. This includes statements made during the bill's introduction, committee consideration and vote and the floor debate and an official commentary that was published with the statute.

   6.2 Canons of statutory construction: canons are rules and guides used by lawyers and courts to interpret a statute. There are two types of Textual Canons and Substantive Canons. Textual canons are used to infer the meaning of a statue from its textual structure. Substantive canons are principles that are derived from the legal effect of a rule.

7. Read through the other sections of the statute chapter in the law text and note any statutory exceptions.

8. Outline the rule

9. Match the facts and circumstances of the problem with each element of outlined rule to see if the element is proven

The match and contract task is done by the function of deductive reasoning. An example can help to clear the issue:

All men are mortal	(Rule (warrant))
AND Socrates is a man	(Fact)
Therefore, Socrates is mortal	(Conclusion (qualified claim))

3.5.3 Legal Reasoning Methods in Our work:

To decide on the most appropriate option for reasoning methods in the field of compliance, we are referring to a survey previously done in the area of legal analysis. Based on the exact words of one of the works (Holdeman Edwards, 2010), "it is impossible to give a general conclusive scheme about the significance of each mentioned reasoning method and on internal hierarchical order between them in case of solving legal problems". It is believed that the process of legal reasoning is something more than simply applying ready-made rules to established facts. As said there is a notion accepted in all countries with codification system to consider textual and grammatical interception of rules as the most valid system. It was also concluded that the value of all other methods remains relative and each may contribute to the interception of the law based on conditions. Therefore, the central and basic method of reasoning selected for our framework is textual analysis which also takes advantage from some other methods. One of the other methods being used here is Historical argumentation (Legislative Intend) in order to interpret the meaning of legal terms, words and intents. Also according to OCEG, compliance has been defined to adhere to laws and policies (Open Compliance & Ethics Group (OCEG)). Therefore, we are considering both textual and rule based analysis methods, historical reasoning as well as policy reasoning. We are also taking advantage of Traditional analysis in which we use the previous experiences of experts in compliance, security and system development in our framework by using of patterns in order to analyse laws to further requirements of system. The rest of methods such as analogy argumentation are left to feature work regarding different nature of source and the complexity which is out of space of current work.

3.5.4 Rule-based and Textual Analysis:

As discussed before, one of the main elements of textual analysis is to perform logical decomposition, where a rule is broken down to three separate components (Neumann, 2009). first is a set of elements which collectively is called a test. Second is a result which happens when the required elements of the test are available or to be said are satisfied. The final component is a casual term that determines if the result is mandatory (shall), prohibitory (shall not), or discretionary (may). Some rules also contain one or two exceptions which defeat the rules even if the elements are satisfied (Neumann, 2009). There are three different ways that a rule's elements are satisfied to reach the result. The first is when it is necessary that all requirement elements are satisfied. In such cases the elements are separated using the word "*and*". The second condition is called Alternative Elements when the presentation of either element concludes the result. In such cases the word "*or*" is used to separate the elements. The final situation is when it is up to the court to balance and weight different factors to decide if the result is applicable to the case. It is called Factor Test. In the process of legal analysis, in a deductive reasoning function, the elements of rules are matched to the case to prove if they are true or false (Neumann, 2009). There are some rules which have criteria and guidelines instead of testing elements to define the scope of the rule and empowering the authority to make decision or perform the task defined by the rule.

When the rule is decomposed to its constructing elements, lawyers normally draw a diagram to outline the rule and sometimes reorganize the structure of the rule (Huhn, 2002). This makes the understanding of the legal text easier and helps to easily match the facts of the case with the rule. To clear the explained analysing techniques, we are analysing number of rules from the articles of General Data Protection Regulation 2012. The analysis in this stage consists of rules decomposition to primitive elements of facts and conclusions together with the casual mandatory terms and exceptions if valid. Regarding the space limitation here, we only have mentioned analysis of some articles here and the rest are listed in APENDIX II. As it can be seen, facts and results sometimes have overlaps together.it should be considered that based on the type of the mandatory term used in each conclusion, it has been divided to four groups of Result (no mandatory term), Obligation(shall), Permission(may), Prohibition (shall not) and Recommendation(should). At the end we are reorganising and formalising the articles in number of related and extracted rules. Each rule is a combination of facts and conclusions. In this way, we have solved the complexity of articles of law and have made the understanding easier. We have indexed facts, conclusions and following rules by numeric assigns here and also based on if facts and rights belong to Law (L), Standard (S) and Guideline(G). The indexed system is used for referring in future chapters. Also reader should consider that since we have not explained the analysis of all the GDPR articles here, the numeric systems used for them may not be ascending.

- Article 4: Definitions

    1. *data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person*

1st.LFACT : The natural person is identified

2nd.LFACT :. The natural person can be identified

3rd.LFACT :. Identification is directly

4th.LFACT :. Identification is indirectly

5th.LFACT :. Identification is by means

6th.LFACT :. The mean is used by controller

7th.LFACT :. The mean is used by natural person

8th.LFACT :. Mean is used by legal person

9th.LFACT :. Identification is by reference to an identification number

10th.LFACT :. Identification is by reference to a location data

11th.LFACT :. Identification is by reference to an online identifier

12th.LFACT .: Identification is by reference to the- person physical factor(s)

13th.LFACT :. Fact12 is true regarding physiological, genetic, mental, economic, cultural and social identity of the person

LRESULT1st :. Natural person is a Data subject

1stLRULE :. 1st.LFACT ∧ 3rd.LFACT -> LRESULT1st

2ndLRULE : 1st.LFACT ∧ 4th.LFACT∧ 5th.LFACT ∧ 6th.LFACT ∧9th.LFACT-> **L**RESULT1st

3rdLRULE : 1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧10thL.FACT->LRESULT1st

4thLRULE :1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 11th.LFACT -> **L**RESULT1st

5thLRULE :1st.LFACT ∧4th.LFACT ∧ 5th.LFACT ∧6thL.FACT ∧ 12th.LFACT -> **L**RESULT1st

6thLRULE **:**1st.LFACT ∧ 4thL.FACT ∧ 5th.LFACT∧ 6th.LFACT ∧ 13thL.FACT -> LRESULT1st

7thLRULE **:**1stL.FACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 9th.LFACT ->L RESULT1st

8thLRULE **:**1stL.FACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 10th.LFACT ->**L**RESULT1st

9thLRULE **:**1st.LFACT ∧4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 11th.LFACT -> LRESULT1st

10thLRULE :1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 12th.LFACT -> LRESULT1st

11thLRULE **;**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 9th.LFACT ->LRESULT1st

12thLRULE **:**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 10th.LFACT -> LRESULT1st

13thLRULE :1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 11th.LFACT -> **L**RESULT1st

14thLRULE :1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8thL.FACT ∧ 13th.LFACT ->LRESULT1st

15thLRULE :1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 9th.LFACT -> LRESULT1st

16thLRULE **:**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 10th.LFACT -> LRESULT1st

17thLRULE **:**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 11th.LFACT ->L RESULT1st

18thLRULE **:**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 12th.LFACT -> **L**RESULT1st

19thLRULE :1st.LFACT∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 9th.LFACT -> LRESULT1st

20thLRULE **;**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 10th.LFACT -> **L**RESULT1st

21stLRULE **;**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 11th.LFACT -> **L**RESULT1st

22ndLRULE **;**2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 9th.LFACT ->LRESULT1st

23rdLRULE **:**2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 10th.LFACT -> LRESULT1st

24thLRULE : 2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 11th.LFACT -> **L**RESULT1st

25thLRULE : 2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 13th.LFACT -> **L**RESULT1st

26thLRULE :2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 9th.LFACT -> LRESULT1st

27thLRULE **:**2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 10th.LFACT -> LRESULT1st

28thLRULE :2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 11th.LFACT-> LRESULT1st

29thLRULE **:**2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 12th.LFACT -> **L**RESULT1st

30thLRULE :2nd.LFACT∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 9th.LFACT-> **L**RESULT1st

31stLRULE **:**2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT∧ 8th.LFACT ∧ 10th.LFACT-> **L**RESULT1st

32ndLRULE **:**2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT∧ 8th.LFACT∧ 11th.LFACT-> LRESULT1st

33rdLRULE :2nd.LFACT ∧ 4th.LFACT∧ 5th.LFACT∧ 8th.LFACT∧ 13th.LFACT -> LRESULT1st

34thLRULE :2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT∧ 8th.LFACT ∧ 9th.LFACT-> LRESULT1st

35thLRULE **:**2nd.LFACT∧ 4th.LFACT∧ 5th.LFACT ∧ 8th.LFACT∧ 10th.LFACT->LRESULT1st

36thLRULE **:**2nd.LFACT∧4th.LFACT∧ 5th.LFACT∧ 8th.LFACT∧ 11th.LFACT -> LRESULT1st

37thLRULE **:**2nd.LFACT∧ 4th.LFACT ∧ 5th.LFACT ∧ 8th.LFACT ∧ 12th.LFACT -> LRESULT1st

38thLRULE :2nd.LFACT∧ 4th.LFACT ∧ 5th.LFACT∧ 8th.LFACT ∧ 9th.LFACT-> **L**RESULT1st

39thLRULE **:**2nd.FACT∧ 4th.FACT ∧ 5th.FACT ∧ 8th.FACT∧ 10th.FACT -> RESULT1st

40thLRULE **:**2nd.FACT∧ 4th.FACT∧ 5th.FACT∧ 8th.FACT ∧ 11th.FACT-> RESULT1st

41stLRULE :2nd.LFACT ∧ 4th.LFACT ∧ 5th.LFACT∧ 8th.LFACT ∧ 13th.LFACT-> LRESULT1st

2. ‘*personal data’ means any information relating to a data subject*;

14th.LFACT . . Information relates to data subject

LRESULT2nd The information is personal data

42ndLRULE 14th.LFACT-> LRESULT2nd

As it is seen, we were able to decompose Article 4, the definition for data subject to numbers of simpler rules. Although the numbers are huge, but it is very easier and more understandable to read through each of them. Similar to article above, other definition articles are also analysed and provided in APENDIX II:

- *Article 2: This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal* *data which form part of a filing system or are intended to form part of a filing system.*

15th.LFACT : personal data is being processed (processor is processing personal data)

16th.LFACT : processing is wholly by automated means

17th.LFACT : processing is partly by automated means

18th.LFACT : processing is by other than automated means (processor is processing by other than...)

19th.LFACT : process form part of filling system

20th.LFACT : process is intending to form part of a filling system

LRESULT3rd : This Regulation applies to the processing of personal data

43rdLRULE : 15th.LFACT^ 16th.LFACT ->**L**RESULT3rd

44thLRULE : 15th.LFACT^ 17th.LFACT->**L** RESULT3rd

45thLRULE : 15th.LFACT^ 18th.LFACT ^19th.LFACT-> **L**RESULT3rd

46thLRULE : 15th.LFACT^ 18th.LFACT ^20th.LFACT-> LRESULT3rd

- *Article 5: Personal data must be:*

  a) *processed lawfully, fairly and in a transparent manner in relation to the data subject;*

15th.LFACT: personal Data is being processed (Processor is processing personal data)

1stLObligation : personal data shall be processed lawfully (processor has the obligation to process data lawfully)

2ndLObligation : personal data shall be processed fairly (processor has the obligation to process data fairly)

3rdLObligation : personal data shall be processed in a transparent manner in relation to the data subject (processor has the obligation to process personal data in a transparent manner …)

47thLRULE : 15th.LFACT -> 1stLObligation

48thLRULE : 15th.LFACT -> 2ndLObligation

49thLRULE : 15th.LFACT -> 3rdLObligation

- *Article 6:*

3- *Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of their personal data for one or more specific purposes;

21st.LFACT . data subject has given consent

22nd.LFACT. The consent is to the processing of personal data

23rd.LFACT . Personal data belongs to data subject

24th.LFACT . Processing of personal data is for one or more processing purposes

In most cases of laws, articles are in following of each other to provide further information how to perform previous articles by more detailed instructions. Here, Article 6 of Data Protection Regulation is an example of this case in which it applies more obligation in respect to article 5. As seen, it is providing more condition for a process of personal data to be lawful. However, to follow our analysing process, facts and obligations extracted from Aticle6 are confusing. In order to make the above facts and obligation more clearly and as previous permanent strategy, the introductory section (number 31) will be referred which makes a different in the facts and obligations as following. In fact, we are referring to cannons and history of law in order to interpret this article.

31-*In order for processing to be lawful, personal data should be processed on the basis of the consent of the person concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation*.

1stLObligation. Processing shall be lawful

25th.LFACT . Legitimate basis is laid down in this Regulation

26th.LFACT . Legitimate basis is laid down in Union Law

27th.LFACT . Legitimate basis is laid down in Member State Law

LRecommendation1st . Personal data should be processed on the basis of the data subject consent

LRecommendation2nd . Personal data should be processed on the basis of some legitimate basis

50thLRULE : 15th.LFACT ∧ 23rd.LFACT ∧ 21st.LFACTT ∧ 1stObligation -> LRecommendation1st

51stLRULE : 15th.LFACT ∧ 23rd.LFACT ∧ 24th.LFACT∧ 1stLObligation ->LRecommendation2nd

52ndLRULE : 15th.LFACT ∧ 23rd.LFACT ∧ 25th.LFACT∧ 1stLObligation -> LRecommendation2nd

53rdLRULE 15th.LFACT ∧ 23rd.LFACT ∧ 26th.LFACT∧ 1stLObligation -> LRecommendation2nd

The legitimate basis being mentioned above, indeed are the other rules of the article 6 (rules (b), (c) and (d)) which their irrelative scope to the application area here, made us to ignore them from further analysing.

- *Article 30:* Security of processing

1. *The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation*

4thLObligation . The controller has the obligation to implement appropriate technical measures

5thLObligation . The controller has the obligation to implement appropriate organizational measures

28th.LFACT . Technical measures are to be to ensure a level of security

29th.LFACT . Technical measures are to be appropriate to the risks

30th.LFACT . Risks are represented to the processing of personal data

31st.LFACT . Risks are represented to the nature of personal data to be protected

6thLObligation . The controller has the obligation to have regarded the state of the art (same for cost of implementation)

Facts 28,29,30,31 logically can be translated as obligations. Since the direct syntax of the above rule doesn't indicate this (using our analysis approach), we are using introductory part of 66 which has a simpler format to be analysed by our approach:

66. In order to maintain security and to prevent processing in breach of this Regulation, the controller or processor should evaluate the risks inherent to the processing and implement measures to mitigate those risks. These measures should ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks and the nature of the personal data to be protected. When establishing technical standard and organisational measures to ensure security of processing, the Commission should promote technological neutrality, interloper ability and innovation, and, where appropriate, cooperate with third countries.

32nd.LFACT . In order to maintain security

33rd.LFACT . Risks are inherent to the processing

7thLObligation . The controller (processor) has the obligation to evaluate the risks

8thLObligation . The controller (processor) has the obligation to implement risk mitigation measures

LRecommendation3rd . Security measures is recommended to ensure an appropriate level of security

LRecommendation4th . Controller is recommended to take into account the state of art

LRecommendation5th . Controller is recommended to take in to account cost of measure's implementation

34th.LFACT : cost of implementation is related to risk

35th.LFACT : cost of implementation is related to the nature of personal data processing

54thLRULE : 15th.LFACT∧ 32nd.LFACT ∧ 33rd.LFACT -> 7thLObligation

55thLRULE : 15th.LFACT∧ 32nd.LFACT ∧ 33rd.LFACT ^ 7thLObligation

-> 8thLObligation

56thLRULE : 8thLObligation → LRecommendation3rd

57thLRULE 8thLObligation→ LRecommendation4th

58thLRULE : 7thLObligation ∧ 34th.LFACT∧ 35th.LFACT → LRecommendation5th

In this section, we present the initial analysis on articles of General Data Protection Regulation 2012. In this way, we were able to represent the primary analysis method employed in our work in order to decompose complex sentences of laws to simpler rules consisting of facts and results. Results of rules consists of obligation, permission, prohibition and recommendations or results. The other advantage of lay analysis method used here, was to formalise legal sentences and also being able to conclude from a simple fact to number of obligations, recommendation, permissions and prohibitions instructed by law.

3.5.5 `Cellular Analysis of Legal Texts

As expressed before, legal rules and text are composed of ambiguity and complex elements. Although as explained before, a rule is categorised to three elements of testing (fact), result and casual term with an addition of exception element, but the work of analysis is not compressed to this. As it has been said a rule is a structured idea composed of different terms which the presence of all of them cause the result and the absence of one cause it's non-operation (Connelly, 2006). This fact is also true regarding other components of the rule such as the result. In fact, each and every word in a rule text is important and missing of their consideration in legal analysis fails the precise application of the law. In such cases enumeration adds clarity. In such a situation along from the existence of each word of a rule in its application, understanding the meaning of each of them play a key role in law analysis and application. To explain the problem, we use an example here. This example is taken from (Neumann, 2009):

Common law burglary is committed by breaking and entering the dwelling of another in the night-time with intent to commit a felony therein.

The testing elements of the above rule are enumerated as bellow:

1. A breaking
2. And an entry
3. Of the dwelling
4. Of another

5. In the night time

6. With intent to commit a felony therein

To examine the application of burglary rule and how laws are analysed by lawyers a case had been chosen from (Neumann 2009).

"Welty and Lutz are students who have rented apartments on the same floor of the same building. At midnight, Welty is studying, while Lutz is listening to a Radiohead album with his new four-foot speakers. Welty has put up with this for two or three hours, and finally she pounds on Lutz's door. Lutz opens the door about six inches, and, when he realizes that he cannot hear what Welty is saying, he, steps back into the room a few feet to turn the volume down, without opening the door further. Continuing to express outrage, Welty pushes the door completely open and strides into the room. Lutz turns on Welty and orders her to leave. Welty finds this to be too much and punches Lutz so hard that he suffers substantial injury. In this jurisdiction, the punch is a felonious assault. Is Welty also guilty of common law burglary?"

To find the answer to the question the author has used following reasoning and analysis by matching the enumerated elements of rule with the case facts (Neumann, 2009).

1. A breaking: if a breaking can be the enlarging of an opening between the door and the jam without permission, and if Lutz's actions do not imply permission, there was a breaking.

2. And an entry: Welty walked into the room therefore she "entered" for the purpose of the rule on burglary

3. Of the dwelling: Lutz's apartment is a dwelling

4. Of another: and it is not Welty's dwelling

5. In the night time; midnight is night time

6. With intent to commit a felony therein: did Welty intent to assault Lutz when she strode through the door? If not, this element is missing.

Giving another example which is an article of Netherland Civil Law also companies to the clarification of talking subject from other point of view:

Article 1401: every wrongful act, which brings damage to another, creates an obligation for the one whose guilt has caused this damage, to compensate it.

Applying the rule and interpreting it needs more consideration on the word "*act"* which has been accompanied by the adjective "*wrongful".* Therefore, this rule should apply to conditions where a wrongful act has occurred and it also has brought damage to other. The question which arises immediately is "when is an action wrongful?" to answer this question we need the definition of the word wrongful defined by other or same legal resources. The answer was found in Supreme Court of the state. Based on the definition, wrongful acts are specified to any actions against the law or actions that infringe somebody else's private right. Its definition later was extended by highest court of state as any action against good morals or against the care which should be exerted in social life towards another person or another's good (Holdeman, 2010).

Along from the mentioned reason to break fact and result of a law rule into its composing elements and extract key terms, as explained this task is also performed in order to solve the problem of legal ambiguity and to define and interfere legal terms based on other available legal resources. In classical view on law analysis as mentioned before, this is to satisfy processes 4,5,6 of law analysis procedure.

Although the methods discussed here are about legal analysis and reasoning applied in judgment and court decision making, the same techniques are used here in legal compliance as well since we think the nature of legal analysis is common between compliance and legal argument. The other reason of simulating lawyer's techniques here is the speciality and friction area of work regarding its social and legal effect. In the field of legal compliance, it is practiced to adopt laws to an application in order to avoid further legal punishments. In fact, it is an overtaking step behind referring a case to a court or related authority. Obviously it is beneficial to analyse and understand what laws require and apply it to practical environment in order to avoid any aftermaths.

In order to perform this stage of analysis, we need to extract key words or terms from facts and results. These words mostly include the ones with meanings that carry more information within them compared to other words in a sentence. In other word we select these words and terms in order to extract knowledge and meaning from them based on other compliance resources. Grammatically these words include any nouns and verbs in facts and results and include stakeholders of law, verbs and objects. An important and key step to identify and distinguish these words is to refer to Definitions of law and other compliance resources related to the law such as policies, guidelines and standards. Standards, guidelines and policies relevant to a law, often include common terms with the same or different syntax. For example, ISO 29100 which provides rules in support of Data Protection Act, use the term "*Personally Identifiable Information*" instead of "*Data Subject"* in GDPR and ISO 27000 series. It has been defined and explained in more detail in 29100 which can be used and referred from GDPR. In fact, this stage is a pre-step for next methods of law analysis as discussed before such as historical, policy and experimental analysis. Each of extracted words and terms will be defined in more details based on definitions from law, policy, standard, guideline or experimental resources or compliance will transfer to more application level using word's definitions from mentioned resources. We use the following example from GRDP Article to examine cellular analysis of law.

"The controller shall provide any information and any communication relating to the processing of personal data to the data subject in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child."

15th.LFACT: personal data is being processed

36th.LFACT There is some information

37th.LFACT There is some communication

38th.LFACT Information is related to the processing

39th.LFACT Communication is related to the processing

40th.LFACT Information addresses a child

9thLObligation controller shall provide information to the data subject

10thLObligation Controller shall provide information in intelligible form

11thLObligation controller shall provide communication to the data subject

12thLObligation controller shall provide communication in intelligible form

13thLObligation Form shall use clear language

14thLObligation Form shall use plain language

15thLObligation Language shall be adopted to data subject

59thLRULE 15th.LFACT ^ 36th.LFACT ^ 38th.LFACT -> L.9thObligation

60thLRULE 15th.LFACT ^ 37th.LFACT ^ 39th.LFACT -> **11**th.LObligation

61stLRULE 15th.LFACT ^ 36th.LFACT ^ **38**th.LFACT ^ 109th.LFACT -> 9th.LObligation

62ndLRULE 15th.FACT ^ **37**th.LFACT ^ 39th.LFACT ^ 109th.LFACT -> 11th.LObligation

63rdLRULE 9th.LObligation -> 10th.LObligation

64thLRULE 11th.LObligation -> **12**th.LObligation

65thLRULE 10th.LObligation -> **L.13th**Obligation

66thLRULE 12th,LObligation -> **13th**.LObligation

67thLRULE 10rd.LObligation -> 14th.LObligation

68thLRULE 13th.LObligation -> 15th.LObligation

69thLRULE 14th.LObligation -> **15th**.LObligation

Using the grammatical analysis of the text above and also referring to definitions from GDPR, ISO 29100, ICO and ISO 27000, we could extract following key words and terms and later refer to each of mentioned resources for more meaning and detail:

1. Controller
2. Data Subject
3. Process
4. child
5. Information
6. Communication
7. Intelligible form
8. Clear language
9. Plain Language

As It had been shown, any of the particular compositing elements of the guideline are actually providing a fact or obligation which their non-existence causes imprecise implementation of the law. For example, if the information is provided to the data subject in an intelligible form but it has not used a plain and also a clear language, the controller is not complying to its obligation to the data subject. Therefore, we need to understand the meaning of clear and plain language in detail in order to apply it in the form provided to the data subject.

3.5.6 Compliance Ontology

The process of Rule Analysis, is supported in our framework by a compliance ontology consisting of laws and regulations as reference of compliance. In an ontology, knowledge about a domain is modelled using a knowledge representation language with a reasoning mechanism. The knowledge representation languages such as RDF and OWL are used to create a set of terms as well as to specify classes, properties and relationships between classes and objects in the domain (Haarslev & Moller 2001). The basic building block of these languages is triples of subject-predicate-object which is called a statement. This is being represented as a relationship between two classes in the knowledge domain (class-objectproperty-class).

To have the classes, object and data properties in compliance ontology, also to make the triples of subject-predicate-object, the law analysis techniques explained in previous sections (Textual Analysis) are being used here. The parsed elements of rules of law (nouns, verbs) provide a thesaurus of legal concepts that are categorised in this ontology into number of classes and the relationship between them. Therefore, each statement consisting of above triple, models a fact, obligation, permission, prohibition or recommendation of a rule or statement either in law or regulation. According to our framework and as discussed before, Compliance Ontology refers to both law and Regulation. Based on our compliance process, the primary reference is to laws, and regulations (standards, guidelines and policies) will be referred later in the process of interfering and refining laws. Therefore, we provide discussions for Law Ontology in this section and Regulation Ontology in Laws Interpretation & Refinement Section.

3.5.6.1 Law Ontology

Here, in Law Ontology, we have two main types and levels of classes. First are those which are commonly used in any law being referred in this ontology. Therefore, we have high level classes of Legal-Actor and Legal-Object as general classes in this ontology. Nouns parsed from legal text are the resource for Legal-Actor and Legal-Object. Legal-Actors are stakeholders of law which the law imply a right to them. They are instructed to perform or not to perform an action, or are given some rights to be claimed of. Legal-Objects are some physical or non-physical resources which based on law, actions shall or may or should be performed on them. Second types of general classes are those which represent knowledge regarding the structure of laws in general. These classes include the Territory of law, Subject of law and Architectural structure of laws such as Chapters and Articles. Figure3.2 represents a schema of the first categorisation of classes in Law Ontology along with their links and relationships (object-properties). Second categorisation of classes are specifically dedicated to the type of law in this ontology.

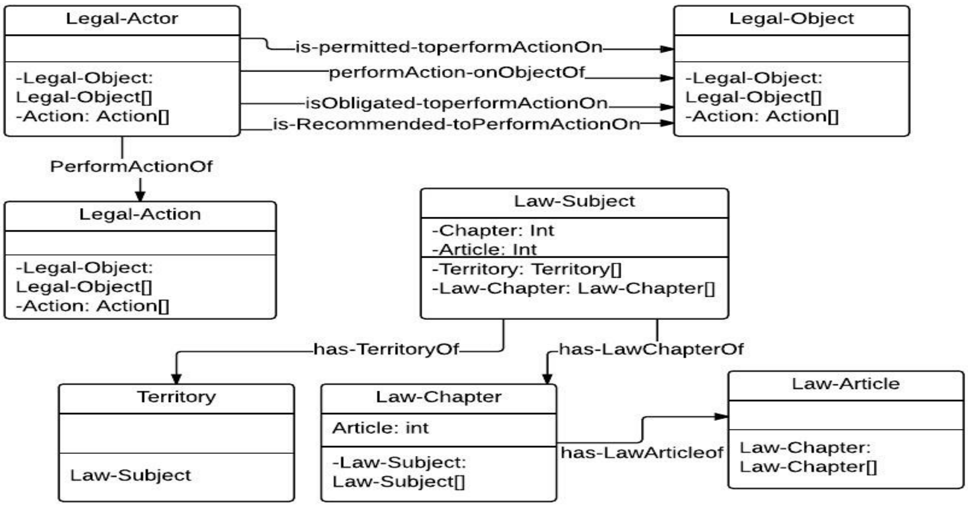


Figure3.2 . Law Ontology

Having above general classes and properties, Figure3.3 represents domain based classes based on articles from Data Protection domain, although the classes are not limited to these categories.

Since the focus of compliance in this research is on General Data Protection Regulation (GDPR) 2012, the second types of classes here are extracted from GDPR context. Based on GDPR, Law's stakeholders such as controller, data subject, processor, data representative and others are subclasses of the class Legal-Actor. Resources such as personal data, information, consent, contact detail, identity and others are under a general category of Legal-Object, but still are categorised to sub-classes of object based on their type (Figure3.4).

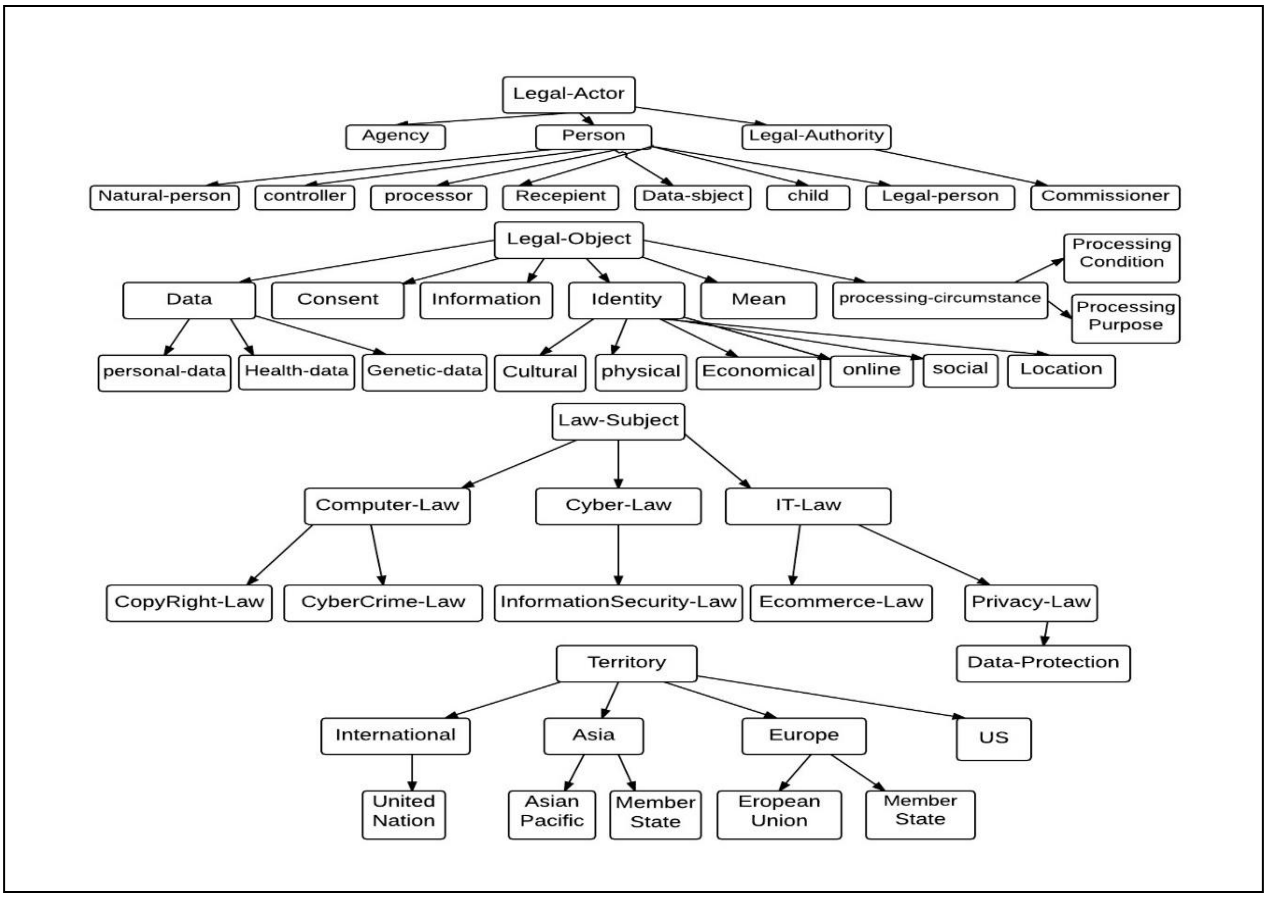


Figure3.3 . Class Hierarchy in Data Protection Ontology

These classes are related to each other through some object-properties which are the verbs we extracted from law's text. Facts, obligations, permissions, recommendations and prohibitions of law are drawn by connecting relating classes by object-properties. In a format of subject-predicate-object, the statements in Law Ontology are listed as six types of general statements as below. In order to make the obligations and other rights traceable, we are following the same indexing system used in previous sections:

General Statements:

- Obligation: Legal-actor isObligated-ByLaw-Art-ToperformAction-onObjectOf some object
- Permission: Legal-actor isPermitted-ToperformAction-onObjectOf some object
- Prohibition: Legal-actor isProhibited-ToperformAction-onObjectOf some object
- Recommendation: Legal-actor isRecommended-ToperformAction-onObjectOf some object
- Fact: Legal-actor performAction-onObjectOf some Legal-object
- Fact: Legal-object performAction-onObjectOf some Legal-object/Legal-Actor
- Fact: Law-Subject has-ChapterOf some Law-Chapter
- Fact: Law-Chapter has-ArticleOf some Article
- Fact: Law-Subject has-TerritoryOf some Territory

Examples:

- *Obligation: controller/processor 'is-obligated-ByDPA-Art5(a)-ToprocessLawfully-PersonalDataOf some Personal-Data*
- *.Obligation. The controller 'is-obligated-ByDPA-Art7(1)-To-bearBurderOfproof-forConsentOf'some consent*
- *Permission. Data-Subject isPermitted-ToWithdraw-ConsentOf Some Consent*
- *Prohbition. Controller isProhibitted-ToObtainAdditionalInformation-forIdentification of some identity*
- *Recommendation.. Controller/processor 'is-Recommended-ByDPA-Art6(1)To-ProcessOnBasisConsentOf-DataSubjectOf some Data-Subject*

- *Fact: Processor Process-PersonalDataOf some PersonalData*
- *Fact: Information is-RelatedTo-DataSubjectOf some Data-Subject*
- *Fact: DataProtection-Regulation-2012 has-ChapterOf Controller and Processor*
- *Fact: CONTROLLER AND PROCESSOR has-ArticleOf Responsibilit-of-Controller*
- *Fact: DataProtection-Regulation-2012 has-TerritoryOf EU*

3.5.6.2 Rules in Compliance Ontology

The compliance model contains a rule set that allows for rule-based reasoning in order to produce a legal reasoning infrastructure. This is to impose legal rights from articles of laws to the right stakeholders. As described and defined in previous sections, and as it is defined by legal professionals and researchers, analysis of law is about to find the application of a rule to a set of relevant facts (Connelly, 2013). A rule of law is a constitutional provision or a statute which as an enforcement statement establishes a standard of conduct. Legal reasoning and analysis answers to the question if the rule applies to the real case facts.

Several conditions are held in the body of rules. As a consequence of executing the rules, the rights of law are depicted on legal actors. For instance, as a consequence of executing a rule, a controller will have the obligation to process personal data lawfully.

Regarding above definitions, and considering the rule and reasoning infrastructure in ontology, we found a similarity between legal reasoning task and legal rules to ontological rules and reasoning technique. Therefore, we found an opportunity to model and formalise legal rules in ontological format. Extracted and listed Rules of law which had been mentioned in section 4.8 as further relationships between facts and conclusions of facts are drawn by Rules in ontology. A rule is used in ontology in order to make further relationships between statements. It is built from an antecedent which implies a consequent. Intuitively the meaning of a rule is: “whenever (and however) the conditions specified in the antecedent hold, then the conditions specified in the consequent must also hold” (Connelly, 2013, p. 91). The general format of a rule in ontology is as following:

Fact(s) -> consequence(s)

where both *antecedent* and *consequent* are conjunctions of atoms written $a_1 \wedge ... \wedge a_n$.

In ontology, facts and consequences are shown by connecting variables of related classes using object or data properties. Variables are indicated using the standard convention of prefixing them with a question mark (e.g.?x). Using this syntax, a rule asserting that the composition of parent and brother properties implies the uncle property would be written:

$$parent(?x,?y) \wedge brother(?y,?z) \Rightarrow uncle(?x,?z)$$

Following above formats and mapping them to Law Ontology, we were able to depict an ontological format for the rules from GDPR articles which had been analysed before. Based on the type of consequence, we have following categorisations for rules. For each category we have provided some examples from section 3.5.4 with their ontological formats:

- Obligation Rules: These rules indicate a duty and obligation on Legal-Actors or even objects in some cases.

47thLRULE: 14th.LFACT -> 1stLObligation

47thLRULE: *Processor(?x), process-PersonalDataOf(?x, ?z), process-processOf(?x, ?y) -> 'is- obligated-ByDPA-Art5(a)-To-processLawfully-PersonalDataOf'(?x, ?z)*

48thLRULE : 15th.LFACT -> 2ndLObligation

48thLRULE: *Processor(?x), process-PersonalDataOf(?x, ?z), process-processOf(?x, ?y) -> 'is-obligatedBy-DPA-Art5(a)-To-ProcessFairly-PersonalDataOf'(?x, ?z)*

50thLRULE: 15th.LFACT ^ 23rd.LFACT ^ 21st.LFACTT ^ 1stLObligation -> LRecommendation1st

50thRULE: *Processor(?x), 'is-obligated-ByDPA-Art5(a)-To-processLawfully-PersonalDataOf'(?x, ?z), process-PersonalDataOf(?x, ?z), process-PersonalDataOf-DataSubjectOf(?x, ?p), process-processOf(?x, ?y) -> 'is-obligated-ByDPA-Art6(1)To-ProcessOnBasisConsentOf-DataSubject'(?x, ?p)*

- Permission Rules

254rdLRULE: LRecommendation1st-> LPermission1st

254rdRULE: *has-given-ConsentOf(?x, ?y) -> 'is-permited-ByDPA-Art7(3)-To-withdraw-ConsentOf'(?x, ?y)*

- Prohibition Rules

255thLRULE: LPermission1st-> LProhbition1st

255thLRULE: *'is-permited-ByDPA-Art7(3)-To-withdraw-ConsentOf'(?x, ?y) ->*

is-prohibited-ByDPA-Art7(4)-notEffectTheLawfulnessOf-Process (?y,?z)

268thLRULE: 68th.LFACT ∧ ~58th.LFACT -> LProhbition2nd

268thLRULE: *RevealsRaceOf-DataSubject(?y,?w), has-given-ConsentOf(?x,?z) -> is-Obligated-NotToProcess-PersonalDataOf(?w,?y)*

- Recommendation Rules

50thLRULE: 15th.LFACT ∧ 23rd.LFACT ∧ 21st.LFACTT ∧ 1stLObligation -> LRecommendation1st

50thLRULE: *isProcessing-PersonalDataOf(?x,?y), belongTo-DataSubjectOf(??y,?z), hasGiven-Consentf(?x,?w),Is-ObligatedTo-ProcessLawfully-PersonalDataOf(?x,?y) -> is-ObligatedTo-ProcessBasedon-ConsentOf(?x,?w)*

- Definition Rules: These are the set of rules which represents definitions from law

43rdLRULE: 15thLFact ∧ 16thLFact16 -> 3thLResult3

43rdLRULE: *performed-ByProcessingMeanOf(?x, ?y), performed-onPersonalDataOf(?x, ?z)*

->Process(?x)

3.5.7 Application of Law to System Context:

The second stage in our compliance process is to apply analysed laws to system context. We have divided this process to numbers of steps as following sections. These involves to model the system context firstly in order to find a similar platform between system context and legal requirements and secondly to perform legal reasoning and map laws to system. Following sections explain these steps in more details:

3.5.7.1 Modelling System by i* Modelling Language:

Considering the main goal of this project which is to comply software systems with relevant legal demands, and regarding the main objectives of the proposed framework to begin the compliance process from the very early stages of software development, it is necessary to have a system modelling framework as the main body and component of the proposed framework in which laws can be applied to it later. As described in previous section, one of the critical actions in law analysis and law application is to find and map the facts of law in a case in order to apply and implement legal rules in that case. The process of legal reasoning finishes when its parsed elements are applied to the case, here the system context. To do this, parsed elements of the rule should be found and matched to system context. As the result obligation, permission and prohibition will be applied to system context. In this context each of subject arguments from facts along with heir coordinate operator and object argument (statement) should be first found and mapped into the system context.

As it has been also defined, from law commands legal relations between certain people are generated and those related, take part in the law, having rights (Neumann, 2009) to perform compliance in software development, a modelling component is required which itself has ability to represent the people and stakeholder aspect of system and social relationship between them. In this way, the system developer will be able to model the system and also model the legal relationship between system people at the same time. To answer this demand, it was required to investigate through system modelling languages which recognize the primacy of social actors and their relations. Among different approaches I* framework has been an attempt to introduce some aspects of social modelling and reasoning into information system engineering methods, especially at the requirement level which has stimulated considerable interest in a socially-motivated approach to system modelling and design (Neumann, 2009). I* brings social understanding into the system engineering process by putting selected social concepts into the core of daily activity of system analysers and developers by adopting a social ontology for the main modelling construct. In order to have the system context in a closer format to parsed elements of law and make the mapping process easier, we use i* which models the business processes of the system in format of its stakeholders (Actor) dependencies to other agents in order to achieve their Goals, perform their Task and access their Resources (Yu et al., 2010). i* modelling language is an agent oriented and goal-modelling approach to the early stages of requirement engineering, that is based on describing and analysing social relationships. One of the main reason of selecting i* approach for legal compliance is the fact that social models allow the human issues of security, privacy, and trust to be systematically analysed and addressed within an engineering process. In i*, security, privacy, and trust can be modelled initially as high-level soft-goals of some actors (Yu et al., 2010).

Traditionally, the task of the requirements analyst is to collect requirements statements from stakeholders: the customer and representatives of users. These statements say what the system should do (functionality) and at what levels of quality (non-functional properties such as performance, reliability, extensibility, usability, and costs). For large systems, there can be a large number of such statements coming from many stakeholders. The analyst aims to ensure that these statements are consistent (i.e., they do not contradict each other), complete (i.e., they fully reflect what the stakeholders are expecting from the system), and unambiguous (i.e., sufficiently precise so that they will not be misinterpreted by the developers) (Yu et al., 2010). i* Modelling language addresses issues that should come before the traditional requirements analysis activities, as said early requirements engineering which aim is to understand the underlying motivations and intentions behind the proposed system. In such a method, Intentional actors have wants and desires. They perform actions to fulfil their aims and desires. The central conceptual modelling construct in i* is actor. Actor refers to an active entity which is capable of performing some actions. The actor can be a human, software or hardware or even the combination. Since i* is an intentional modelling framework except from some other non-intentional frameworks such as UML and as its name (i*) stands for distributed intentionality, its other main focus is on the intentions which the actors want to achieve. These intentions can be addressed by number of questions such as; what does each actor want? how do they achieve what they want? Who do they depend on to achieve what they want? The intentions which actors want to achieve have been categorized in i* by concepts of goal, task and resource. In such a system, Actors do not exist in isolation. They exist in some shared environment with other actors, and interact with each other. They relate to each other at an intentional level. Thus their interactions are not predefined sequences of actions and reactions, but are coordinated through their respective wants, desires, and commitments. These interactions are represented in i* Model as dependencies of actors to each other in order to fulfil their desires and tasks.

As said, as far as i* focus on aspects of being social, actually it defines the well-being of an actor as its dependencies to other actors, as saying they depend on each other to achieve goals, to perform tasks, and to furnish resources. The dependencies in i* are depicted in two different networks of *Strategic Dependency (SD)* and *Rational Dependency (RD)*. SD is a network of directed dependency relationship among the actors. A dependency link indicates that one actor (the depender) depends on another (the dependee) for something (the dependum). Depends on if the dependum is stated as an assertion, activity or an entity or material object, it defines *Goal Dependency, Task Dependency or Resource Dependency.* In goal dependency, the depender wants the dependee to makes the assertion true without specifying the methods to achieve the goal. Therefore, the dependee is free to adopt any course of action to achieve the goal. Types of different dependency relationship provide a way to convey the kinds of freedom allowed in a relationship. This may be done by dependee taking a task dependency to perform the action depending on other actors. It also may be conveyed by taking resource dependency or soft-goal dependency in which the dependum is a quality such as fast, secure or others.

A goal dependency is the highest level of an agent desire in i*. A goal may be soft or hard, depending on whether it indicates a functional or non-functional requirement of the agent. At the refinement stage, an agent may adopt task dependency or resource dependency in order to satisfy its goal or task. Other tasks, goals and resources may also decompose a task. In such a systematic approach that utilizes concepts of Actor, Goal, Task and Resource, the requirement engineer is able to progress through an incremental process of system requirements. Figure 4.4, 4.5, 4.6, 4.7, 4.8 and 4.9 represents a graphical model of the concepts available in i* Modelling language (I* WiKi).

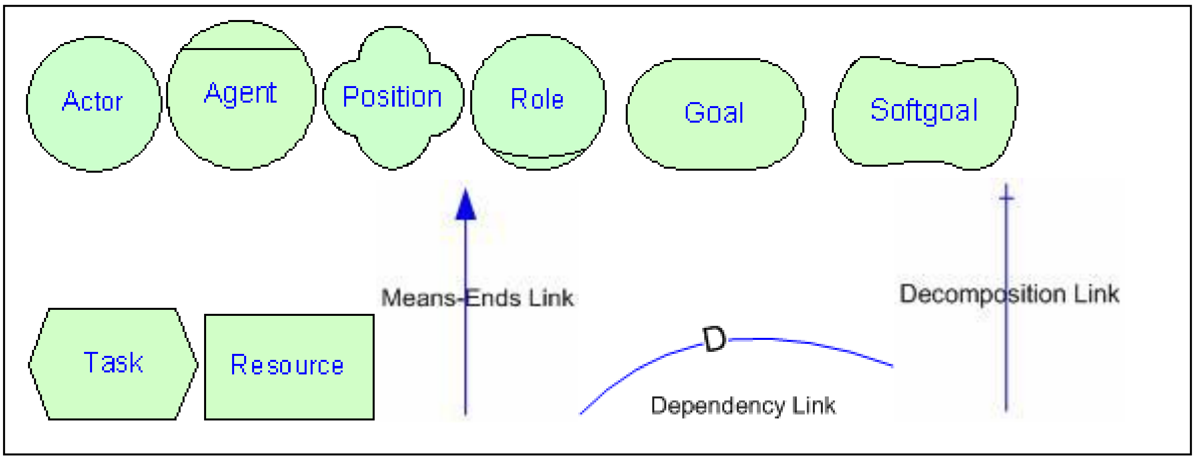


Figure3.4 . i* Concepts

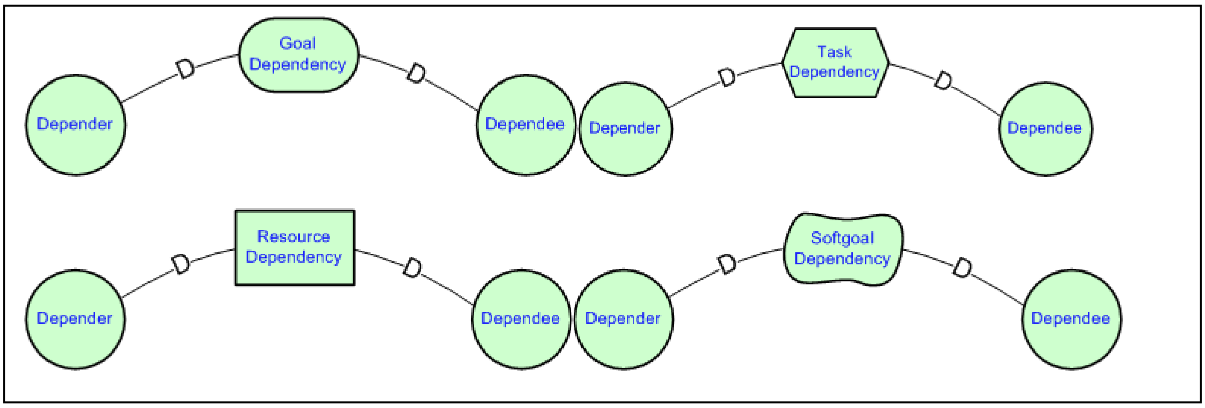


Figure3.5 . i* Dependency

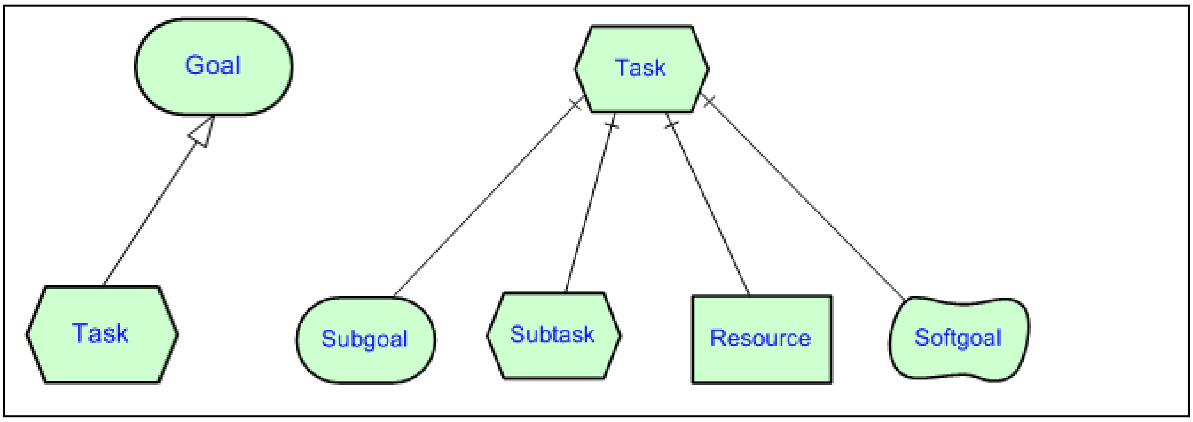


Figure3.6 .i* Means-end & Decomposition Links

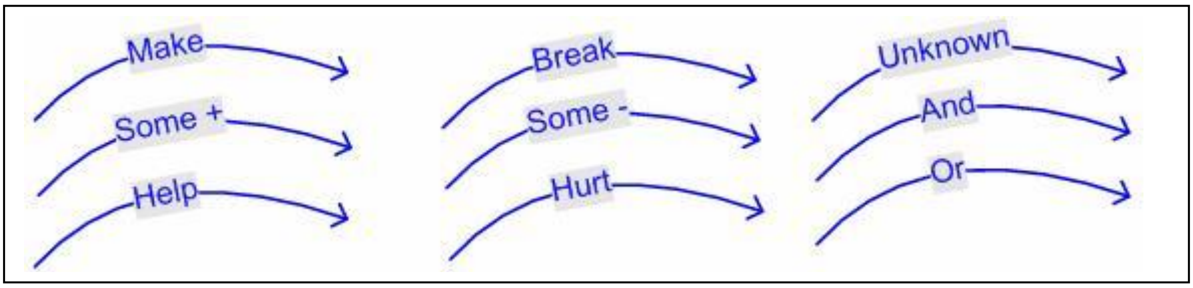


Figure3.7 . i* Contribution Links

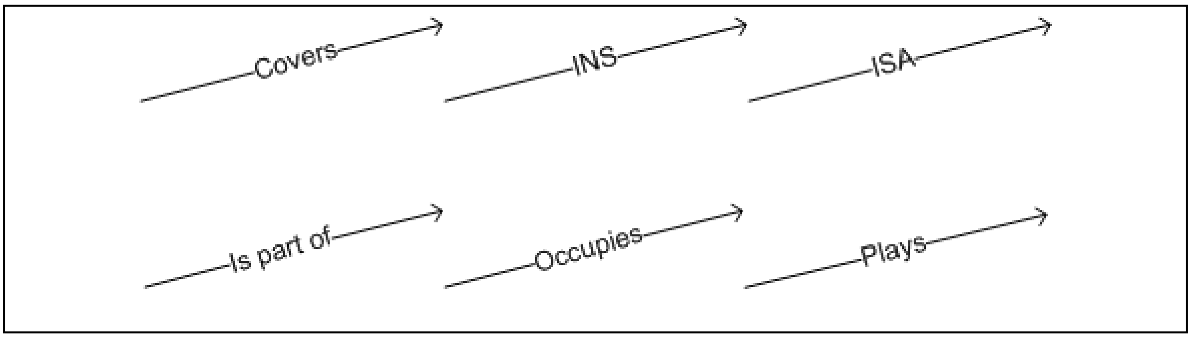


Figure3.8 . i* Actor Association Links

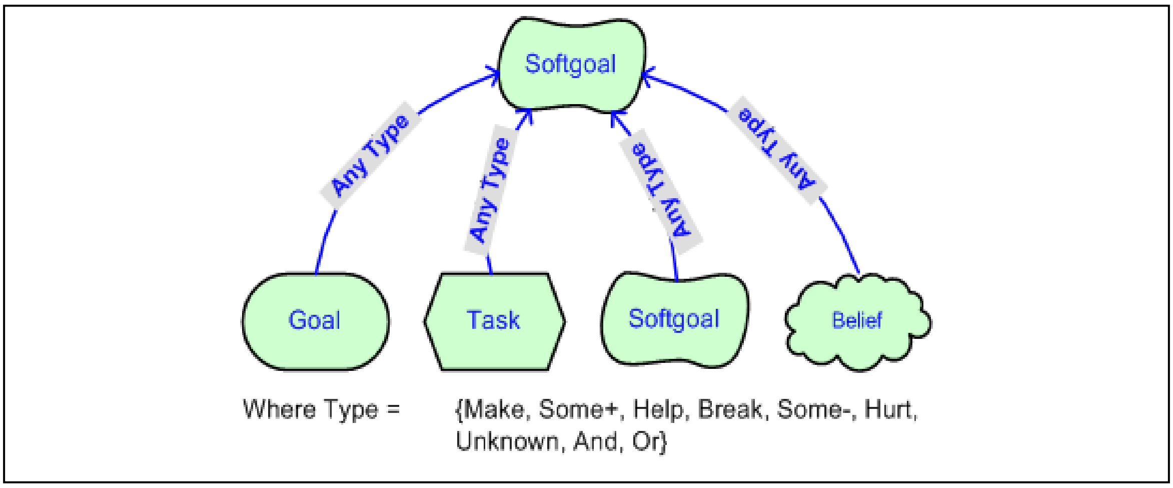


Figure3.9 . i* Softgoal Contributions

As said, we have two types of diagrams in i*, or to say early requirements of system are depicted in two different stages and strategy in i*. *Strategy Dependency (SD) Model* in which the network of intentional, strategic relationships among actors are drawn. And Strategic Rational (SR) Model in which the actors with the SD model are "opened up" to show their specific intentions. Since our aim is to define an ontology model of concepts in i* in later stages of this research, and as far as we need to represent the i* knowledge in form of triple of subject-predicate-object, we found concepts from SR closer to the triple form and will consider SR as the i* reference model in our ontology. Therefore we are considering following concepts in SR (I* WiKi):

- Goal (Hard-goal): Represents and intentional desire of an actor, the specifics of how the goal is to be satisfied is not described by the goal. This can be described through task decomposition.

- Soft-goals are similar to (hard) goals except that it addresses non-functional requirements of system such as security, quality and etc. The means to satisfy such goals are described via contribution links from other elements.

- Task: The actor wants to accomplish some specific task, performed in a particular way. A description of the specifics of the task may be described by decomposing the task into further sub-elements.

- Resource: The actor desires the provision of some entity, physical or informational. This type of elements assumes there are no open issues or questions concerning how the entity will be achieved.

- Means-end: These links indicate a relationship between an end, and a means for attaining it. The "means" is expressed in the form of a task, since the notion of task embodies how to do something, with the "end" is expressed as a goal. In the graphical notation, the arrowhead points from the means to the end.

- Decomposition: A task element is linked to its component nodes by decomposition links. A task can be decomposed into four types of elements: a sub-goal, a subtask, a resource, and/or a soft-goal - corresponding to the four types of elements. The task can be decomposed into one to many of these elements (I* WiKi):

- Contribution: the link represents different ways in which a goal may contribute in achievement of its super-goal. To do so we have following types of contributions:

  2. Make: A positive contribution strong enough to satisfice a soft-goal.

  3. Some+: Either a make or a help contribution, a positive contribution whose strength is unknown

  4. Help: A partial positive contribution, not sufficient by itself to satisfice the soft-goal.

  5. Unknown: A contribution to a soft-goal whose polarity is unknown.

  6. Break: A negative contribution sufficient enough to deny a soft-goal.

  7. Some-: Either a break or a hurt contribution, a negative contribution whose strength is unknown

  8. Heart: A partial negative contribution, not sufficient by itself to deny the soft-goal

  9. OR: The parent is satisfied if any of the offspring are satisfied.

  10. AND: The parent is satisfied if all of the offspring are satisficed

- Association: These types of link represents relationship between actors as following:

  1. Is-part-of: Roles, positions, and agents can each have subparts

  2. ISA: The ISA association represents a generalization, with an actor being a specialized case of another actor

  3. Play: The plays association is used between an agent and a role, with an agent playing a role. The identity of the agent who plays a role should have no effect on the responsibilities of that role, and similarly, aspects of an agent should be unaffected by the roles it plays

4. Occupy: This link is used to show that an agent occupies a position, meaning that it plays all of the roles that are covered by the position.

5. INS: This association, represents instantiation and is used to represent a specific instance of a more general entity.

3.5.8 i* Modelling Ontology

A unique ontology is considered in our model in order to support i* system modelling component of our framework, also to perform the task of legal reasoning (Law application) by making a connection between two ontologies of i* and Law (Generally Compliance Ontology). Fig3.10 represents the taxonomy of i* as it is developed as a component of our compliance framework in i* ontology. Considering the concepts of i* Modelling Language in previous section, and the fact that we have two categories of concepts in i* as elements and links, we have totally 4 classes, 5 sub-classes and 70 object-properties in i* ontology (matrix of links & classes). The primitives in the category hierarchically of classes include actor, goal, task and resource concepts.

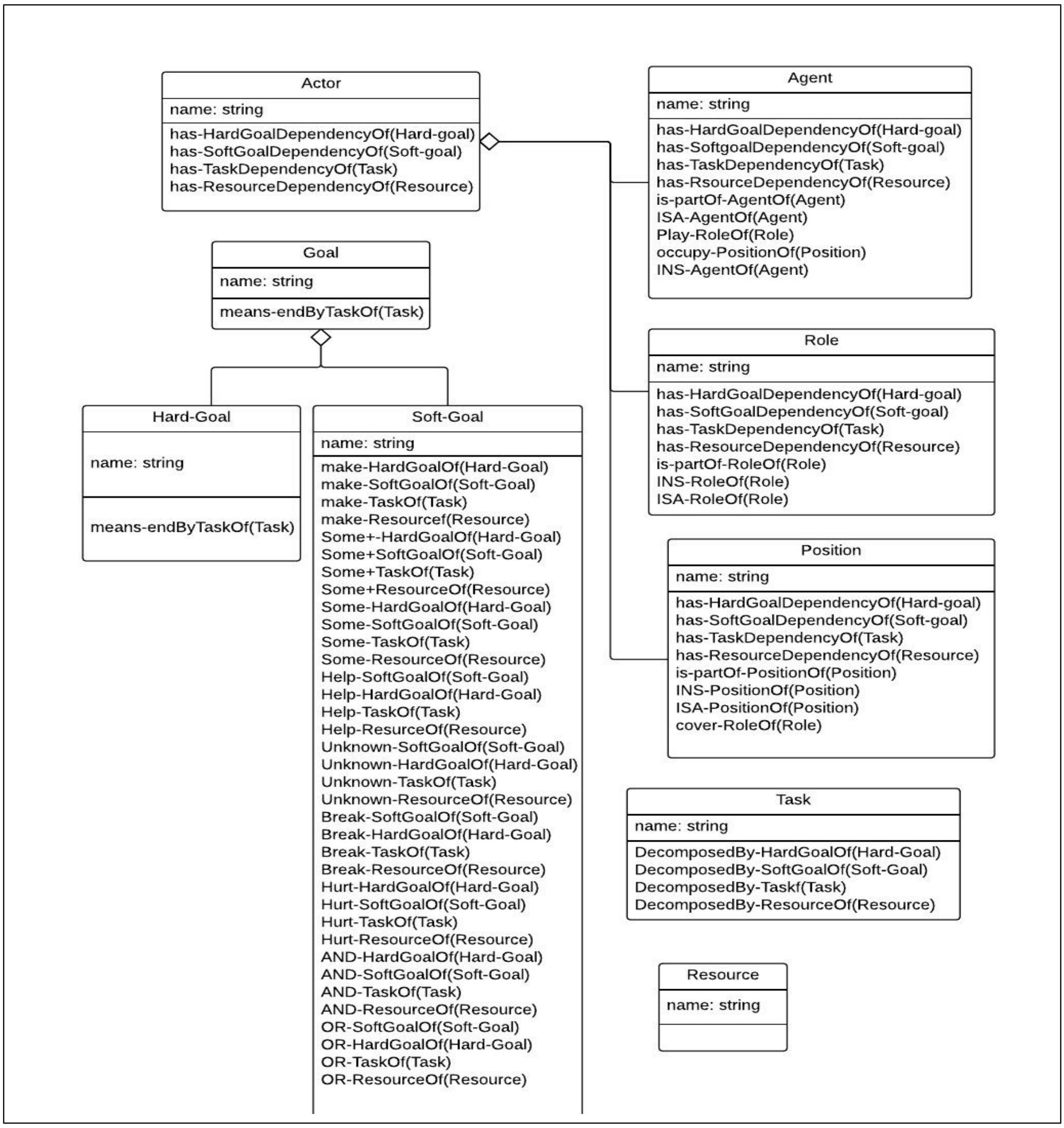

Actor
name: string
has-HardGoalDependencyOf(Hard-goal)
has-SoftGoalDependencyOf(Soft-goal)
has-TaskDependencyOf(Task)
has-ResourceDependencyOf(Resource)
Agent
name: string
has-HardGoalDependencyOf(Hard-goal)
has-SoftgoalDependencyOf(Soft-goal)
has-TaskDependencyOf(Task)
has-RsourceDependencyOf(Resource)
is-partOf-AgentOf(Agent)
ISA-AgentOf(Agent)
Play-RoleOf(Role)
occupy-PositionOf(Position)
INS-AgentOf(Agent)
Goal
name: string
means-endByTaskOf(Task)
Role
name: string
has-HardGoalDependencyOf(Hard-goal)
has-SoftGoalDependencyOf(Soft-goal)
has-TaskDependencyOf(Task)
has-ResourceDependencyOf(Resource)
is-partOf-RoleOf(Role)
INS-RoleOf(Role)
ISA-RoleOf(Role)
Hard-Goal
name: string
means-endByTaskOf(Task)
Soft-Goal
name: string
make-HardGoalOf(Hard-Goal)
make-SoftGoalOf(Soft-Goal)
make-TaskOf(Task)
make-Resourcef(Resource)
Some+-HardGoalOf(Hard-Goal)
Some+SoftGoalOf(Soft-Goal)
Some+TaskOf(Task)
Some+ResourceOf(Resource)
Some-HardGoalOf(Hard-Goal)
Some-SoftGoalOf(Soft-Goal)
Some-TaskOf(Task)
Some-ResourceOf(Resource)
Help-SoftGoalOf(Soft-Goal)
Help-HardGoalOf(Hard-Goal)
Help-TaskOf(Task)
Help-ResurceOf(Resource)
Unknown-SoftGoalOf(Soft-Goal)
Unknown-HardGoalOf(Hard-Goal)
Unknown-TaskOf(Task)
Unknown-ResourceOf(Resource)
Break-SoftGoalOf(Soft-Goal)
Break-HardGoalOf(Hard-Goal)
Break-TaskOf(Task)
Break-ResourceOf(Resource)
Hurt-HardGoalOf(Hard-Goal)
Hurt-SoftGoalOf(Soft-Goal)
Hurt-TaskOf(Task)
Hurt-ResourceOf(Resource)
AND-HardGoalOf(Hard-Goal)
AND-SoftGoalOf(Soft-Goal)
AND-TaskOf(Task)
AND-ResourceOf(Resource)
OR-SoftGoalOf(Soft-Goal)
OR-HardGoalOf(Hard-Goal)
OR-TaskOf(Task)
OR-ResourceOf(Resource)
Position
name: string
has-HardGoalDependencyOf(Hard-goal)
has-SoftGoalDependencyOf(Soft-goal)
has-TaskDependencyOf(Task)
has-ResourceDependencyOf(Resource)
is-partOf-PositionOf(Position)
INS-PositionOf(Position)
ISA-PositionOf(Position)
cover-RoleOf(Role)
Task
name: string
DecomposedBy-HardGoalOf(Hard-Goal)
DecomposedBy-SoftGoalOf(Soft-Goal)
DecomposedBy-Taskf(Task)
DecomposedBy-ResourceOf(Resource)
Resource
name: string

Figure3.10 .i* Ontology Classes

The children categories of goal entity as soft-goal and hard-goal share common characteristics but are otherwise heterogeneous. Same is true regarding sub-classes of actor as agent, role and position. Different types of dependencies between i* concepts are drawn as object properties which relates types of classes. Refinement levels of goal and task (means-end, decompose) are also available as properties. Associate links between actors are also considered as object-properties

Considering different types of relationships between i* ontology, different types of object-properties are available in i* ontology. Following ontological statements represents the types of triples in i* Ontology:

- Dependency:

    1. *Soft-Goal Dependency: Actor has-SoftGoalDependencyOf some Soft-Goal*

    2. *Hard-Goal Dependency: Actor has-HardGoalDependencyOf some Hard-Goal*

    3. *Task Dependency: Actor has-TaskDependencyOf some Task*

    4. *Resource Dependency: Actor has-ResourceDependencyOf some Resource*

- *Means-end: Hard-Goal means-endByTaskOf some Task*

- *Decomposition:*

1. *Task decompositedBy-HardGoalOf some Hard-Goal*

2. *Task decompositedBy-SoftGoalOf some Soft-Goal*

3. *Task decompositedBy-TaskOf some Task*

4. *Task decompositedBy-ResourceOf some Resource*

- *Contribution:*

    1. *ISA:*

        a) *Agen ISA-AgentOf some Agent*

        b) *Role ISA-RoleOf some Role*

c) *Position ISA-PositionOf some Position*

2. *Is-part of:*

   a) *Agent Is-partOf some Agent*

   b) *Role Is-partOf some Role*

   c) *Position Is-partOf some Position*

3. *INS:*

   a) *Agent INS-AgentOf some Agent*

   b) *Role INS-RoleOf some Role*

   c) *Position INS-PositionOf some Position*

4. *Play-RoleOf: Agent Play-RoleOf some Role*

5. *Cover-RoleOf: Position cover-RoleOf some Role*

6. *Occupy-PositionOf: Agent ocuppy-PositionOf some Position*

In run time situation each of i* ontology classes should be instanced by individuals from system context and relationships between them should be constructed using mentioned object-properties. As the result the system is modelled and ready to be used for the purpose of compliance and law application. It should be considered that the process of system modelling is a continuous process in which different levels of requirements will be depicted in different stages until the phase where the developing system is discovered. After system discover, system analysis by i* model still will continue to discover system requirements. Regarding no further relationship on mentioned properties, we do not have ontology rules in i* ontology.

3.5.9 Legal Reasoning

Having the laws analysed and the system modelled with mentioned concepts from i*, the next stage will be to apply laws to the modelled system. In other word, nouns and verbs from law facts should be found and matched to actors, goals, tasks and resources in the system context modelled by i*. First of all, and as most important committals of this stage, it is important to find out if the law is related and applicable to the developing system. One of the most determining factors of this purpose is the experience of the system developer and his/her knowledge of the law and specially its material and territorial scope. Since the goal here is to introduce a general compliance framework which addresses mostly non-experienced developers, we do not trust on the experience of the developers but will use the experience of smart developers as a determining factor in this stage. For example, in the context of the case study of developing an ecommerce system, based on previous experiences we know that Data Protection laws apply to e-commerce systems which deal with customer’s personal data processing. For this purpose, we have a specific component in our framework which is taking advantage of previous experiences regarding related laws and regulations to scope of any software system. This component also helps the design of system and extracting details requirements using design patterns. This part will be discussed in future chapters. In this component software systems are categorised and listed based on different types of information systems as web application, data base, Educational systems, financial systems and others. Each types of these system may also be categorised to other types such as ecommerce as a type of web application. Each category has been defined to have number of related laws to be complied. In this way we are using available experiences and knowledge in order to find relevant regulatory to each type of IS. In such a way developer can have a list of complying laws to system context without further efforts.

The other determining factor is the context of the law itself. There is a part in each law regarding the scope of law which generally determine the applicable areas of the law. This is being used to confirm the validity of previous experiences to determine complying laws. For this reason, developer should refer to a part of law which is often called material and territory scope of law. Material scope determine the main business where laws apply and territory is related to the geographic authority of law application. When the general scope of law application is identified, the next step will be to determine the application of each rule of law to details of business processes of system.

As explained before the facts of rules are actually conditions and criteria for the related rights and predicates or in other word they are the application areas of laws. From other point, the goals, tasks and resources of system actors modelled by i* are the facts in the environment of the system which are happening in real world and business process of the system. In other word, the law is applicable in a part of system where the exact facts or their synonym are found in the list of system goals, tasks or resources. It was described in Section 3.5.6 how facts and rights of rule of law are decomposed to cellular elements. To perform the general and detailed application of law, the task will be to map and match these elements to modelled system concepts in i*. In this way nouns are mapped to actors, objects and resources in modelled system and verbs to goal and task dependencies and other links. Figure 3.11 illustrates the application of article 14 of GDPA using i* graphical objects to explain how the process works. The application process is also explained in this section.

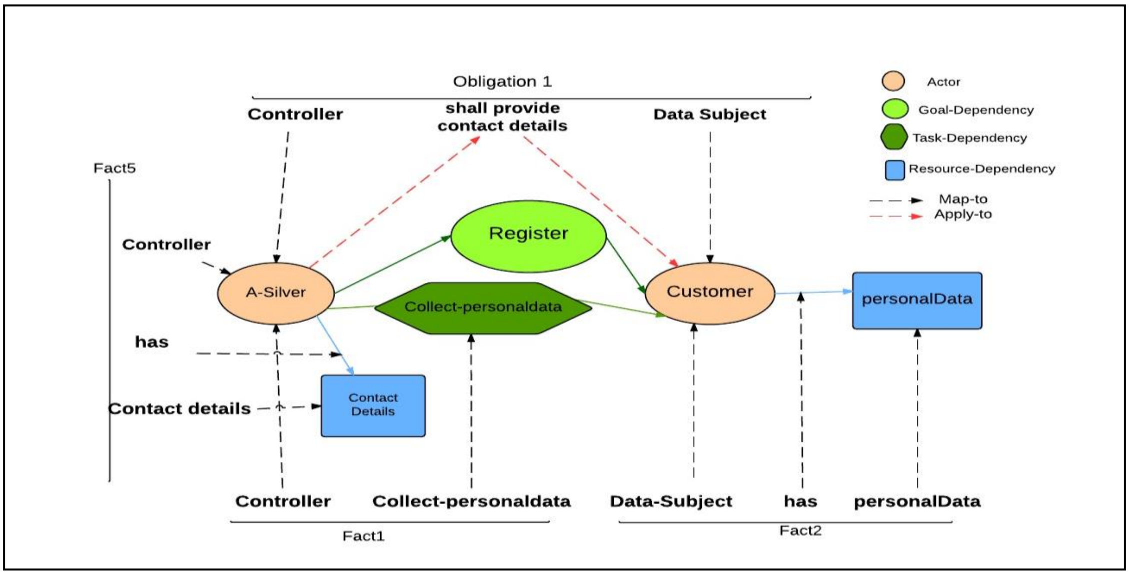


Figure3.11 . Application of GDPA Article 14 to Esilver Case

To examine the explained processes of law application, we are giving a short example here. We refer to analysed elements of some Articles of General Data Protection Regulation from. The rest of law application process examination are also mentioned in APENDIX II. The process of law application logically and based on discussed matters, should start from the articles related to scope of law and definitions in order to find out if the whole scope of law applies to our case study.

Article 2: Material Scope

“This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.”

Article 3: Territorial Scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.

2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the Union; or

(b) the monitoring of their behaviour.

As explained in Section 3.5.6, the above text was analysed and following facts, result and rules were concluded:

15th.LFACT: personal data is being processed (processor is processing personal data)

16st.LFACT: processing is wholly by automated means

17nd.LFACT: processing is partly by automated means

18rd.LFACT: processing is by other than automated means (processor is processing...)

19th.LFACT: process form part of filling system

20th.LFACT: process are intend to form part of a filling system

21th.LFACT. Processing of personal data is in context of some activities

22th.LFACT. Controller is performing the activities

23th.LFACT. Processor is performing the activities

24th.LFACT. Controller is established in the Union

25th.LFACT. Processor is established in the Union

26st.LFACT: Data subject resides in Union

27nd.LFACT: processing is related to the offering of goods or services to data subjects

28rd.LFACT: processing is related to monitoring of data subject behaviour

29th.FLACT. The processing takes place within the Union

30th.FACT. The processing does not take place within the Union

250stLRULE: 15th.LFACT ∧ 18th.LFACT∧ 25th.LFACT ∧ 21th.LFACT ^ 31th.LFACT ->**L**RESULT7th

251ndLRULE: 15th.LFACT ∧ 21th.LFACT∧ 22th.LFACT ∧ **24**th.LFACT ^ **32**th.LFACT -> **L**RESULT7th

252rdLRULE: 15th.LFACT ∧ 23th.LFACT∧ 25th.LFACT ∧ 21th.LFACT ^ 31th.LFACT ->**L**RESULT7th

253thLRULE: 15th.LFACT ∧ **23**th.LFACT∧ 25th.LFACT ∧ 21th.LFACT ^32th.LFACT ->**L**RESULT7th

To understand the precise meaning of the above text in case of the reader not being familiar with concepts of Data-subject, processor, controller or personal data, he/she should refer to the part of law consisting the definitions of the law in order to find the matching objects in system context. Therefore, the law application process of law scopes needs to be interrupted by application of definitions to system context. The task of applying definitions to system context is a parallel task in which each definition is depended on other definitions.

Article 4: Definitions

Definition2: personal data: *'personal data' means any information relating to a data subject;*

14th.LFACT. Information relates to data subject (data subject has information)

LRESULT2nd. The information is personal data

42ndLRULE: 14thLFact14-> LRESULT2nd

Considering the resources of *customer-name and customer-ContactDetails* in our system modelled by i* and following resource dependencies, result2 will be concluded:

ESilver-Customer has-ResourceDependencyOf customer-name ->

Data-subject has personal-data

Customer-name *is* personal-data

Information is personal-data

Definition3; data subject: *'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;*

1st.LFACT. The natural person is identified (controller/processor identify the natural-person)

4th.LFACT. Identification is indirectly

5th.LFACT. Identification is by means

6th.LFACT. The mean is used by controller/processor (controller/processor use the mean)

11th.LFACT. Identification is by reference to an online identifier-

LRESULT1st: Natural person is a Data subject

9thLRULE**:**1st.LFACT ∧4th.LFACT ∧ 5th.LFACT ∧ 7th.LFACT ∧ 11th.LFACT -> **L**RESULT1st

Esilver-company has-TaskDependencyOf identify ESilver customer ∧

Controller identify the natural-person

Identify-the customer decomposedBy-ResourceOf Internet ∧

Identification is-By mean

Identify-the customer decomposedBy-SoftGoalOf indirectly-identification ∧

Identification is indirectly

Esilver-company has-GoalDependncyOf use-Internet ∧

Controller use-the Mean

Identify-the customer decomposedBy-ResourceOf IP-Address →

Identification is by reference to online-identifier

Esilver-Customer is Data-subject

Natural-person is Data-Subject

At this point, having the definitions of law existed in our system context, we are able to proceed the process of law application of articles of law to system context.

250stLRULE: 15th.LFACT ∧ 23th.LFACT∧ 25th.LFACT ∧ 21th.LFACT ∧ 31th.LFACT ->**L**RESULT7th

Esilver-Staff has-TaskDependencyTo collect-Customer'sPersonaldata ∧

Processor collect personal data

Collect-CustomerPersonaldata is-decomposedByResourcef Esilver-Website-RegistrationFormPage

Processing is wholly by automated means

∧ keep-CustomerPersonaldata means-endWithTaskOf collect-Customer'sPersonaldata ∧

Processing of personal-data is in contextOf some activity

Esilver-company has-goalDependencyTo keep-CustomerPersonaldata ∧

Controller performs operations on personal data

Esilver-company has-goalDependencyTo establish-in-Italy →

Controller is established in Europe

Data-Protection-Regulation applies to collect-Customer'sPersonaldata

Data Protecction Regulation applies to processing-of-personaldata

The context of the case study of B-Silver Company as the controller indicates that the company is established in Italy and also the processing of personal data regarding its physical branches or the website itself, all are occurring within the Union scope. Therefore, the facts of above predicate are valid here and the regulation applies wherever personal data is being processed. Since the designing website of B-Silver is desired to promote its products internationally, the question will be if the law has considered protection guards for international customer personal data as well. First of all, the direct context of article3 has not specified any special categories of data subject and it means protection of all type of data subject's personal data are covered by law. Also clause 12 of introductory section has clearly described the case as "The protection afforded by this Regulation concerns natural persons, whatever their nationality or place of residence, in relation to the processing of personal data". Therefore, following facts also can be added to rules regarding application of law.

41st.LFACT The data subject may have any nationality

42nd.LFACT The data subject may have any place of residence

Comparing the scope of law and context of e-commerce system dealing with customers and their personal data, it can be concluded that the law should be applied on any place of system where the personal data is being processed. Followings are indicting that the regulation applies to any point of system context where personal data is being processed. We refer to Figure4.11 and search through the traditional and system requirements among goals, task and resources to match and compare them to scope of law. The below list is the matching context from modelled law:

Membership-creator has-TaskDependencyOf record customer personal data

Processor processing data subject personal data

ESilver-company has-TaskDependencyOf transfer customer personal data to third parties
Processor prcs ds pd

ESilver-website has-TaskDependencyOf receive user-credentials

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf receive customer personal data

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf save customer personal data

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf represent customer personal data

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf retrieve customer personal data (from database)

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf delete customer personal data

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf track customer visited websites

Prsr prcs ds pd

ESilver-website has-TaskDependencyOf send payment confirmation to the customer

Prsr prcs pd ds

Esilver-website has-TaskDependencyOf collect-customer'sWeb-surfing-behaviours

Prsr prcs ps

Collect-customer'sWeb-surfing-behaviour is-decompositedByResourceOf cookie

PS is-performedBy mean

As it is approved above, the fact of article 2 of the regulation regarding material scope of law and the application of the law wherever personal data is being process was valid. The last two facts from system context as mentioned above, which are regarding collecting customers web surfing behaviors using website cookie, makes a confusion if the law should apply here or not.

Web surfing behavior is some information related to customer, therefore it should be personal data. But the introductory section of 24, has other guidelines about using cookies as following:

24. “*When using online services, individuals may be associated with online identifiers provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. It follows that identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances*.”

As far as this case is confusing regarding if the information saved in cookies and used by web server is personal data and should be complied with the regulation, further requirements are required. Obtaining these information requires using of another component of our framework which will be explained in future sections. Thus, we follow by applying other articles of GDPR.:

Article5. Principles relating to personal data processing

- *Article 5: Personal data must be:*

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

15th.LFACT: personal Data is being processed (Processor is processing personal data)

1stLObligation: personal data shall be processed lawfully (processor has the obligation to process data lawfully)

2ndLObligation: personal data shall be processed fairly (processor has the obligation to process data fairly)

3rdObligation: personal data shall be processed in a transparent manner in relation to the data subject (processor has the obligation to process personal data in a transparent manner …)

47thLRULE: L15th.FACT -> 1stLObligation

48thLRULE: 15th.LFACT -> 2ndLObligation

49thLRULE: 15th.LFACT -> 3rdLObligation

Esilver-Staff has-TaskDependencyOf collect-Customer’sPersonaldata →

Processor collect personal data

Esilver-Staff has-obligationTo process fairly customer's pesonaldata ∧

Processor has obligation to process personal data fairly

Esilver-Staff has-obligationTo process lawfully customer's pesonaldata ∧

Processor has obligation to process personal data fairly

Esilver-Staff has-obligationTo process customer's pesonaldata in transparent to customer ∧

Processor has obligation to process personal data in transparent to data subject

Article6: lawfulness of processing

Processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

(a) The data subject has given consent to the processing of their personal data for one or more specific purposes;

23th.LFACT. Personal data belongs to data subject

1stLObligation: personal data shall be processed lawfully (processor has the obligation to process data lawfully)

25nd.LFACT. Legitimate basis is laid down in this Regulation

26rd.LFACT. Legitimate basis is laid down in Union Law

27th.LFACT. Legitimate basis is laid down in Member State Law

LRecommendation1st. . Personal data should be processed on the basis of the data subject consent

LRecommendation2nd. Personal data should be processed on the basis of some legitimate basis

50thLRULE: 15th.LFACT ∧ 23rd.LFACT ∧ 21st.LFACT ∧ 1stLObligation -> LRecommendation1st

51thLRULE: 15th.LFACT ∧ 23rd.LFACT ∧ 24th.LFACT∧ 1stLObligation ->LRecommendation2nd

Above article is in following of previous article to process lawfully. In fact, this is defining further condition for a lawful process. Therefore, the application area in system context is as it was for obligation1.

Esilver-Staff has-TaskDependencyOf collect-Customer’sPersonaldata ∧

Processor collect personal data

Esilver-Staff has-obligationTo process lawfully customer’s pesonaldata ∧

Processor has obligation to process personal data lawfully

Esilver-customer has-ResourceDependencyOf Customer’s personal data →

Data-subject has personal data

Esilver-Staff has-obligation-To process Customer’s personal data on basis of consent

Processor has obligation to process personal data on basis of consent

Any of resulted rights (obligation, permission, prohibition, and recommendation) may result to a new goal, task or resources in system context in order to implement them.

Esilver-customer has-TaskDependencyOf give consent

Esilver-website has-ResourceDependencyOf consent-form-page

Give-consent is-decomposedBy-HardGoalOf accept consent conditions

Accept-consent-condition meansEndBy-TaskOf sign consent

Esilver-customer has-TaskDependencyOf sign consent

Article 30: Security of processing

The controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected, having regard to the state of the art and the costs of their implementation.

32rd.LFACT. In order to maintain security

33th.LFACT. Risks are inherent to the processing

7thLObligation. The controller (processor) has the obligation to evaluate the risks

8thLObligation. The controller (processor) has the obligation to implement risk mitigation measures

LRecommendation3th. Security measures is recommended to ensure an appropriate level of security

LRecommendation4th. Controller is recommended to take into account the state of art

LRecommendation5th. Controller is recommended to take in to account cost of measure's implementation

34th.LFACT: cost of implementation is related to risk

35th.LFACT: cost of implementation is related to the nature of personal data processing

15th.LFACT: personal data is being processed

54thLRULE: 15th.LFACT∧ 32nd.LFACT ∧ 33rd.LFACT -> 7thLObligation

55thLRULE: : 15th.LFACT∧ 32nd.LFACT ∧ 33rd.LFACT ^ 7thObligation

-> 8thObligation

56thLRULE 8thLObligation → LRecommendation3rd

57thLRULE 8thLObligation→ LRecommendation4th

58thLRULE : 7thLObligation ∧ 34th.LFACT∧ 35th.LFACT → LRecommendation5th

Esilver-Staff has-TaskDependencyOf collect-Customer'sPersonaldata ∧

Processor collect personal data

Esilver-Staff has-SoftGoalDependencyOf maintain security ∧

Processor wants to maintain security

Eavesdropping-risk hurt Collect-Customer's Personal data →

Risk are inherit to processing

Esilver-staff has obligation to evaluate the risk of eavesdropping

Processor has obligation to evaluate risk

Esilver-staff has obligation to evaluate the risk of eavesdropping ∧

Processor has obligation to evaluate risk

Eavesdropping-risk hurt Collect-Customer’s Personal data ∧

Risk are inherit to processing

Esilver-Staff has-TaskDependencyOf collect-Customer’sPersonaldata ∧

Processor collect personal data

Encryption mitigates eavesdropping ∧

Measure mitigates risk

Esilver-staff has obligation to evaluate the risk of eavesdropping →

Processor has obligation to evaluate risk

Esilver-staff has obligation to implement measures

Processor has obligation to implement risk mitigation measures

The last number of obligations and rights implemented to system context will be considered in our risk assessment component n details later, here we have an introduction to them but later these requirements will be integrated with requirements from risk assessment.

As explained, we were able to apply rules of law which we were able to analyse them before in to right points of system context. Sometimes to do (so as some examples showed), there are confusion in application area regarding the ambiguity and general language of law. To solve this problem terms of law should be interpreted in more details with usage of other components of our framework or system context may requirement more technical analysis. These all will be discussed din future sections of this chapter.

3.5.10 Design ontology

In previous section we explained how previous experiences in both development and compliance domains, helps the process of compliment. The knowledge and experience of developer support to find out the relevant laws to context of different types of information system, even to application points of system. We are providing a component for our framework here which supports and implement elements of experience in compliance process names as Developing System Ontology. In this ontology experimental knowledge is represented using two models. The first relates different types of information system to their related laws and regulation. The second model helps to elicit design and implemental requirements refined from legal requirements using design and security patterns. Figure 3.12 is showing different classes in this ontology along with their object properties.

One of the oldest and most widely used systems for classifying information systems is known as the pyramid model (Laudon & Laudon, 1988). The categorisation is based on the fact that different kinds of systems found in organizations exist to deal with the particular problems and tasks that are found in organizations. Consequently, most attempts to classify Information systems into different types rely on the way in which task and responsibilities are divided within an organization. As most organizations are hierarchical, the way in which the different classes of information systems are categorized tends to follow the hierarchy. This is often described as "the pyramid model" because the way in which the systems are arranged mirrors the nature of the tasks found at various different levels in the organization (Laudon & Laudon, 1988). The categorisation in our ontology model is also based on pyramid model.

Each of above classes of system, have their own sub-classes which are different categories of each type.

As shown in Fig 3.12, classes in this ontology all inherit three types of object-properties. The first one is an outer-link relationship which relates classes of this ontology to class of Law-Subject in Law Ontology. The second object-property is also an inner-link relationship in which system types are related to relevant patterns in order to support the design and elicitation of more technical requirements refined by legal requirements. The last one is also an outer-link connecting classes here to class of Territory in Law & Regulation Ontologies. The reason of using this object-property is to identify the geographic area of system establishment in order to find relevant laws in that area. This process is performed by number of rules in ontology as some samples are mentioned below:

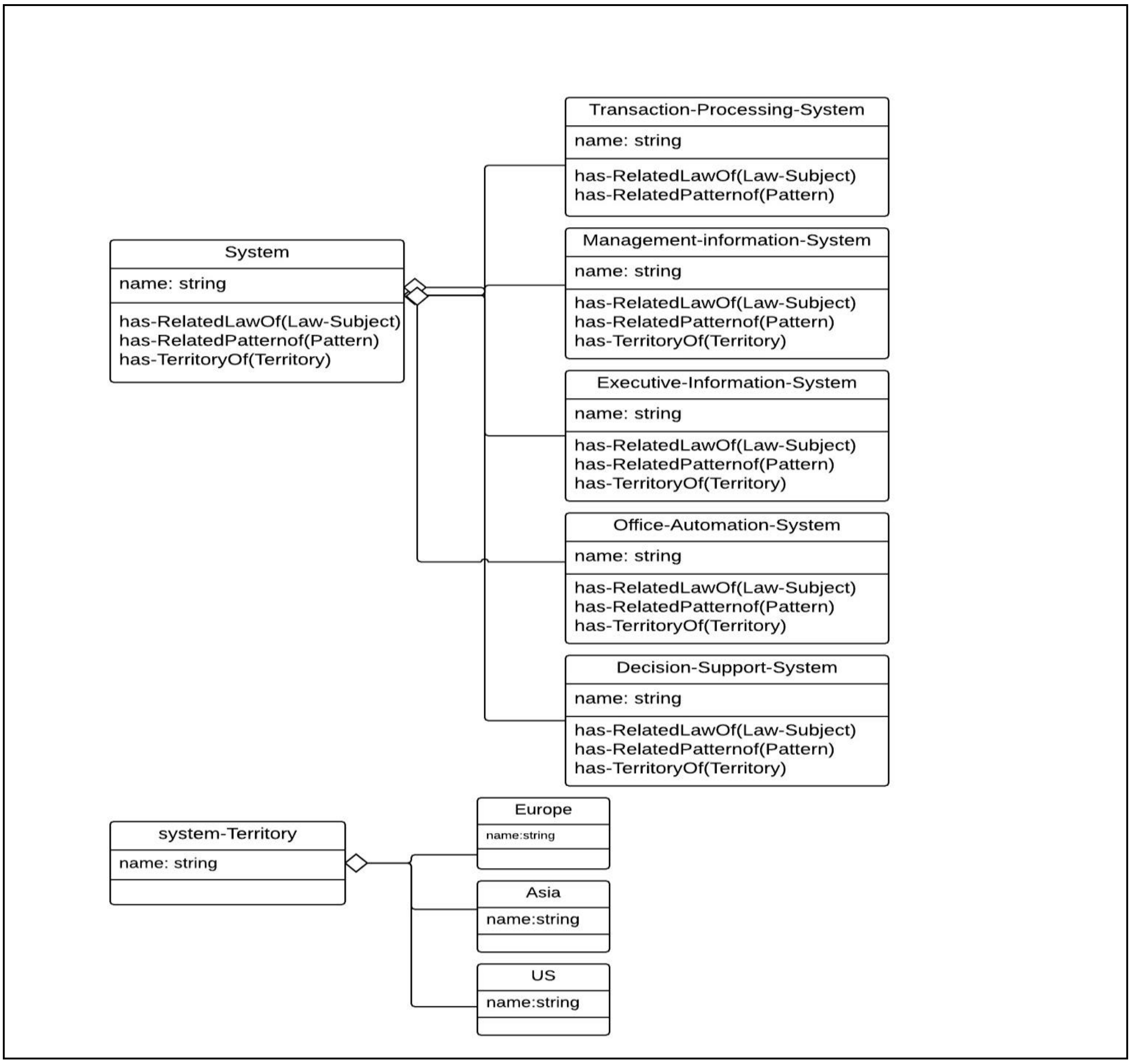

Transaction-Processing-System
name: string
has-RelatedLawOf(Law-Subject)
has-RelatedPatternof(Pattern)
Management-information-System
name: string
has-RelatedLawOf(Law-Subject)
has-RelatedPatternof(Pattern)
has-TerritoryOf(Territory)
System
name: string
has-RelatedLawOf(Law-Subject)
has-RelatedPatternof(Pattern)
has-TerritoryOf(Territory)
Executive-Information-System
name: string
has-RelatedLawOf(Law-Subject)
has-RelatedPatternof(Pattern)
has-TerritoryOf(Territory)
Office-Automation-System
name: string
has-RelatedLawOf(Law-Subject)
has-RelatedPatternof(Pattern)
has-TerritoryOf(Territory)
Decision-Support-System
name: string
has-RelatedLawOf(Law-Subject)
has-RelatedPatternof(Pattern)
has-TerritoryOf(Territory)
system-Territory
name: string
Europe
name:string
Asia
name:string
US
name:string

Figure3.12 . Developing System Ontology

- Related-Law :

  System has-RelatedLawOf some Law-Subject

- Territory:

  System has-TerritoryOf some Territory

- Pattern

  System has-RelatedPatternOf some Pattern

- Rules:

  — Ecommerce (?x), has-TerritoryOf(?x,'European-Union') ->

    has-RelatedLawOf (?x,'DataProtectionRegulation-2012')

  — Sale-Management-System(?x), has-TerritoryOf(?x,'UK') ->

    Has-RelatedLawOf(?x,'DataProtectionAct-1998')

  — Ecommerce (?x), has-TerritoryOf(?x,'UK') ->

    has-RelatedLawOf (?x,'EcommerceRegulation-2002')

The application of current ontology is in a stage of system modelling when traditional and classic requirements are depicted and system to be developed is identified. The system type can be discovered in two levels. First is the very beginning stage of system design where for example we know tht we need to design an ecommerce. Second stage is after a circle of requirement analysis. In this stage requirements will be designed by patterns related to a system. Regarding the Esilver case, when it is discovered that the developer or system-user is considering to design an ecommerce for company business, following relationships help developer to identify types of laws and patterns related to ecommerce:

- Esilver-website has-TerritoryOf some Europe ->
- Esilver has-RelatedLawOf DataProtectionRegulation-2012
- Esilver-website has-PatternOf some UI-Pattern

3.5.11 Law Application by Ontological Individuating System and Reasoner

One of the best advantages of using ontology in compliance and legal domains, along from the huge knowledge repository that it provides, is its usage in the process of law application. Ontology provides an infrastructure in which each types of its classes can be instanced by individuals from different cases. In fact, each class defines a set of individuals which inherit all the attributes and properties from class. Individuals are the last in their heretical and cannot be instanced anymore. For example, in Family Ontology, general statements and rules are constructed in order to define family relationships such as *woman is-motherOf some person or person has-parentOf some person.* In case of Johnson *family* these statements are instanced with individuals from Johnson family such as Anna *is-motherOf Adam and Adam has-parentOf David.*

As explained before in the process of law application, laws apply where their facts are existed. Facts of law rules are explained in a genera language. In legal reasoning rule's facts are mapped and matched to case studies and the result is judges based on rights of rule. To perform this process in ontology, each facts classes should be instanced by individuals from case study and related object-properties relates these classes in order to makes the fact statements. Finally, ontological reasoner decides automatically if all elements of facts are instanced with individuals meaning that the fact is available and result to the application of rights of law. This is exactly performing the task of mapping facts elements (arguments, operators) to system context as explained in previous section. Following examples from Esilver case and using the format of ontological rules as explained before help to clarify the subject matter:

- Processor (Esilver-staff), process-PersonalDataOf (Esilver-staff, Customer-personldata), process-processOf (Esilver-staff, collect-personaldata)

-> 'is-obligated-ByDPA-Art5(a)-To-processLawfully-PersonalDataOf'(?Esilver-staff, Customer-personaldata)

- Processor (Esilver-staff), process-PersonalDataOf (Esilver-staff, Customer-personaldata), process-processOf (Esilver-staff, collect-personaldata) -> 'is-obligatedBy-DPA-Art5(a)-To-ProcessFairly-PersonalDataOf'(Esilver-staff,Customer-personaldata)

- Processor (Esilver-staff), 'is-obligated-ByDPA-Art5(a)-To-processLawfully-PersonalDataOf'(Esilver-staff, Customer-personaldata), process-PersonalDataOf(Esilver-staff, collect-personaldata), process-PersonalDataOf-DataSubjectOf (Esilver-staff, Esilver-customer) -> 'is-obligated-ByDPA-Art6(1)To-ProcessOnBasisConsentOf-DataSubject'(?Esilver-staff, Esilver-customer)

- is-obligated-ByDPA-Art6(1)-To-ProcessOnBasisOf-DataSubjectConsentOf'(Esilver-staff, Esilver-customer) -> 'is-obligated-ByDPA-Art7(1)-To-bearBurderOfproof-forConsentOf'(Esilver-staff, Esilver-customer)

As talked before, these individuals are coming from system context modelled by i*. In other word they are goals, tasks, actors and resources in i*. In ontology classes are provided along with their all object and data properties. Task of developer will be to first have a knowledge of these classes and properties, look and search into system goals, task, resource and actors and where available individual Law & Regulation ontology classes by i* model individuals. In this way system contexts elements are both individuals of i* and Law & Regulation ontologies.

A semantic reasoner or rules engine is able to infer logical consequences from a set of asserted facts or axioms. Pellet (Sirin & Parsia, 2004) is an open source, Java reasoner for OWL ontologies which we are using in this work. It provides standard and cutting-edge reasoning services and can be used with both Jena (McBride, 2002) and OWL API libraries to provide reasoning. It provides functionalities to see the species validation, check consistency of ontologies, classify the taxonomy and check ontologies (Sirin & Parsia, 2004). Here in our work, pellet reasoner also helps to perform the task of legal reasoning and result from available facts filled by individuals from system context to rights from rules in order to apply rights at correct points of system.

Other usability of reasoner in our work is in refinement and interpretation of legal terms or policy terms and mapping and integrating components of framework together which will be discussed in future sections. In fact, reasoner works based on some description logic operators as mapping, integration, inheriting and refinement. As seen in Figure3.2 the components in our framework are connected to each other using some relations such as mapped, integrated, and refined and etc.

3.5.12 Laws Interpretation & Refinement

To perform similar interception to examples above, legal authorities use three different methods of analysis as grammatical (to find the semantic meaning), historical (to investigate the history of the institution) and teleological (aiming at social goals). As explained in Section 4.8 different law analysis methods are available which some have been mentioned as Historical analysis and Policy Analysis. In these methods, other legal resources such as cannon of laws or policies related to the law are used in order to analyse and interpret legal terms in order to find out their definitions and meaning in details. We are using same methods in our approach by adding further components to our framework. Historical analysis in our approach has been explained in previous sections by usage of definitions and introductory sections of each law in order to understand the meanings behind each article of law. Policy analysis is employed in our work using other components from local authority guidelines and standards. We found these resources as the most valid and trustable references for legal interpretation, also for legal refinement. As far as compliance is to find practical solution for legal requirements, mentioned references can be used as more detailed and further requirements of system in refinement of legal requirements. In this way critical legal terms are being defined and refined by mentioned resources. Obligations, permissions and prohibitions extracted from legal texts, should be refined and composed to application level requirements to complete the compliance process. In this stage, quality of legal requirements is dealt more than the quantity. To do this, other components of the framework such as Standards and Local Authority Guidelines are referred to obtain more detailed requirements of the system. This being done through a hierarchy process based on the abstraction level of the resource. The application of this stage is also exercised using the same case study of B-Silver, and refining Obligation1 of Article 14 by guidelines from ISO/IEC 29100 and ICO. Using semantic web, makes a suitable infrastructure in which each class and concept and property in Law & Regulation ontology can be traced by its URL to its definitions by standard and guidelines components. Therefore, an ontology is also considered for each of these components. Same is true regarding definitions and refinement of terms in standards and guidelines which can be referred to other components such as patterns. This is where using Description Logic Operations in ontology such as refinement, mapping and others makes sense. This will be discussed in detail in future sections.

In next sections, we are explaining standards and authority guidelines being used in our framework as separate components in order to interpreted and refine legal terms.

3.5.13 Refinement and Interpretation by Standards

The activity to drive or refine further requirements of system is a task to be performed in order to gather, specify, analyse, and validate a subset of system requirements prior to system implementation and verification. The high level requirements of the system and its stakeholders found in previous stage of analysis are decomposed to more sufficient detailed requirements in order to validate system developers with the system requirements. This is the stage of requirement engineering where sub-requirements will be determined. The type of task which performs the process of requirement refinement is also supported in various system analysis methodologies. For example, this is done in i* by number of defined relations between i* concepts such as *decompose*, *means-end* and others which refined stakeholder goals and task by number of other goals or tasks. Since the purpose here is compliance and we are looking for a systematic and static simulating component for our framework, and also based on market and business demand in compliance, international tools such as ISO standards is selected here to refine legal requirements of laws to further detailed requirements. In fact, the usage of ISO in its type is not a must here. It absolutely depends on the complying law to select a relevant standard or guidelines from an according providing body. Since ISO is the most valuable and known international standard with a comprehensive list of available standards in different felids, it has been used here as a sample of refinement reference.

ISO; the International Organization for Standardization and IEC; the International Electro Technical Commission which their technical committees collaborate in field of mutual interests, together form the specialised system for worldwide standardization. ISO/IEC 27000 series of standards were prepared by Joint Technical Committee (ISO/IEC JTC 1) in 2005 with the purpose to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS). The reason of selecting these series of standards which are specialized on information security as a reference at this point of work, is the requirement of one of the most important obligations of General Data Protection Regulation to protect the security of personal data collected by data controllers. In fact, by studying and analysing ISO 27000 series, we are refining the principle of GDPR as mentioned in section 2 of the regulation titled as Data Security.

This model incorporates the features on which experts in the field have reached a consensus as being the international state of the art. ISO 27000 series help organisations through design and implementation of their ISMS (Information Security Management System) by number of defined security requirements and a process approach based on PDCA Model (Plan, Do, Check, Act). Although the ISMS solution by ISO/IEC series covers all types of organizations regardless of type, size and nature, but they should be scaled and implemented in accordance with the needs and size of the organisation. The security requirements designed by ISO 27000 series, are provided by number of defined security controls customized to the needs of organisations. To describe the whole structure of ISO 27000 series, this is sufficient to mention that the series include number of standards each focused on a specific area of information security. Table3.2 has listed the series standards with their focused area of information security:

STANDARD	AREA
ISO/IEC 27000	Overview and vocabulary
ISO/IEC 27001	Requirements
ISO/IEC 27002	Code of practice for information security management
ISO/IEC 27003	Information security management system implementation guidance
ISO/IEC 27004	Information security management — Measurement
ISO/IEC 27005	Information security risk management
ISO/IEC 27006	Requirements for bodies providing audit and certification of information security management systems
ISO/IEC 27007	Guidelines for information security management systems auditing
ISO/IEC 27008	Guidance for auditors on ISMS controls
ISO/IEC 27010	Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	Information security management guidelines for telecommunications organizations
ISO/IEC 27013	Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
ISO/IEC 27014	Information security governance
ISO/IEC 27015	Information security management guidelines for financial services
ISO/IEC 27031	Guidelines for information and communication technology readiness for business continuity
ISO/IEC 27032	Guideline for cyber security
ISO/IEC 27033-1	Network security - Part 1: Overview and concepts
ISO/IEC 27033-2	Network security - Part 2: Guidelines for the design and implementation of network security
ISO/IEC 27033-3	Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
ISO/IEC 27033-5	Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
ISO/IEC 27034-1	Application security - Part 1: Guideline for application security
ISO/IEC 27035	Information security incident management

ISO/IEC 27036-3	Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

Table3.2 .ISO 27000 Series of Standards

Since the limit of this project does not allow the full study of all series of ISO 27000, we only examine one or two ISO standard here as samples. Our selection criteria are their close matter of subjects to the context of the project here. ISO 27000 as an introductory to the series is important to be studied. ISO 27003 is useful to give implementation guidelines and 27034 is important since it provides guidelines for application security. 27034 is focusing on the importance to consider security requirements from application design level. ISO 27000 is a general and very high level guideline document which guides organization how to generally implement an Information Security Management System (ISMS) using the ISO controls provided in the rest of the 27000 series. It also has vocabulary of terms used in the whole series. In definition of Data Protection, we also found ISO 29100 which is specially considered for compliance and refinement of Data Protection laws. "This International Standard provides a high-level framework for the protection of personally identifiable information (PII) within information and communication technology (ICT) systems. It is general in nature and places organisational, technical, and procedural aspects in an overall privacy framework."(International Organisation of Standardisation. Privacy Framework). Therefore, at the start point of Data Protection requirement's refinement we have selected ISO 29100 **.** Privacy framework described in ISO 29100, is based on some components related to the privacy of personal data processing as following (International Organisation of Standardisation-Information technology, 2013):

- Actors and roles: For the purposes of this standard, it is important to identify the actors involved in the processing of PII.

- Interactions: The actors identified in the previous clause can interact with each other in a variety of ways.

- Recognizing PII: To determine whether or not a natural person should be considered identifiable, several factors need to be taken into account. In particular, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to identify that natural person.

- Privacy safeguarding requirements: The purpose of this clause is to provide an overview of the different factors that can influence the privacy safeguarding requirements that are relevant to a particular organization or privacy stakeholder processing PII.

- Privacy policies: The top management of the organization involved in the processing of PII should establish a privacy policy

- Privacy controls: Organizations should identify and implement privacy controls to meet the privacy safeguarding requirements identified by the privacy risk assessment and treatment process

- Privacy Principles: The privacy principles described in this standard were derived from existing principles developed by a number of states, countries and international organizations. This framework focuses on the implementation of the privacy principles in ICT systems and the development of privacy management systems to be implemented within the organization's ICT systems. These privacy principles should be used to guide the design, development, and implementation of privacy policies and privacy controls. Additionally, they can be used as a baseline in the monitoring and measurement of performance, benchmarking and auditing aspects of privacy management programs in an organization

The strategy in our approach to comply with ISO is to explain incoherent and unclear concepts from laws with definitions from standards. As standards define terms and concepts of laws in more detail, we almost have same or synonym terms in laws and standards. Standards are also textual documents which include mandates on stakeholders, we use the same analysing techniques as used for laws here as well. Although this is mentioned that the standard itself does not impose an obligation to anyone except if it is imposed by a regulation or a contact (International Organisation of Standardisation-Information technology, 2013). Later we map or integrate GDPR definitions with ISO concepts from its principles. In other word, privacy principles are used to refine and define GDPR analysed rules

Same as any other legal document, ISO guidelines also starts with definition of terms and concepts used in the text. We start the analysing process from ISO 29100 definitions. The rest of analysing are in APENDIX II

PII: Information can be considered to be PII in at least the following instances:

- if it contains or is associated with an identifier which refers to a natural person (e.g., a social security number);

- if it contains or is associated with an identifier which can be related to a natural person (e.g., a passport number, an account number);

- if it contains or is associated with an identifier which can be used to establish a communication with an identified natural person (e.g., a precise geographical location, a telephone number); or

- if it contains a reference which links the data to any of the identifiers above.

1st.SFACT : information contains an identifier

2nd.SFACT : information associates with an identifier

3rd.SFACT : identifier refers to a natural person

4th.SFACT : identifier can be related to a natural person

5th.SFACT : identifier can be used to establish a communication with a natural person

1st.SRESULT : information can be considered to be PII

1st.SRULE : 1th.SFACT ^ **3**th.SFACT -> 1stSRESULT

2nd.SRULE : 1th.SFACT ^ 4th.SFACT ->1stSRESULT

3rd.SRULE : **2**th.SFACT ^ 3th.SFACT ->1stSRESULT

4th.SRULE : **1**st.SFACT ^ 5th.SFACT -> 1stSRESULT

If information contains an identifier and the identifier is related to a natural person, in such a situation the information can be considered PII. Therefore, directly we can conclude 1thSRULE from SFACT 1 and 2. Same is true regarding FACTs 3 to 5.

In previous section we also analysed GDRP text and extracted following rules:

GDPR:

2; *'personal data' means any information relating to a data subject*;

14th.LFACT. Information relates to data subject

LRESULT2nd. The information is personal data

LRESULT2nd = 1st**S**RESULTh

42ndLRULE: 14th.FACT-> **L**RESULT2nd

PII$_s$ = Personal Data

From GDPR, a condition for information to be personal data is to be related to a natural person. But one may not be sure about how information is related to data subject. In such situation, rules 51 to 57 from standard helps us. Based on this if information contains an identifier and identifier associates with a natural person, then it identifies the natural person or in other word is related to that person. Consequently, information is personal data or PII.

51stRULE : 1th.SFACT ^ **3**th.SFACT -> 14th.LFACT

52ndRULE 1th.SFACT ^ 4th.SFACT -> 14th.LFACT

53rdRULE : 2th.SFACT ^ 3th.SFACT -> 14th.LFACT

54thRULE : 2th.SFACT ^ 3th.SFACT -> 14th.LFACT

55thRULE : **1**th.SFACT ^ 5th.SFACT -> 14th.LFACT

.In other word, we can conclude the same results using logical reasoning

51stRULE **:**1th.SFACT ^ **3**th.SFACT -> 1thSRESULT

LRESULT2nd = 1stSRESULT4th

42ndRULE**:** 14th.FACT-> **L**RESULT2nd

An abstract method to also conclude Rules 51 to 55 is to equal same concepts in above rules from Standard and GDPR as following:

Information$_{s\ t}$=-Information$_{GDPR}$

Natural Person$_{st}$ = Natural person $_{GDPR}$

In definition of PII Principle, which is equal to data subject, standard has given following text. Right after coming rules are what we have extracted from these text. Later we use them to define meaning of data subject in more detail.

PII principals: PII principals provide their PII for processing to PII controllers and PII processors and, when it is not otherwise provided by applicable law, they give consent and determine their privacy preferences for how their PII should be processed. PII principals can include, for example, an employee listed in the human resources system of a company, the consumer mentioned in a credit report, and a patient listed in an electronic health record. It is not always necessary that the respective natural person is identified directly by name in order to be considered a PII principal. If the natural person to whom the PII relates can be identified indirectly (e.g., through an account identifier, social security number, or even through the combination of available attributes), he or she is considered to be the PII principal for that PII set.

2nd.SRESULT : PII Principal provides his/her PII for processing to PII Controller

3rd.SRESULT : PII Principal provides his/her PII for processing to PII Processor

4th.SRESULT : PII Principal give consent

5th.SRESULT : PII Principal determines their privacy preferences

6th.SFACT : consent is for the way PII is processed

7th.SFACT : privacy preferences are for the way PII are processed

8th.SFACT : natural person is identified directly

9th.SFACT : identification is by name

10th.SFACT : natural person is identified indirectly

11th.SFACT : identification is by account identifier

12th.SFACT : identification is by social security number

6th.SRESULT : natural person is PII Principal

5th.SRULE : 8th.SFACT -> 6th.SRESULT

6th.SRULE **:** 8th.SFACT ^ **9**th.SFACT -> 6th.SRESULT

7th.SRULE :10st.SFACT -> 6th.SRESULT

8th.SRULE : 10st.SFACT ^ **11**nd.SFACT -> 6th.SRESULT

9th.SRULE : 10st.SFACT ^ 12rd.SFACT -> 6th.SRESULT

10th.SRULE : RESULT9th -> 6th.SRESULT

11th.SRULE : RESULT10th ->6th.SRESULT

12th.SRULE : RESULT10th -> 6th.SRESULT

13th.SRULE : RESULT10th -> 6th.SRESULT

We have also following analysed text regarding data subject from GDPR which we could find a relevancy to mentioned definitions from ISO:

1st.LFACT The natural person is identified

2nd.LFACT :. The natural person can be identified

3rd.LFACT :. Identification is directly

4th.LFACT :. Identification is indirectly

1stLRULE :. 1st.LFACT ^ 3rd.LFACT -> **L**RESULT1st

2nd.LRULE: 1st.LFACT ^ 4th.LFACT^ 5th.LFACT ^ 6th.LFACT ^9th.LFACT ^ 11nd.SFACT -> **L**RESULT1st

1stLRULE : 1st.LFACT ^ 4th.LFACT ^ 5th.LFACT ^ 6th.LFACT ^ 9th.LFACT ^ 12th.S.FACT -> LRESULT1st

1stLRULE:. 1st.LFACT ^ 3rd.LFACT ^ **9**th.SFACT -> **L**RESULT1st.

:

In another word, the standard adds another criterion to the direct identification of natural person as having name. In the ontology reasoner will be performed automatically regarding the equalisation of Natural Person$_{st}$ = Natural person $_{GDPR}$ and when we have an instance of individual for both. The point of this paragraph was to explain how standard can add value to rules in GDPR and sometime vice versa.

Based on ISO 29100, Privacy Principles are categorised to following groups which are similar or same to articles from GDPR:

– The privacy principles of ISO/IEC 29100

1. Consent and choice

2. Purpose legitimacy and specification

3. Collection limitation

4. Data minimization

5. Use, retention and disclosure limitation

6. Accuracy and quality

7. Openness, transparency and notice

8. Individual participation and access

9. Accountability

10. Information security

11. Privacy compliance

We are practicing number of above principles here to refine GDPR rules. Same as previous text, we first analyse standard text and then try to mix and match extracted rules with rules from GDPR. It should be mentioned that we are not taking all analysed rules and only pick up the one which can refine any GDPR rules.

1. Consent and choice:

Adhering to the consent principle means: - presenting to the PII principal the choice whether or not to allow the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the natural person's consent. The PII principal's choice must be given freely, specific and on a knowledgeable basis; - obtaining the opt-in consent of the PII principal for collecting or otherwise processing sensitive PII except where applicable law allows the processing of sensitive PII without the natural person's consent; - informing PII principals, before obtaining consent, about their rights under the individual participation and access principle; - providing PII principals, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and - explaining to PII principals the implications of granting or withholding consent.

For a PII controller, adhering to the choice principle means: - providing PII principals with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice and to give consent in relation to the processing of their PII at the time of collection, first use or as soon as practicable thereafter; and - implementing the PII principal's preferences as expressed in their consent.

RESULT13th: PII Principal give consent

13th.SFACT : PII controller/processor processes PII

14th.SFACT : PII belongs to PII principle

15th.SFACT : PII principal cannot freely withhold consent

16th.SFACT : applicable law specifically allows the processing without the natural person's consent

17th.SFACT : controller/processor is collecting sensitive PII

18th.SFACT : PII principals has right under individual participant principle

19th.SFACT : PII principals has right under access principle

20th.SFACT : PII principals has right under individual participant

1st.SObligation : PII controller/processor is obligated to present the PII principal the choice to allow processing

2nd.SObligation: PII controller/processor is obligated to present the PII principal the choice to not allow processing

3rd.SObligation : the choice must be given freely

4th.SObligation : the choice must be given specific

5th.SObligation : the choice must be given based on knowledge

6th.SObligation : the choice must be obtained by consent of PII Principal

7th.SObligation : controller/processor has obligation to inform the principal of his/her individual participant's rights before consent

8th.SObligation : controller/processor has obligation to inform the principal of his/her access rights before consent

9th.SObligation : controller/processor has obligation to inform the principal of his/her individual participant rights before consent

10th.SObligation : controller/processor has obligation to inform the principal of *openness, transparency and notice* information before consent

11th.SObligation : controller/processor is obligated to present to PII principle mechanism to exercise their choice

12th.SObligation : mechanism must be clear

13th.SObligation : mechanism must be *easily understandable*

14th.SObligation : mechanism must be *accessible*

15th.SObligation : mechanism must be *affordable*

16th.SObligation : controller has obligation to take consent from PII principal

17th.SObligation : controller has obligation to implement PII principal preference in consent

14th.SRULE : **13**th.SFACT ^ **14**th.SFACT ^ 17th.SFACT -> **16th**.SObligation

15th.SRULE : 16th.SObligation ->1th.SObligation

16th.SRULE : 16th.SObligation -> **2th.S**Obligation.

17th.SRULE : 1th.SObligation ->3nd.SObligation

18th.SRULE : 1th.SObligation ->4rd.SObligation

19th.SRULE : 1th.SObligation -> 5th.SObligation

20th.SRULE : **16**th.SObligation^ **18**th.SFACT -> **7th**.SObligation

21st.SRULE : **16th**.SObligation ^ 19th.SFACT -> **8th**.SObligation

22nd.SRULE : 16th.SObligation^ 20st.SFACT -> **10th**.SObligation

23rd.SRULE : 1th.SObligation ->11th.SObligation

24th.SRULE : **.11th**.SObligation -> 12st.SObligation

25th.SRULE : 11th.SObligation -> 13nd.SObligation

26th.SRULE : 11th.SObligation -> 14rd.SObligation

27th.SRULE : 11th.SObligation -> 16**th**.SObligation

In above rules, we are giving some information of the information necessary to be mentioned in a consent. For example, rule 15 and 16 determines that the consent shall let the data subject to allow or not to allow processing of his/her information. Or rule 20 and 21 determines the rights of data subject which shall be mentioned in the consent, if he/she has any. These can be access rights or individual participant rights. Rules 23 to 27 is obligating the controller to let data subject try his/her choice to give or not give consent with different methods. It doesn’t say about the type of method just it mentions its criteria such as being easy, understandable. These are mostly options given in consents.

We have concept of consent in GDPR too. GDPR talks about some general aspect of consent such as being in written declaration and its format. But it does not mention the information that consent shall include. Above standard rules, can refine consent in GDPR into more requirements.

GDPR:

15th.LFACT. Processor/controller is processing personal data

LRecommendation1st: Data subject should give consent

22th.LFACT :The consent is for processing of personal data.

23th.LFACT:Personal data belongs to data subject

80th.LFACT: The consent is for processing purposes.

81th.LFACT: Consent is in context of a written declaration

82th.LFACT: Written declaration concerns other matters except from consent

21th.LFACT : Data subject has given his/her consent

16th.LObligation: The controller shall bear the burden of proof for consent

17th.LObligation: Consent must have distinguished appearance for its requirements

LPermission1st :Data subject may withdraw consent

LProhbition2rd: Withdrawal shall not affect the lawfulness of process.

24ndRULE: 15th.LFACT ∧ 21th.LFACT ∧ 23th.LFACT ∧ 24st.LFACT ∧ LRecommendation.1st -> 16th.LObligation

25rdRULE: LRecommendation1st-> LPermission1st

26thRULE: LPermission1st-> LProhbition1st

27thRULE: LRecommendation1st ∧ 81h.LFACT ∧ 82th.LFACT -> 17th.LObligation

LRecommendation6th. The consent should be given explicitly

LRecommendation7th. The consent should be given by appropriate methods.

18th.LObligation. The consent shall enable data subject to be aware of his consent to processing of personal data

LRecommendation8th. The consent should enable an indication of data subject wishes

LRecommendation9th. The indication should be given freely

LRecommendation10th. The indication should be specific.

LRecommendation11th. The indication should be informed

LPermission3th. The consent may be given by ticking a box on a website

LPermission4th. The consent may be given by a statement

LPermission5th. The consent may be given by a conduct

19th.LObligation. The consent shall indicate data subject's acceptance of processing personal data

20th.LObligation. The indication shall be clear.

28th.LRULE: 17th.LObligation -> 18th.LObligation

29th.LRULE: 17th.LObligation -> LRecommendation6th

30th.LRULE: 17h.LObligation-> LRecommendation7th

31thRULE: 17th.LObligation -> LRecommendation8th

32th.LRULE : LRecommendation8th -> LRecommendation9th

33st.LRULE: LRecommendation8rd -> LRecommendation10th

34nd.LRULE: LRecommendation8rd -> LRecommendation11th

35rd.LRULE: LRecommendation8rd ->19th.LObligation

36th.LRULE: 17th.LObligation -> LPermission1st

37th.LRULE: 17th.LObligation -> LPermission2nd

38th.LRULE: 17th.LObligation -> LPermission3rd

15th.LFACT = **13**th.S.FACT

LRecommendation2nd= **16th**.SObligation (conflict!)

LRecommendation7th=11th.SObligation = (conflict!)

28th.SRULE **82**th.LFACT ^ 64thFACT→7th.SObligation

29th.SRULE **82**th.LFACT ^→8th.SObligation

30th.SRULE **82**th.LFACT →9th.SObligation

31st.SRULE 82th.LFACT →**10**th.SObligation

32nd.SRULE **82**th.LFACT →11th.SObligation.

33rd.SRULE :LRecommendation8th -> 1st.SObligation

34th.SRULE :LRecommendation8th ->2nd.SObligation

35th.SRULE :**L**Recommendation7th-> 12th.SObligation

36th.SRULE :LRecommendation7th-> **13th.S**Obligation

37th.SRULE :LRecommendation7th -> **14th.S**Obligation

38th.SRULE : LRecommendation7th -> 16th.SObligation

$\text{Consent}_{\text{ST}} = \text{Consent}_{\text{GDPR}}$

$\text{Choise}_{\text{ST}} = \text{wish}_{\text{GDPR}}$

$\text{Mechanism}_{\text{ST}} = \text{Methods}_{\text{GDPR}}$

From above guidelines from ISO 29100, we can understand that some of the instructions by GDPR are being repeated here with some little changes. As shown above some of the facts and rights in these two different documents are equal. Therefor rules extracted from each can be amended by equal facts in order to integrate the requirements of GDPR with ISO standard or vice versa, as shown above. For example, Recommendation 2 is almost the same as obligation 16. One obligating controller to ask for data subject choice, the other recommend indication of user's wishes. This is a conflict as one recommend where the other obligates. When we have concepts of consent and wish and choice equal, recommendation 21 to 23 and permission 41 to 43 automatically will apply on consents and all criteria will be inherited from one to other. In other word, standard is giving more detail for the concept of "consent" and is defining more criteria for it. This fact is sometimes true in opposite direction. GDPR sometimes is giving detail information for concepts in standard. For example, GDPR here add more value to standard by inheriting FACT 116 to other consents for a written declaration consent.

7. Openness, transparency and notice

Adhering to the openness, transparency and notice principle means:

- providing PII principals with clear and easily accessible information about the PII controller's policies, procedures and practices with respect to the processing of PII;

- including in notices the fact that PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller;

- disclosing the choices and means offered by the PII controller to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and

- giving notice to the PII principals when major changes in the PII handling procedures occur. Transparency, including general information on the logic underlying the PII processing, can be required, particularly, if the processing involves a decision impacting the PII principal. Privacy stakeholders that process PII should make specific information about their policies and practices relating to the management of PII readily available to the public. All contractual obligations that impact PII processing should be documented and communicated internally as appropriate. They should also be communicated externally to the extent those obligations are not confidential.

In addition, the purpose of the processing of PII should be sufficiently detailed in order to allow the PII principal to understand:

- the specified PII required for the specified purpose;

- the specified purpose for PII collection;

- the specified processing (including collection, communication and storage mechanisms);

- the types of authorized natural persons who will access the PII and to whom the PII can be transferred; and

- the specified PII data retention and disposal requirements

21st.SFACT : PII controller/processor process PII

22nd.SFACT : PII belongs to PII principle

23rd.SFACT : PII controller has policies regarding processing PII

24th.SFACT : PII controller has procedures regarding processing PII

25th.SFACT : PII controller has practices regarding processing PII

26th.SFACT : PII controller disclose PII to privacy stakeholders

27th.SFACT : Major changes occur in PII processing

28th.SFACT : PII controller has identity

29th.SFACT : PII controller has contact details

30th.SFACT : personal data are processed for some purposes

31st.SFACT : processing purposes include some specified processing

32nd.SFACT : processing purposes include some specified processing PII

33rd.SFACT : processing purposes include collecting purposes

34th.SFACT : processing purposes include specified processing

35th.SFACT : communication mechanism is a specified processing

36th.SFACT : storage mechanism is a specified processing

37th.SFACT : some type of authorised persons has access to PII

38th.SFACT : PII controller transfer PII to third parties

39th.SFACT : processing purposes include PII data retention requirements

40th.SFACT : processing purposes include PII data disposal requirements

18th.SObligation . PII controller has obligation to provide PII Principal with clear information about controller's policies

19th.SObligation . PII controller has obligation to provide PII Principal with clear information about controller's procedures

20th.SObligation . PII controller has obligation to provide PII Principal with clear information about controller's practices

21st.SObligation . PII controller has obligation to provide notice to PII principal

22nd.SObligation . PII controller has obligation to include in notice the fact of PII being processed

23rd.SObligation . PII controller has obligation to include in notice the purpose of processing

24th.SObligation . PII controller has obligation to include in notice the types of privacy stakeholders

25th.SObligation . PII controller has obligation to include in notice identity of controller

26th.SObligation . PII controller has obligation to include in notice contact details of controller

27th.SObligation : controller has obligation to give processing change notice

28th.SObligation **:** PII controller has obligation to include in notice purposes of processing

29th.SObligation : PII controller has obligation to include in notice detail purposes of processing

30th.SObligation : PII controller is obligated to include in notice specified processing

31st.SObligation : PII controller is obligated to include in notice specified collecting purposes

32nd.SObligation : PII controller is obligated to include in notice specified processing PII

33rd.SObligation : PII controller is obligated to include in notice communication mechanisms

34th.SObligation : PII controller is obligated to include in notice specified processing PII

35th.SObligation : PII controller is obligated to include in notice storage mechanisms

36th.SObligation : PII controller is obligated to include in notice specified processing PII

37th.SObligation : PII controller is obligated to include in notice list of authorised persons to access PII

38th.SObligation : PII controller is obligated to include in notice list of third parties

39th.SObligation : controller is obligated to include in notice data retention requirements

40th.SObligation : controller is obligated to include in notice data disposal requirements

In following line, we are refining rules from GDPR which specify the materials that should be mentioned in a notice to data subject. 39th Rule is elicited from standard which dictates obligation of openly, transparency and notice to controller. From other side, 46th Rule from standard obligates necessity of privacy notice to include controller's identity. And 22 obligations from law also obligates same thing without motioning requirement for notice. Therefore, we can refine law requirement with elicited rules from standard for the requirement of privacy native. Now, rules in standard can determine the type of information that GDPR was asking for to be included in notice. According to rule 40, to 60 rules, this information includes policies, practices and procedures and changes of processing, also identity and contact detail of controller and other information. Therefore, all rules from 40 to 60 will be inherited to 88th Fact from GDPR.

51stLRULE: 14thL.FACT ^ ***96***th.LFACT ^ 99th.L.FACT -> 22th.LObligation.

22th.LObligation. = 25th.SObligation

39th.SRULE :**10**th.SObligation ->**21**th.SObligation.

40th.SRULE : 21th.SObligation. ->39th.SObligation.

41st.SRULE : 21th.SObligation ^ 23th.SFACT-> **18**th.SObligation

42nd.SRULE : **21**th.SObligation ^ 24th.SFACT-> 19th.SObligation

43rd.SRULE : 21th.SObligation ^ 25th.SFACT-> 20th.SObligation

44th.SRULE **:**21th.SObligation ^ 26th.SFACT-> 24th.SObligation .

45th.SRULE **:**21th.SObligation ^ 27th.SFACT-> 27th.SObligation

46th.SRULE : 21th.SObligation ^ 28th.SFACT-> 25th.SObligation

47th.SRULE : 21th.SObligation ^ 29th.SFACT -> 26th.SObligation

48th.SRULE : 21th.SObligation ^ 30th.SFACT -> **23th.S**Obligation

49th.SRULE : **23th.S**Obligation -> 29th.SObligation.

50th.SRULE : 23th.SObligation ->30th.SObligation

51st.SRULE : 23th.SObligation -> **31th.S**thObligation

52nd.SRULE : 23th.SObligation -> **32th.S**Obligation

53rd.SRULE : **23**th.SObligation -> **33th.S**Obligation

54th.SRULE : 23th.SObligation -> **34th.S**Obligation

55th.SRULE : **23th.S**Obligation -> 35th.SObligation

56th.SRULE : **23th.S**ndObligation -> **36**th.SObligation

57th.SRULE : **23th.S**Obligation -> **37**th.SObligation

58th.SRULE : **23th.S**Obligation -> **38**th.SObligation

59th.SRULE : 23th.SObligation -> **39**th.SObligation

60th.SRULE : 23th.SObligation -> **40**th.SObligation

In this section, we shown how to analyse rules from standard. We practice ISO 29100, since it is related to data protection. extracted elements of ISO 29100, helps construction of its equivalent concepts in ontology, together with their relationships. Integration between ISO and GDPR, also will be constructed in ontology, using logical functions of mapping, inheriting and others.

3.5.14 Standard Ontology

Refinement of laws by standards is also supported in this framework with a corresponding ontology. The taxonomy of this ontology cover commonly used terms and concepts in ISO/IEC ISMS family of standards. Also the hierarchical order of its concepts and their relationship, models and implements the inter-related organisation of ISO series. although standard does not have the authority of law to determine and impose rights on stakeholders, but it follows almost similar format of texts to law (simpler) and imposes rights to stakeholders to perform or not to perform an action. Therefore, the concept categorisation in Standard Ontology almost follows the order in Law Ontology. It consists of top classes of *ISO-Action*, *ISO-Actor* and *ISO-Object*. Two extra classes are specified to the structure of standard in general as *Standard-Subject* and *Standard-Section*. The categorisation in Actor and Object, also in Action classes are also mostly same to Law ontology since it is refinement of same concepts. Still the sub-categories depend on different types of these concepts in each ISO standard. Figure 3.13 illustrates the hierarchy of classes in Standard Ontology, hence Figure 3.14 represents a sub-category of classes based on definitions from ISO 29100. Similar concepts to Law Ontology are represented by different terminology in -ISO. For example, Data Subject in Law Ontology is represented as PII Principle in ISO 29100, hence Personal Data is represented as Personally Identifiable Information (PII). Similar concepts in different ontologies are equalled by a facility called as *Equivalency* in ontology. Both classes and properties in ontology can be equivalent of other classes and properties. Equivalency in classes imposes the properties of one to others. As an example if data-subject has an obligation in Law Ontology it will also be imposed to PII Principal in ISO Ontology. This makes the task of compliance easier especially when mapping, integration and refinement are the case. In fact, this is being one of the main reason why ontology has been selected as the skeleton platform for this framework. The equivalency between classes and properties is not only between GDPR and ISO 29100, but also between ISO standards together. Annex A in ISO/IEC 29100, provides a list of similar terminology in 29100 and 27000 series. Below table has been taken from Annex A. Making mutual equivalency of ISO 29100, GDPR and ISO 27100 series. This even makes the compliance task more convenience since it makes correspondence between different compliance components and apply one's requirements to others at same time. Analysed parts of guidelines in standards including facts and rights (obligation, recommendation, permission, prohibition) are constructed in ontology using statements of triples (subject-property-object). Rules are constructed by *Rule*s in ontology. Mapping between concepts and statements are constructed by *Equivalency*, and integration and refinement are also made by *Equivalency* and *Rule*s in ontology.

ISO/IEC 29100 concepts	**Correspondence with ISO/IEC 27000 concepts**
Privacy stakeholder	Stakeholder
PII Information	asset
Privacy breach	Information security incident
Privacy control	Control
Privacy risk	Risk
Privacy risk management	Risk management
Privacy safeguarding requirements	Control objectives

Table3.3 Comparing ISO/IEC 29100 and ISO/IEC 27000 concepts

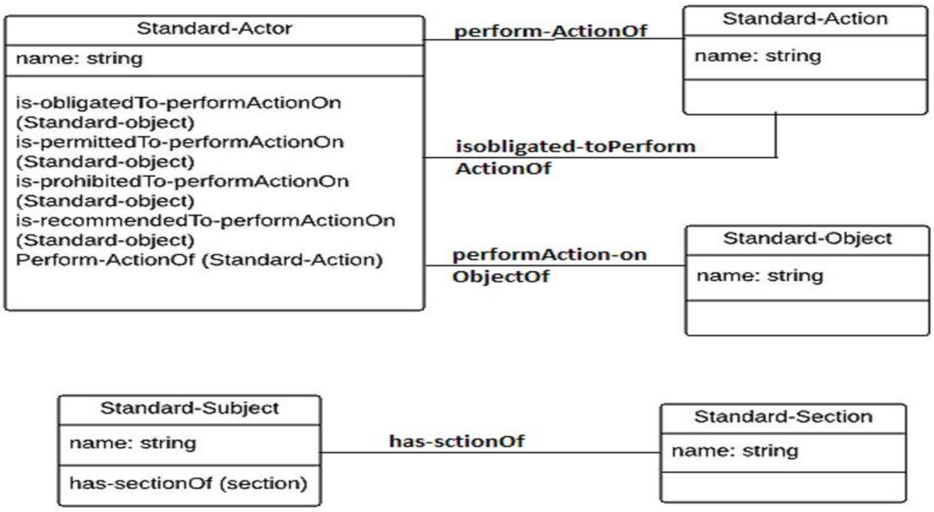

Standard-Actor
name: string
is-obligatedTo-performActionOn (Standard-object)
is-permittedTo-performActionOn (Standard-object)
is-prohibitedTo-performActionOn (Standard-object)
is-recommendedTo-performActionOn (Standard-object)
Perform-ActionOf (Standard-Action)
perform-ActionOf
Standard-Action
name: string
isobligated-toPerform ActionOf
performAction-on ObjectOf
Standard-Object
name: string
Standard-Subject
name: string
has-sectionOf (section)
has-sctionOf
Standard-Section
name: string

Figure3.13 . Standard Ontology

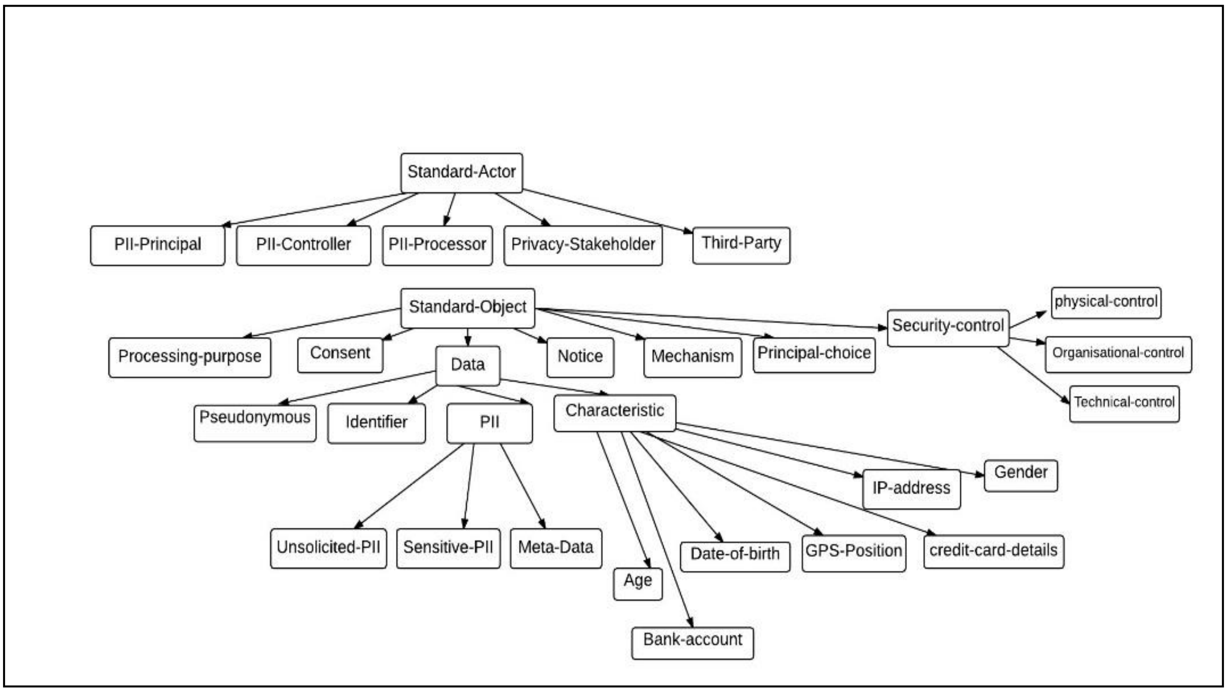


Figure3.14 . Standard Ontology Sub-classes

Regarding the structure of standard documents and having synonyms to law's terminology, statements (consisting of triples) in standard ontology are close to the ones in Law Ontology:

General Statements:

- Obligation: Standard-actor isObligated-ByStandard-ToperformAction-onStandardObjectOf some Standard-object
- Permission: Standard-actor isPermitted-ByStandard-ToperformAction-onObjectOf some Standard-object
- Prohibition: Standard-actor isProhibited-ByStandard-ToperformAction-onObjectOf some Standard-object
- Recommendation: Standard-actor isRecommended-ByStandard-ToperformAction-onObjectOf some Standard-object

- Fact: Standard-actor performAction-onObjectOf some Standard-object
- Fact: Standard-object performAction-onObjectOf some Standard-object
- Fact: Standard-Subject has-SectionOf some Standard-Chapter

Examples:

- *Obligation: PII controller/processor 'is-obligated-ByISO29100-ToProvideNoticeOf some Notice*
- *Fact: PII-Controller desires-toProtect-Information AssetOf some Information-asset*

Above statements makes rules of standards. Rules are also categorised to ones which makes obligations, permissions, recommendations and prohibitions which are concluded from corresponding facts. Except from inner-links in Standard ontology which represents rules indicating guidelines of standard, here we also have outer-links which represents integration and refinements of rules of Law & Ontology with standards and also different standards together. Example below shows some samples both from inner-links and outer-links:

Inner-link:

- *Process-PIIoF(?x,?y), desire-Toprotect-PIIOf(?x,?y), Process-ProcessOf(?x,?z) →*

Is-obligatedTo-EstablishISMS-On(?x,?z)

Outer-link:

- *Process-PersonalDataOf(?x,?y), want-toMaintainSecurityOn-PersonaldataOf(?x,?y) , Process-ProcessOf(?x,?z)→ Is-obligatedTo-EstablishISMS-On(?x,?z)*
- *Process-PersonalDataOf(?x,?y), want-toMaintainSecurityOn-PersonaldataOf(?x,?y) , Process-ProcessOf(?x,?z), Information-asset(?T)→ Is-obligated-ToIdentify (?x,?T)*
- *Is-RecommendedTo-enableIndicateWishesOf(?z,?y) → is-ObligatedToGiveFreely(?z,?y)*

3.5.15 Refinement and Definition of law by Authority Guidelines

One of the regulatory resources to be considered here in order to refine legal requirements and terms to more detailed requirements are the guidelines and best practices provided by governmental authorities. Regarding the practiced compliance law here, GDPR, Information Commissioners Office guidelines in UK has been taken for requirement refinement. Information Commissioners are assigned in each member states of EU as independent officials with the mission to upload information rights in the `public interests and promote data privacy to individuals. The role of information commissioner is created under the order of Data Protection Directive 95/46 and its different assigned version of national laws in European countries. A sample of it is the *Information Commissioner's Office* in the United Kingdom(ICO) which deals with Data Protection Act 1998 and the Privacy and Electronic Communications (EC Directive) Regulations 2003 across the UK; and the Freedom of Information Act 2000 and the Environmental Information Regulations 2004 in England, Wales and Northern Ireland and, to a limited extent, in Scotland. Some of the mirroring positions in Europe are as the Commission nationale de l'informatique et des libertés in France and the Federal Commissioner for Data Protection and Freedom of Information in Germany. Here we will practice the guidelines provided by ICO in UK as a sample. ICO has a list of guidelines for organisations how to comply with laws listed above and for public how to access their rights based on the mentioned laws. ICO's guidelines are helpful firstly to understand the meaning of the law's terms and secondly to explain and refine the principles of law. It almost helps in definition of concepts and providing organisational controls not technical controls. Principles of ICO are the subject matters of each article of law and the areas which the law has preceded. It should be considered that the available guidelines of ICO at the moment are regarding to Data Protection Act 1998 of UK which had been a respond to European Data Protection Directive 95/46. Since we are examining the compliance to Data Protection Regulation 2012, and as far as ICO does not have any comprehensive guidelines regarding this new regulation and not any amended national laws (as known yet), therefore the only common principles of the Directive and Regulation are being discussed here. But the key matter is the importance of existence of a component in our proposed framework which specifies on the application of regarding official authority's guidelines and bet practices. The process here is to study through the guidelines document of ICO and analyse the text in the same manner that laws and standards had been analysed using the legal reasoning and cellular analysis methods. The reference being used here is "The Guide to Data Protection" by Information Commissioner Office of UK (Information Commission Office 2012, Guide to Data Protection; Data controllers and data processors: what the difference is and what the governance implications are?; Privacy Notice, Code of Practice).

The section of "Key definitions of Data Protection Act" in ICO guideline, has definitions for terms of *Data, filing system, personal data, processing, Data Subject, Data Controller, Data Processor, Processing Purposes* and *Third Party*. This section is an alternative support for the similar part of *definitions* in the Regulation document to help the complier have more understanding of the law's terms. We have the following texts from the guidelines document which are analysed similar to analysis of laws and standards. The rest of analysis are mentioned in APENDIX II:

Definition Rules:

‘Data: Information that is held on computer, or is intended to be held on computer, is data. So data is also information recorded on paper if you intend to put it on computer.’

1st.GFACT Information is held on computer

2nd.GFACT Information is intended to be held on computer

3rd.GFACT Information are recorded on a paper

4th.GFACT you intend to put information on computer

1st.GRESULT Information is data

1st.GRULE 1st.G.FACT ->1st.GRESULT

2nd.GRULE 2nd.GFACT -> 1sr.GRESULT

3rd.GRULE 3rd.G.FACT ^ 4th.GFACT -> 1st.GRESULT

$\text{Information}_L = \text{Informations}_S = \text{Information}_G$

Since we do not have any definition in GDPR or standard for information, above facts and result can add knowledge to our framework by using ICO component.

‘Idenitfiability: - An individual is 'identified' if you have distinguished that individual from other members of a group. In most cases an individual’s name together with some other information will be sufficient to identify them. Simply because you do not know the name of an individual does not mean you cannot identify that individual. The starting point might be to look at what means are available to identify an individual and the extent to which such means are readily available to you.’

5th.GFACT Individual is distinguished from other members of a group

6th.GFACT Individual has name together with some other information

7th.GFACT	Individual’s name is not known
8th.GFACT	There are means available to identify an individual
9th.GFACT	The means are available
2nd.GRESULT	The individual is identified
4th.GRULE	5tht.GFACT -> 2nd.GRESULT
5th.GRULE	6th.GFACT -> 2nd.GRESULT .
6th.GRULE	7th.G.FACT ^ 8th.GFACT ^ 9th.GFACT -> 2nd.GRESULT

Based on GDPR definition, a person would be data subject if he/she was identifiable. Since above facts from ICO are specifying conditions for an individual to be identified, therefore above facts can be added to GDPR facts regarding data subject in order to clarify this term. It should be mentioned that individual in ICO is the same as natural person in GDPR. Also we had some definition for identifying a natural person from standard. Based on above lines, we can amend Data subject facts as following:

GDPR:

1st.LFACT	The natural person is identified
2nd.LFACT	The natural person can be identified
3rd.LFACT	Identification is directly
4th.LFACT	Identification is indirectly
5th.LFACT	Identification is by means
6th.LFACT	The mean is used by controller
7th.LFACT	The mean is used by natural person
8th.LFACT	Mean is used by legal person
9th.LFACT	Identification is by reference to an identification number
10th.LFACT	Identification is by reference to a location data
11th.LFACT	Identification is by reference to an online identifier

12th.LFACT Identification is by reference to the person physical factor(s)

13th.LFACT Fact12 is true regarding physiological, genetic, mental, economic, cultural and social identity of the person

LRESULT1st Natural person is a Data subject

And:

1stLRULE :. 1st.LFACT ∧ 3rd.LFACT -> LRESULT1st

2nd.LRULE: 1st.LFACT ∧ 4th.LFACT∧ 5th.LFACT ∧ 6th.LFACT ∧9th.LFACT-> LRESULT1st

3rd.LRULE: 1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧10th.LFACT-> LRESULT1st

4th.LRULE: 1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 11th.LFACT -> LRESULT1st

5th.LRULE: 1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧ 12th.LFACT -> LRESULT1st

6th.LRULE **:**1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT∧ 6th.LFACT ∧ 13th.LFACT -> LRESULT1st

51th.FACT = 1st.FACT = RESULT11th

Name$_S$ = Name$_G$

MeanL = Mean$_G$

8th.GFACT = 5th.LFACT.

1stLRULE :. 1st.LFACT ∧ 3rd.LFACT -> LRESULT1st

5th.GRULE : 6th.GFACT ^ 9th.SFACT -> 2th.GRESULT =>.

1stLRULE :. **1st.LFACT**∧ **6th**.GFACT -> LRESULT1st.

6th.GRULE 7th.G.FACT ^ 8th.GFACT ^ 9th.GFACT -> 2nd.GRESULT

2nd.LRULE: 1st.LFACT ∧ 4th.LFACT∧ ^ 5th.LFACT ∧ 6th.LFACT ∧9th.LFACT-> **L**RESULT1st

2nd.LRULE: : 1st.LFACT ∧ ^ 8th.GFACT ^ 9th.GFACT ^ 5th.LFACT ∧ 6th.LFACT ∧9th.LFACT-> **L**RESULT1st

As shown above, we have integrated GDPR rules to clarify direct and indirect identicicablity of natural person with more criteria. First rule in GDPR (1st..LRUL) species that if a natural person is identified and identification is directly, then he/she is data subject. 5th.GRULE from ICO determines condition for a natural person to be identified by having a name. Therefore, we amended 1st.LRULE from GDPR by adding criteria for direct identification of natural person (having name). In similar process, we species conditions for indirect identification of natural person without name and using some mean for identification. Therefore, we amended 2nd.LRULE by some criteria from ICO for indirect identification (2nd.GRULE).

Similar concepts of Names and Means are also mapped to each other. 1stRULE and 2ndRULE also are integrated with more criteria from ICO and also standard.

Following instructions are provided by ICO in order to indicate how a process may be lawful and fairly:

Processing personal data fairly and lawfully (Principle 1):

'This is the first data protection principle. In practice, it means that you must:

- *have legitimate grounds for collecting and using the personal data;*
- *not use the data in ways that have unjustified adverse effects on the individuals concerned;*
- *be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;*
- *handle people's personal data only in ways they would reasonably expect;*
- *make sure you do not do anything unlawful with the data*

Fairness generally requires you to be transparent – clear and open with individuals about how their information will be used.

Fairness requires you to:

- *be open and honest about your identity;*

- *tell people how you intend to use any personal data you collect about them (unless this is obvious);*

- *usually handle their personal data only in ways they would reasonably expect; and*

- *above all, not use their information in ways that unjustifiably have a negative effect on them.*

Is it possible to use or disclose personal data for a new purpose?

You should explain why you want to use an individual's personal data at the outset, based on your intentions at the time you collect it.

If you intend to make a significant change, such as proposing to disclose customer information to others, you will usually need to get your customers' consent.

Personal data will be processed fairly only if certain information is given to the individual or individuals concerned. The oral or written statement that individuals are given when information about them is collected is often called a "fair processing notice", although our recent guidance uses "privacy notice" instead.

In general terms, a privacy notice should state:

- *your identity and, if you are not based in the UK, the identity of your nominated UK representative;*

- *the purpose or purposes for which you intend to process the information; and*

- *any extra information you need to give individuals in the circumstances to enable you to process the information fairly.*

Depending on the circumstances, you may go beyond the basic requirements of the law for example by telling people:

- *If you intend to pass the information on, the name of the organization involved and details of how they use the information*

- *How long you and or other organization intend to keep the information*

- *Whether replies to questions are mandatory or voluntary*

- *The consequence of not providing the information, for example non receipt of benefits*

- *Whether the information will be transferred overseas*

- *What are you doing to ensure the security of information?*
- *About their rights and how they can exercise them, for example the fact that a person can obtain a copy of his personal information or object to direct marketing*
- *Who to contact if they want to complain or know more about how their information is used*
- *About the right to complain to information commissioner if there is a problem*

The need to actively communicate a privacy notice is strongest where:

- *You are collecting sensitive information*
- *The intended use of information is likely to be unexpected or objectionable*
- *Providing personal data or failure to do so will have a significant effect on individuals*
- *The information will be shared with other organisation in a way that wouldn't be expected.*

By 'actively communicate' we mean take a positive action to provide a privacy notice to a member of the public, for example by sending a letter, reading out a script or distributing an email.

There can be strong pressures to share personal public and private sector contexts. However, an organization decision to share information does not negate its duty to treat people fairly. This means that prior to sharing information, the organization holding it must consider carefully what any recipient is going to do with the information, and what the effect on people is likely to be. It is good practice to obtain an assurance about this, for example in form of a written agreement.

Privacy notices can be provided through a variety of media:

- *Orally: fact-to-face or when you speak to someone on the phone; it is a good idea to document it.*
- *In writing: printed media, printed adverts, forms such as financial application forms or job application forms*
- *Through signage, for example an information poster in a public area*
- *Electronically: in text messages, on websites, in email*

It is good practice to use the same media you use to collect information to deliver the privacy notice.

A layered notice can be useful for privacy notice. A layered notice usually consists of a short notice and a longer notice. The short notice consists of basic information, such as the identity of organization and the way in which the personal data will be used. The short notice consists of a link to the second, longer notice which provides much more detailed information. The longer notice can, in turn, contain links to further materials, explaining relatively specialist issues such as the circumstances in which information may be disclosed to the police.'

10th.GFACT : Data Processor is processing personal data

11th.GFACT : Data Processor is collecting personal data

1st.GObligation : Processor is obligated to process Personal data fairly

2nd.GObligation : Processor is obligated to process Personal data lawfully

3rd.GObligation: Processor is obligated to process personal data fairly

12th.GFACT . Data controller (data processor) use data in specific ways

13th.GFACT . The ways have unjustified adverse effects on the individual's concern

14th.GFACT . Data controller intend to use personal data in specific ways

15th.GFACT . People reasonably expect their personal data to be handled in specific ways

16th.GFACT . Data controller has an identity

17th.GFACT . Data controller use personal data for new purpose

18th.GFACT . Data controller disclose personal data for a new purpose

19th.GFACT . Data controller has reasons to use personal data at the outset

20th.GFACT . Personal data belongs to individuals

21st.GFACT . Data controller intend to disclose personal data to others

22nd.GFACT . Data controller is not based on UK

23rd.GFACT . Data controller has a nominated representative in UK

24th.GFACT . Data controller keeps personal data for a period

25th.GFACT . Data controller transfer personal data to overseas

4th.GObligation Obligation 16 and 17. Data controller (data processor) is obligated to use ways to ensure the security of personal data

GPermission1st . Data subjects is permitted on some rights based on law

GPermission2nd . Data subjects is permitted to complain to data controller regarding the process of their personal data

GPermission3rd . Data subjects is permitted to complain to ICO about the process of their personal data

26th.GFACT . Data controller collects sensitive personal data

27th.GFACT . The way is not expected by data subjects

28th.GFACT . The way is objectionable by data subjects

5th.GObligation . Controller is obligated to take positive action for privacy notice

29th.GFACT . Data controller collects personal data in a medium

6th.GObligation . Data controller must have legitimate grounds for collecting the personal data

7th.GObligation . Data controller must have legitimate grounds for using personal data

GPermission4th . Data controller must not use the data

8th.GObligation . Data controller must be transparent about his intention to use data

9th.GObligation . Data controller must give appropriate privacy notice to individuals

10th.GObligation . Data controller (data processor) must handle people's personal data based on their expectation

GProhbition1st . Data controller (data processor) must make sure not to do unlawful things with personal data

11th.GObligation . Data controller must be open with individuals about the ways of using their personal data

12th.GObligation . Data controller must be clear with individuals about the ways of using their personal data

13th.GObligation . Data controller must be honest about his identity

14th.GObligation . Data controller must be open about his identity

15th.GObligation . Data controller must explain to individuals the reason of using their personal data at outset

16th.GObligation . Explanation must be based on data controller's intention at the time of personal data collection

17th.GObligation . Data controllers must get customer's change consent

18th.GObligation . Data controller must state the identity of Data controller in privacy notice

19th.GObligation . Data controller must state the identity of Data controller representative in Privacy notice

20th.GObligation . Data controller must state the purposes of processing personal data in Privacy notice

GPermission5th . Data controller may state the further fairly processing information in Privacy notice

GPermission6th . Data controller may state the name of outset organization in Privacy notice

GPermission7th . Data controller may state the details of the outset usage of information in Privacy notice

GPermission8th . Data controller may state the period of using personal data in Privacy notice

GPermission9th . Data controller may state mandatory reply questions in Privacy notice

GPermission10th . Data controller may state the voluntary reply questions in Privacy notice

GPermission11th . Data controller may state the consequences of not providing information in Privacy notice

GPermission12th . Data controller may state the overseas transfer of information in Privacy notice

GPermission13th . Data controller may state the provided security to information in Privacy notice

GPermission14th . Data controller may state the rights of individuals in Privacy notice

GPermission15th . Data controller may state the method of exercising individual’s rights in Privacy notice

GPermission16th . Data controller may state the contact details to complain in Privacy notice

GPermission17th . Data controller may state the right to complain to ICO in Privacy notice

GPermission18th . Data controller may need to actively communicate the privacy notice with individuals

GPermission19th . Data controller may take a positive action

GPermission20th . Data controller may send a letter

GPermission21st . Data controller may read out a script

GPermission22nd. Data controller may distribute an email

GPermission23rd . Data controller may obtain an assurance for sharing personal data

GPermission24th . Data controller may obtain a written agreement to share personal data

GPermission25th . Data controller may provide Privacy notice through a variety of media

GPermission26th . Data controller may provide privacy notice orally

GPermission27th . Data controller may provide privacy notice face-to-face

GPermission28th . Data controller may provide privacy notice on telephone

GPermission29th . Data controller may document the privacy notice

GPermission30th . Data controller may provide privacy notice in writing

GPermission31st . Data controller may provide privacy notice in printed media

GPermission32nd. Data controller may provide privacy notice in printed adverts

GPermission33rd . Data controller may provide privacy notice in forms

GPermission34th . Data controller may provide privacy notice through signage

GPermission35th . Data controller may provide privacy notice through information poster in public area

GPermission36th . Data controller may provide privacy notice electronically

GPermission37th . Data controller may provide privacy notice in text message

GPermission38th . Data controller may provide privacy notice on website

GPermission39th . Data controller may provide privacy notice in email

GRecommendation1st . Data controller may provide privacy notice in same information collecting medium

GPermission40th Data controller may provide a layered notice

GRecommendation2nd . The layered notice consists of a short notice

GRecommendation3rd . The short notice contains the basic information

GRecommendation4th . The basic information is such as the organization identity

GRecommendation5th . The basic information is such as the processing ways

GRecommendation6th . The basic information is such as processing purposes

GRecommendation7th . The short notice contains a link to longer notice

GRecommendation8th . The longer notice contains more detailed information

GRecommendation9th . The longer notice may contain some links

GRecommendation10th . Links are to further materials

GRecommendation11th . Further materials explain specialist issues

GRecommendation12th . Further materials are such as circumstances to disclose information to police

7th.GRULE :2nd.GObligation → 5th.GObligation

8th.GRULE : G.2ndObligation -> 6th.Obligation

9th.GRULE : 2nd.GObligation-> GProhbition1st

10th.GRULE : 1th.GObligation -> 8th.GObligation.

11th.GRULE : 7th.GObligation→ 8th.GObligation

12th.GRULE : 1st.GObligation -> 10th.GObligation

13th.GRULE : 8th.GObligation -> 5th.GObligation.

14th.GRULE : 1st.GObligation → 13th.GObligation

15th.GRULE : 1st.GObligation→ 14th.GObligation.

16th.GRULE : 1st.GObligation ^ 25th..GFACT ^ 19th.G.FACT -> 15th.GObligation.

17th.GRULE : 15th.GObligation -> 16th.GObligation

18th.GRULE : 13th.GObligation^ 14th.GObligation ^ 16th.GFACT ^ 9th.GObligation -> 18th.GObligation

19th.GRULE : 13th.GObligation^ 14th.GObligation ^ 16th.GFACT ^ 9th.GObligation ^ 23th.GFACT ^ 22th.GFACT-> 19th.GObligation.

20th.GRULE : 9th.GObligation ^ 30th.S.FACT -> 20th.GObligation

21st.GRULE : 9th.GObligation ^ 31th.SFACT -> 20th.GObligation

22nd.GRULE : 9th.GObligation ^ 32th.SFACT-> 20th.GObligation

23rd.GRULE : 9th.GObligation ^ 33th.SFACT -> 22th.GObligation

24th.GRULE : 9th.GObligation ^ 34th.SFACT ^ 30th.S.FACT -> 20th.GObligation

25th.GRULE : 9th.GObligation ^ 35th.SFACT -> 20th.GObligation

26th.GRULE : 9th.GObligation ^ 36th.SFACT -> 20th.GObligation

27th.GRULE : 9th.GObligation ^ 27th.SFACT -> 27th.SObligation

28th.GRULE : 9th.GObligation ^ 27th.SFACT -> 17th.GObligation

29th.GRULE : 9th.GObligation -> GPermission6th

30th.GRULE : 9th.GObligation -> GPermission7th

31st.GRULE : 9th.GObligation ^ 24th.FACT -> GPermission8th

32nd.GRULE : 15th.GObligation -> GPermission12th

33rd.GRULE : 9th.GObligation ^ GPermission1st -> GPermission14th

34th.GRULE : 9th.GObligation ^ GPermission2nd -> GPermission14th

35th.GRULE : 9th.GObligation ^ GPermission3th -> GPermission14th

36th.GRULE : 9th.GObligation ^ 29th.GFACT -> GRecommendation1st

37th.GRULE : 9th.GObligation -> GPermission40th

38th.GRULE : GPermission40th -> GRecommendation2nd.

39th.GRULE : GRecommendation.2th -> GRecommendation.3th

40th.GRULE : GRecommendation.3th -> GRecommendation5th

41st.GRULE : GRecommendation3th -> GRecommendation6th

42nd.GRULE : GRecommendation2th -> GRecommendation7th

43rd.GRULE : GRecommendation7th -> GRecommendation8th

44th.GRULE : GRecommendation7th -> GRecommendation9th

45th.GRULE : GRecommendation9th -> GRecommendation10th

46th.GRULE : GRecommendation10th -> GRecommendation11nd

47th.GRULE : GRecommendation10th -> GRecommendation12nd

48th.GRULE : 9th.GObligation ^ 26th.GFACT -> GPermission18th

49th.GRULE : GPermission18th -> GPermission19th

50th.GRULE :GPermission19th -> GPermission20th

51st.GRULE :GPermission19th -> GPermission21th

52nd.GRULE : GPermission19th -> GPermission22th

53rd.GRULE : 9th.GObligation -> GPermission25th

54th.GRULE : GPermission25th -> GPermission26th

55th.GRULE : GPermission25th -> GPermission27th

56th.GRULE : GPermission25th -> GPermission25th

57th.GRULE : GPermission25th -> GPermission30th

58th.GRULE : GPermission30th -> GPermissiond31th

59th.GRULE : GPermission30th -> GPermission32th .

60th.GRULE : GPermission30th -> GPermission33th

61st.GRULE : GPermission30th -> GPermission34th .

62nd.GRULE : GPermission30th -> GPermission35th

63rd.GRULE : 9th.GObligation -> GPermission36th

64th.GRULE : GPermission36th -> GPermission37th

65th.GRULE : GPermission36th -> GPermission38th

66th.GRULE : GPermission36th -> GPermission39th

$\text{Privacy-notice}_{\text{ICO}} = \text{Notice}_{\text{ST}}$

$\text{Identity}_{\text{L}} = \text{Identity}_{\text{G}}$

1st.GObligation = 2nd.LObligation

1nd.GObligation =1st.LObligation

8th.GObligation =3rd,LObligation

9th.GObligation = 21th.SObligation.

39th.SRULE:**10**th.SObligation ->**21**th.SObligation.

In above analysed rules, we first examined the condition for lawful and fairness processing based on ICO. As the main requirement for fairness process, we also have concept of *Privacy Notice (PN)* in ICO. The article taken from ICO here, is mostly providing criteria for *Privacy Notice (PN)*. These criteria are divided to three groups. First it includes the information including in PN. Secondly it deals with the format and structure of privacy notice and lastly it deals with the methods of PN communication with data subject. Privacy Notice is a concept which was also discussed in standard by the concept "*Notice"*. We also showed in previous section how the requirement of notice from standard was inherited to GDPR. Here standard rules regarding Notice can be amended by more rules from ICO to specify more criteria for it. Since 21th Obligation from standard equals to 9th obligation from ICO, then all obligation and others rights extracted from 9th ICO obligation also are inherited to standard and law.

Here we tried to analyse guidelines from ICO, the Information Commissioner Office in United Kingdom as a sample of *Authority Guideline* component of framework. To do so we used same legal reasoning technique to separate statements into facts and results. As far as these guidelines are prepared in sequence and for more meaning and refinement of legal requirements extracted from GDPR and standards, we have some same concepts, obligations and other rights from these resources here which are mapped together. As explained this has been done in order to define and refine analysed results from GDPR. In such situations, new facts or results are inherited to previous facts and results from GDPR or standard. Therefore, requirements from two components of Law, Standard and Local Authority Guidelines are sometimes integrated and inherited from each other.

3.5.16 ICO Ontology

ICO Ontology support the refinement of laws and standards by number of similar concepts and classes to Law and Standard ontology. This is due to the instructural structure of ICO guidelines in which obligation, permission, recommendation and prohibitions are provided to controllers, processors and data subjects. ICO Actor, Action and Object as the top level classes and their sub-classes which are almost equivalent to similar concepts in Law and Standard, support refinement process. Likewise, the Standard Ontology, here we have inner-links and outer-links relation sin ICO Ontology. Regarding the same structure, we don’t repeat the materials. Inner-links connects ICO rules a triples together, where outer-links connects ICO to Standard and Law Ontologies. The following Images (Figure3.15, Figure3.16) shows the ICO classes in general and also their sub-categories. In a same process to Standard Ontology, similar or same terminologies of ICO ontology and the rest of ontologies are equivalent to each other. Consequently, they inherit each other’s object and data properties. Individual class corresponds to Natural-Person in GDPR.

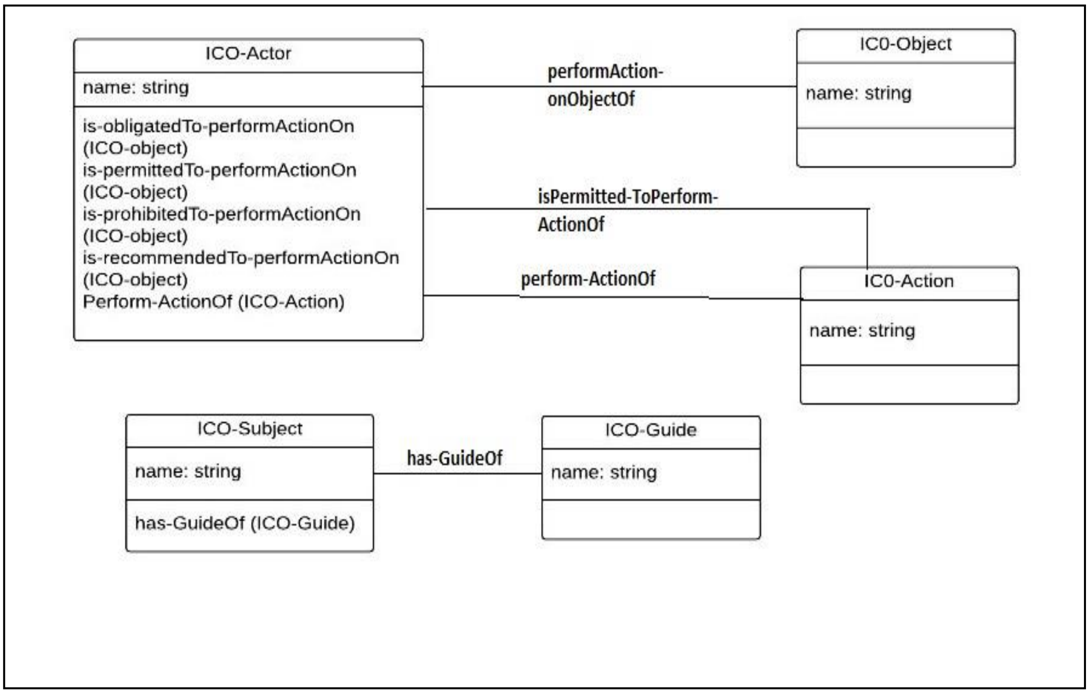

ICO-Actor
name: string
is-obligatedTo-performActionOn (ICO-object)
is-permittedTo-performActionOn (ICO-object)
is-prohibitedTo-performActionOn (ICO-object)
is-recommendedTo-performActionOn (ICO-object)
Perform-ActionOf (ICO-Action)
performAction-onObjectOf
IC0-Object
name: string
isPermitted-ToPerform-ActionOf
perform-ActionOf
IC0-Action
name: string
ICO-Subject
name: string
has-GuideOf (ICO-Guide)
has-GuideOf
ICO-Guide
name: string

Figure3.15 ICO Ontology

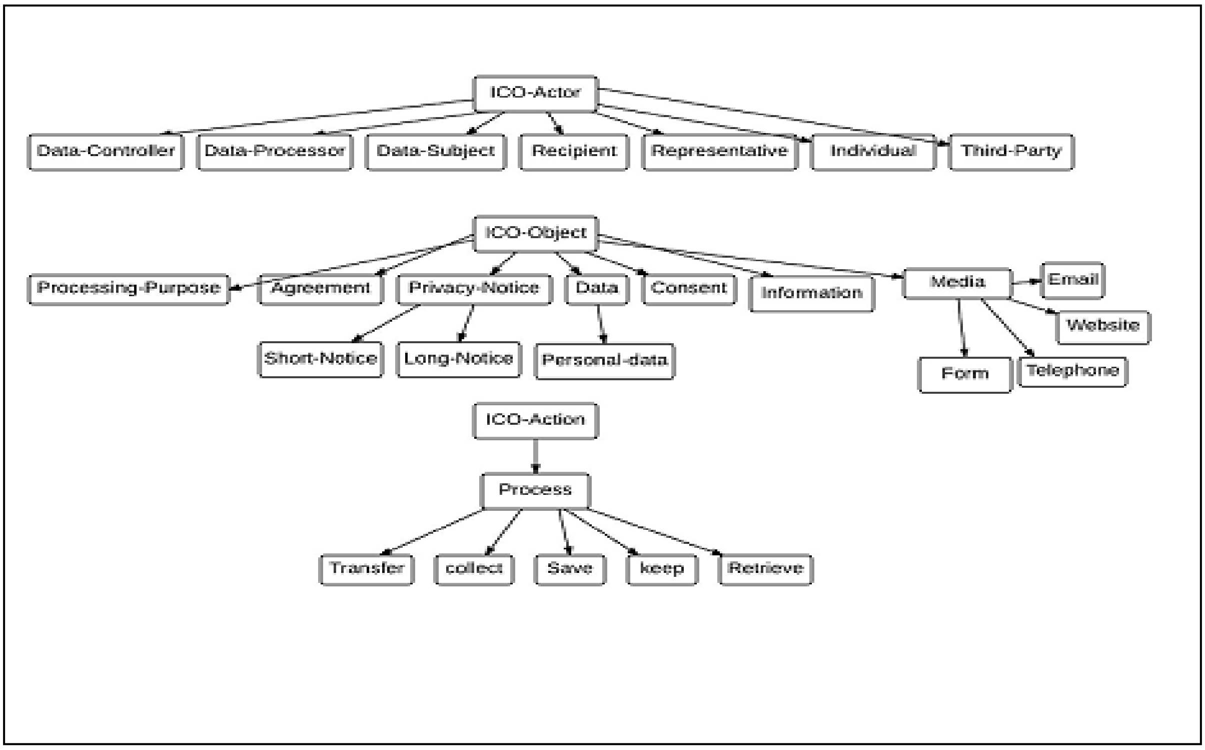


Figure4.16

Figure3.16 ICO Sub-Classes

The analysed rules of ICO guidelines are being represented here in their ontological format of triples. In following samples, we have instances of both mapping and integration between two ontologies of GDPR and ICO as showed above.

Examples:

- *distinguishFromOtherMember-IndividualOf (?x,?y) ∧ has-NameOfIndividualOf (?x?y) ∧ has-InformationAboutIndividualOf(?x?y) → identify-IndividualOf(?x?y)*

.

- *Identify-IndividualOf (?x,?y), is-associtedByNameOfIndividual(?x,?y), is-processed-ToLearnAbout-IndividualOf(?x,?y), is-Inprofessionof-controller(?x,?z), Identify-InPersonalLifeOf(?x,?y), impact-personaldataof-individualof(?x,?y) → relates-ToDataSubjectOf(?x,?y)*

- *Is-obligatedTo-processFairly-PersonalDataOf (?x,?y) ∧ is-obligatedTo-takeConsentfrom-DataSubjectOf (?x, ?z) → Is-obligatedTo-GivePrivacyNoticeTo-IndividualOf(?x, ?z)*

- *Processing-Personaldataof(?x,?y), process-processOf(?x,?z), belongTo(?y,?w) → provide-InPrivacyNotice-IdentityOfController(?x,?x)*

- *provide-InPrivacyNotice-IdentityOfController(?x,?x), Privacy-notice(?k) → Is-permittedTOprovide-processingPeriod-inNoticeOf(?x,?k)*

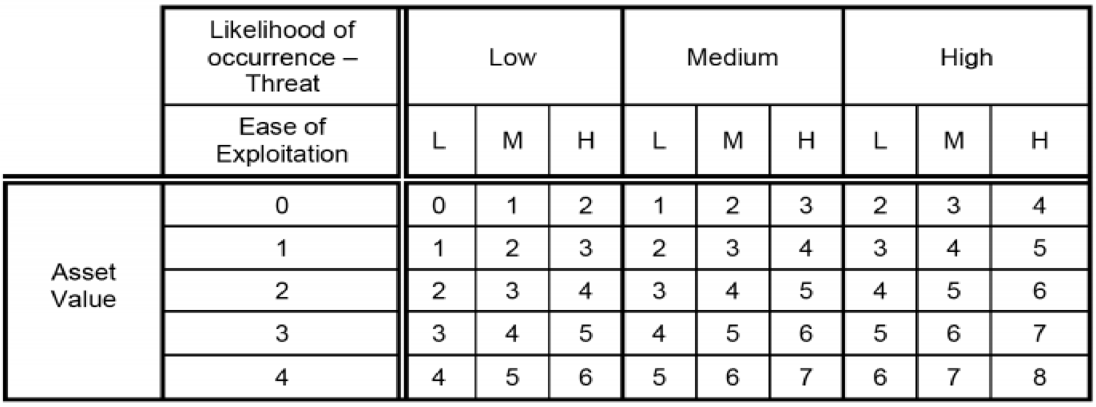
- *provide-InPrivacyNotice-IdentityOfController(?x,?x), Privacy-notice(?k) → Is-permittedTO-takePositiveAction-forNoticeOf(?x,?k)*

- *Is-permittedTO-takePositiveAction-forNoticeOf (?x,?k) → Is-permittedTo-sendByEmail-NoticeOf(?x,?k)*

In this section we have been able to represent ontological relationship between ICO classes and also to make further relationship between ICO and other ontologies. These relationships were provided by description operations in ontology such as mapping, integration, inherit and other operations.

3.5.17 Risk Analysis

Based on OCEG, an organised and complete Compliance procedure should always be accompanied by a well-defined risk assessment (Open Compliance & Ethics Group (OCEG) 2009). To fulfil this requirement, a risk assessment component is employed in our framework in which the process and concepts are based on ISO/IEC 27005. This process address threads that target the objectives of system and laws and regulation. To do this, ISO 27005 introduces four stages of plan, do, act and check. Here we only address the first two stages and their sub activities of context establishment, Risk assessment and risk treatment. Information system risk assessment is a continues process in which the context of system is established and risks and threats are assessed using a risk assessment plan. If this provides sufficient information to effectively determine the actions to modify the risks to acceptable level, the process is finished and risk treatment follows. Otherwise another iteration of risk assessment with revised context will be conducted. To say in detail, risk assessment contains of two approaches; High-level ISMS and Detailed ISMS. It normally starts with high-level assessment of risks in which a more general scope of context establishment is considered. Context establishment includes activities of determining risk evaluation criteria, risk acceptance criteria, Impact criteria and scope and boundary of system. These factors help to identify assets, and evaluate the value of assets and their risks. For example, an asset with low business value, low value of confidentiality and integrity and low cost of replacement will be evaluated as a low valued asset. In such a condition there is no need for detailed risk assessment and general security controls such as a firewall are considered for system. Where an asset is valued high, then detailed ISMS approach will be performed in which the evaluation context is in more details and also assets, threat against them and their vulnerabilities are identified and values are assigned to them. These values are later used in order to evaluate risk value based on some available methods. Many of these methods make use of tables and combines subjective and empirical measures. Here we are using *Matrix with Predefined Values* method from Table3.4. In such methods, firstly assets are valued in terms of their costs, law enforcement, loos of goodwill, commercial order and other contexts. Then the level of ease of exploitation of vulnerability and likelihood of threat against assets are determined and are evaluated by qualitative values of low, to medium and high. Finally, the asset value, and the threat and vulnerability levels relevant to each type of consequence are matched based on a pre-defined matrix and each combination are resulted to a relevant measure of risk valued from 0 to 8. For example, an asset valued of 4, with a threat likelihood and ease of vulnerability exploitation of medium will have risk level value of 6. Finally, the assessed value of risk is evaluated against risk acceptance level (defined in context establishment). If the risk level is higher appropriated controls are considered or risk is avoided or transferred. Otherwise the risk will be retained.



	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Table3.4 ISO 27005-Matrix with Predefined Values

Using risk assessment in this framework is due to OCEG demand for this requirement, also in refinement of Security Principle in GDPR. Security controls in ANNEX A of 27002 is also used in order to find security solutions for risks. Referring to ISO 27005, the following text is useful and taken to be analysed here. Same as other compliance resources discussed in previouse section, we are using law analysis and cellular analysis technique here s well:

‘The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review.

Context establishment: the context for information security risk management should be established which involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries and establishing an appropriate organization operating the information risk management

Basic Criteria: an appropriate risk management approach should be selected or developed that address basic criteria such as: risk evaluation criteria, impact criteria, risk acceptance criteria.

Risk evaluation criteria: risk evaluation criteria should be developed for evaluating the organization’s information risk considering following:

- *The strategic value of the business information system*
- *The critically of the information assets involved*

- *Legal and regulatory requirements and contractual obligations*

- *Operational and business importance of availability, confidentiality and integrity*

- *Stakeholder's expectations and perception and negative consequences for goodwill and reputation*

Impact criteria: impact criteria should be specified and developed in term of degree of damage or cost to the organization caused by an information security event considering the following:

- *Level of classification of the impacted information asset*

- *Breaches of information security*

- *Impaired operation*

- *Loss of business and financial value*

- *Disruption of plans and deadlines*

- *Damage of reputation*

- *Breaches of legal, regulatory or contractual requirement*

Risk acceptance criteria: an organization should define its own scales for level of risk acceptance. Risk acceptance criteria often depend on the organization's policies, goals, objectives and interest of stakeholders. Risk acceptance criteria should be set up considering the following:

- *Business criteria*

- *Legal and regulatory aspect*

- *Operation*

- *Technology*

- *Finance*

- *Social and humanitarian factors*

Scope and boundaries: The organization should define scope and boundaries of information security risk management. When defining scope and boundary, the organization should consider the following information:

- *The organization's strategic business objectives, strategies and policies*

- *Business processes*
- *The organization's function and structure*
- *Legal, regulatory and contractual requirements applicable to the organization*
- *The organization's information security policy*
- *The organization's overall approach to risk management*
- *Information assets*
- *Location of the organization and their geographical character*
- *Constraint affecting the organization*
- *Expectations of stakeholders*
- *Socio-cultural environment*
- *interface*

Information security risk assessment:

Input: basic criteria, the scope and boundaries, and the organization for the information security risk management process being established

Action: Risks should be identified, qualified or qualitatively described and priotaritised against risk evaluation criteria and objectives relevant to the organization.

Risk assessment consists of following activities:

- *risk analysis*
  - a. *risk identification*
  - b. *risk estimation*
- *risk evaluation*

Risk analysis:

a. risk identification:

input: scope and boundaries for the risk assessment to be conducted, list of constitutes with owners, location, function, etc.

Action: the assets with the established scope should be identified

Output: a list of assets to be risk managed and a list of business processes related to the assets and their relevance.

Identification of threats

input: information on threats obtained from incident reviewing, assets owners, users, and other sources including external threat catalogues

Action: threats and their sources should be identified

Output: a list of threats with the identification of threat type and source

Identification of existing controls:

Input: documentation of controls, risk treatment implementation plans

Action: existing and planned controls should be identified

Output: a list of all existing and planned controls their implementation and usage status

Identification of vulnerabilities:

Input: a list of known threats, list of assets and existing controls

Action: vulnerabilities that can be exploited by threats to cause harm to assets or to the organization should be identified.

Output: a list of vulnerabilities in relation to assets threats and controls; a list of vulnerabilities that do not relate to any identified threat for review

Identification of consequences:

Input: a list of assets, a list of business processes, and a list of vulnerabilities where appropriate related to assets and their relevance

Action: the consequences that losses of confidentiality, integrity and availabity may have on the assets should be identified

Output: a list of incident scenarios with their consequences related to assets and business processes'

Following lines, represent a sample of facts, result and rights and consequently Rules from above text from IS27500. We have limited the job to the requirements which are closer to elicited Security requirements in previous sections. The purpose is to make integration between them.

RObligation1st . The organization is obligated to assess information security risks

RObligation2nd . The organization is obligated to treat information security risks

RObligation3rd . The organization is obligated to establish its context

RObligation4th . Organisation is obligated to perform risk acceptance

RObligation5th . Organisation is obligated to perform risk communication

RObligation6th . Organisation is obligated to perform risk monitoring

RObligation7th . Organisation is obligated to perform risk review

RObligation8th . Organisation is obligated to set the basic criteria

RObligation9th . Organisation is obligated to define the scope and boundaries

RObligation10th . Organisation should select risk management approach

RObligation11th . Organisation should develop an appropriate risk management approach

RObligation12th . The approach should address basic criteria

RObligation13th . Organisation is obligated to set risk evaluation criteria

RObligation14th . Organisation is obligated to set risk impact criteria

RObligation15th . Organisation is obligated to set risk acceptance criteria

RRecommendation1st . Risk evaluation criteria should be developed considering the strategic value of the business information systems

RRecommendation2nd . Risk evaluation criteria should be developed considering the critically of the information assets involved

RRecommendation3rd . Risk evaluation criteria should be developed considering the legal and regulatory requirements and contractual obligations

RRecommendation4th . Risk evaluation criteria should be developed considering the operational and business importance of availability, confidentiality and integrity

RRecommendation5th . Risk evaluation criteria should be developed considering Stakeholder's expectations and perception and negative consequences for goodwill and reputation

RRecommendation6th . Impact criteria should be specified in term of degree of damage to organization (data controller/processor should specify ...)

RRecommendation7th . Impact criteria should be developed in term of degree of cost to organization (data controller/processor should develop ...)

RFACT1st Fact134. The damage is caused by information security event

RRecommendation8th . Data controller should consider the level of classification of the impacted information asset

RRecommendation9th . Data controller should consider breaches of information security

RRecommendation10th . Data controller should consider impaired operation

RRecommendation11th . Data controller should consider loss of business and financial value

RRecommendation12th . Data controller should consider disruption of plans and deadlines

RRecommendation13th . Data controller should consider damage of reputation

RRecommendation14th . Data controller should consider breaches of legal, regulatory and contractual requirement

RRecommendation15th . The organization should consider its business process

RRecommendation16th . The organization should consider its functions and structure

RRecommendation17th . The organization should consider its information security policy

RRecommendation18th . The organization should consider its Information assets

RRecommendation19th . The organization should consider location of the organization and their geographical character

RRecommendation20th . The organization should consider constraints

RRecommendation21st . Data controller/processor should identify risks

RRecommendation22nd . Data controller/processor should quantify risks

RRecommendation23rd . Data controller/processor should qualitatively describe the risks

RRecommendation24th . Data controller/processor should prioritise risks against risk evaluation criteria

RRecommendation25th . Data controller/processor should prioritise risks against objectives

RFACT2nd . Objectives are relevant to the organizations

RObligation16th . Organization is obligated to perform risk analysis

RObligation17th . Organisation is obligated to perform risk evaluation

RObligation18th . Organisation is obligated to perform risk identification

RObligation19th . Organisation is obligated to perform risk estimation

RRecommendation26th . Data controller/processor should identify the assets

RFACT3rd . Assets are within the established scope

RRecommendation27th . Data controller/processor should prepare list of constitutes

RRecommendation28th . Data controller/processor should prepare list of constituter's owners

RRecommendation29th . Data controller/processor should prepare list of constituter's function

RRecommendation30th . Data controller/processor should prepare list of constituter's location

RRecommendation31st . Data controller/processor should prepare list of assets

RRecommendation32nd . Data controller/processor should prepare list of business processes

RRecommendation33rd . Data controller/processor should review incidents

RObligation20th . Data controller/processor is obligated to obtain information about threats

RRecommendation34th . Data controller/processor should obtain information from incidents

RRecommendation35th . Data controller/processor should obtain information from asset's owners

RRecommendation36th . Data controller/processor should obtain information from users

RRecommendation37th . Data controller/processor should obtain information from other resources

RRecommendation38th . Data controller/processor should prepare a list of threats

RRecommendation39th . Data controller/processor should prepare a list of threats' resources

RRecommendation40th . Data controller/processor should identify a list of existing controls

RObligation21st . Data controller/processor is obligated to identify a list of vulnerabilities

RObligation22nd . Data controller/processor is obligated to identify a list of consequences

RRULE1st:	RObligation1st -> RObligation3rd
RRULE2nd	RObligation1st -> RObligation4th
RRULE3rd	RObligation1st -> RObligation5th
RRULE4th	RObligation1st-> RObligation8th
RRULE5th	RObligation1st -> RObligation9th
RRULE6th	RObligation1st->RRecommendation1st
RRULE7th	RRecommendation1st → RRecommendation6th
RRULE8th	RRecommendation1st → RRecommendation7th
RRULE9th	RObligation3rd→ RObligation9th
RRULE10th	RObligation3rd -> RObligation12th
RRULE11th	RObligation12th→ RObligation13th
RRULE12th	RObligation12th→ RObligation14th
RRULE13th	RObligation12th→ RObligation15th
RRULE14th	RObligation13th→ RRecommendation1st
RRULE15th	RObligation13th→ RRecommendation2nd
RRULE16th	RObligation13th→ Recommendation26

RRULE17th	RObligation13th→ RRecommendation4th
RRULE18th	RObligation13th→ RRecommendation5th
RRULE19th	RObligation13th∧RFACT1st→ RRecommendation6th
RRULE20th	RObligation13th→ RRecommendation7th
RRULE21st	RObligation14th→ RRecommendation6th
RRULE22nd	RObligation14th→ RRecommendation7th
RRULE23rd	RObligation14th→ RRecommendation8th
RRULE24th	RObligation14th→ RRecommendation9th
RRULE25th	RObligation14th→ RRecommendation10th
RRULE26th	RObligation14th→ RRecommendation11th
RRULE27th	RObligation14th→ RRecommendation12th
RRULE28th	RObligation14th→ RRecommendation13th
RRULE29th	RObligation14th→ RRecommendation14th
RRULE30th	RObligation15th→ RRecommendation15th
RRULE31st	RObligation15th→ RRecommendation16th
RRULE32nd	RObligation15th → RRecommendation17th
RRULE33rd	RObligation15th → RRecommendation18th
RRULE34th	RObligation15th → RRecommendation19th
RRULE35th	RObligation1st→ RObligation16th
RRULE36th	RObligation1st→ RObligation17th
RRULE37th	RObligation3rd→ RObligation18th
RRULE38th	RObligation16th→ RRecommendation26th
RRULE39th	RObligation18th→ RRecommendation26th
RRULE40th	RRecommendation26th→ RRecommendation27th
RRULE41st	RRecommendation26th→ RRecommendation28th
RRULE42nd	RRecommendation26th→ RRecommendation29th
RRULE43rd	RRecommendation26th→ RRecommendation30th

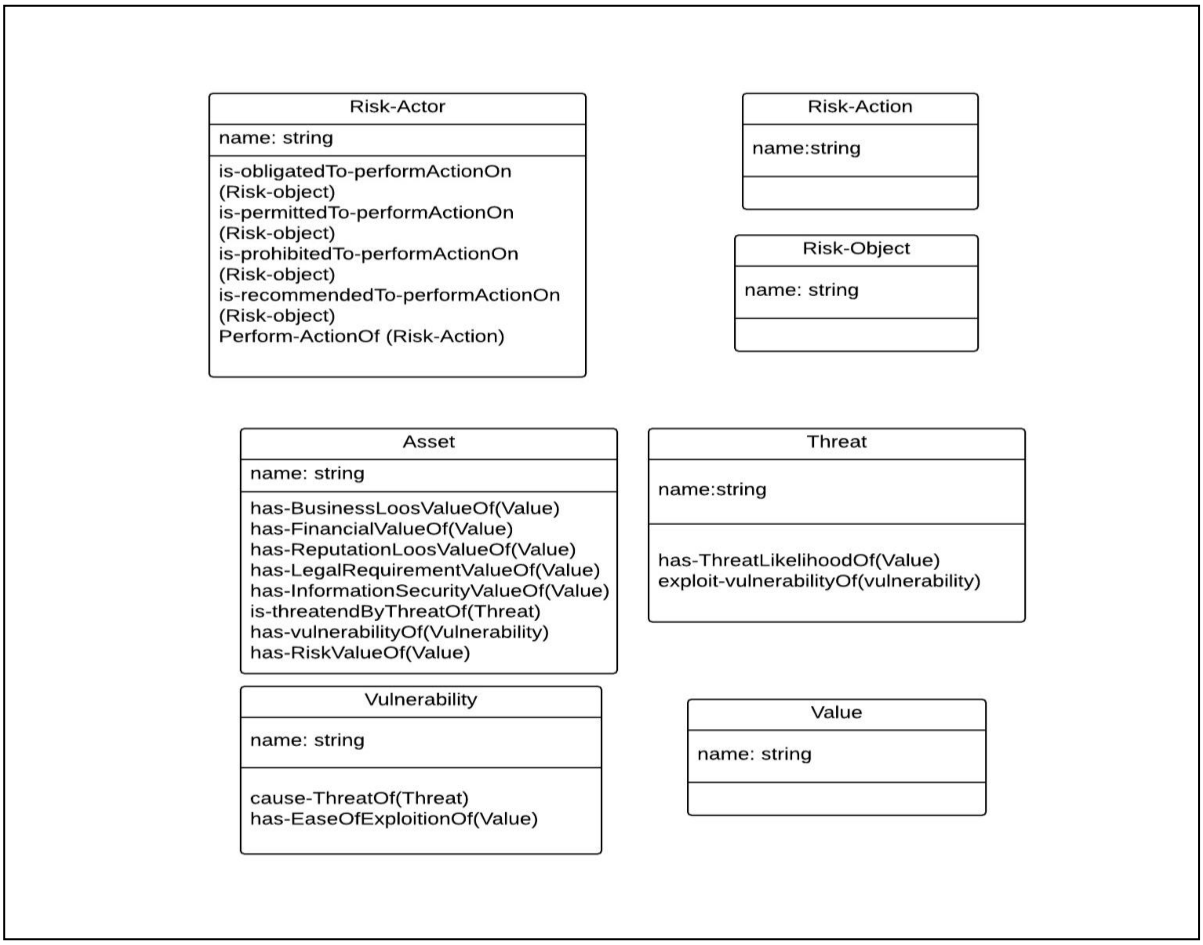
RRULE44th	RRecommendation26th → RRecommendation31st
RRULE45th	RRecommendation26th → RRecommendation32nd
RRULE46th	RRecommendation26th →RRecommendation33rd
RRULE47th	RRecommendation26th → RRecommendation34th
RRULE48th	RRecommendation26th → RRecommendation35th
RRULE49th	RRecommendation26th → RRecommendation36th
RRULE50th	RRecommendation26th → RRecommendation37th
RRULE51st	RObligation20th→ RRecommendation38th
RRULE52nd	RObligation20th→ RRecommendation39th
RRULE53rd	RObligation21st→ RRecommendation26th
RRULE54th	RObligation21st→ RRecommendation38th
RRULE55th	RObligation21st→ RRecommendation40th
RRULE56th	RObligation22nd→ RRecommendation31st
RRULE57th	RObligation22nd→ RRecommendation32nd

The above analysed text from ISO 27005, are general guidelines regarding the process and tasks needs to be done in ISRM. We provide these types of guidelines in our model in order to instruct the user about the general process. But they are also implemented in our model using number of concepts and object properties along with rules. For example, in order to adhere to RRequirement31 to prepare a list of assets, we are also using concepts from Annex B of ISO 27005. Annex B is also providing a list of assets normally used in an organisation or system. We are also using Annex A for a list of Scope and Boundaries, Annex C for a list of Threats, Annex D for Vulnerabilities and Annex E for Risk assessment approaches. Theses annexes provides prepared list for mentioned resources, but an organisation may still need and have extra information which in this case it can use the general guidelines to prepare the list of requires information.

3.5.18 Risk Ontology

The ontology supporting the risk assessment component of this framework, includes relevant concepts to risk such as asset, threat, vulnerability, risk-actor, value and others (Figure 3.17). Further categorisation of these concepts are based on Annex B, C and D of ISO27005.

The general orders of risk assessment address by ISO 27005, as analysed in previous section are provided in Risk Ontology by classes, object-properties and further ontological rules on them. The types of these properties are same to types of rights (obligation, permission, prohibition and recommendation) as explained in other ontologies. The considerable here is that we have omitted to have concepts from Scope & Boundary in Risk Ontology. This is due to the fact that this task is already performed in our framework with component of i* modelling. In fact, the context of system is modelled there and scope and boundaries are specified. The rest of Context Establishment task and its concepts as Impact Criteria, Evaluation Criteria and Risk Acceptance Criteria are each identified by a related property in our ontology. These properties help the risk assessment by specifying criteria for valuing assets against criteria such as Business-loos, Financial Value and others by quantitative values using number of data-properties. This is being done in order to calculate the final value of an asset, also to calculate risk-acceptance value. We also have number of other properties here in Risk Ontology. These properties are related to the concepts of risk assessment which are not directly documented in ISO 27005, but are depicted from the guidelines and the methods used in risk assessment approaches. Following list presents different types of properties used in Risk Ontology in our model:



Risk-Actor
name: string
is-obligatedTo-performActionOn (Risk-object)
is-permittedTo-performActionOn (Risk-object)
is-prohibitedTo-performActionOn (Risk-object)
is-recommendedTo-performActionOn (Risk-object)
Perform-ActionOf (Risk-Action)
Risk-Action
name:string
Risk-Object
name: string
Asset
name: string
has-BusinessLoosValueOf(Value)
has-FinancialValueOf(Value)
has-ReputationLoosValueOf(Value)
has-LegalRequirementValueOf(Value)
has-InformationSecurityValueOf(Value)
is-threatendByThreatOf(Threat)
has-vulnerabilityOf(Vulnerability)
has-RiskValueOf(Value)
Threat
name:string
has-ThreatLikelihoodOf(Value)
exploit-vulnerabilityOf(vulnerability)
Vulnerability
name: string
cause-ThreatOf(Threat)
has-EaseOfExploitionOf(Value)
Value
name: string

Figure3.17 . Risk Ontology

- Obligation: Risk-Actor is-obligated-ToperformAction-OnRiskObjectOf some Risk-Object

    - *Example: Risk-Assessor is-obligated-ToAssesInformationSecurityRiskOn-ProcessingOf some Process*

- Permission: Risk-Actor is-permitted-ToperformAction-OnRiskObjectOf some Risk-Object

- Prohibition: Risk-Actor is-prohibited-ToperformAction-OnRiskObjectOf some Risk-Object

- Recommendation: Risk-Actor is-recommended-ToperformAction-OnRiskObjectOf some Risk-Object

- *Example:* Risk-Assessor is-recommended-ToSelectRiskApproachOf some Risk-Approach

- Facts:

    - Context Establishment:
        - Asset has-FinancialValueOf some quantitative-Value
        - Asset has-BusinessLoosValueOf some quantitative-Value
        - Asset has-LegalRequirementValueOf some quantitative-Value
        - Asset has-InformationSecurityValueOf some quantitative-value
        - Asset has-RiskAcceptanceValueOf some quantitative-value
    - Risk Evaluation Matrix:
        - *Asset has-RiskValueOf some quantitativeValue*
        - *Asset is-threatenedByThreatOf some Threat*
        - *Asset has-VulnerabilityOf some Vulnerability*
        - *Threat has-ThreatLikelihoodOf some qualitative-Value*
        - *Vulnerability has-EaseOfExploitionOf some qualitative-Value*
        - *Vulnerability cause-ThreatOf some Threat*

Further rules are depicted on above properties in order to complete rules from ISO 27005 guidelines, to take and select a risk assessment approach appropriate to the value of assets and finally to calculate the level and value of risk for each asset. Following list represents sample of these rules in Risk Ontology. We should mention that the following list covers only inner-links (Rule of Risk-Ontology itself) from Risk Ontology:

- Obligation, Permission, Prohibition and Recommendation Rules:

  - *Risk-Assessor (?y), Scope(?x)→ Is-RecommendedTo-IddentifyAseestFor-ScopOf (?y,?x)*
  - *Is-RecommendedTo-IddentifyAseestFor-ScopOf (?y,?x) → Is-RecommendedTo-PrepareListOf-ConstitueOwnerOf(?y?x)*

  - *Asset(?x), Risk-Assesor(?y) → is-ObligatedToPerform-RiskAssesmentOn (?y,?x)*
  - *is-ObligatedToPerform-RiskAssesmentOn (?y,?x) → is-ObligatedTo-EstablishContextOn(?y,?x)*

- Context Establishment Rules:

  - *Asset(?x), has-BusinessLoosValueOf(?x,?y), has-FinancialValueOf(?x,?z), has-LegalRequirementValueOf(?x,?w), has-InformationSecurityValueOf(?x,?p), has-ReputationLoosValueOf(?x,?t) → has-AssetValueOf(?x, ?(y+z+w+p+t)/5)*

- Risk Assessment Matrix Rules:

  - *Asset(?x), has-RiskValueOf(?x,'4'), has-ThreatLiklihoodOf(?y,'Medium'), has-EaseOfExploitionOf(?z,'High'), is-threatenedByThreatOf(?x,?y), has-VulnerabilityOf(?x,?z), is-ExploiteByThreatOf(?z,?y) → has-RiskValueOf(?x,'6')*
  - *Asset(?x), has-RiskValueOf(?x,'1'), has-ThreatLiklihoodOf(?y,'High'), has-EaseOfExploitionOf(?z,'High'), is-threatenedByThreatOf(?x,?y), has-*

VulnerabilityOf(?x,?z), is-ExploiteByThreatOf(?z,?y) → has-RiskValueOf(?x,'5')

- *Asset(?x), has-RiskValueOf(?x,'4'), has-ThreatLiklihoodOf(?y,'Low'), has-EaseOfExploitionOf(?z,'Low'), is-threatenedByThreatOf(?x,?y), has-VulnerabilityOf(?x,?z), is-ExploiteByThreatOf(?z,?y) → has-RiskValueOf(?x,'4')*

Individuals to these concepts are given from system context and the final risk value is calculated based on Risk Matrix with Predefined Values in Annex E of ISO27005. The matrix is drawn in Risk Ontology by number of data properties assigned to concepts of asset, threat, Likelihood and Vulnerability-Ease-of-Exploitation to give quantitative values (1-8) and qualitative values (law, medium, high) to them; and also by number of rules defined on the mentioned data properties as shown above.

Up to this level, we only participated in providng inner-links in Risk Ontology which are relations between risk ontology concepts. Following rules indicates outer-links between Risk Ontology and other ontologies in our framework. These outer-links are used to map, integrate, inherit or refine rights and rules from other components by risk assessment rules.

In same process to other ontologies, similar terminologies in different ontologies are mapped together using *Equivalency* equipment in ontology. Here is same in Risk Ontology. The categorisation for *Asset* class in this ontology indicates similarity to *Resource* class in i*, also *Object* in Law, Standard and ICO ontology. Making them equal also makes the risk assessment task very easy. As explained before one of the obligations addressed by Risk Assessment is to identify assets in system context. As far as these are already performed in i* ontology and resources and objects are identified and also equivalent to assets in risk ontology, there is no extra task for Risk-Assessor to identify the assets. Although the obligation helps him/her to identify non-depicted assets.

In order to show how properties and rules from previous ontologies are refined to Risk Ontology rules and properties we are representing following examples:

GDPR:

32nd.LFACT . In order to maintain security

33rd.LFACT . Risks are inherent to the processing

Fact48: personal data is being processed

7thLObligation. The controller (processor) has the obligation to evaluate the risks

8thLObligation. The controller (processor) has the obligation to implement risk mitigation measures

LRecommendation3rd. Security measures is recommended to ensure an appropriate level of security

LRecommendation4th. Controller is recommended to take into account the state of art

LRecommendation5th. Controller is recommended to take in to account cost of measure’s implementation

34th.LFACT: cost of implementation is related to risk

35th.LFACT: cost of implementation is related to the nature of personal data processing

54thLRULE : 15th.LFACT∧ 32nd.LFACT ∧ 33rd.LFACT -> 7thLObligation

55thLRULE : 15th.LFACT∧ 32nd.LFACT ∧ 33rd.LFACT ^ 7thLObligation

56thLRULE : : 8thLObligation → LRecommendation3rd

57thLRULE :8thLObligation→ LRecommendation4th

58thLRULERule :: 7thLObligation ∧ 34th.LFACT∧ 35th.LFACT → LRecommendation5th

RRULE58th 7thLObligation -> RObligation1stRObligation1st

RRULE1st: RObligation1st -> RObligation3rd

RRULE2nd RObligation1st -> RObligation4th

RRULE3rd RObligation1st -> RObligation5th

RRULE4th RObligation1st-> RObligation8th

RRULE5th RObligation1st -> RObligation9th

RRULE6th RObligation1st->RRecommendation1st

The above rules indicate that Obligation7 from GDPR results to first Obligation in Risk ontology both obligating performance of risk assessment. As far as first risk obligation concludes other obligations (3,4,5,8,9), these obligtions will be refined by Obligation 7 also.

Each of these last mentioned obligations also are refined to further obligations and recommendations based on what has been analysed in previous section. Therefore, this refinement is also concluded for Obligation7 from GDPR.

Inherit is depicted in this model by equivalency between Assets from Risk Ontology and Resource and Objects from other ontologies as following:

PersonalInformation-asset (Risk)= Personal-Information (GDPR/ICO)= PII (Standard)

PII(?X) ∧ Is-ThretenedByThreatf(?y,?z) →

Is-ThretenedByThreatOf(?x,?z)

The above text in fact is not illustrated rule in our ontology, but is concluded when the reasoner runs. It means any threat that are threatening asset of y in Risk Ontology is also inherited to PII X, Personal-information in GDPR and ICO and also to the individual from system context modelled by i*.

The last types of outer-links properties in Risk Ontology are used in order to perform risk treatment. The integration is from Risk Ontology to Standard Ontology where it has guided using of controls to treat vulnerabilities and risks. Following is showing some examples:

Risk-Assessor(?x), Is-threatenedBy-threatOf (?y, ?z)), Data-Corruption(?z) → Is-RecommendedToBackUp-AssetOf (?x,?y)

Risk-Assessor(?x), Is-threatenedBy-threatOf (?y, ?z)), Eavesdropping(?z) → Is-RecommendedToEncrypt-AssetOf (?x,?y)

Risk-Assessor(?x), Is-threatenedBy-threatOf (?y, ?z)), System-penetration(?z) → Is-RecommendedTo-perormPenetrationTesting (?x,?y)

3.5.19 Refinement by Patterns

Based on the nature of software development which is an incremental process of analysing and modelling step by step requirements of the system, the methodology in this work is also an incremental development of the system and its requirements. One of the important issues which should be considered during system designing and modelling is the recent growth of usage of *design patterns* in software engineering communities. As is being discussed, it also has been addressed by a component of our framework. Design patterns which record the design experiences of expert programmers are being reused as references for those with fewer experiences. It also has been proved that design patterns have modified the traditional approach to system modelling (Gamma et al., 2012). Reuse of design solutions for several similar problems support software engineering in saving time, cost and efforts avoiding system design from scratch and also improve the quality of design and reliability. The theory here is to use available patterns to model the system in order to avoid a repeat of out-and-out. Using patterns in refinement of depicted requirements is happening here in different levels of system analysis. In other word design patterns are being used at different levels of abstraction of system analysis. First is where initial requirements are modelled by i* and each of the traditional and primitive requirements will be linked to a pattern in order to be implemented. Here mostly design patterns depended to the type of system will be used. The second place is to refine legal and standard and also risk depicted requirements with a solution from patterns. Here mostly we use patterns for non-functional requirements such as security patterns.

To avoid confusion, it is necessary to mention that, conceptual modelling as the provider of conceptual primitives that a designer use to think-of an application provides the basic lexicons and syntaxes which can be used to define a design pattern. But a non-experienced designer can also use design patterns to think about application requirements and solutions rather than in terms of pure modelling, since the language of patterns are also based on problems (requirements) and solutions. Therefore, using design patterns is same as defining a high-level design model as the skeleton of modelling which can be reused times and times with additional and changed requirements in each different application (Gamma et al., 2012). This method is beneficial here since the main aim is to acknowledge system developers and designers with a framework in order to comply their developing systems with related legal frameworks. The addressed system developers and designers with high probability are using design patterns in their processes as this is common these days. Even they are designing from scratch, the framework works still as a general approach. From other point using design patterns is economical here since the most consideration is on compliance rather than modelling.

based on the words from “Jan Borchers”:

"A pattern language is a hierarchically structured collection of design patterns that leads the designer from abstract, large-scale to concrete and small-scale design issues."

As it has been told there is no single and standard format for this documentation and different pattern authors have used different formats but some are more common. One of the most common formats which are being used by new pattern authors are that introduced by *Gang of Four* (Gamma et al., 2012) and is using the following format containing below sections:

- **Pattern Name and Classification:** A descriptive and unique name that helps in identifying and referring to the pattern.

- **Intent:** A description of the goal behind the pattern and the reason for using it.

- **Also Known As:** Other names for the pattern.

- **Motivation (Forces):** A scenario consisting of a problem and a context in which this pattern can be used.
- **Applicability:** Situations in which this pattern is usable; the context for the pattern.
- **Structure:** A graphical representation of the pattern. Class diagrams and Interaction diagrams may be used for this purpose.
- **Participants:** A listing of the classes and objects used in the pattern and their roles in the design.
- **Collaboration:** A description of how classes and objects used in the pattern interact with each other.
- **Consequences:** A description of the results, side effects, and trade-offs caused by using the pattern.
- **Implementation:** A description of an implementation of the pattern; the solution part of the pattern.
- **Sample Code:** An illustration of how the pattern can be used in a programming language.
- **Known Uses:** Examples of real usages of the pattern.
- **Related Patterns:** Other patterns that have some relationship with the pattern; discussion of the differences between the pattern and similar patterns.

In this stage, we are proposing the concept of using patterns to refine elicited requirements, also we provide a short list of patterns related to the case study examined in this project. This is due to the fact that currently there is huge catalogue of design patterns available. One can decide on the database of patterns he/she wants. This applicates more in case of this framework which is using security and privacy patterns as well. Regarding our case study, e-commerce application we have selected UI (User Interface) design patterns. A list of practiced patterns are provided in Section 4. 2 (Tables). Therefore, in our ontological model, here we have catalogue of number of pattern's lists. In other word, we do not provide any information from patter's inside information (based on the standard format. We propose an ontological format of pattern for future, where pattern's concepts are modelled and formalised and correlation to other ontologies are constructed.

3. 6 Required Technologies for the Semantic Rule-Based Software Privacy by Design (KN-SoPD) Approach

The semantic rule-based approach calls for some requirements to be fulfilled by the implementations they rely on. One of the most critical requirements, which influences the technologies those implementations utilise, is the way in which the knowledge is represented in the model.

As data modelling and knowledge representation are crucial for the semantic rule-based approach. Indeed, a formal modelling language is necessary to enable us to implement the conceptual model of our Ontology-based Compliance framework. Therefore, the Ontology Web Language (OWL) which is a family of knowledge representation languages for authoring ontologies is employed for this implementation.

Additionally, among implementation needs are technologies that support the modelling, manipulating, serialising and parsing of such models. In order to produce compliance effects, where laws and authority guidelines can be applied to system context and be mapped and refined to each other, our system needs an expressive rules language and a reasoning engine for to interpreting the rules.

‘‘This work was conducted using the Protégé resource, which is supported by grant GM10331601 from the National Institute of General Medical Sciences of the United States National Institutes of Health” (Musen, 2015, p.57). Protégé is a free and open-source ontology editor with a suite of tools to construct domain models and knowledge based application with ontologies. Protégé fully supports the latest OWL 2 Web Ontology Language. We trusted the known application of Protégé in different projects and the competition of Protégé with other ontology editors such as Apollo, OntoStudio, Protégé, Swoop and TopBraid Composer Free Edition in the work done by Alatrish (2013). This researcher has compared mentioned editors using different criterions such as generality, expressiveness, complexity, documentation and scalability and price. The first important metric for us to decide on an editor was the generality and price. We found Protégé as an open-source and very well-known tool. Having a graphical environment with less complexity and being easy to learn, were other reasons we selected protégé for this approach.

We have called our designed semantic-based automated tool for the compliance of software design to privacy laws as AU-SoPD (Automated-based Software Privacy by Design). A complete manual of implementation of this tool is provided in APPENDIX III. Here we are discussing the technology to implement the tool with some examples.

3.6.1 Data Modelling with OWL

The Web Ontology Language, OWL (Sirin & Parsia, 2004), is a knowledge representation language for authoring ontologies. OWL facilitates greater machine interpretability of human knowledge by providing additional vocabulary and formal semantics. In our Ontology-based Compliance system, the components of our framework are modelled using OWL.

OWL is based on description logic, thus its construction has well-defined meanings which are used to describe domain concepts and their relationships in an ontology. For instance, in the domain of Laws, concepts such as *Controller* or *Personal-Data* will be modelled as classes in OWL. For example, a law stakeholder called *ESilver-Company* is created as an individual of the class Controller. Also, *Customer-Name* is created as an individual of the Personal-Data class. If Controller and Topic have a relationship such as "*Controller collect Personal-Data*", this relationship can be created in OWL as a link between Controller and Personal-Data concepts. The existence of this generic, somewhat abstract relation, would allow stating specific knowledge in a given setting (called facts or assertions), such as "*Controller collect Personal-Data*". Furthermore, OWL offers different constructions for expressing further restrictions on the relationships among concepts, including cardinality and domain and range restrictions such as union and disjunction. It also has a rich vocabulary for describing relations among classes, properties and individuals. For instance, a class can be an IntersectionOf or a UnionOf some other classes. Additionally, we can state that a property is Transitive, Symmetric, InverseOf another one, or Equivalent of another one. Also, we can specify that a class instance is the Same Individual as another instance, or is different from a certain other instance. Our ontological links between different components of framework mostly drives on *Equivalency*, where same concepts with different terminologies are mapped together. The result is inhabitation of all properties of a class to its equivalent.

As a result of formalising the descriptions of Compliance models in OWL we are able to support reasoning on knowledge base, reusing data and sharing data. OWL also enables the inferring new knowledge that is not explicitly stated in OWL ontologies. It also has some appropriate features including valuable expressive power, formal syntax and semantics, and practical reasoning systems. These features make it a suitable language for representing ontology.

3.6.2 Semantic Rules using SWRL

SWRL (Semantic Web Rule Language) (Horrocks, 2002) is a semantic rules language based on a combination of Ontology Web Language and Rule Mark-up Language for formalising the expression of rules. It is an emerging XML-based framework for building rules on top of OWL ontology.

OWL has a set of basic implicit reasoning mechanisms based on description logic. OWL needs additional rules to express relations that cannot be represented by ontological reasoning. Ontologies require a rule system to make further inference for deriving further information that cannot be captured by ontologies, and rule systems require ontologies in order to express rules in terms of OWL concepts and relationships. Rules can be used to infer new knowledge from existing OWL knowledge bases. In our approach, SWRL is used as a reasoning and inference mechanism to express compliance techniques in where rules of laws and legal authorities are build using SWRL on OWL statements, are applied to system context and constructed rules also are mapped and refined from each other also using of SWRL.

SWRL extends OWL's expressiveness while preserving a simple syntax. It is also compatible with OWL syntax and semantics, since they are both combined in the same logical language. It extends the set of OWL axioms to enable Horn-like rules to be combined with an OWL knowledgebase. It also allows developer to use a variety of rule engine store as on with the SWRL rules stored in an OWL knowledge base.

In our compliance model, rules of laws, standards and guidelines are presented using SWRL that are not easily or naturally modelled within OWL. The logic underlying our framework (Figure 3.1) is explicitly captured on the basis of a rule-based model. As a consequence of executing -the rules, refinement, mapping and inheriting of different components of framework are generated in order to implement the concept of compliance in our model. Moreover, the rules can be easily modified in case of change in laws and guidelines, thus increasing the flexibility and extensibility of our system.

3.6.3 Individualling Process in Protégé

One of the critical activities in designing an ontology is differentiating between classes and instances of them. Here is the activity where a real-world scenario from a specific domain is constructed using the knowledge represented in an ontology. For example, E-Silver Company is an instance of the class *Controller* in Law Ontology or E-Silver Customer is an instance of Class *data-subject*. Individuals are semantically related to each other using statements.

3.6.4 Pellet Reasoner

Compatible reasoner for protégé are pellet, Fact++, RacerPro and KAON2. We have selected Pellet which is an open-source, JAVA-based OWL 2 reasoner. As a consequence of executing pellet reasoner, SWRL rules are generated and refinement, mapping and inheriting of different components of framework works in order to implement the concept of compliance in our model. One of the key tasks of reasoned in our approach is the application of law to system context. Therefore, rules are automatically applied on any corresponding areas of system context (individuals).

3. 7 Summary

This chapter has presented the design of the semantic rule-based approach for a compliance framework for developing software systems which we called KN-SoPD. It also illustrated the features of this approach needed for developing a flexible and extensible automated system supporting our conceptual model called AU-SoPD. These features are the separation of the models using ontology, defining refinement, mapping and inheriting strategies using semantic rules. In this chapter we also studied the factors that have an effect on designing and implementing the models. The domain models were then presented from the perspective of domain independence, their classes and properties were represented and where practiced by a simple case study with respect to accuracy of evaluation.

Lastly, the required technologies for implementing the Ontology-based Compliance framework, based on semantic rule-based approach were discussed. The proposed approach in this research is an answer to the demand of Privacy by Design. PRD is a recently introduced concept in domain of compliance to data protection laws. This is to ensure software products and business processes take compliance to data protection and privacy essential in very early stages of their development; design. KN-SoPD, is a useful conceptual model which can be used as a reference model for software developer or compliance officers in order to instruct them on a stage-by-stage process through compliance of a designing system or organisation. The advantage of this model is its unique umbrella of different resources from requirement engineering to laws, standards to best practices. Although KN-SoPD has been developed here for compliance to privacy, but the general conceptual model is designed in a way that can be used for compliance to any law. The designed automated tool (AU-SoPD), provides a very easy to be used environment for developers. The user interface only requires users to instance defined ontological concepts with individuals from system or business context and fill the ontological facts. The logical reasoner and defined rules in this approach, automatically calculates where application of law is necessary in system context and show elicited requirements. It has been developed in a way that all requirements from law to standards and best practices are resulted and shown in same time. But the query-based interface enables the user to trace back any extracted requirement to its parent-compliance resource where the requirement have been refined from. AU-SoPD can be used as a huge repository and knowledge representation environment in compliance to data protection only for design purposes. One can use this approach to know about the obligations and their rights of system stakeholders and how they can be implemented and refined with further but high-level requirements. For example, using his tool, we can know that one of the requirements of compliance to data protection for an ecommerce application is to provide a privacy notice to viewers in the web site. To do this, further requirements are recommended to user as a need for a layered structure of notice and the information that should be included in it. It also guides the user to take a model of on-line privacy notice by using of sign-in or Privacy Notice design pattern in order to fulfil the elicited requirements. The developer can take this knowledge to develop a system in compliance with privacy. They do not need to have any further information and knowledge of where to apply the laws or when and how refine a high-level legal requirement. No manual guideline or reasoning functions are required.

4. EVALUATION

The aim of this chapter is to evaluate our semantic rule-based approach of Software Privacy by Design in order to examine whether it fulfils the objectives of this research. Throughout the evaluation process, we will use the KN-SoPD system which is implemented based on our framework. For more detail and guidelines regarding KN-SoPD, one can refer to the manual provided and attached in APPENDIX IV. This manual also has provided information regarding constructing KN-SoPD tool.

After this introduction, in Section 4.1 the methodology of evaluation is described. Section 4.2 describes the benefits of using an ontology-based system for software privacy by design based on a semantic rule approach. These benefits are recognised through evaluating the findings of using a case study with some effectiveness factors determined by a very creditable resource for privacy by design in software application.

Section 4.3 provides a summary and conclusion of our evaluation methodology.

4. 1 Methodology

In order to exercise the effectiveness of the proposed and designed approach to compliance in this research, also to examine the correctness of extracted compliance requirements, we are firstly taking a case study here to evaluate our framework and its supporting tool which is called KN-SoPD. Based on definitions, "A case study is a method for learning about a complex instance, based on a comprehensive understanding of that instance obtained through extensive description and analysis of that instance taken as a whole and in its context. We use case studies for in-depth consideration of the results of a project or group of projects or to illustrate given points" (Morra & Friedlander, 1998, p.21).

Regarding to the sensitivity of the financial and privacy aspect of e-commerce application requirements, it has been selected here to be analysed against its privacy requirements. The case is to design and analyse requirements for web site of an Italian supplier of silver-made artefacts briefly called B-Silver. This case has been provided in a previous research known as AWARE which also had been analysed with i* methodology (Bolchini & Paolini, 2004). We have chosen this case and also have added further design to it in order to synchronise the work with other researches. Whole stages of designing E-Silver case by KN-SoPD are presented in APPENDIX IV. In order to validate the outputs of our case study design by KN-SoPD, further to this we evaluate extracted requirements for this case with outputs of a project called OWASP Top 10 Privacy Risks (Open Web Application Security Projects (OWASP)).

In fact, we are investigating if the privacy requirements extracted for E-Silver with KN-SoPD, are really addressing the aims and objectives of Privacy by Design as had been defined by GDPR. OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted. The OWASP Top Ten is a powerful awareness project for web application security and privacy which has provided a list of top 10 most critical privacy risks to web applications. The Project provides tips on how to implement privacy by design in web applications with the aim of helping developers and web application providers to better understand and improve privacy. We are mostly focusing on a risk numbered as P5 in OWASP list called "Non-transparent Policies, Terms and Conditions" regarding the works being concentrated mostly in our research. OWASP outcomes is being trusted here since it has been approved by organisations such as OECD. This case has been evaluated from 9 different aspects as listed below. These are key factors found in OWASP documents used to measure the effectiveness of policies, terms and conditions in order to avoid risk P5 (Open Web Application Security Projects (OWASP)).

- Easy to find
- Fully describe data processing
- Understandable for non-lawyers
- Complete but KISS
- User Consent
- User Language
- Collected data
- Readability tester
- Actively communicated

The second stage of our evaluation, is about comparing our work with similar works in privacy by design of software systems. To do this, we have selected 12 studies. The following are the criteria to select the works:

- Does the work add value to the state-of-the-art?
- If the objective of work was Privacy by Design or the work is known sufficiently in privacy subject (academic or industrial)
- Does the work propose sufficient concepts/relations to deal with privacy aspects?
- Each work should be selected from a section in Section2.LITERATURE REVIEW
- If the work is one of the most cited in its domain and the publication year is a close date
- If the work proposes an PRD approach with similar or close components to our work. From the works with same components and concepts we choose the one with most number of components.

The evaluation is against the 7 principles of PRD introduced by Cavoukian (2011). We have detailed each of these principles with some concepts and characteristics of PRD. To do so, we also referee to the definition of each principle by Cavoukian. Following is a list of the 7 principles along with their characteristics:

1. Proactive not Reactive; Preventative not Remedial: In short, Privacy by Design comes before-the-fact, not after. To examine this property, we have divided it to: having RE methodology in the approach or having some elements of design and having risk assessment in design; to have RE, the approach should have the same concepts or synonyms of actor, agent, goal, task, stakeholder, non-functional requirements, etc. To have a proactive compliance, it is also important to consider the risks against system as soon as possible. Therefore, it is necessary to have Risk Assessment in design; which includes concepts of risk, threat, attack, asset, vulnerability, treatment, controls

2. Privacy as the Default: This property is also defined by following attributes: Purpose Specification, Collection Limitation, Data Minimization, Use, Retention, and Disclosure Limitation. We have shortened these attributes totally to processing purpose (PP) and technical controls for data minimisation and collection minimisations. These technical controls are mostly user centric technologies.

3. Privacy Embedded into Design (A systemic, principled approach to embedding privacy, detailed privacy impact and risk assessments). In short it means there should be a systematic methodology to enforce legal requirements to software development and requirements elicited by RE. This property also is divided to systematic Integration of policy requirements in design and application of law on system context. In our competition we satisfy these properties with concepts of integrate, map, apply, inherit, link, etc.

4. Full Functionality – Positive-Sum, not Zero-Sum mean that approach shall satisfy all legitimate objectives − not only the privacy goals. It is divided to satisfying privacy goal or satisfying other legitimate goals. To have this we consider if all compliance resources such as standards, law, directive and guidelines have been taken in an approach with examining of same concepts.

5. End-to-End Security – Lifecycle Protection (Security, Applied Security). To have an end to end security we may even have security minded in organisational controls (orgc), in technical controls (tc) or have a technical approach (ta) to security such as identity management approaches. We also examine security of an approach with existence of concepts such as integrity (int), availability (avl), confidentiality (con), authentication(authc), authorisation(auths) and non-reputation (nrp), principles of security.

6. Visibility and Transparency -Accountabilty, Openness, monitor, evaluate, and verify Compliance. for accountability, first all rights and documents should have been specified (right), and we shall have controls for lawfulness (lwf) and

fairness (fs) of process, for openness we shall have concept of Privacy Notice (PN), and have transfer to third party policy (trs), and for compliance monitoring we test it by if the approach has a post design compliance verification methodology for auditing (aud) and monitoring (mon)

7. Respect for User Privacy: to have respect for user privacy we test it by concepts of consent (cst), accuracy of processing data (acr), user access (uac), communicate information about processor to the public which is tested by privacy notice (pn), controller or processor identity (ci, pi)

The result of the comparition is calculated by a score given to each work. This score is calculated based on the number of concepts included or not-included in each work and following formula is used for calculation:

Included = √ non-included= × partially-included = Ᵽ unknown = - number = N

Total-Score =N (√) * 2 + N (Ᵽ) - N (×)

4. 2 Case Study Evaluation

4.2.1 Non-transparent Policies, Terms and Conditions:

This risk is prioritised as risk number five in the series of OWASP Top 10 Privacy Risks. This is to check if web-sites are not providing sufficient information to describe how data is processed, such as its collection, storage, processing and deletion and failure to make this information easily accessible and understandable for non-lawyers. All web-sites that allow input of data and online forms and collect personal information should have clear policies that outline how data will be used, shared, and retained. In following sections, we are testing if the requirements extracted for ESilver website are addressing requirements specified by OWASP for P5. The evaluation is based on a checklist and countermeasures provided by OWASP for P5 (Open Web Application Security Projects (OWASP)).

We are investigating the requirements for P5 in our model based on a top-down process in compliance when it starts from GDPR and refined by standard, ICO and finally design patterns.

Generally speaking, and from higher level of compliance in our approach, the requirement for transparent policies, terms and conditions is considered in our approach by Law Ontology and specifically by (Article 5 of GDPR). Having transparent policies is a property for lawful and fair process of personal data as defined by Article 5 of GDPR. Rules depicted from Article 5 of GDPR along with their equal rules from standard and ICO, are represented and listed in Table4.1. The result of implementing and applying these rules on ESilver case study are also in APPENDIX VI.

Subject	GDPR	Standard	ICO	Pattern
Transparent Policies, terms and conditions	Article5 1st.LObligation 2nd.LObligation 3rd.LObligation	18th.SObligation 20th.SObligation 21th.SObligation	8th.GObligation 9th.GObligation 2nd.GObligation 3rd.GObligation	Account Registration/Privacy Policy

Table4.1 . Non-Transparent Policies, Terms & Conditions

4.2.2 Easy to Find:

According to OWASP countermeasures to avoid risk P5, one of the key factors to investigate controls for P5 is to find out how easily the terms and conditions and policies regarding privacy of personal data of customers are addressed and represented in a web site. This a property which almost is addressed by implementation components such as patterns, but are defined in higher levels of compliance with general rules as well, which can be found in Table4.2.

Subject	GDPR	Standard	ICO	Pattern
Easy to find	10rd.LObligation 12th.LObligation	14.SObligation	GPermission25th GPermission26th	Account Registration/Privacy Policy

			GPermission27th GPermission28th GPermission30nd GPermission31rd GPermission33th GPermission34th GPermission35th GPermission36th GPermission37th GPermission38th GPermission39 GRecommendation4st GPermission40nd	Privacy-policy pop-up Set-up notice

Table4.2 . Easy to Find

4.2.3 Fully Describing Data Processing

Next countermeasure to estimate if a web site has implemented appropriate methods and controls for to acknowledge its privacy policies, is to check if it has fully described what it is doing with personal data. This criterial is detailed in OWASP guideline to characteristics if privacy policy contains the information of processor, transferring data, analysis performed, retention time, rights and others. Following table shows how our compliance components and rules are addressing these requirements.

Subject	GDPR	Standard	ICO	Pattern

Fully describing data processing	22thObligation	23nd.SObligation	13th.GObligation	Account Registration/Privacy Policy
	23thObligation	24rd.SObligation	14th.GObligation	
	24thObligation	25th.SObligation	15th.GObligation	Providing a list of used cookies and widgets in privacy notice
	25thObligation	26th.SObligation	18th.GObligation	
	26thObligation	27th.SObligation	19st.GObligation	Opt-out Button
	27thObligation	28th.SObligation	20nd.GObligation	DO-NOT-TRACK
		29th.SObligation	GPermission5th	
		30th.SObligation	GPermission6th	
		31th.SObligation	GPermission7th	
		32st.SObligation	GPermission8th	
		33nd.SObligation	GPermission9st	
		34rd.SObligation	GPermission10nd	
		35th.SObligation	GPermission11rd	
		36th.SObligation	GPermission12th	
		37th.SObligation	GPermission13th	
		38th.SObligation	GPermission14th	
		39th.SObligation	GPermission15th	
		40th.SObligation	GPermission16th	

Table4.3 Fully Describing Data Processing

4.2.4 Understandable for Non-Lawyers

Using a context for privacy policy which is not vague and genera like legal text is a key factor to make a transparent policy. Web site designers must take in consideration a plain and clear language for user to understand their terms and conditions. This is being addressed by number of articles, principles and guide notes in GDPR, ISO 29100 and ICO godliness noted in Table 4.5.

Subject	GDPR	Standard	ICO	Pattern

Understandable for non-Lawyers	13th.LObligation 14th.LObligation 15th.LObligation	12st.SObligation 13nd.SObligation		Account Registration/Privacy Policy Visual notice(pictograms) Auditory notice

Table4.4 . Understandable for Non-Lawyers

4.2.5 Complete but KISS

Web designers are recommended by OWASP, also by guidelines to attempt to use short privacy notices. This is to help users to quickly get aware with legal requirements and their rights. This is almost done by a layered structure of privacy notices and number of links to external materials. These requirements are almost addressed by ICO guidelines.

Subject	**GDPR**	**Standard**	**ICO**	**Pattern**
Complete but KISS	LPermission3nd LPermission4rd LPermission5th		GPermission40nd GRecommendation2rd GRecommendation3rd GRecommendation7th GRecommendation8th GRecommendation9th	Account Registration/Privacy Policy (Pictograms) Layered notice

Table4.5 Complete but KISS

4.2.6 User Consent

Regarding the importance and necessity of the matter of user allowance for processing his/her personal data, numbers of obligations and recommendations from GDPR, standard and ICO are specified to the subject of user consent. This is in situation in which a spate article in GDPR, a principle in ISO 29100 and a guideline in ICO are considered with this title. Following table is listing the rights elicited from each regarding the consent of user.

Subject	**GDPR**	**Standard**	**ICO**	**Pattern**

User Consent	Recommendation1st Recommendation2nd 5thObligation Permission1st 8thObligation	30thObligation 31stObligation 35thObligation 45thObligation	99thObligation 88thObligation 89thObligation	Account Registration/Privacy Policy Track-User Blocking-notice Non-blocking notice

Table4.6 User Consent

4.2.7 User Language

Providing privacy policy and user consent in different languages is an attempt to make privacy policy understandable for all users. Thus can also be categorised under the countermeasure of Understandable for non-lawyers. Obligations and recommendation from laws and standard and also ICO are almost the same mentioned in Table4.5. In application level this countermeasure can be taken into consideration with a UI pattern of Language Menu. Since the case study of Esilver is an e-commerce implementing in Italy, it can be provided in different European languages such as Italic, English, French and possibly Spanish or others.

4.2.8 Actively Communicated

This is a requirement directly addressed by ICO. This is a considering recommend when controller or processor are collecting sensitive personal data of data subject. Thus there is a need for a user consent directly addressed to the user instead of using normal methods of taking consent such as online forms. To actively communicate the consent with the user, ICO has recommendations such as sending email and letters to data subjects or using awareness scripts. These are mentioned by detail in following table and showing how this important is addressed in our approach.

Subject	GDPR	Standard	ICO	Pattern
Actively communicate			**G**Permission18th **G**Permission19st **G**Permission20nd **G**Permission21rd **G**Permission22th	Automatic email Just-in-time-click Context-depended notice Persistence notice Decoupled notice

Table4.7 . Actively Communicated

4.2.9 Collected Data

This countermeasure requires the data controller to explain to user which data are being collected and the collecting purposes. This also had been considered by GDPR, standard and ICO and being addressed in our approach by number of obligations and recommendations based on following table.

Subject	GDPR	Standard	ICO	Pattern
Collected Data		31th.SObligation		Account Registration/Privacy notice Browser Cookie

Table4.8 . Collected Data

4.2.10 Readability Tester

The main point of using readability tester is to make sure the context of web sites and specifically here, privacy notices on websites are readable and clear for users. This has been addressed by number of rules of law and regulations. Different technologies are available to perform this task automatically on web sites in order to test the scale of readability of web contents which are mentioned in pattern category.

Subject	GDPR	Standard	ICO	Pattern
Readability Tester	13th.LObligation 14th.LObligation 15th.LObligation	12th.SObligation **13**nd.SObligation **14**rd.SObligation		Readability Score Screen Reader

Table4.9 Readability Tester

4. 3 PRD Approaches Comparison

In this section, we are comparing our work with other similar approaches from our literature review list. We have selected 12 other woks to be compared (Table4.10, Table4.11). The metrics we used for comparison, are based on the PRD principles defined by Cavoukian (2011). Since these principles are very general and regarding the notion of our work which is an ontology-based approach we examine each of these principles with related taxonomy of concepts in each domain. We opted these concepts during our literature review. The eighth property to be evaluated is not a PRD principle and is just selected to evaluate the usability of the works.

Author	Article	Year	Citation	Components	Concepts
Anderson	A security policy model for clinical information systems	1996	414	Risk assessment, Security Policy, General Medical Council and the British Medical Association	Threat, risk, control, policy, security, guideline, privacy, confidentially, access control, consent, notification, processor name, patient access, integrity, encryption, transmit
Breaux et al	Mapping Legal Requirements to IT Controls,	2013	230, 3	Law, standard, automated tool	Law, data protection, privacy, standard, right, notice, consent, stakeholder, constraint, obligation, IT controls, link, map
Gangemi et al	Some Ontological Tools to Support Legal Regulatory Compliance, with a Case Study	2003	58	Ontology, law, directive, Hohfeld, compatibility assessment	Law, data protection, directive, Right, Obligation, privilege, permission, power, subject, asset, natural person, information, fact
Gharib et al	Ontologies for Privacy Requirements Engineering: A Systematic Literature Review	2016		Ontology, policy, privacy, security, organisational, risk, treatment,	Actor, goal, agent, role, decomposition, information, personal information, own, trust, monitoring, risk, threat, attack, vulnerability, privacy, privacy mechanism, confidentiality, purpose of use, notice, anonymity, transparency, authentication, authorization, accountability, non-reputation
Hanson & Leenes	Privacy and Identity Management for Everyone/Europe, PRIME,	2005	109	Law, direction, privacy, identity management, user-centric tool individual	Data protection, consent, privacy negotiation, anonymity, accountability,, encryption, security
Humberg & Poggenpohl.	Using Ontologies to Analyze Compliance Requirements of Cloud-Based Processes.	2014	4	Cloud, ontology, RE, law, directive, standard, data protection, security, UML, BSPM, risk analysis, automatic tool, formalization, design-time and run-time compliance	Map, activity, security, IT controls, organisational control, security, privacy, integrate, risk, audit, Rule, Rule elements, situation, constraint, artifact, process, property, map,
International Business Machine Corporation	Privacy Guidelines for Developing Software and Services	2007		Guideline, privacy, software development life cycle, standard	Data protection, privacy, security, consent, notice, data minimization, IT controls, transform
Islam et al	A Framework to Support Alignment of Secure Software	2011	36	Framework, RE, Risk, Hohfeld, UML, i*, data protection, privacy,	Align, map, right, actor, goal, take, resource, activity, risk, threat, vulnerability, treatment, security, authentication, authorization,

	Engineering with Legal Regulations			security, security pattern, standard	access control, availability, non-reputation, organisational control, IT control
Kalloniatis	Addressing privacy requirements in system design: The PriS method, Requirement Engineering Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements	2008 2013	109 32	RE, Piracy, RE, Knowledge Development (EKD) framework, formalization, i*	Data protection, identification, authentication, authorization, data protection, anonymity, pseudonymity, unlinkability and unobservability,security,goal, process, decomposition, integrity, transparency, access control, stakeholder, threat, weakness, has-impact-0n, user, pattern, user, IT control, organisational control, encryption tool, Administrative tools, Information tools, Anonymizer products, services and architectures, Pseudonymiser tools, Track and evidence erasers, actor, task, agent, resource, map, link
Langheinrich	Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems	2001	895	privacy by design, ubiquitous computing, law,	Privacy, data protection, notice, choice and consent, IT control, organisational control, security, Anonymity and Pseudonymity, Proximity and Locality, Access and Recourse
May et al	Privacy APIs: Access control techniques to analyze and verify legal privacy policies	2006	114	Privacy, policy, access control technique, formalization, law, audit	Transfer, action, creation, right establishment, notification, logging, consent
Rahmouni et al	Semantic Generation of Clouds Privacy Policy	2015		Cloud, ontology, privacy, risk, security, access control, law, directive, extensible access control markup language (XACML)	Notice, consent, stakeholder, map, data protection, enforce, action, subject, resource, purpose, obligation, right, encryption, access control, anonymity, allow, deny, risk

Table4.10 Compliance Approaches for PRD

As an example, Breaux & Antón (2008) introduced a framework to elicit rights and obligations from legal texts using language patterns. He classified concepts elicited from laws to classes of stakeholder, right, obligation, constraints and etc. Although his work is considered in RE, but no specific methodology in this domain was used in his framework. Thus he did not have taxonomies of RE methodologies concepts such as actor, task, goal, etc. In his later work, Breaux et al (2013), he took a framework to map the elicited legal requirements to IT controls from number of standards. Therefore, we extended his ontology with concepts of map, organisational and technical controls (orgc, tc), standard (st), security (sec), refine (ref) and others. Similar to this we evaluated our work. We filled the checklist of concepts with elements from i*, rights, privacy and its elements (cont, notice, etce), data protection, map, link, refine and security and its elements. As the wok is a knowledge-base (ontology), we picked the concept of knowledge (knw) too. Finally, we evaluated each work with he scoring system as described before.

To fill the checklist, we did not have any positive or negative answer to the concepts we were not sure about their existence in listed works. Ᵽ also represent if a concept was partially participated in a work. It should be mentioned that having a less score compared to theirs, does not mean a negative evaluation of the work. Although we have opted the works from PRD, some may be typically addressing other objectives of PRD.

Since we have number of components in our framework, from i* for RE, to law, law analysis, data protection, privacy by design, design patterns, standards and guidelines and risk analysis, and regarding the usage of ontology and semantic web relating and linking all these components, we had most of the concepts from Table5.10 existences in our work. Since our work is a knowledge-based approach to assist software developers and compliance officers to get knowledge from compliance requirements and their design solution in software development or business process, we did not provide a technical solution such as identity management approach. But we should have some design patterns (security pattern) available for this. Although it is not mentioned in current work, but the work is capable to be extended by this pattern and also it has been provided in conceptual platform of current approach.

Authors	Proactive not Reactive															Privacy as the Default			Privacy Embedded into Design		
	nfr	RE	dsg	acr	st	obj	act	tsk	agn	goal	thrt	vul	ass	thm	Risk	prs	clm	dm	integr	apply	map
Zarrabi (2016)	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	×	×	√	√	√
Kalloniatis,(2008)		√	√	√	√		√			√	√	√		√		√	√	√		√	√
Islam, (2011)	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√				√	√	√
Kalloniatis, (2013),	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√		
I BM (2007)		√	√													√	√	√	×	×	×
May et al. (2006)		√	√			√	√														√
Langheinric (2001)		×															Ᵽ	Ᵽ			
Gangemi et al. (2003)					√	√	√		√							√				√	
Humberg et al. (2014)		√		√		√	√		√		√	√		√	√					√	√
Gharib et al (2016)		Ᵽ		√		√	√		√	√	√	√	√	√	√	√			×	×	×
Hanson & Leenes (2005)	×	×		×	×	×	×	×	×	×						√	√	√	×	×	×
Anderson (1996)	×	×	×	×	×	×	×	×	×	×	√	√	√	√	√	×	×	×	×	×	×
Breaux, (2013)		√	√	×	√	×	×	×	×	×	√	√	√	√	√	√	Ᵽ	Ᵽ	√		√
Rahmouni, (2015)				Ᵽ	Ᵽ	Ᵽ	Ᵽ								√	√				√	

	Full Functionality								End-to-End Security											
link	law	Data-pr	prcy	stnd	dr	gl	ref	dec	orgc	tlc	con	ath	Int	atr	avl	nrpt	Id-mg	encry	Acc-	sec
√	√	√	√	√	√	√	√	√	√	√	Ᵽ	Ᵽ	Ᵽ	Ᵽ	Ᵽ	Ᵽ	Ᵽ	Ᵽ	Ᵽ	√
		√	√	×	×	×		√	√	√	√	√	√	√	√	√	√	√	√	√
	√	√		√	√		√	√		√	√	√	√	√	√	√	√	√	√	√
		√	√					√	√	√	√	√	√	√	√	√	√	√	√	√
×	√	√	√						√	√	√	√	√	√	√	√	√	√	√	√
	√		√							√	√								√	√
	√	√	√			√			√	√	Ᵽ	Ᵽ	Ᵽ	Ᵽ	Ᵽ	√	√	√	√	√
√	√	√	√		√				×	×	×	×	×	×	×	×	×	×	×	×
	√	√	√	√	√			√	√	√										√
×	√	√	√		√			√	√	√	√	√	√	√	√	√				√
×	√	√	√		√	√				√	√	√	√	√	√	√	√	√	√	√
×	×	×	√			√	×	×	√	√	√	√	√	√	√	√	√	√	√	√
	√	√	√	√			√		√	√	√	√	√	√	√	√	Ᵽ	√	√	√
	√	√	√	×	√		×	×	×	√								√	√	√

Visibility &Tansparency					Respect for User Privac			Usability					Total Score
right	Trs	ntc	mn	Is-cmp	const	Usr-cr	Uacc	aut	knw	eas	frm	reuse	
√	P	√	×	×	√	×	×	√	√	P	√	√	81
	√		√		√	√	√	√			√	√	69
√								×	×			√	72
	√	√			√							√	76
		√			√	P	√	×	√		×		43
	√						√				√		28
		√			√			×	P				32
√	√	√	√	√	√	×	×	√	√	√	√		28
√	√	√	√		√			√	√	P	√		57
√	√	√	√		√				√	P			60
	√	√			√	√	√	√	×	√			39
	√	√			√		×		×				19
√	√	√			√			√			√		61
√	√	√			√			√	√	P	√		37

Table4.11 Comparing PRD Approaches

4. 4 Conclusion

In this chapter, we were able to evaluate our work with a trusted resource which had been successful in recent years in collecting privacy risks against web applications and other electronic medias. OWASP TOP 10 Privacy Risk for Web Application (Open Web Application Security Projects (OWASP)), has provided a list of ten most critical privacy risks against web application and is recognised by key organisations in this industry such as OECD. OWASP has introduced number of countermeasures in order to avoid each risk. We used a case study and designed it with our approach, AU-SoPD. Complete process of AU-SoPD design is available in APPENDIX IV. Our attempt in this research was almost to address one of the key requirements of GDPR to *provide privacy notice* for processing of personal data to data subject and its circumstances. Therefore, we evaluated our work and the result of practicing KN-SoPD with Esilver case study with risk P5 "*Non-Transparent Policies, Terms & Conditions",* from the list provided by OWASP. The process of evaluation includes matching and comparing the elicited requirements for the case study practiced with AU-SoPD by OWASP countermeasures for P5. The requirements may have been elicited by each ontological component of our approach either from GDPR, related standards or ICO or by technological solutions addressed by design patterns. The result of our evaluation process showed that each of OWASP countermeasures has been addressed by number of rules from laws and regulations in our approach and also technical and design solution. This is in a situation where each countermeasure is addressed with at least one of our compliance resources, in some cases they are addressed by all. Although here we only assessed one of privacy risks, but our approach is able to address most of privacy requirements since it is an integrated compliance solution covering laws, standards and guidelines. Therefore, if one of these resources lack in covering a legal requirement, the others will do this importance for sure. This has been defined as the key difference between our work and similar previous researches.

In second stage of our evaluation process, we compared our approach with number of other recently developed approaches by researchers around the world. We tried to select the closest one to ours which considerable amount of referencing. Our evaluation was against the type and number of ontological concepts used in each approach. Based on our test, KN-SoPD had the most concepts compared to other works. It shows that our attempt to cover most possible elements of compliance and design was successful. Some other works strength from having more technical terminolies, hence ours are more conceptual. We can address this in our future work.

As mentioned before, we have used European Data Protection Directive as the reference model of privacy for our approach. Comparing to other works, this approach may lack in full supporting of other national and international privacy frameworks. This is a limitation which can be addressed in future works. Although our study with other privacy legislations in shows that there is a simultaneous pollicisation in establishment of international legal frameworks regarding Data Protection and similarity between their rules. Therefore, considering a key and comprehensive framework such as European Data Protection will almost address other legislations too.

5. Conclusion, Limitations and Future Works

5.1 Introduction:

We opted an ontology based framework for the compliance of software systems in their design stage. This is a framework which has the definitions in management level of software development compliance, also concepts that assist the implementation of compliance specifically for the concept of "Privacy by Design". Privacy by design has been introduced in General Data Protection Regulation (2012) with the purpose of taking compliance to privacy in design of products particularly information systems.

5.2 Achieved Objectives:

Our aim was to achieve number of objectives in design of the components of the proposed framework in this work, called as KN-SoPD. Main structure of KN-SoPD has been constructed based on GDPR organisation and integrated with ISO/IEC standards and Information Commissioner Office guidelines. In other word, the implementation of compliance is by using controls from ISO standards, guidelines from organisations such as ICO, using design and security patterns and well-known and experienced security and privacy requirements. The framework also makes it possible to perform a risk analysis on system and legal objectives and requirements. This is to ensure that the compliance is always accompanied by a risk assessment methodology. The ontological implementation of the framework is an alternative through number of objectives. First it provides a huge repository of compliance concepts and terminology, from laws and regulation, to standards and authority guidelines and finally implementation controls and patterns. The query based platform of ontology eases the task of complier to retrieve requirements appropriated to the level of development. Both conceptual and practical frameworks here, support the task of legal reasoning in order to analyse legal texts and apply them to system context. This is with the usage of rule textual analysis, and using ontological reasoning infrastructure. The next objective is addressing requirement engineering process, particularly to the goal oriented modelling language concepts. This addresses the requirement of Policy by Design which takes policy compliance as one of the earliest requirements of system. Requirement engineering methodology also is modelled by our ontological framework. Thus we are able to integrate RE and compliance together. The whole structure of the platform makes it possible to trace back any of compliance requirements to its root from laws, policies, standards, guidelines or etc. This is also an objective for one of the main necessities of ISMS; documentation and specification. The other advantage of using ontology in this work is the different types of links that ontology provides between different ontologies. This provides us an automated solution for the conceptual model of our framework.

5.3 Contribution to Knowledge:

A system developer, compliance officer or a student in both domains, can use this approach (KN-SoPD) and its supporting automated tool (AU-SoPD) to retrieve information about how to comply a developing software system or a business process with Data Protection. They can design an initial model of their system which is in conformance with privacy laws and regulation. This approach conforms compliance to data protection, ISO 27000 series and ISO 29100 in same time and in an integrated and systematic method. The rules specified in these resources are mostly defined in parallel or in definition of each other. To make compliance to all these resources in same time is not an easy task and often performed manually by consultations and referring to manuals. AU-SoPD is an easy to use tool which improve compliance and quality assurance efficiently. Indeed, we did not see reference to Information Commission's guidelines in our literature review. We also used UK ICO Office's guidelines as a support to understand data protection concepts in more detail. The main contribution of current work, is the method that has been used to integrate different resources of compliance to data protection under a unique umbrella which needs very less effort of the user to use it. In other word, the user only needs to use AU-SoPD interface in order to fill the Facts with context from developing system. Running the reasoner, all rights from law, standard and guideline will automatically have derived and applied in right points of the system. Filling the Facts, a risk assessment methodology will also perform automatically on system context and risks, vulnerabilities and their controls are elicited on system context.

5.4 Limitation and Future Works:

Current work also may be critiqued for some limitations such as being a compliance approach only to GDPR which has not considered national implementation of this regulation, or other laws rather than data protection. In other word based on one of 7 principles of GPRD, one may claim that KN-SoPD does not have full functionality. Since any data protection law takes its principle from OECD, they mostly have similar concepts, thus compliance to a referenced framework such as GDPR will almost satisfy most requirements of other data protection laws. But our future aim is also to extend he current work with national versions of data protection law and also with other IT laws. In this case one of the other limitations can be covered which is overlapping of different laws. The other limitation of this work is the scope of technical controls and design and security patterns used in current work. The huge size of current pattern libraries, also the dependency of each of them on type of designing system was a constraint to achieve this goal at the moment. Regarding different number of component in the proposed framework here, we were limited to usage of a specific domain of software systems, which was web applications. Thus, we only practiced patterns related to web applications. But the positive point is the generality of the conceptual model of proposed approach which can later be extended by other components and also its flexibility to changes of law. Other critical point might be the huge number of the conceptual components in KN-SoPD. It may make it looking complicated. But the automated tool, AU-SoPD makes the work easy. From another point of view, we almost tried to draw the links, maps, inherits and other relationship between ontologies using a limited number of description logics in protégé. In future plan for extension of this framework with more laws and standards, we will use more advanced description logics to epic relationships.

Future works can also be specified to comprehensive integration of more components in KN-SoPD. Other laws and standards can be modelled and integrated with current approach in future. In this case, number of ontological rules will vast and may make complication. Thus, the methodology to define and integrate rules should be improved. As said, at the moment component integration in this approach trust on ontological processes of mapping, integration, inherit and others. When more laws and regulation added, this integration more will trust on law structure, their similarities and differences. Thus it needs more study on structure of laws and consequently will make a more developed integration system. Obviously such a project needs a team work to be proposed which can be built based on current work basis and skeletons.

Providing privacy and legal patterns also is an aim which we look to present in future. In order to avoid the manual process of textual analysis of laws and regulation, future works may also focus on using an automated Natural Processing Language technology (Indurkhya & Damerau 2010) to pars legal text and integrating this technique with ontology. In this step we can suggest a text knowledge extraction methodology known as "Operator Grammar" (Zelling 1981) which also has very close definitions to ontological concepts, although some similar works has been done recently. (Maynard et al. 2016). Post-design compliance auditing also can be considered in future.

REFERENCES

Aleven. V. (1999) *Teaching Case-Based Argumentation through a Model and Examples Empirical Evaluation of an Intelligent Learning Environment.* Available at: https://www.semanticscholar.org/paper/Teaching-Case-Based-Argumentation-through-a-Model-Aleven-Ashley/c6ac63f1e07115c24a5a110c22ad6e4b318c566c (Accessed: 27 January 2016).

Anderson, R. (1996) ‘ A security policy model for clinical information systems’, *In Proc. of the 1996 IEEE Symposium on Security and Privacy*, pp.30-43. doi: 10.1109/SECPRI.1996.502667

Antonio. G., & Harmelen. F.V. (2004) ‘*A Semantic Web Primer’*. Cambridge, Massachusetts, London, United Kingdome: TFLeBOOK. MIT Press..

APEC ELECTRONIC COMMERCE STREEING GROUP. http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx

APEC ELECTRONIC COMMERCE STREEING GROUP. “APEC CROSS-BORDER PRIVACY RULE SYSTEM. http://www.apec.org/Meeting-Papers/Leaders-eclarations/1994/1994_aelm.aspx

Aqvist, L. (1994) *Deontic Logic, Handbook of Philosophical Logic: Volume II Extensions of Classical Logic.* Synthense Library

Ashley, P. & Moore, D. (2002), *Enforcing Privacy Within an Enterprise Using IBM Tivoli Privacy Manager for E-business,* IBM DEVELOPERWORKS, Available at: http://www.ibm.com/ developerworks/tivoli/library/t-privacy/index.html (Accessed 25 December 2016)

Awad. A., Decker. G., Weske. M. (2008) ‘Efficient Compliance Checking Using BPMN-Q and Temporal Logic. Business Process Management’, *Lecture Notes in Computer Science. Volume 5240. pp 326-341*. Doi: 10.1007/978-3-540-85758-7_24

Backes, M., Camenicsh, J., Sommer, D. (2005) ‘Anonymous yet accountable access control’, *In Proceedings of the Workshop on Privacy in the Electronic Society 2005*. pp40-46. Doi: 10.1145/1102199.1102208 .

Banisar, D. & Davies, S. (1999) ‘Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Survalliance Laws and Development’, *The John Marshall Journal of Information Technology & Privacy Law, Volume 18 Issue 1.*

Basel Committee on Banking Supervision. (2004) *Compliance and the Compliance Function in Banks*, USA: Basel Committee on Banking Supervision.

Beach. TH., Rezgui. Li., & T Kasim. Y.H. *(*2015) 'A rule-based semantic approach for automated regulatory compliance in the construction sector', *Expert Systems with Applications,* 42 (12) , pp. 5219-5231. doi: 10.1016/j.eswa.2015.02.029

Bechhofer, S., Volz, R. & Lord, P. (2003), 'Cooking the semantic web with the owl api', *ISWC 2003'of Lecture Notes in Computer Science, Springer Berlin Heidelberg*, 2870, pp. 659–675.

Bell, D. & LaPadula, L. (1973) 'Secure Computer Systems: Mathematical Foundations', Mitre Corporation Technical Report', Aviable at: https://pdfs.semanticscholar.org/a3f6/208403fef265fd0e4ad2b4c7ed4c33d45ff2.pdf (Accessed on February 2015).

Benjamin, V.R., Casanovas, P., Breuker. J., Gangemi, A. (2005) 'Law and the Semantic Web, an Introduction', *Lecture Notes in Computer Science,* 3369, pp 1- 17.

Berners-Lee, T. (2006) *Artificial intelligence and the semantic web:* Aaai2006 keynote, PowerPoint slides.

Besnard, Ph., Hunter, A., (2008) *Elements of Argumentation*, USA: MIT Press

Betz, S. & Reimer, U. (2016) 'Requirements Engineering and Business Process Management as preconditions for the application of the Cloud Blueprinting Model', *Modellierung 2016 Workshopband, Lecture Notes in Informatics (LNI)*

Bhatia,J., Evans, M.C.,Wadkar, Breaux,T.D. (2016) 'Automated Extraction of Regulated Information Types Using Hyponymy Relations', *RE Workshops,* PP 19-25. Doi: 10.1109/REW.2016.018

Bhatti. R & Grandison, T. (2007) 'Toward Improved Privacy Policy Coverage in Healthcare Using Privacy Refinement', *In Secure Data Management. Springer*. *SDM 2007. Lecture Notes in Computer Science,* 4721. Doi: 10.1007/978-3-540-75248-6_11

Blobel, B. (2004) 'Authorisation and access control for electronic health record systems', *International Journal of Medical Informatics*, 73(3). Doi: 10.1016/j.ijmedinf.2003.11.018

Bolchini, D. & Paolini, P. (2004) 'Goal-driven Requirement Analysis for Hypermedia Intensive Web-Applications', *Requirement Engineering Conference*, p.p 85-103

Bonatti, P. A. & Samarati, P. A. (2002) 'uniform framework for regulating service access and information release on the web', *Journal of Computer Security*. 10(3), pp. 241–271.

Bonneau, J., Preibusch, S., (2009) The Privacy Jungle: On the Market for Data Protection in Social Networks, Economics of Information Security and Privacy pp 121-167

Bonneau, J., Anderson, J., Church, L. (2009) 'Privacy-Enabling Social Networking Over Untrusted Networks', *The 5th Symposium On Usable Privacy and Security*. CA, USA.

Bons, R.W.H., Lee, R.M., Wagenaar, R.W., Wrigley, C.D. (1995) 'Modelling interorganizational trade using documentary petri nets'. Proceedings of the Twenty-Eighth Hawaii International Conference, 3, pp.189–198. Doi: 10.1109/HICSS.1995.375561

Booch, G., Rumbaugh, J., Jacobson, I. (1999) *The Unified Software Development Process*, 1th edition. Addison-Wesley.

Borchers, J. (2001) *A Pattern Approach to Interaction Design.* 1th edition. John Wiley & Sons.

Busboom, A., Schuler, S., Walsch, A. (2017) 'formalSpec — Semi–automatic Formalization of System Requirements for Formal Verification', *3rd International Workshop on Applied Verification for Continuous and Hybrid Systems, EPiC Series in Computing,* 43. PP 106–114

Brandies, L. & Warrien, S. (2012) *The Right to Privacy*. Editions Artisan Devereaux, USA: LLC Publication.

Breaux, T. D, & Antón A. I. (2008) 'Analyzing regulator rules for privacy and security requirements', *IEEE transactions on software engineering*, 34(1).

Breaux, TD., Anton. A, Spafford, E.H. (2008) 'A Distributed Requirement Management Framework for Legal Compliance and Accountability', *Journal of Computers and Security,* 28(1-2). Doi: 10.1016/j.cose.2008.08.001

Breaux, TD., Gordon, D., Papanikolaou, N., Pearson, S. (2013) 'Mapping Legal Requirements to IT Controls', *RELAW Conference*, pp11-20.

Breaux, TD., Vail, MD., Antón, A. (2006) 'Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations', *Requirement Engineering Conference,* pp 46-54.

Brekeur, J, & Winkel, R. (2003) 'Use and Reuse of Legal Ontologies in knowledge Engineering and Information Management', *ICAIL Workshop on Legal Ontologies & Web Based Legal Information Management*, Lecture Notes in Computer Science (LNCS), 3369. Doi: 10.1007/978-3-540-32253-5_4.

British Medical Association (BMI). Available at: https://www.bma.org.uk/. (Accesed on January 2017).

Brodie, M.L. (1984) 'On the Development of Data Models', *Journal of Conceptual Modelling, Springer Veilag,* pp. 19-47.

Brucker, A. & Petritsch, H. (2009) 'Extending access control models with Break-glass', *Proceeding of 14th ACM Symposium on Access Control Models and Technologies*, pp 197-206. Doi: 10.1145/1542207.1542239

Bruninghaus, S., Ashley, K.D. (1999) ‘Toward Adding Knowledge to Learning Algorithms for Indexing Legal Cases’, *ICAIL '99 Proceedings of the 7th international conference on Artificial intelligence and law*. Pp.9-17. Doi: 10.1145/323706.323709

Byun, J., Bertino, E., Li, N. (2005) ‘Purpose-based Access Control of Complex Data for Privacy Protection’, *Proceedings of the tenth ACM symposium on Access control models and technologies.* pp 102-110. Doi: 10.1145/1063979.1063998

Camenisch, J., Leenes, R., Sommer, D. (2010) ‘Digital Privacy, PRIME, Privacy and Identity Management for Europe’, *Lecture Notes in Computer Science*, *Springer-Verlag Berlin Heidelberg*. Pp.3-89. doi: 10.1007/978-3-642-19050-6

Casellas, N., Nieto, J., Meroño, A., Roig, A., Torralba, S., Reyes, M., Casanovas, P. (2010) ‘Ontological Semantics for Data Privacy Compliance: The NEURONA Project’, *The Association for the Advancement of Artificial Intelligence Symposium*

Cassasa, M. (2004) ‘Dealing with privacy obligations: Important aspects and technical approaches’, *TrustBus 2004*, pp. 120–131. Available at:

Cavoukian, A. (2011) *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, Information & Privacy Commissioner, Ontario, Canada. Available at: https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf. (Accessed December 2015)

Cavoukian, A. (2011), A regulator’s perspective on Privacy by Design, Information & *Privacy Commissioner of Ontario, Canada.* Available at*:* https://fpf.org/wp-content/uploads/A-Regulators-Perspective-on-Privacy-by-Design.doc. (Accessed December 2015)

Chandrasekaran, B., Josephson, J. R. & Benjamins, V. R. (1999) ‘What are ontologies, and why do we need them?’. *IEEE Intelligent Systems* 14(1). pp. 20–26.

CENELEC EN 50128. (1997) *Railway Applications: Software for Railway Control and Protection Systems*, Version 1997

Cirulli, PH. Heinlein, PH. James,D. Telfer, D. (1997) *Application of groupware to ISO 9000 registration via facilitated work sessions*. USA: IBM Publication.

Compagna, L., Khoury, P. E., Massacci, F., Thomas, R., and Zannone, N., (2007) ‘How to capture, model, and verify the knowledge of legal, security, and privacy experts: a pattern-based approach’. *In Proceedings of the 11th international conference on Artificial intelligence and law, ACM*. pp. 149–153.

Connelly, A., (2006), ‘Legal Analysis and Reasoning from Precedent’, *Stanford Encyclopaedia of Philosophy*. Available at: https://plato.stanford.edu/entries/legal-reas-prec/. (Accessed January 2015)

Darimont, R. & Lemoine, M. (2006) ‘Goal-oriented analysis of regulations modelling and their validation and verification’, *Conference: Proceedings of the CAISE*06 Workshop on Regulations Modelling and their Validation and Verification*, Available at:

https://www.researchgate.net/publication/220921689_Goal-oriented_Analysis_of_Regulations. (Accessed December 2016)

Decreus, K., Kharbili, M., Poels, G., Pulvermueller, E. (2009) ‘Bridging Requirements Engineering and Business Process Management’, *Workshop for Requirements Engineering and Business Process Management, Conference on Software Engineering*. pp.215-225

Decreus, K., Poels, G., (2010) ‘A Goal-Oriented Requirements Engineering Method for Business Processes’, *Conference on Advanced Information Systems Engineering (CAiSE*, *Lecture Notes in Business Information Processing*, 72. pp29-43.

Department for Business Innovation & Skills. (2013*) Information Security Breaches Survey*. Technical Report. London: Department for Business Innovation & Skills.

Desai, N., Mallya, A. U., Chopra, A. K., Singh, M. P. (2005) Owl-p: ‘A methodology for business process development’, *Agent-Oriented Information Systems 2005*, pp. 79– 94.

Dolog, P. (2006) ‘Knowledge Representation and Reasoning in Personalized Web-Based e-Learning Applications’, *VSB-Technical University of Ostrava*. Available at: https://pdfs.semanticscholar.org/79bf/b2dc1f6529e8d55eb99d7a18fdc7498bebf1.pdf. (Accessed on Jnauary 2016)

Dritsas, S., Gymnopoulos, L., Karyda, M., Balopoulos, T., Kokolakis, S., Lambrinoudakis, C., and Katsikas, S. (2006) ‘A knowledge-based approach to security requirements for e-health applications’, *Electronic Journal for E-Commerce Tools and Applications*. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.529.8652&rep=rep1&type=pdf. (Accessed on January 2015).

DuCharme, B. (2011) *Learning SPARQL*. Sebastopol, California, United States: O'Reilly Media.

European Commission Justice (2012) *Protection of Personal Data*, Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (Accessed on June 2012)

European Commission. Available at: http://ec.europa.eu/news/economy/100303_en.htm. (Accessed on January 2013)

Fensel, D., Horrocks, I., Harmelen, F. v., Decker, S., Erdmann, M., Klein, M. C. A. (2000) *Knowledge Acquisition Modeling and Management, Proceedings of the 12th European Workshop on,', EKAW '00, Springer-Verlag*, pp. 1–16

Fenz, S. Goluch, G. ; Ekelhart, A., Riedl, B. (2007) ‘Information Security Fortification by Ontological Mapping of ISO/IEC 27001 Standard’. *Dependable Computing. PRDC 2007. 13th Pacific Rim International Symposium on*. Doi: 10.1109/PRDC.2007.29

Ferrel. T.K., Ferrel. U.D. (2000) *RTCA DO-178B/EUROCAE ED-12B*. Available at: http://www.davi.ws/avionics/TheAvionicsHandbook_Cap_27.pdf. (Accessed on June 2016)

Finley, J. Ellwood, K. Hoadley, J. (2014) ‘Launching a New Food Product or Dietary Supplement in the United States, Industrial, Regulatory and National Consideration’, *Annual Review of Nutrition. Volume 34. PP 421-447.* Doi: 10.1146/annurev-nutr-071813-105817

Frehse, G et al. (2011) ‘ SpaceEx: Scalable Verification of Hybrid Systems, *Computer Aided Verification’Springer.* pp 379–395.

Gamma, E., Helm, R., Johnson, R., Vissides J. (2012) *Design Patterns: Elements of Reusable Object-oriented Software*, 40th Edition. Addison Wesley

Gandhi, R.A. & Lee, S.W. (2011), ‘Discovering Multidimensional Correlations among Regulatory Requirements to Understand Risk’, *ACM Trans. Soft. Engr. Method.* 20(4), Article 16

Gangemi, A., Guarino, N., Masolo, C., Oltramari, A., Schneider, L. (2002) ‘Sweetening Ontologies by DOLSE’, *Proceedings of the 13th International Conference on Knowledge Engineering and Knowledge Management, Ontologies and the Semantic Web,* PP 166-181. Doi: 10.1007/3-540-45810-7_18

Gangemi, A., Prisco, A., Sagri, M.T; Steve, G. (2003) ‘Some Ontological Tools to Support Legal Regulatory Compliance, with a Case Study’, *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems".* pp 607-620. Doi: 10.1007/978-3-540-39962-9_64

Garner, B.A. (2014) *Black’s Law Dictionary.* 8th Edition, London: Thomsohn Ruiters,

Garris, S. (2008) *Efficient, Usable Proof-Construction Strategies for Distributed Access-Control Systems,* Carnegie Mellon University, Department of Electrical and Computer Engineering, PhD Thesis.

Garzotto, F., Paolini, P. Bolchini, D., Valenti, S. (1999) ‘Modelling-by-Patterns of Web Applications’, *International Conference of Conceptual Modelling*. 1727. pp 293-306, doi: 10.1007/3-540-48054-4_24

General Medical Council (2013) *Good Medical Practice*, London, UK.

Genesereth. M & Fikes. R. (2014) *Knowledge Interchange Format Version 3.0 Reference Manual,* Stanford Logic Group Report (Stanford University), Available at: http://logic.stanford.edu/kif/Hypertext/kif-manual.html. (Accessed on February 2015)

German Federal Office for Information Security (BSI), Bundesamt f¨ur Sicherheit in der Informationstechnik, (2006) *BSI-Grundschutz Katalog.* Germany: German Federal Office for Information Security (BSI).

Ghanavati, S. Amyot, D. & Peyton, L. (2007) ‘Towards a framework for tracking legal compliance in healthcare., *19th International Conference on Advanced Information Systems Engineering (CAiSE'07),* pp. 218-232. Doi: 10.1007/978-3-540-72988-4_16 , [CrossRef]

Gharib, M., Giorgini, P., Mylouolos, J. (2016) ‘Ontologies for Privacy Requirements Engineering, A Systematic Literature Review’, *Journal of arXiv preprint arXiv*:1611.10097

Gerber, M; Solms, R.V. (2008) ‘Information Security Requirement- Interpreting the Legal Aspects’ *Computer & Security*. 27(5–6), pp 124–135.

Giorgini, P., Massacci, F., Mylopoulos, J., Zannone, N. (2005) ‘Modelling security requirements through ownership, permission and delegation’, In *Proceedings of the 13th IEEE International Requirements Engineering Conference (RE'05), IEEE Computer Society Press.* Doi: 10.1109/RE.2005.43

Glass, R, L. (2003) *Facts and Facilities of Software Engineering*. Addison Wesley Publication.

GlobalPlatform, Available at: http://www.globalplatform.org/aboutus.asp. (Accessed on February 2011)

GlobalPlatform, Available at: http://www.globalplatform.org/specificationssystems.asp. (Accessed on February 2011)

Goedertier. S, Vanthienen. J. (2006) ‘Designing Complaint Business Processes with Obligations and Permissions’, *International Conference on Business Process Management*. Available at: https://pdfs.semanticscholar.org/3594/e6e8a9343933a7c39c3f7bd72e333239af68.pdf. (Accessed on December 2015).

Goedertier. S, Vanthienen. J. (2006) ‘Compliant and Flexible Business Processes with Business Rules’, *Conference of Business Process Modelling, Development, and Support*. Available at: http://ceur-ws.org/Vol-236/paper3.pdf. (Accessed on March 2014)

Gonçalves, P. (2013) ‘Towards an ontology for orthopaedic surgery, application to hip resurfacing’, *Proceedings of the Hamlyn Symposium on Medical.* Available at: http://www.est.ipcb.pt/laboratorios/robotica/papers/hamlyn2013_paulo.pdf. (Accessed on March 2014)

Gruber, T. R. (1993) ‘A translation approach to portable ontology specification’, *Journal of Knowledge Acquisition*, 5(2), pp. 199–220

Guha, R.V.; & Douglas B. (1990) ‘CYC: A Mid-Term Report’, *AI Magazine*, 11 (3). pp. 32–59

Gurses, S., Troncoso, C., Diaz, C. (2011) ‘Engineering Privacy by Design’, *Allen Institute for Artifitual Inteligence.* Available at: https://www.esat.kuleuven.be/cosic/publications/article-1542.pdf. (Accessed on January 2015)

Haarslev, V. & M¨oller, R. (2001) ‘Racer system description’, *Proceedings of the First International Joint Conference on Automated Reasoning, IJCAR ’01*, Springer-Verlag, pp. 701–706. Doi: 10.1007/3-540-45744-5_59

Hansen K. T. & Gullesen I., (2002) ‘Utilizing UML and Patterns for Safety Critical Systems’ *Proc. Workshop on Critical Systems Development with UML, in conjunction with the International Conference on the UML*.

Hanson. M, Leenes. R. (2005) ‘Privacy and Identity Management for Eeryone/Europe, PRIME’, *workshop on Digital identity management.* PP 20-27

Hayhurst, K. J. & Holloway C. M. (2001) ‘Challenges in Software Aspects of Aerospace Systems’, *Proc. Annual NASA Goddard Software Engineering Workshop*.

Heflin, J. & Hendler, J. (2001) ‘A Portrait of the Semantic Web in Action’, *IEEE Intelligent Systems,* 16(2). pp.54-59. Doi: 10.1109/5254.920600

Hoepman, J. (2013) ‘Privacy Design Strategies’, *IFIP International Information Security Conference*, pp. 446-459. Doi*:* 10.1007/978-3-642-55415-5_38

Hohfeld, W. N. (1913) ‘Fundamental Legal Conceptions as Applied in Judicial Reasoning’, *Yale Law Journal* 23(1). pp.710-770[CrossRef]

Holdeman Edwards, L. (2010) *Legal Writing; Process, Analysis, and Organization*, , 5th Edition, Aspen Publishers.

Home Office, United Kingdom. (2013*), Cyber Crime: A Review On Evidence*. London: Home Office, Research Report 75

Houmb, S. Islam, H., Knauss, S, E., Jürjens, J. & K. (2010) ‘Schneider, Eliciting Security Requirements and Tracing them to Design: An Integration of Common Criteria, Heuristics, and UMLsec’, *Requirements Engineering Journal (REJ),* 15(1,), PP 63-93. [CrossRef]

Horrocks, I. (2002) ‘A description logic for the semantic web’, *IEEE Data Eng. Bull.* 25(1), pp. 4–9.

Huhn, W.R., (2002) *5 Types of Legal Arguments*, 2nd Edition, Carolina Academic Press.

Humberg. T, Wessel. C, & Poggenpohl. D.(2014) ‘Using Ontologies to Analyse Compliance Requirements of Cloud-Based Processes’. *Cloud Computing and Services Science. Communications in Computer and Information Science*, (453), pp. 36-51

Indurkhya, N., Damerau, F.J. (2010) *Handbook of Natural Language Processing,* Second edition.USA: CRC Press, Taylor and Francis Group.

Information Commission Office, United Kingdom (2011) *Data controllers and data processors: what the difference is and what the governance implications are?* Available at: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf. (Accessed on January 2013).

Information Commission Office, United Kingdom (2010) *Guide to Data Protection*. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/. (Accessed on January 2013).

Information Commission Office, United Kingdom, (2010), *The Privacy Divided, the Business Case for Investing in Proactive Privacy Protection*, Volume 1, Available at: https://ico.org.uk/media/about-the-ico/documents/1042345/privacy-dividend.pdf. (Accessed on January 2013).

Information Commission Office, United Kingdom, (2008), *Privacy by Design*, Available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf. (Accessed on January 2013).

European Commission, Information society (2011) *Summary of legislation*, Available at: http://europa.eu/legislation-summaries/information-society/ index-en.htm. (European Commission)

Information Technology Forum, ITechLaw (2010) Available at: https://www.itechlaw.org/.(Accessed on January 2011)

Ingolfo, S., Jureta, I., Siena, A., Perini, A., Susi, A. (2014) 'Nomos3; Legal Complaince of Rules and equirements', *International Conference of equirement Engineering, Conceptual Modeling*, pp 275-288

International Business Machine Corporation. (2004), *IBM Lotus workplace for Business Controls & Reporting*. IBM Redbooks Publication. REDP-4021-00

International Business Machine Corporation, (2007) *Privacy Guidelines for Developing Software and Services*, Version 2.1, IBM Publication

International Business Machine Corporation, Microsoft Trust Center (2014) *Building Global Trust Online, Microsoft Perspective for Policymakers*, Available at: https://www.microsoft.com/en-us/trustcenter/ (Access on October 2016)

International Organisation of Standardisation. Information technology — Security techniques (2013), *Information security management systems — Overview and vocabulary. ISO/IEC 27000.* Available at: http://www.27000.org/. (Accessed on January 2013)

International Organisation of Standardisation Information technology — Security techniques (2013) *Information security risk management — Overview and vocabulary. ISO/IEC 27005.* Available at: http://www.27000.org/. (Accessed on January 2013)

International Organisation of Standardisation (2012) *Privacy Framework. ISO/IEC 29100*. Available at: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. (Accessed on January 2013)

Islam, S, Mouratidis, Wagner, H., S. (2010) 'Toward a framework to elicit and manage security and privacy requirements from laws and regulation', *Lecture Notes in Computer Science*,6182,pp.255-261.
[CrossRef]

Islam, S. Mouratidis, H. & Jürjens J. (2011) 'A Framework to Support Alignment of Secure Software Engineering with Legal Regulations', *Journal of Software and Systems Modelling (SoSyM), Theme Section on Non-Functional System Properties in Domain-Specific Modelling Languages (NFPinDSML),* 10(3). pp.369-394. [CrossRef]

Islam, S. & Houmb, H. (2010) 'Integrating Risk Management Activities into Requirements Engineering', *In Proc. of the 4th IEEE International Conference on Research Challenges in IS.* Doi: 10.1109/RCIS.2010.5507389

Islam, SH; Mouratidis, H, & Wagner, S. (2010) 'Toward a Framework to Elicit and Manage Security and Privacy Requirements from Laws and Regulations', *International Working Conference on Requirements Engineering: Foundation for Software Quality*, pp.255-261. Doi: 10.1007/978-3-642-14192-8_23

I* WiKi. (2009) Available at: www.istarwiki.org, (Accessed on October 2010).

Jakus. G, Milafinovic. V, Omerovic. S, & Tomazic. S. (2013) *Concepts, Ontologies and Knowledge Representation.* SpringerBriefs in Computer Science.

Josang. A, Pope. S, (2005) 'User Centric Identiry Management', *AusCERT Conference, Journal of Trust Management* 2(1). Doi: 10.1186/s40493-014-0009-6

Jürjens J. (2003) 'Developing Safety-Critical Systems with UML', *Proc. International Conference on the UML*, pp. 360-372.

Kalloniatis, C., Kavakli, E., (2008) 'Addressing privacy requirements in system design: The PriS method', *Requirement Engineering*, 13. pp.241–255

Kalloniatis, C., Mouratidis, H., Islam, S. (2013) 'Evaluating Cloud Deployment Scenarios Based on Security and Privacy Requirements', *Requirements Engineering*, 18. Pp.299-319. Doi: 10.1007/s00766-013-0166-7

Kandek, W. (2015) 'The Web App Security Puzzle', *Infosecurity Journal*. 12(2). pp.17

Karp, P. D., Chaudhri, V. K., Thomere, J. (1999) 'Xol: An xml-based ontology exchange language', Technical report, SRI International. Available at: https://www.sri.com/work/publications/xol-xml-based-ontology-exchange-language. (Accessed on December 2016)

Kiyavitskaya, N., Zeni, N., Breaux, TD., Antón, A., Cordy, J.R., Mich, L., Mylopoulos,J. (2007) 'Extracting rights and obligations from regulations: toward a tool-supported process', *ASE Conference*, pp 429-432

Kirpatrick, G. (2009) 'The Corporate Governance Lessons from the Financial Critics' *OECD Journal: Financial Market Trends*, 2009(1), pages 61-87

Kifer, M., Lausen, G., Wu, J. (1995) *Logical foundations of object-oriented and frame-based languages Journal*, 42(4), pp. 741–843

Kobsa, A., (2002) ‘Personalized Hypermedia and International Privacy’, *Communications of the ACM* 45(5), PP. 64-67

Kulesza, J. (2012) *International Internet Law*. 2nd edition. Taylor and Francis

Kwon, J., Johnson, M. (2012) ‘Security practices and regulatory compliance in the healthcare industry’, *Journal of Information in Health and Biomedicion*, 20 (1): 44-51

Langheinrich, M., (2001) ‘Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems’, *International Conference on Ubiquitous Computing*, pp 273-291. Doi: 10.1007/3-540-45427-6_23

Laudon, K.C. & Laudon, J.P. (1988) *Management Information Systems*, 2nd edition. Macmillan

Lioyd, I. J. *(*2011) *Information Technology Law*, 6th Edition, Oxford University Press.

Liu, Y., Muller, S., Xu, K.(2007) ‘A Static Compliance-Checking Framework for Business Process Models’. *IBM Systems Journal* ,46.

Lu. R, Sadiq.SH, Governatory.G. (2007) ‘Compliance Aware Business Process Design’, *BPM 2007 International Workshops*, *Lecture Notes in Computer Science* 4928. pp. 120-131

Macgregor, R. (1999)’ Retrospective on Loom’, *Information Sciences Institute*. Available at: http://www.isi.edu/isd/LOOM/. (Accessed on Jnauary 2014)

Massacci, F., Prest, M., Zannone, N. (2004) ‘Using a security requirements engineering methodology in practice: The compliance with the Italian Data Protection Legislation’, *Computer Standards & Interfaces*, 27(5). pp.445-455

Massey, A., Otto, P., Hayward, J., Anton, A. (2010) ‘Evaluating Security and Privacy Requirements for Legal Compliance’, *Journl of Requirement Engineering*, 15(1). pp 119–137

May, M. J., Gunter, C. A., Lee, I. (2006) ‘Privacy APIs: Access control techniques to analyse and verify legal privacy policies’, *Proc. of the 19th Computer Security Foundations Workshop*. Doi: 10.1109/CSFW.2006.24

Maynard, D., Bontcheva, K., Augenstein, I. (2016) *Natural Language Processing for Semantic Web*. 1th edition. Morgan & Claypool Publication.

Mead, N. R. (2006) *Identifying security requirements using the security quality requirements engineering (SQUARE) Method, in Integrating Security and Software Engineering,"* pp. 44-69, Idea Publishing Group.

Mellado, D., Medina, E. & Piattini, M. (2007) ‘A common criterion based security requirements’ *engineering process for the development of secure information system*, *Computer standards & interfaces*, 29. pp.244-253, [CrossRef]

Mead, N, R. (2013) 'A History of International Requirements Engineering Conference', *IEEE 21th International Conference On Requirements Engineering*. doi: 10.1109/RE.2013.6636721

Medic, A. & Golubovic, A. (2010) 'Making Secure Semantic Web', *Universal Journal of Computer Science and Engineering Technology*, 1 (2), pp.99-104

McBride, B. (2002) 'Jena: A semantic web toolkit', *IEEE Internet Computing*, 6(6), pp.55–59.

Microsoft. (2008) *Privacy guidelines for developing software products and services*, Version 3.1, Available at: http://download.microsoft.com. (Accessed on Decmber 2016).

Morra, L. & Friedlander, A. (1998) *Case Study Evaluation*. The Word Bank Publication.

Mouratidis, H. (2004) *A security oriented approach in the development of multiagent systems: Applied to the management of the health and social care needs of older people in England*, PhD thesis, University of Sheffield, U.K.

Mouratidis, H. & Giorgini, P. 'Secure Tropos, A security-oriented extension of the Tropos methodology', *International Journal of Software Engineering and Knowledge Engineering*, 17(2).Doi:10.1142/S0218194007003240
[CrossRef]

Mouratidis, H. Jürjens, J., Fox, J. *(*2006).' Towards a comprehensive framework for secure systems development', *CAiSE, Lecture Notes in Computer Science* 4001, pp. 48-62, Springer-Verlag.
[CrossRef]

Montjeweff. A. (1999) *An Instructional Environment for Learning to Solve Legal Cases PROSA*. University of Amsterdam. PhD Thesis.

Myloupolos. J, Chung. L, Yu. E. (1999) 'From Object-Oriented to Goal-Oriented Requirement Engineering'. *Communication of ACM*. 42(1). PP.31-37

National Electrical Manufacturers Association-USA (NEMA), European Coordination Committee of the Radiological and Electromedical Industry (COCIR), Japan Industries Association of Radiological Systems(JIRA), *Break-glass an approach to granting emergency access to healthcare systems*. Available at: http://www.nema.org/prod/med/security/upload/Break-GlassEmergency Access to Healthcare Systems.pdf. (Accessed on January 2012)

Neri, F. *(*2006*) Evaluation of OntoLearn, a methodology for automatic learning of domain ontologies*. *IOS Press,*

Neumann, R. K. (2009) *Legal Reasoning and Legal Writing*, 6th Edition. Aspen Publication,

Noy, N. F. & Musen, M. A. (2000) 'Prompt: Algorithm and tool for automated ontology merging and alignment', *in 'Proceedings of the Seventeenth National Conference on*

Artificial Intelligence and Twelfth Conference on Innovative Applications of Artificial Intelligence', AAAI Press, pp. 450–455

Olsen, Th., Mahler, T., (2007) 'Identity Management and Data Protection Law; Risk, Responsibility and Compliance in 'Circle of Trust-Part III', *Computer Law and Security Review*, 23(5), PP. 415–426

Ontology & Semantic Web Online Tutorials. Available at: http://www.obitko.com/tutorials/ontologies-semantic-web/operations-on-ontologies.html. (Accessed on January 2014).

Open Compliance & Ethics Group (OCEG) (2009) *GRC Capability Model "Red Book" 2.0.* OCEG Publication.

Open Compliance and Ethic Group, OCEG, (2011) *Governance, Risk and Compliance Forum. GRC Capability Model*.Available at:. http://www.oceg.org/resources/grc-capability-model-red-book/ , (Accessed on January 2015)

OpenOME. Available at: .http://istar.rwth-aachen.de/tikiindex.php?page=OpenOME#General Information. (Accessed on January 2015)

Open Web Application Security Projects (OWASP), https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

Organisation of Economic Co-operation and Development. Available at: http://www.oecd.org/about/. (Accessed on January 2015)

Orriens, B., Yang, J., Papazoglou, M.P. (2005) 'A rule driven approach for developing adaptive service oriented business collaboration'. IEEE International Conference on Services Computing, 2006. SCC '06. *ICSOC*. PP.61–72. Doi: 10.1109/SCC.2006.14

Otto P. N. & Antón, A. I. (2007) 'Addressing legal requirements in requirements engineering', *15th IEEE International R. E. Conference*, doi: 10.1109/RE.2007.65

Panagacos, Th., (2012). *The Ultimate Guide to Business Process Management: Everything You Need to Know and How to Apply It to Your Organization*. CreateSpace Independent Publishing Platform. pp. 6–7.

Patel-Schneider, P. F., Hayes, P. & Horrocks, I. (2004) *OWL web ontology language semantics and abstract syntax, Technical report*, Available at: https://www.w3.org/TR/owl-semantics/. (Accessed on January 2014).

Paradkar, S. (2011), *The Anatomy of Software Framework. Software Oriented Architecture Organisation.* Avaialble at: http:// SOAInstitute.Org/ .(Accessed on January 2014).

PCI Security Standard Council. (2016) *Payment Card Industry Data Security Standard.* Version 2. PCI Security Standard Council Press.

Pearson, S., (2009), ‘Taking Account of Privacy when Designing Cloud Computing Services’, *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, PP 44-52

Ponoela, A, M. Casellas, N. Torralba, S. Reyes, M, Casanova, P. (2010), ‘Legal Compliance Support with an Ontology based Information System’, Available at: http://ddd.uab.cat/record/128207

PricewaterhouseCoopers. Available at: https://www.pwc.com/. (Accessed on September 2015)

Information Commission Office, United Kingdom, (2012) *Privacy Notice, Code of Practice*. Available at: https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf. (Accessed on September 2012).

Quah, A., R¨ohm, U., (2013), ‘User Awareness and Policy Compliance of Data Privacy in Cloud Computing’, *Proceedings of the First Australasian Web Conference (AWC 2013)*, 144, pp 3-12.

Rahmouni, H.B., Munir, K., Mont, M.C., Solomonides, T. (2015) ‘Semantic Generation of Clouds Privacy Policy’, *International Conference on Cloud Computing and Services Science*, 512. PP. 15-30

Rahmouni. H.B, Solomonides. T, Casassa Mont. M., Shiu. S. (2009) ‘Ontology-Based Privacy Compliance on European Healthgrid Domains’. *Stud Health Technol Inform;* PP.147-183

Rifaut, A. & Dubois, E. (2008) ‘Using Goal-Oriented Requirement Engineering for Improving the Quality of ISO/IEC 15504 based Compliance Assessment Framework’, *International Requirements Engineering. RE '08*. Doi: 10.1109/RE.2008.44

Robertson. S, Robertson, & J. (2012) *Mastering the Requirement Process-Getting Requirements Right*, 3rd ed. USA: Pearson Education

Rochelle, G. (2003). Microsoft plans App to aid companies with Financial Controls. Contents Issue Magazine. ISSN 0893-8377

Roebuck, W., & Dresner, D. (2005) *ICT Legal Compliance, A Bright Future or a Marriage of Convenience? Legal Guidelines, IT Law for IT Professionals*, 1th edition, Principia Publication

Rolland, C., Nurcan, S., Grosz, G. (1999) ‘Enterprise Knowledge Development: The Process View’. *Information and Management Journal*, pp.165 - 184.

Rossi. G, Schwabe. D, Lyardet. F. (2000), ‘Abstraction and Reuse Mechanisms in Web Application Models’, *Workshops on Conceptual Modeling Approaches for EBusiness and the World Wide Web and Conceptual Modeling the Rule Markup Initiative. RuleML (2012). PP76-88.* Doi: 10.1007/3-540-45394-6_8.

Rostad, L., & Edsburg, O., (2006) 'A study of access control requirements for healthcare systems based on audit trails from access logs', *In Proc. of the 2006 Annual Computer Security Applications Conference*, doi: 10.1109/ACSAC.2006.8.

Roy, J.F., Kealey, J., & Amyot, D. (2006) 'Towards integrated tool support for the User Requirements Notation.*'* *SAM 2006: Language Profiles - Fifth Workshop on System Analysis and Modelling. Lecture Notes in Computer Science.* 4320. pp 198–215.

Rubenstein, I., Good, N., (2013) 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents', *Berkeley Technology Law Journal*, 28(2). doi:10.15779/Z38G11N

Ruiter, J., Warnier, M. (2011) 'Privacy Regulations for Cloud Computing Compliance and Implementation in Theory and Practice', *Computers, Privacy and Data Protection: An Element of Choice*, PP 293-314.

Ruopeng. Lu, Sadiq. Sh, Governatori. G. (2007) 'Compliance Aware Business Process Design', *Business Process Management Workshops. Lecture Notes in Computer Science*. 4928. pp 120-131.

Ryan. H, Spyns. P, Leenheer. P.D, Leary. R. (2003) 'Ontology-Based Platform for Trusted Regulatory Compliance Services', *On The Move to Meaningful Internet Systems: OTM 2003 Workshops. Lecture Notes in Computer Science* , 2889. pp 675-689.

Sadiq. Sh, Governatori. G, & Naimiri. K. () 'Modelling Control Objectives for Business Process Compliance', *International Conference on Business Process Management*, pp.149-166. Doi: 10.1007/978-3-540-75183-0_12

Saleh, M.S, Alrabiah, A, & Backry, S.H, (2005) 'A STOPE Model for the Investigation of Compliance with ISO 17799-2005', *Information Management & Computer Security*, 15(4), pp.283 – 294.

Schaar, P. (2010) 'Privacy by Design', *Identity in Information Society*, 3(2). pp 267–274.

Schmidt, R. Bartch, CH. Oberhauser, R. (2007), 'Ontology Based Representation of Compliance Requirements for Service Processes', Available at: https://www.semanticscholar.org/paper/Ontology-based-Representation-of-Compliance-Schmidt-Bartsch/83cafe951736c0d07ce5ff8bb7d9b3e8ea9a0a7a. (Accessed on March 2014).

Scholer, S. Zink, O. (2008), *SAP Governance, Risk and Compliance.* 2nd edition. SAP PRESS.

Scholten, P., (1931), *Methods of Private Law*, First Edition.

Schumm, D., Laymann, F., Ma, Zh., Scheibler, Th., Strauch, S. (2010) Integrating Compliance into Business Processes Process Fragments as Reusable Compliance Controls, Available at: http://webdoc.sub.gwdg.de/univerlag/2010/mkwi/. (Accessed on January 2014).

Schumm, D.; Türetken, O., Kokash, N., Elgammal, A., Leymann, F., Heuvel, W. (2010), 'Business process compliance through reusable units of compliant processes', *Proceedings of the 1st International Workshop on Engineering SOA and the Web (ESW '10),* pp.325-377. Doi: 10.1007/978-3-642-16985-4_29.

Selioukova, Y., (2001) *Business Process Modeling in Software Requirements Engineering for Small and Medium Software Projects*, Lappeenranta University of Technology, Department of Information Technology, Master's Thesis.

Seshia, S., (2011), *Introduction to Temporal Logic*, University of California Berkeley, Technical Report, Available at: https://people.eecs.berkeley.edu/~sseshia/fmee/lectures/TemporalLogicIntro.pdf. (Accessed on Mrch 2014).

Seng, J.-L. & Kong, I. (2009) 'A schema and ontology-aided intelligent information integration', *Expert Systems with Applications*. 36(7), pp. 10538 – 10550.

Shamsaei, A. Amyot, D & Pourshahid, A. (2011) 'A Systematic Review of Compliance Measurements Based on Goals and Indicators', *Lecture Notes in Business Information Processing* . 83, pp 228-237

Sheth, A., Bertram, C., Avant, D., Hammond, B., Kochut, K., Warke, Y. (2002) 'Managing semantic content for the web', *IEEE Internet Computing*. 6(4), pp. 80–87.

Siena, A., Mylopoulos, J., &Perini, A., (2008), *From laws to requirements*, 1st International Workshop on Requirements Engineering and Law

Sirin, E. & Parsia, B. (2004), Pellet: An owl dl reasoner, in 'Proceedings of the 2004 International Workshop on Description Logics (DL2004)', Vol. 104, CEUR-WS.org, Whistler, British Columbia, Canada.

Smith, B., Floridi L. (2003) *The Blackwell Guide to the Philosophy of Computing and Information*, Oxford: Blackwell, pp. 155–166

Smullen, D., Breaux, T.D. (2016) 'Modeling, analyzing, and consistency checking privacy requirements using eddy', *HotSos 16, Proceeding of the Symposium and Bootcamp on the Science of Security,* pp 118-120

Sommerville, A. (1993) *Medical Ethics Today, Its Practice and Philosophy*, British Medical Association (BMA)

Sommerville, I. (2006) *Software Engineering*, 7th ed. Harlow, UK: Addison Wesley.

Susanto, H; Mulhaya, F.B; Almunawar, M.N., Tuan, Y.C. (2012) 'Refinement of Strategy and Technology Domains, STOPE View on ISO 27001'. Available at: https://arxiv.org/ftp/arxiv/papers/1204/1204.1385.pdf. (Accessed on March 2014).

Susanto, H; Almunavar, M.N, Tuan, Y.CH. () Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Redness Level. Available at:

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.377.926. (Accessed on January 2014).

Integrated the Health Enterprise, IHE (2006) *The patient care coordination technical framework: Basic patient privacy consents*, Available at: http://www.ihe.net/Technical_Framework/upload/IHE_PCC_TF_BPPC_Basic_Patient_Privacy_Consents_20060810.pdf. (Accessed on January 2015).

Transatlantic Technology Law Forum. Available at: http://www.law.stanford.edu/organizations/programs-and-centers/transatlantic-technology-law-forum. (Accessed on January 2015).

Tsarkov, D. & Horrocks, I. (2006) 'Fact++ description logic reasoner: system description', *Proceedings of the Third international joint conference on Automated Reasoning, IJCAR'06*, pp. 292–297

Turetken. O, Elgammal. A, Heuvel. W, Papazoglou. M. (2011) 'Enforcing Compliance on Business Processes Through the Use of Patterns'. *European Conference on Information Systems.* Available at: http://aisel.aisnet.org/ecis2011/5/. (Accessed on March 2013)

United Nation (UN). Available at: http://www.un.org/en/index.html. (Accessed on March 2011).

User Interface Design Patterns-UI Patterns, Available at: http://ui-patterns.com/.(Accessed on March 2013)

User Interface Design Patterns-UI Patterns, *Shopping Cart Pattern*, Available at :http://ui-patterns.com/patterns/ShoppingCart. (Accessed on March 2013)

USA Government Congressional Reports, *The Health Insurance Portability and Accountability Act 1996*, Rept. 104-736. US Government Publication Office, H.

Van Eemerence, F.H. (2004) *A Systematic Theory of Argumentation*, Cambridge University Press.

Vicent, P; Silva, M.M. (2011) 'A Conceptual Model for Integrated Governance, Risk and Compliance'. *Advanced Information Systems Engineering. Lecture Notes in Computer Science* . 6741. pp 199-213

Vossen, P. (1997) 'EuroWordNet: a multilingual database for information retrieval', *DELOS workshop on Cross-language Information Retrieval.* Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.146.3050. (Accessed on June 2014).

Wagner, L., Fifarek, A., Gross, K., (2016), SpeAR — specification and analysis for requirements tool, Availabl at: https://github.com/ AFifarek/SpeAR. (Accessed on March 2014).

Warren, S.D. & Barren, L. D., (1890), *The Right to Privacy*, IV (5). Harvard Law Review.

Wedekind, J. (2008) *Web Design Patterns, a Future Approach*? Available at: https://www.yumpu.com/en/document/view/6841311/web-design-patterns-a-future-approach. (Accessed on January 2015).

Weiss, M., Amyot, D. (2005) 'Business process modelling with URN', *International Journal of E-Business Research* 1(3). pp.63–90.

Wilson, C. (1987) 'A Comparison of Commercial and Military Computer Security Policies', *in Proceedings of the IEEE Symposium on Security and Privacy*. pp 184-194

World Wide Web Consortium. Available at: https://www.w3.org/. (Accessed on Jnuary 2014).

Yarandi, M. (2013) *Semantic Rule-based Approach for Supporting Personalised Adaptive E-Learning*. Phd Thesis. University of East London

Yu, E., Dobbie, G., Jarke, M., Purao, S. (2014) '*Conceptual Modeling'*, Internation Conference of Requirement Engineering

Yu, E., Georgani, P., Maiden, N., Mylopoulos, J. (2010) *Social Modelling for Requirement Engineering, an Introduction.* 1th edition. MIT Press

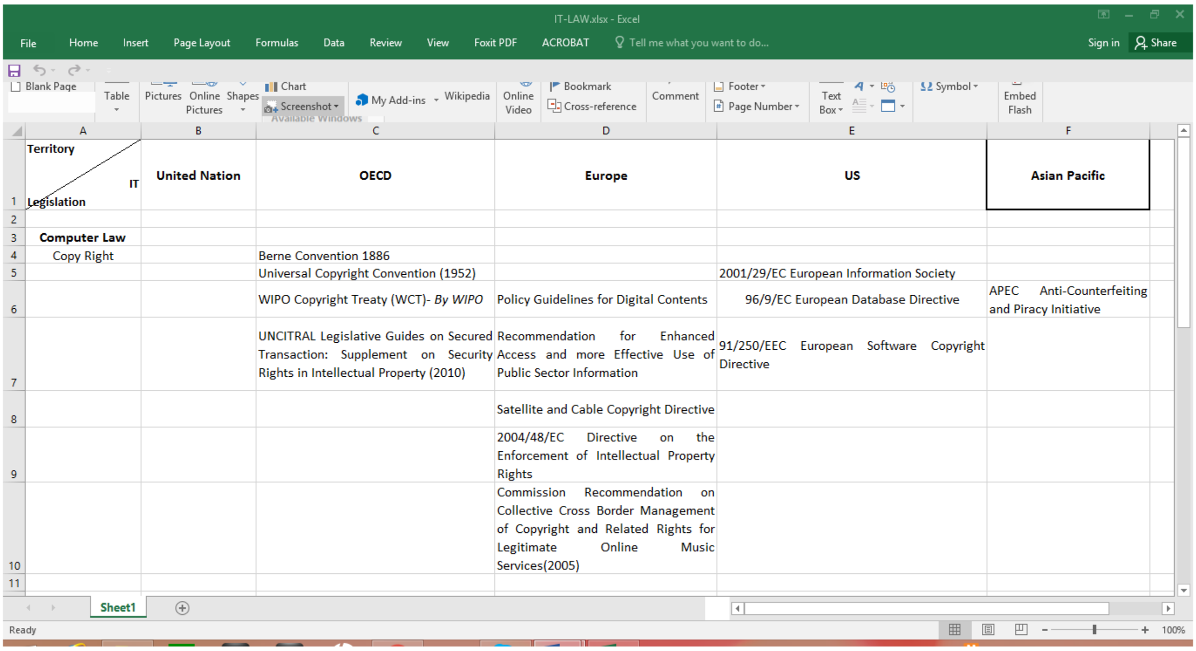
Yu, E. (2009) 'Social Modelling and i*', *Conceptual Modelling: Foundations and Applications.* Available at: http://www.cs.toronto.edu/pub/eric/JMfest09-EY.pdf. (Accessd on January 2012).

Zelling, S.H. (1981) 'Operator Grammer of English'. *Synthese Language Library.* 14. PP 412-435

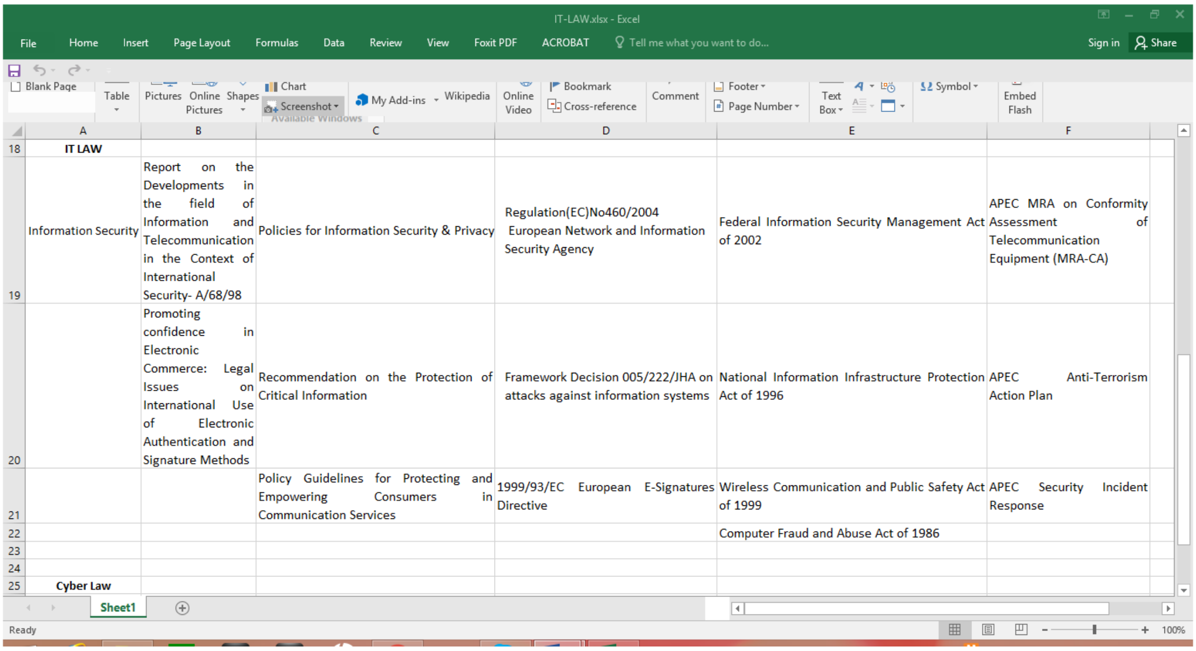
Zhong. B. T. Luo. H. B. Hu. Y. Z, Sun. J. (2012) 'Ontology-Based Approach for Automated Quality Compliance Checking against Regulation in Metro Construction Project'. *Proceedings of the 1st International Workshop on High-Speed and Intercity Railways. Lecture Notes in Electrical Engineering* . 148, pp 385-396

Zoughbi. G., Briand. L., Labiche. Y. (), 'Modeling Safety and Airworthiness (RTCA DO- 178B) Information – Conceptual Model and UML Profile', *Journal of Software and Systems Modeling*, 10(3). Pp.337-367

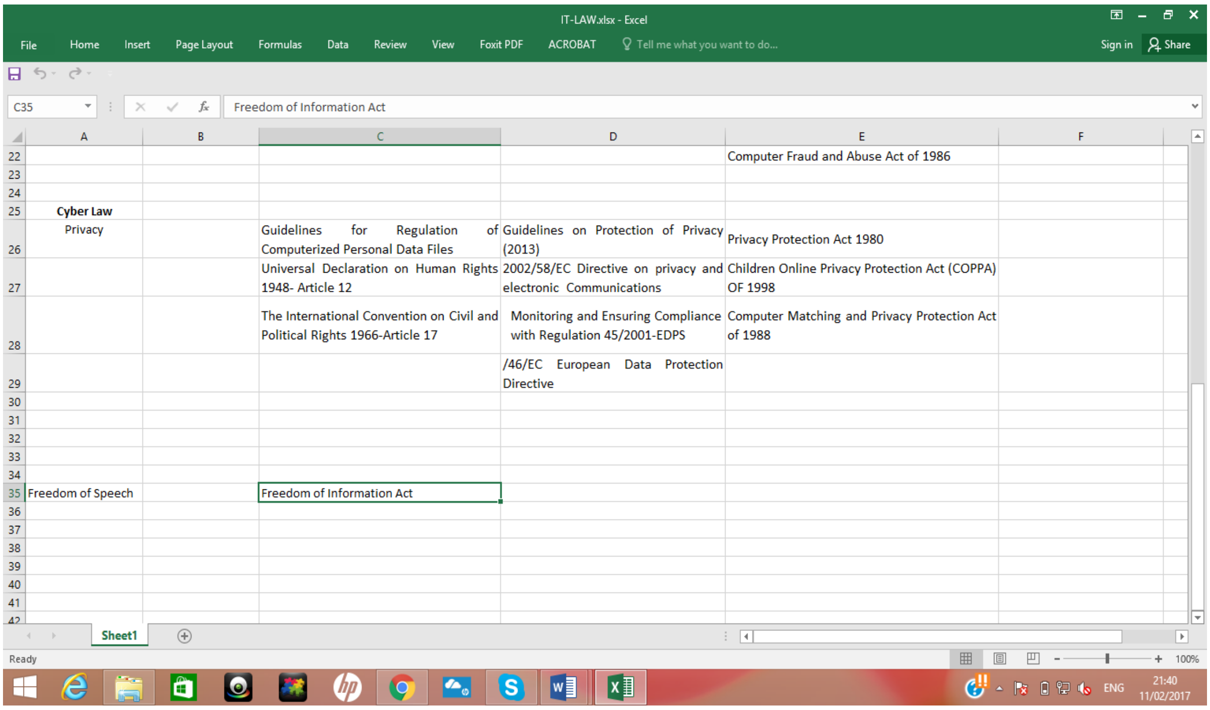
APPENDIX I: IT LAW LEGISLATION



	A	B	C	D	E	F
1	**Territory** **IT** **Legislation**	**United Nation**	**OECD**	**Europe**	**US**	**Asian Pacific**
2						
3	**Computer Law**					
4	Copy Right		Berne Convention 1886			
5			Universal Copyright Convention (1952)		2001/29/EC European Information Society	
6			WIPO Copyright Treaty (WCT)- *By WIPO*	Policy Guidelines for Digital Contents	96/9/EC European Database Directive	APEC Anti-Counterfeiting and Piracy Initiative
7			UNCITRAL Legislative Guides on Secured Transaction: Supplement on Security Rights in Intellectual Property (2010)	Recommendation for Enhanced Access and more Effective Use of Public Sector Information	91/250/EEC European Software Copyright Directive	
8				Satellite and Cable Copyright Directive		
9				2004/48/EC Directive on the Enforcement of Intellectual Property Rights		
10				Commission Recommendation on Collective Cross Border Management of Copyright and Related Rights for Legitimate Online Music Services(2005)		
11						



	A	B	C	D	E	F
18	**IT LAW**					
19	Information Security	Report on the Developments in the field of Information and Telecommunication in the Context of International Security- A/68/98	Policies for Information Security & Privacy	Regulation(EC)No460/2004 European Network and Information Security Agency	Federal Information Security Management Act of 2002	APEC MRA on Conformity Assessment of Telecommunication Equipment (MRA-CA)
20		Promoting confidence in Electronic Commerce: Legal Issues on International Use of Electronic Authentication and Signature Methods	Recommendation on the Protection of Critical Information	Framework Decision 005/222/JHA on attacks against information systems	National Information Infrastructure Protection Act of 1996	APEC Anti-Terrorism Action Plan
21			Policy Guidelines for Protecting and Empowering Consumers in Communication Services	1999/93/EC European E-Signatures Directive	Wireless Communication and Public Safety Act of 1999	APEC Security Incident Response
22					Computer Fraud and Abuse Act of 1986	
23						
24						
25	**Cyber Law**					



C35 | Freedom of Information Act

	A	B	C	D	E	F
22					Computer Fraud and Abuse Act of 1986	
23						
24						
25	**Cyber Law**					
26	Privacy		Guidelines for Regulation of Computerized Personal Data Files	Guidelines on Protection of Privacy (2013)	Privacy Protection Act 1980	
27			Universal Declaration on Human Rights 1948- Article 12	2002/58/EC Directive on privacy and electronic Communications	Children Online Privacy Protection Act (COPPA) OF 1998	
28			The International Convention on Civil and Political Rights 1966-Article 17	Monitoring and Ensuring Compliance with Regulation 45/2001-EDPS	Computer Matching and Privacy Protection Act of 1988	
29				/46/EC European Data Protection Directive		
30						
31						
32						
33						
34						
35	Freedom of Speech		Freedom of Information Act			
36						
37						
38						
39						
40						
41						
42						

Table1 .International IT Laws

APENDIX II: ANALYSING, APPLICATION AND REFINMENT OF RULES OF GDPR

- **GDPR Analysis**

> *3. 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction;*

43rd.LFACT . Some operation(s) are performed upon personal data(s) (processor performs operation(s) on personal data)

44th.LFACT . The operation(s) are performed by automated means

45th.LFACT . The operation(s) are performed without automated means

46th.LFACT . Example of processing is collection (processor collects personal data)

47th.LFACT . Example of processing is recording (processor records personal data)

48th.LFACT . Example of processing is organization (processor organizes personal data)

49th.LFACT . Example of processing is structuring (processor structure personal data)

50th.LFACT . Example of processing is storage (processor store personal data)

51st.LFACT . Example of processing are also adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction (processor adapt, alter, retrieve, use, disclose, … personal data)

LRESULT4th : the operation(s) is processing

1stLRULE : 43rd.LFACT ∧ 44th.LFACT -> LRESULT4th

2ndLRULE : 43rd.LFACT ∧ 45th.LFACT -> LRESULT4th

3rdLRULE : 43rd.LFACT ∧ 45th.LFACT ∧ 46th.LFACT-> LRESULT4th

4thLRULE : 43rd.LFACT ∧ 44th.LFACT ∧ 47th.LFACT-> LRESULT4th

5thLRULE : 43rd.LFACT ∧ 44th.LFACT ∧ 48th.LFACT-> LRESULT4th

6thLRULE : 43rd.LFACT ∧ 44th.LFACT ∧ 49th.LFACT-> LRESULT4th

7thLRULE : 43rd.LFACT ∧ 44th.LFACT ∧ 46th.LFACT-> LRESULT4th:

8thLRULE : 43rd.LFACT ∧ 45th.LFACT7 ∧ 47th.LFACT-> LRESULT4th

9thLRULE : 43rd.LFACT ∧ 45th.LFACT∧ 48th.LFACT-> LRESULT4th

10thLRULE : 43rd.LFACT ∧ 45th.LFACT ∧ 49th.LFACT-> LRESULT4th

11thLRULE : 43rd.LFACT ∧ 45th.LFACT ∧ 46th.LFACT-> LRESULT4th

5: *'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data;*

52nd.LFACT : A natural person determines the purpose of processing

53rd.LFACT :. A natural person determines the condition of processing

54th.LFACT :. A natural person determines the means of processing

55th.LFACT :. Natural person determines above alone

56th.LFACT :. Natural person determines above jointly by others

57th.LFACT :. A legal person determines the purpose of processing

58th.LFACT :. A public authority determines the purpose of processing

59th.LFACT :. An agency determines the purpose of processing

60th.LFACT :. Anybody determines the purpose of processing

61st.LFACT : Fact 25, 26, 27 and 28 are true about legal person, public authority, agency or any body

LRESULT5th : Natural person is controller

LRESULT6th Agency is a controller

12thLRULE : 52nd.LFACT ∧ 53rd.LFACT ∧ 54th.LFACT ∧ 55th.LFACT ->LRESULT5th

13thLRULE : 52nd.LFACT ∧ 53rd.LFACT ∧ 54th.LFACT ∧ 56th.LFACT-> LRESULT5th

6: *processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;*

62nd.LFACT . A natural body process personal data

63rd.LFACT . A legal person process personal data

64th.LFACT . A public authority process personal data

65th.LFACT . An agency process personal data

66th.LFACT . Anybody process personal data

67th.LFACT . Processing is behind the controller

LRESULT7th : Natural person is processor

14thLRULE : 62nd.LFACT ∧ 67th.LFACT -> LRESULT7th

15thLRULE : 63rd.LFACT ∧ 67th.LFACT -> LRESULT7th

16thLRULE : 64th.LFACT ∧ 67th.LFACT -> RESULT6th

17thLRULE : 65th.LFACT∧ 67th.LFACT -> RESULT6th

18thLRULE : 66th.LFACT ∧ 67th.LFACT > RESULT6th

- Article 3: Territorial Scope

1**. This Regulation applies to the processing of personal data** in the context of the activities of an establishment of a controller or a processor in the Union.

2. **This Regulation applies to the processing of personal data** of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:

(a) the offering of goods or services to such data subjects in the Union; or

(b) the monitoring of their behaviour.

3. **This Regulation applies to the processing of personal data** by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

15th.FACT. The personal data is being processed (controller/processor is processing personal data)

68th.LFACT . Processing of personal data is in context of some activities

69th.LFACT . Controller is performing the activities

70th.LFACT . Processor is performing the activities

71st.LFACT . Controller is established in the Union

72nd.LFACT . Processor is established in the Union

73rd.LFACT : Data subject resides in Union

74th.LFACT : processing is related to the offering of goods or services to data subjects

75th.LFACT : processing is related to monitoring of data subject behaviour

76th.LFACT : controller is established in non-union place

77th.LFACT : The national law of a Member State applies by virtue of public international law in that place.

LRESULT8th : This regulation applies to the processing of personal data

For more clarification of the article, we also refer to clause 19 of introductory section which adds some extra facts to the predicate above:

78th.LFACT . The processing takes place within the Union

79th.LFACT . The processing does not take place within the Union

Since the result in Article 2 and 3 are the same, we have admitted same rules of Article 2 as below:

19thLRULE : 15th.FACT ∧ 68th.FACT∧ 69th.FACT ∧ **71**th.FACT ^ 78th.FACT -> RESULT8th

20thLRULE : 15th.FACT ∧ **70**th.FACT∧ 72th.FACT ∧ 68th.FACT ^ 78th.FACT ->RESULT8th

21stLRULE : 15th.FACT ∧ 68th.FACT∧ 69th.FACT ∧ 70th.FACT ^ 78th.FACT -> RESULT7th

22ndLRULE : 15th.FACT ∧ 70th.FACT∧ 72th.FACT ∧ 68th.FACT ^78th.FACT ->RESULT8th

23rdLRULE : 15th.FACT ∧ 70th.FACT∧ 72th.FACT ∧ 68th.FACT ^ 78th.FACT ->RESULT8th.

- *Article 7:*

1-The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3- The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

15th.FACT. Processor/controller is processing personal data.

LRecommendation1st: Data subject should give consent.

22th.LFACT. The consent is for processing of personal data

23th.LFACT. Personal data belongs to data subject

80th.LFACT . The consent is for processing purposes

81st.LFACT . Consent is in context of a written declaration

82nd.LFACT . Written declaration concerns other matters except from consent

21th.FACT. Data subject has given his/her consent.

16thLObligation . The controller shall bear the burden of proof for consent

17thLObligation . Consent must have distinguished appearance for its requirements

LPermission1st . Data subject may withdraw consent

LPermission2nd. Withdrawal shall not affect the lawfulness of process

24thLRULE : 15th.LFACT ∧ 21th.LFACT ∧ 23th.LFACT ∧ 24st.LFACT ∧ LRecommendation.1st -> 16^{th}.LObligation .

25thLRULE : LRecommendation1st-> LPermission1st.

26thLRULE : LPermission1st-> LProhbition1st..

27thLRULE LRecommendation1st ∧ 81h.LFACT ∧ 82th.LFACT -> 17th.LObligation

To understand the meaning of above rule indicating the *burden of proof for consent,* in more details, Part 25 of introductory section of Regulation will be studied and analysed to further facts and obligations:

25. *Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data. Silence or in activity should therefore not constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. If the data subject's consent is to be given following an electronic request, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.*

LRecommendation6th. The consent should be given explicitly

LRecommendation7th. The consent should be given by appropriate methods

18thLObligation . The consent shall enable data subject to be aware of his consent to processing of personal data

LRecommendation8th. The consent should enable an indication of data subject wishes

LRecommendation9th. The indication should be given freely

LRecommendation10th . The indication should be specific

LRecommendation11th . The indication should be informed

LPermission3rd . The consent may be given by ticking a box on a website

LPermission4th . The consent may be given by a statement

LPermission5th . The consent may be given by a conduct

19thLObligation . The consent shall indicate data subject's acceptance of processing personal data

20thLObligation . The indication shall be clear

28thLRULE : 17th.LObligation -> 18th.LObligation.

29thLRULE : 17th.LObligation -> LRecommendation6th.

30thLRULE : 17th.LObligation-> LRecommendation7th..

31stLRULE : 17th.LObligation -> LRecommendation8th.

32ndLRULE : LRecommendation8th -> LRecommendation9th.

33rdLRULE : LRecommendation8th -> LRecommendation10th

34thLRULE : LRecommendation8th -> LRecommendation11th

35thLRULE : LRecommendation8th ->19th.LObligation .

36thLRULE : 17th.LObligation -> LPermission1st

37thLRULE : 17th.LObligation -> LPermission2nd

38thLRULE : 17th.LObligation -> LPermission3rd

39thLRULE : LPermission3rd -> 19th.LObligation

- *Article 9:*

1-*The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.*

2- Paragraph 1 shall not apply where:

(a) the data subject has given consent to the processing of those personal data, subject to the conditions laid down in Articles 7 and 8, except where Union law or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; or...

14th.FACT. Processor/controller is processing personal data

83rd.LFACT . Personal data reveals race origin

84th.LFACT . Personal data reveals ethic origin

85th.LFACT . Personal data reveals political opinion

86th.LFACT . Personal data reveals religion

87th.LFACT . Personal data reveals beliefs

88th.LFACT . Personal data reveals trade union membership

89th.LFACT . Personal data are genetic data

90th.LFACT . Personal *data* concern health

91st.LFACT . Personal *data* concern sex life

92nd.LFACT . Personal *data* concern criminal convictions

93rd.LFACT . Personal *data* concern criminal convictions related security measures

94th.LFACT . Data subject has given consent to the processing of those personal data

LProhibition1st . Controller/processor shall not process personal data

21stLObligation . Controller/processor shall process personal data

40thLRULE : 15th.FACT ∧ ***83***th.LFACT ∧ ~21th.LFACT -> ***L***Prohbition2nd .

41stLRULE : ***15***th.FACT ∧ 84th.LFACT ∧ ~ 21th.LFACT -> LProhibition2nd

42ndLRULE : 15th.LFACT ∧ ***85***th.FACT ∧ ~21th.FACT -> LProhibition2nd

43rdLRULE : 15th.FACT ∧ 86st.FACT ∧ ~21th.FACT > LProhibition2nd

44thLRULE : 15th.FACT ∧ 87nd.FACT ∧ ~21th.FACT -> LProhibition2

45thLRULE : 15th.FACT ∧ 88rd.FACT ∧ ~21th.FACT -> LProhibition2

46thLRULE : 15th.LFACT ∧89th.LFACT ∧ ~21th.FACT -> LProhibition2nd

47thLRULE : 15th.LFACT ∧ 91th.FACT ∧ ~21th.FACT -> LProhibition2nd

48thLRULE : 15th.LFACT ∧ ***92***th.LFACT ∧ ~21th.FACT -> LProhibition2nd

49thLRULE : 15th.LFACT ∧ 93th.LFACT ∧ ~21th.LFACT -> LProhibition2nd

- *Article 10: If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation.*

15th.FACT. Personal data is being processed by controller (the controller process personal data)

23th.FACT. Personal data belongs to natural person

95th.LFACT . Data processed by a controller does not permit the controller to identify a natural person

LProhibition2nd : The controller shall not be obligated to acquire additional information for identification

50thLRULE : 15th.FACT ∧ 23th.LFACT ∧ 83th.LFACT -> LProhibition2nd

- *Article 14: where personal data relating to a data subject are collected,* ***the controller*** ***<u>shall</u> provide the data subject with at least the following information:***

  the identity and the contact details of the controller *and, if any,* ***of the controller's representative and of the data protection officer...***

14th.LFACT. Personal data is related to data subject

96th.LFACT . Controller/Processor collects personal data.

97th.LFACT Controller has representative

98th.LFACT . Controller has data protection officer

99th.LFACT . Controller has identity

100th.LFACT Controller has contact details

101st.LFACT Representative has identity

102nd.LFACT Representative has contact detail

103rd.LFACT Data Protection Officer has identity

104th.LFACT Data Protection Officer has contact detail

22ndLObligation : controller shall provide the data subject with controller's identity

23rdLObligation : controller shall provide the data subject with controller's contact detail

24thLObligation : controller shall provide the data subject with controller's representative identity

25thLObligation : controller shall provide the data subject with representative's contact detail

26thLObligation : controller shall provide the data subject with data protection officer's identity

27thLObligation : controller shall provide the data subject with data protection officer’s contact detail.

51stLRULE : 14thL.FACT ^ ***96***th.LFACT ^ 99th.L.FACT -> 22th.LObligation.

52ndLRULE : 14th.FACT ^ ***96***th.LFACT ^ 100th.LFACT -> 23th.LObligation.

53rdLRULE : 14th.LFACT ∧ 96th.LFACT ^ 97st.LFACT ^ 101th.LFACT-> 24th.LObligation

54thLRULE : 14th.LFACT ∧ ***96***th.LFACT∧ 98nd.LFACT ^ 103th.LFACT ->23th.LObligation

55thLRULE : 14th.LFACT ∧ 96th.LFACT ∧ 98nd.LFACT ∧ 104th.LFACT -> 26th.LObligation

56thLRULE 14th.LFACT ∧ 96th.LFACT ∧ 98nd.LFACT ∧ ***104***th.LFACT -> 27th.LObligation

- **Law Application**

Definition3. Processing

'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording*, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction*;

43th.LFACT. Some operation(s) are performed upon personal data(s) (processor performs operation(s) on personal data)

44th.LFACT. The operation(s) are performed by automated means

46th.LFACT. Example of processing is collection (processor collects personal data)

LRESULT4th: the operation(s) is processing.

76th.LRULE: 43rd.LFACT ∧ 44th.LFACT ∧ 46th.LFACT-> LRESULT4th

Esilver-company has-goalDependencyTo keep-CustomerPersonaldata ∧

Processor performs operations on personal data

Keep-CustomerPersonaldata is-decomposedByResourcef data-base ∧

Operation are performed by automated means

Esilver-company has-TaskDependencyTo collect-Customer’sPersonaldata ->

Processor collect personal data

Collect-Customer’sPersonaldata is process

Operation is process

Definition 5: controller

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

52th.LFACT:. An agency determines the purpose of processing

53th.LFACT. An agency determines the condition of processing

54th.LFACT. An agency determines the means of processing

55th.LFACT. The Agency determines above alone

LRESULT6th: Agency is controller

82th.LRULE: 52nd.LFACT ∧ 53rd.LFACT ∧ 54th.LFACT ∧ 56th.LFACT-> LRESULT5th

Esilver-company has-goalDependencyTo determine-purpose-of-collecting ∧

Processor determine processing purpose

Esilver-company has-goalDependencyTo determine-condition-of-collecting ∧

Processor determine processing condition

Esilver-company has-goalDependencyTo determine-mean-of-collecting ->

Processor determine processing mean

Esilver is controller

Agency is controller

Definition 6: processor

processor means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

62th.LFACT. A natural body process personal data

67th.LFACT. Processing is behind the controller

LRESULT7th: Natural person is processor

83TH.LRULE: 62nd.LFACT ʌ 67th.LFACT -> LRESULT7th.

Esilver-Staff has-TaskDependencyOf Collecting-Customer Personal data ʌ

Natural-person process personal data

Collecting-Customer-Personal-data is-decomposedBy-SoftGoalOf beingBehind-Esilver →

Processing is-behind-controller

Esilver-Staff is processor

Natural-person is Processor

1. *The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes.*

2. If the data subject's consent is to be given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

15th.LFACT: personal data is being processed (processor is processing personal data)

LRecommendation2nd. Personal data should be processed on the basis of some legitimate basis

22th.LFACT. The consent is to the processing of personal data

23th.LFACT. Personal data belongs to data subject

80th.LFACT. The consent is for processing purposes

22th.LFACT. The consent is to the processing of personal data

21th.LFACT. data subject has given consent

16th.LObligation. The controller shall bear the burden of proof for consent

LPermission1st. Data subject may withdraw consent

93nd.LRULE: 15th.LFACT ∧ 21th.LFACT ∧ 23th.LFACT ∧ 24st.LFACT ∧ LRecommendation.1st -> 16th.LObligation

94rd.LRULE: LRecommendation1st-> LPermission1st

Esilver-Staff has-TaskDependencyOf collect-Customer’sPersonaldata ∧

Processor collect personal data

Esilver-customer has-ResourceDependencyOf Customer’s personal data ∧

Data-subject has personal data

Esilver-company has-obligationTo bear burden of proof for consent →

Controller has obligation to bear burden of proof for consent

Esilver-customer has-TaskDependencyOf give consent →

Data-subject has given his/her consent

Esilver-customer has-permissionTo withdraw his/her consent

Data-subject has-permissionTo withdraw his/her consent

Article 14: Information to the data subject

Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer

14th.LFACT:. . Information relates to data subject

LRESULT2nd: The information is personal data

96th.LFACT:. Controller/Processor collects personal data

22th.LObligation: controller shall provide the data subject with controller’s identity

23th.LObligation: controller shall provide the data subject with controller’s contact detail

120th.LRULE: 14thL.FACT ^ ***96***th.LFACT ^ 99th.L.FACT -> 22th.LObligation.

121th.LRULE :14th.FACT ^ ***96***th.LFACT ^ 100th.LFACT -> 23th.LObligation

Esilver-customer   has-ResourceDependencyOf   Customer’s personal data ^

Data-subject   has   personal data

Esilver-Staff   has-TaskDependencyOf   collect-Customer’sPersonaldata →

Processor   collect personal data

Esilver-company has-obligationTo provide ESilver’s identity to Esilver-customer

Controller   has obligation to provide controller’s identity to data-subject

Esilver-company has-obligationTo provide ESilver’s contact details to Esilver-customer

Controller   has obligation to provide controller’s contact detail to data-subject

Article 17: Right to be forgotten and to erasure

The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

15th.LFACT: personal data is being processed (processor is processing personal data)

96th.LFACT. Controller/Processor collects personal data

105th.LFACT . The personal data were processed by controller (the controller has processed personal data).

106th.LFACT . Data is no longer necessary in relation to processing purposes

21th.LFACT. data subject has given consent

LPermission6th . Data subject may withdraw consent

107th.LFACT . The data subject objects on processing of personal data

108th.LFACT . Data subjects makes available his/her personal data

109th.LFACT . Data subject was a child

110th.LFACT The storage period of personal data has expired

111th.LFACT There is no other ground for the processing of the data

LPermission7th . The data subject shall have the right to obtain from controller the erasure of personal data (the data subject has the right to ask the controller to erase…)

57thLRULE : 15th.LFACT ∧ 96th.LFACT ∧ 108th.LFACT ∧ 110th.FACT ^ 111th.FACT → Permission5th.

58thLRULE : 15th.LFACT ∧ 96th.LFACT ∧ 21th.LFACT ∧ LPermission5th.→ LPermission6th

59thLRULE : 15th.LFACT ^ 96th.LFACT ∧ 110th.LFACT -> LPermission6th..

60thLRULE : 15th.LFACT ^ 96th.LFACT ∧ 111th.LFACT -> LPermission6th.

Esilver-customer has-ResourceDependencyOf Customer's personal data ∧

Data-subject has personal data

Esilver-Staff has-TaskDependencyOf collect-Customer'sPersonaldata ∧

Processor collect personal data

~ Esilver-staff has-GoalDependency to use personal data for processing purpose →

~ Processor use personal data for processing purpose

Esilver-customer has permission to ask Esilver-company to erase his/her personal data

Data subject has permission to obtain from controller the erasure of personal data

Article 28. Documentation

Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

15th.LFACT. Personal data is being processed

112th.LFACT . Processing operations are under controller’s responsibility

28thLObligation : Each controller has the obligation to maintain documentation of all processing operations.

61stLRULE : 15th.LFACT ∧ 112th.LFACT → 28th.LObligation.

Esilver-Staff has-TaskDependencyOf collect-Customer’sPersonaldata ∧

Processor collect personal data

Esilver-company has-GoalDependncyOf is responsible for collecting personal data →

Controller is responsible for processing operation

Esilver-company has-obligationTO maintain documentation for collecting personal data

Controller has obligation to maintain documentation for processing

- **Refinement of GDPR by Standards and ICO:**

GDPR:

'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

1st.LFACT: The natural person is identified

2nd.LFACT:The natural person can be identified

.3rd.LFACT :Identification is directly

4th.LFACT :Identification is indirectly

5th.LFACT :Identification is by means

6th.LFACT :The mean is used by controller

7th.LFACT :The mean is used by natural person

8th.LFACT :Mean is used by legal person

9th.LFACT :Identification is by reference to an identification number

10th.LFACT :Identification is by reference to a location data

11th.LFACT Identification is by reference to an online identifier

12th.LFACT Identification is by reference to the person physical factor(s)

13th.LFACTis true regarding physiological, genetic, mental, economic, cultural and social identity of the person

LRESULT1st: Natural person is a Data subject

1stLRULE:. 1st.LFACT ∧ 3rd.LFACT -> **L**RESULT1st

2ndLRULE: 1st.LFACT ∧ 4th.LFACT∧ 5th.LFACT ∧ 6th.LFACT ∧9th.LFACT-> **L**RESULT1st

3rdLRULE: 1st.LFACT ∧ 4th.LFACT ∧ 5th.LFACT ∧ 6th.LFACT ∧10th.LFACT-> **L**RESULT1st

5th.LRULE:1st.LFACT ∧4th.LFACT ∧ 5th.LFACT ∧6th.LFACT ∧ 12th.LFACT -> **L**RESULT1st

There might be confusion regarding understanding of the terms *directly identification* or *indirectly identification* of the natural person as mentioned in law. But definition from ISO 29100 is an alternative here as it is making an extra condition for directly identification by name of the natural person, also indirectly identification by other factors such as *account identifier* or *social security number*. Although these factors (except from name) are also mentioned in definition of law, but it is not clear if they are regarding direct or indirect identification. Also ISO 29100 adds two more condition to the criteria of being PII Principal as providing PII to controller and processor which can amend GDPR rule. Amending rules extracted from GDPR with new facts from ISO 29100, will resolve these ambiguities clearer, especially for new developers unfamiliar with these concepts:

8th.SFACT = 3rd.LFACT

10st.SFACT=4th.LFACT

LRESULT1st = 6th.SRESULT15th

PII Principal$_{s}$ = Data Subject$_{L}$

Direct identifications$_{S}$ = Direct identification$_{L}$

Indirect identification$_{T}$ = Indirect Identification$_{L}$

2nd.LRULE: 1st.LFACT ∧ 4th.LFACT∧ 5th.LFACT ∧ 6th.LFACT ∧9th.LFACT ^ 11nd.SFACT -> **L**RESULT1st

2ndLRULE : 1st.LFACT ^ 4th.LFACT ^ 5th.LFACT ^ 6th.LFACT ^ 9th.LFACT ^ 12th.S.FACT -> LRESULT1st

1stLRULE:. 1st.LFACT ∧ 3rd.LFACT ∧ **9**th.SFACT -> **L**RESULT1st.

Data controller: To determine whether you are a data controller you need to ascertain which organisation decides:

- *to collect the personal data in the first place and the legal basis for doing so*
- *which items of personal data to collect, i.e. the content of the data;*
- *The purpose or purposes the data are to be used for;*
- *Which individuals to collect data about;*
- *Whether to disclose the data, and if so, who to;*
- *Whether subject access and other individuals' rights apply i.e. the application of exemptions; and*
- *How long to retain the data or whether to make non-routine amendments to the data.*

30th.GFACT : the organisation decides to collect the personal data in first place

31st.GFACT : the organisation decides the legal basis for personal data collection

32nd.GFACT : the organisation decides the purpose(s) to use personal data (processing purposes)

33rd.GFACT : the organisation decides on selection of data subject

34th.GFACT : the organisation decides on data disclosure

35th.GFACT : the organisation decides on personal data recipients

36th.GFACT : the organisation decides on data subject rights

37th.GFACT : the organisation decides on data subject access to personal data

38th.GFACT : the organisation decides on exception of data subject access on personal data

39th.GFACT : the organisation decides on personal data retain

40th.GFACT : the organisation decides to make non-routing amendment on personal data.

.

3rd.GRESULT : organisation is data controller

67th.GRULE : 30th.GFACT -> 3rd.GRESULT.

68th.GRULE :*31*st.GFACT -> 3rd,GRESULT

69th.GRULE : *32*nd.GFACT -> 3rd.GRESULT.

70th.GRULE : *33*rd.GFACT -> 3rd.GRESULT.

71st.GRULE : *34*th.GFACT -> 3rd.GRESULT.

72nd.GRULE : *35*th.GFACT -> 3rd.GRESULT.

73rd.GRULE : *36*th.GFACT -> 3rd.GRESULT.

74th.GRULE : *37*th.GFACT -> 3rd.GRESULT.

75th.GRULE : *38*th.GFACT -> 3rd.GRESULT.

76th.GRULE : *39*th.GFACT -> 3rd.GRESULT.

77th.GRULE : *40*th.GFACT -> 3rd.GRESULT.

GDPR:

52th.LFACT. A natural person determines the purpose of processing

53th.LFACT. A natural person determines the condition of processing

54th.LFACT. A natural person determines the means of processing

55th.LFACT. Natural person determines above alone

56th.LFACT. Natural person determines above jointly by others

57th.LFACT A legal person determines the purpose of processing

58th.LFACT. A public authority determines the purpose of processing

59st.LFACT. An agency determines the purpose of processing

60nd.LFACT. Anybody determines the purpose of processing

61rd.LFACT. Fact 25, 26, 27 and 28 are true about legal person, public authority, agency or any body

LRESULT5th: Natural person is controller

LRESULT6th: Agency is a controller

81th.LRULE: 52nd.LFACT ^ 53rd.LFACT ^ 54th.LFACT ^ 55th.LFACT ->LRESULT5th.

82th.LRULE52nd.LFACT ^ 53rd.LFACT ^ 54th.LFACT ^ 56th.LFACT-> LRESULT5th

$\text{Organisation}_{\text{ICO}} = \text{Agency}_{\text{GDPR}}$

3rd.GResult = LResult5th

Two above concepts of Organisation and agency are equal and mapped together from ICO and GDPR ontologies. This is in a situation where 3rdResult from ICO and Result5th from law are equal as well. Therefore, the facts which conclude to 3^{rd}.GResult are automatically inherited to $\text{organisation}_{\text{ICO}}$ and Result5th is concluded from these facts as well. This is adding more criteria for an agency to become controller as well.

Data Processor: A data processor may decide:

- *what IT systems or other methods to use to collect personal data;*
- *How to store the personal data;*
- *The detail of the security surrounding the personal data;*
- *The means used to transfer the personal data from one organisation to another;*
- *The means used to retrieve personal data about certain individuals;*
- *The method for ensuring a retention schedule is adhered to;*
- *The means used to delete or dispose of the data.*

At one extreme, one party will determine what personal data is to be processed and will provide very detailed processing instructions which the other party must follow. The party following the instructions is tightly constrained in what it can do with the data and has no say at all over its content or how it is processed. In this relationship the party providing the detailed instructions (the client) is clearly the data controller and the party following the instructions (the service provider) is the data processor.

41st.GFACT . Party provides detailed processing instructions

42nd.GFACT . Party follow the detailed processing instruction

GPermission41st : Processor is permitted to decide on personal data collecting IT systems

GPermission42nd: Processor is permitted to decide on personal data collecting methods

GPermission43rd : Processor is permitted to decide on the personal data storage methods

GPermission44th : Processor is permitted to decide on the personal data retrieval means

GPermission45th : Processor is permitted to decide on detail of personal data surrounding security

GPermission46th : Processor is permitted to decide on adhering data retention methods

GPermission47th : Processor is permitted to decide on data delectation methods

GPermission48th : Processor is permitted to decide on data disposal methods

4th.GRESULT . Party is data processor

78th.GRULE : 41th.GFACT -> 4th.GRESULT

79th.GRULE : 42th.GFACT ^ 41th.GFACT -> 4th.GRESULT

80th.GRULE : 4th.GRESULT -> GPermission41th

81st.GRULE : 4th.GRESULT -> GPermission42th

82nd.GRULE : 4th.GRESULT -> GPermission43th

83rd.GRULE : 4th.GRESULT -> GPermission44th

84th.GRULE : 4th.GRESULT -> GPermission45th

85th.GRULE : 4th.GRESULT -> GPermission46th

86th.GRULE : 4th.GRESULT -> GPermission47th

87th.GRULE : 4th.GRESULT -> GPermission48th

GDPR:

62th.LFACT. A natural body process personal data

63th.LFACT. A legal person process personal data

64th.LFACT. A public authority process personal data

65th.LFACT. An agency process personal data

66th.LFACT. Anybody process personal data

67th.LFACT. Processing is behind the controller

LRESULT7th: Natural person is processor

83th.LRULE: : 62nd.LFACT ∧ 67th.LFACT -> LRESULT7th

84th.LRULE: 63rd.LFACT ∧ 67th.LFACT -> LRESULT7th

85th.LRULE: 63rd.LFACT ∧ 67th.LFACT -> LRESULT7th

86th.LRULE: : 63rd.LFACT ∧ 67th.LFACT -> LRESULT7th

87th.LRULE: : 63rd.LFACT ∧ 67th.LFACT -> LRESULT7th

4th.GRESULT = **L**RESULT7th

Party$_G$ = Natural Person$_L$ = Individual$_S$

Party$_G$ = Agency$_L$

41h.FACT and 42th.FACT from ICO add new condition for a party to become a processor. Indeed, permissions 41 to 48 are inherited from ICO Ontology to GDPR and make new rights for processor. Provided knowledge's help the complier through a better and clearer understanding of the terms and concepts of the law in order to apply the law to the right person and elements of the system context.

Personal Data: Data which identifies an individual, even without a name associated with it, may be personal data where it is processed to learn or record something about that individual, or where the processing of that information has an impact upon that individual.

43rd.GFACT . Data identifies an individual

44th.GFACT . Data is associated by name

45th.GFACT . Data is processed to learn something about that individual

46th.GFACT . Data is processed to record something about that individual

47th.GFACT . The processing of that information has an impact upon that individual

5th.GRESULT . Data is personal data

There is almost also a flowchart of questions to be passed in order to determine a fact in commissioner's guideline document which in this case is to understand if a data is actually personal data. The flowchart is provided in ICO guidelines for personal data (Information Commission Office 2011, What is personal data? – A quick reference guide). The flowchart includes "if conditions" with a list of questions to be asked in order to determine if data is actually personal data. The questions are converted to the facts here in order to determine if the result of the data being personal data can be achieved as following.

48th.GFACT . A living individual can be identified from the data

49th.GFACT . A living individual can be identified from the information

50th.GFACT . Information is in your possession

51st.GFACT . Information is likely to come in to your possession

52nd.GFACT . Data is related to the identifiable living individual in his personal life

53rd.GFACT . Data is related to the identifiable living individual in his family life

54th.GFACT . Data is related to the identifiable living individual in his business

55th.GFACT . Data is obviously about a particular individual

56th.GFACT . Data is linked to an individual

57th.GFACT . Data provides particular information about that individual

58th.GFACT . Data has biographical significant in relation to the individual

59th.GFACT . Data concentrate on the individual as its central scheme

60th.GFACT . The data does not focus on some other person

61st.GFACT . The data does not focus on some other object

62nd.GFACT . The data does not focus on other event

63rd.GFACT . The data impact an individual personal life

64th.GFACT . The data has the potential to impact an individual personal life

65th.GFACT . The data impact an individual family life

66th.GFACT . The data impact an individual business

5th.GRESULT: Data is personal data

As explained before these new facts adds conditions on GDPR facts for personal data definition as below:

14th.LFACT. Information is related to data subject

LRESULT2nd. The information is personal data

42nd.LRULE: 14th.LFACT-> **L**RESULT2nd

5th.GRESULT = LRESULT2nd.

88th.GRULE : 43th.GFACT ∧ 44th.GFACT∧ 48st.GFACT∧ 50rd.GFACT → 5th.GRESULT

89th.GRULE :43th.GFACT ∧ 44th.GFACT∧ 48st.GFACT ∧ 51th.GFACT→ 5th.GRESULT

90th.GRULE : 48st.GFACT ∧ 55th.FACT ∧ 520th.GFACT → 5GRESULT.

91st.GRULE : 49nd.GFACT ∧ 56th.GFACT ∧ 57th.GFACT → 5GRESULT

92nd.GRULE : 49nd.GFACT ∧ 56th.GFACT ∧ 58st.GFACT∧ → 5GRESULT

Above rules from ICO indicate requreents for data becoming personal data. From ther point based on GDPR, data is personal data if it is related to a data subject. ICO rule can be used here to determine if a data is related to data subject. Since 5th GRESULT is equalu to LRESULT2nd, and 14th.LFACT results to LRESULT2nd, having 5th.GRESULT in ICO will automatically conclude to. 14th,LFACT. This again trusts to the equvalation of concepts. More rules can be depicted by provided facts but the most important one are selected as above.

APPENDIX III: AU-SoPD MANUAL

To understand the process of requirement gathering using i*, application of law to system context and the process of our ontology-based framework which we have called it AU-SoPD, we are studying a simple case study here. The case study is a web site of an Italian supplier of silver-made artefacts briefly called ESilver and we will try to design this web site with regard to its privacy requirements. The concentration here will be to elicit and gather high-level communication requirements, hypermedia specific requirements, content, interaction, navigation and also presentation requirements of a web application and apply any necessary legal demands to the application areas. In order to represent different types of requirements, the categorisation of requirements represented in the work AWARE (Bolchini & Paolini, 2004) is being used as the reference here. Researchers in AWARE have represented web application requirements using i* framework. There are different types of web applications such as e-commerce, healthcare, educational, corporate and others. Regarding the sensitivity of the financial and privacy aspect of the case, e-commerce application requirements have been selected here to be analysed. We have decided to use same case study in AWARE in order to synchronize works and limit the processing time. Although additional analysis and application of relating laws to the case and some major changes has been occurred here. Based on this work, web application requirements are categorised as below:

- Content Requirements: set of ideas and messages and information chunks that the web communicates to its users. In case of e-commerce web application some examples of content requirements are “present details for each item”.

- Structure of Content Requirements: providing initial requirements about the structure of contents. In context of e-commerce example, the structure requirement can be “highlight the price of the item”

- Access path to Contents: navigational path provided to users in order to reach the needed contents. To “allow the registered user to access his/her shopping basket” is an example of this type of requirement in e-commerce context.

- Navigation: requirements that allow the user to navigate from one piece of contents to others. Example is to “related an item to its available colours”.

- Presentation: requirements concern two aspects of graphic and interface layout. Example can be to “present a young style for teenagers in kid’s section”.

- User Operations: the operations which are visible to users to complete some tasks which users can trigger to by interacting with the application. Some examples are to “subscribe to a mailing list” or to “leave a comment on a shopped item”.

- System Operations: these operations are not visible to users but become mandatory to build user operations. Possible system requirements include “force user authorization for building user shopping basket" or "track user navigation and build preference profiles".

- Interactions; these requirements are related to contents and presentation aspects that may need a specific design elaboration. Some examples can be mentioned as to "provide the user with a 3D model of shopping items".

The design firstly starts with considering three major actors of the firm as ESilver, Shop-Manager and the typical client of the company. In order to design related diagrams for B-Silver case study, a supporting tool for i* framework called OpenOME is being used here. Based on the nature of i* modelling, further actors will incrementally be added to the design based on discovered new dependencies of available actors. As the following analysis, new goals and tasks of newly added actors will be discovered as well. In such an incremental process the requirements of system will be discovered. To do so, the initial analysis is based on traditional business of the ESilver Company and traditional requirements are simulated to system requirements (ESilver Website system). Following image is representing the initial requirements of ESilver system both considering the traditional also system requirements.

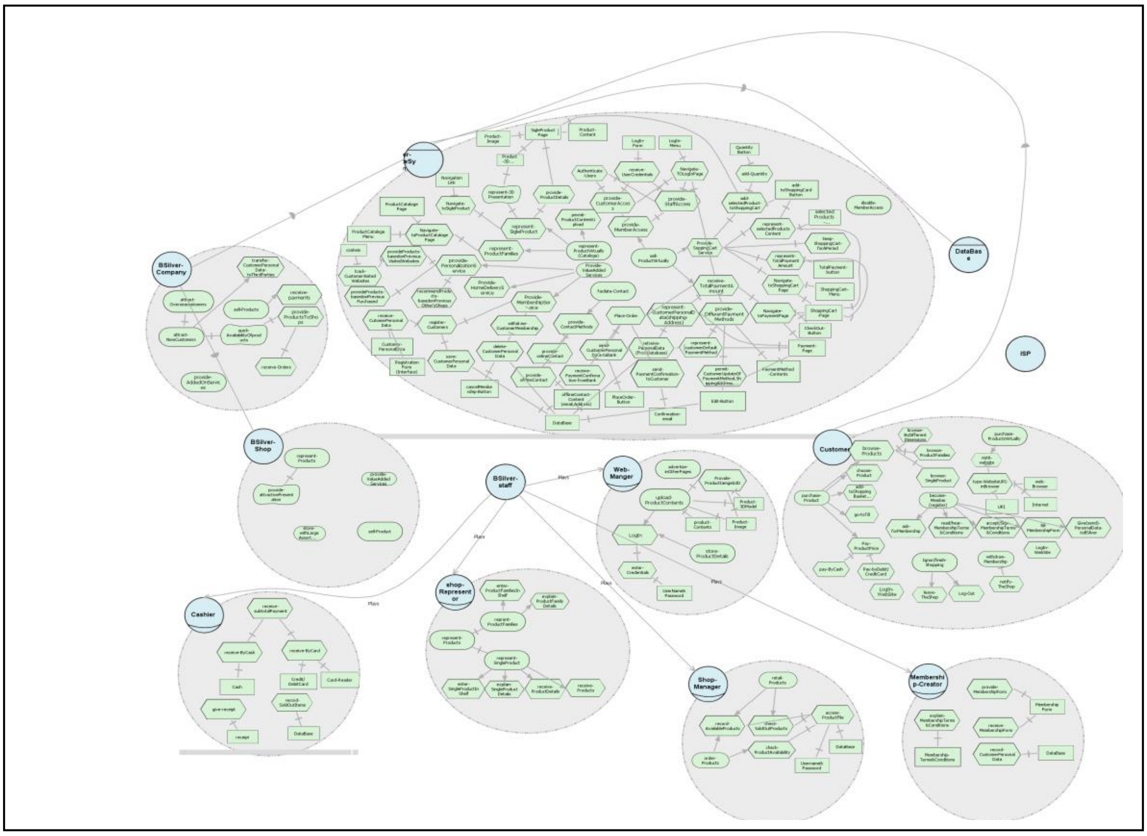


Figure1 . ESilver Case Study Modelled by OpenOME

In design of ESilver case study, we are also using number of web application design patterns. The authors in AWARE, also have introduced usage of design patterns in *"Modelling-by-Patterns" of Web Application* (Rossi et al. 2000). The other important matter that had to be considered was the validity of the pattern resource. There are plenty of different resources which have introduced design patterns in the area of web application design. The most important thing to consider when selecting design patterns is if they are widely shared and circulated across several communities and it's effectively has been proved by several experiences. Therefore we had to find a valid resource of web application pattern repository introduced by expert developers as it has been said that the pattern should have been used by at least three developers except the author of the pattern (Brodie 1984). One of the most reliable repositories of patterns that we could use was belonged to IBM. IBM has introduced a series of patterns for e-business in 2003 (Wedekind, 2008). The introduction document indicates the well and organized structure of patterns also the vast area of cover. But unfortunately IBM pattern repository was not available at time of this project. Another valuable pattern repository could be "*Online WWW Design Pattern Repository"* launched by ACM Special Interest Group on Hypertext, Hypermedia and the Web. This resource was not available as well. In the search for a trusted resource, (User Interface Design Patterns-UI Patterns) was found which has listed number of web pattern libraries such as *UC Berkeley Resource for Building User Interfaces* which is only accessible to authorised users and *User Interface Design Patterns-UI Patterns* which is an open resource and therefore being used in our designs. Using the UI pattern library, we were able to extract requirements from numbers of patterns matching ESilver desired business goals. Number of ESilver high-level business goals with matching design patterns has been provided in the list below:

Business goal	**pattern**
Represent-products	Menus, Pricing table, Product Page, Navigation, Tables, Image zoom, slideshow, Contents
Provide-ValueAddedServices Create-membership Personalize-shopping Fascinate-contact	Menus, Account Registration, Getting Input, Navigation Personalizing Menus, Navigation, Contents
Sell-product	Menus, Shopping Card, Navigation, User Log-In

Table 1. UI Patterns used for ESilver Case Study

The process of applying patterns is to first find the most high-level business goals of the ESilver Company and then search for the most appropriate pattern. For example, to satisfy business goal of “sell-product” the most matching pattern will be the “Shopping Card” pattern:

“Solution:

A shopping cart is a collection of selected products that the user can choose to add more products to or remove products from. Further, the user can choose to change the quantity of each product in the shopping cart, and is presented by a subtotal cost of his or her selected items plus shipping charges, VAT, etc. At any time, the user can choose to continue shopping or proceed to checkout – meaning to paying and ordering what is in the shopping cart.

Whenever a product is presented, a complimenting button lets the user add the respective product to the product cart. The cart can be expected at any time in detail by clicking on a “show cart” link.

When the user chooses to checkout, he is presented with a final list of items on the order, as well as options as to how he or she wants to pay (credit card, wire transfer or cash on delivery).” (User Interface Design Patterns-UI Patterns, Shopping Cart Pattern).We could extract following requirements from above pattern:

1) Add product
2) Remove products
3) Change the quality of products
4) Present subtotal cost plus shipping charges
5) Continue shopping
6) Check out
7) Pay the subtotal amount
8) Show cart details (selected products)
9) Present final list of items on order
10) Present payment methods

As presented in Figure 1, mentioned requirements are modelled as different tasks of ESilver Website Agent and other agents. It should be mentioned that in this section we practiced two components of our framework, i* modelling and using design patterns without considering the ontological solution for them. This has been done in order to make the reader familiar with the concept of our model as a starting point. In following sections, the ontological solution will be practiced with ESilver case study.

○ Evaluation of ESilver Case Study by i* Ontology

The semantic web ontology is an advantage and a key technology for effective information access since they help to overcome the problems of text-free searches by relating and grouping relevant terms in a specific domain. Therefore, in conception environment where queries are based on conception relations between objects using semantic web technology is a big advantage. Example of such environment is the proposed framework in current work. First of all, and as the first component of the framework, we have the i* methodology which includes number of classes such as *actor*, *goal*, *task* and *resource* and the relation between the mentioned classes such as an *actor having goal dependency*, or *an actor having task dependency* or *having a resource dependency*. In application area of any developing system using i* methodology, each of the mentioned classes and their relations can be replaced by real individuals from context of developing system. To clear the discussed matter, we are using some examples as below. The examples are directly taken from the case study of ESilver mentioned modelled by OpenOME in previous section:

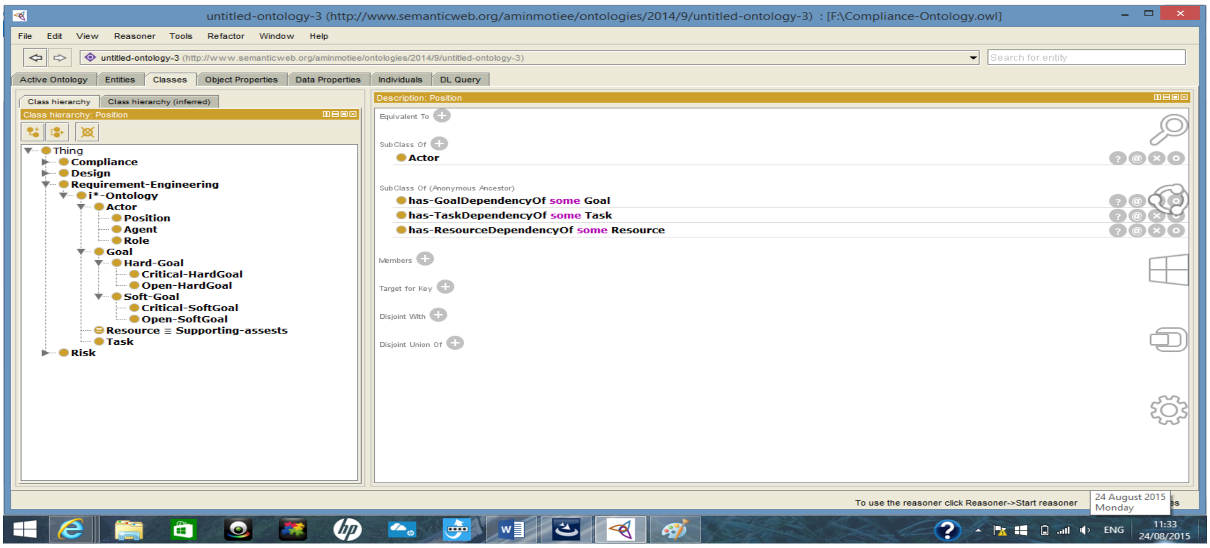
1- Membership-creator has the task to record customer personal data

2- ESilver-company has the task to transfer customer personal data to third parties

3- ESilver-website has the task to receive and check user-credentials

4- ESilver-website has the task to receive customer personal data

As seen in above examples actors of membership-creator and ESilver Company and ESilver website have some task dependency. In following image which are screenshots taken from our ontology based framework implemented by Protégé, we are showing different classes of i* ontology and their implementation and at the end we will test it by out ESilver case study.



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Individuals
DL Query
Class hierarchy
Class hierarchy (inferred)
Class hierarchy: Position
Description: Position
To use the reasoner click Reasoner->Start reasoner
24 August 2015
Monday
ENG
11:33
24/08/2015

```
Thing
  Compliance
  Design
  Requirement-Engineering
    i*-Ontology
      Actor
        Position
        Agent
        Role
      Goal
        Hard-Goal
          Critical-HardGoal
          Open-HardGoal
        Soft-Goal
          Critical-SoftGoal
          Open-SoftGoal
      Resource ≡ Supporting-assests
      Task
  Risk
```

```
Equivalent To
SubClass Of
  Actor
SubClass Of (Anonymous Ancestor)
  has-GoalDependencyOf some Goal
  has-TaskDependencyOf some Task
  has-ResourceDependencyOf some Resource
Members
Target for Key
Disjoint With
Disjoint Union Of
```

Figure2 . i* Ontology. Protégé 3.4

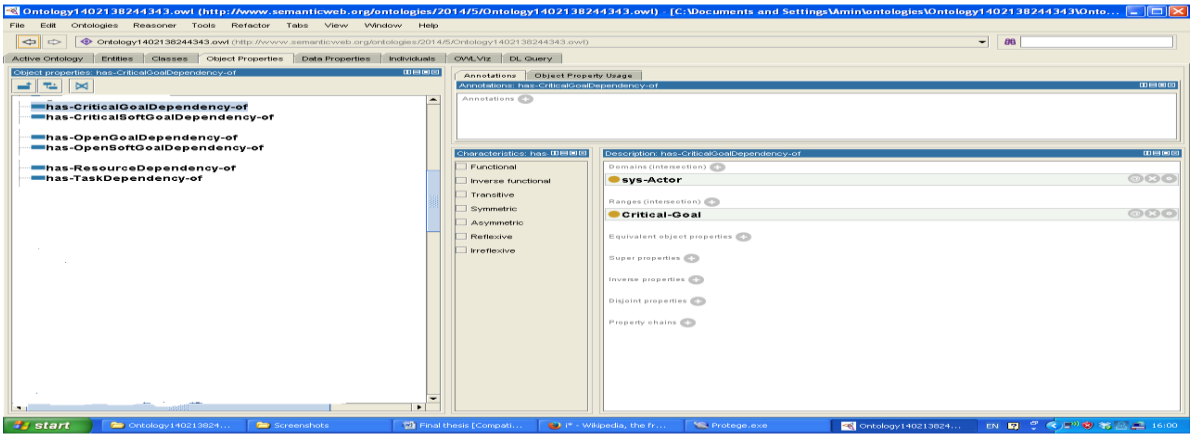
Figure 2 is representing the concepts (classes) of i* ontology as the first component of the proposed framework here. As mentioned before we have used protégé as the ontology making tool here. As visible in the picture above, the classes are categorised under the super class of i* ontology. The first considerable class is called Actor which represents the *Actor* in i*. This is in fact the stakeholder of the system which may have number of goals, tasks or resource dependencies. We have three different classes for goal, task and resource with some subclasses. Based on definitions of i*, an actor may have two types of goals which are represented here as Hard-goal and Soft-goal. Hard-Goal is any functional requirement of actor or system where in contrast Soft-goal is non-functional requirements of actors or system. Each Hard-goal or Soft-goal may also be critical or open depends on if their existence in the system is optional or mandatory. The other classes of i* ontology are task and resource representing the same concepts in the methodology. We have two types of modelling in i* as *Strategic Dependency Model* and *Strategic Rational model.* SD model describes a network of dependency relationships between actors. This model shows what goal or task the actor has and to whom the actor depends in order to perform the task or obtain the goal and a way the actors are called depender and dependee. Some examples are as following:

Membership-creator depends on the customer for the task dependency to record customer personal data

The second model of i*, SR model allows modelling of the goal and task and resource dependencies associated to each actor without considering the dependee. This model provides information regarding the way actors achieve their hard-goals and soft-goals. Some examples are as following:

Membership-creator has the task dependency to record customer personal data

In order to make consistence between framework's components and regarding similar structures of laws to SR model, the relations between i* ontology are mostly focused on SR model. These relations are constructed in ontology using *objectPropery* as represented in following image.



Ontology1402138244343.owl (http://www.semanticweb.org/ontologies/2014/5/Ontology1402138244343.owl) - [C:\Documents and Settings\Amin\ontologies\Ontology1402138244343\Onto...

Ontology1402138244343.owl (http://www.semanticweb.org/ontologies/2014/5/Ontology1402138244343.owl)

Object properties: has-CriticalGoalDependency-of

- has-CriticalGoalDependency-of
- has-CriticalSoftGoalDependency-of
- has-OpenGoalDependency-of
- has-OpenSoftGoalDependency-of
- has-ResourceDependency-of
- has-TaskDependency-of

Annotations: has-CriticalGoalDependency-of

Characteristics: has-

□ Functional
□ Inverse functional
□ Transitive
□ Symmetric
□ Asymmetric
□ Reflexive
□ Irreflexive

Description: has-CriticalGoalDependency-of

Domains (intersection): sys-Actor

Ranges (intersection): Critical-Goal

Equivalent object properties

Super properties

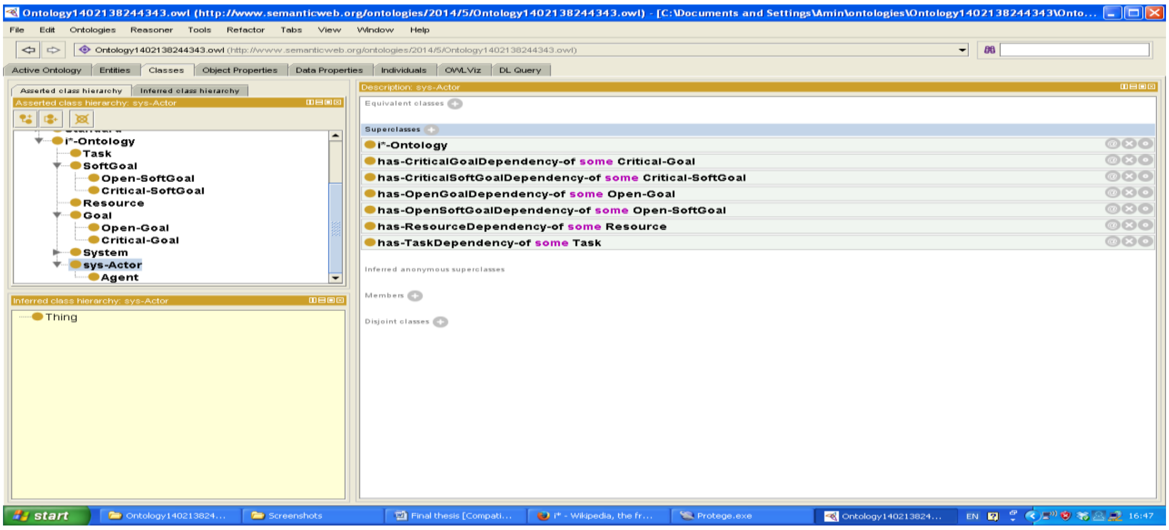
Inverse properties

Disjoint properties

Property chains

Figure3   . i* ObjectProperties

We have 70 ObjectProperties in i* ontology which some are shown in Figure 3. When constructing ObjectProperties in protégé one strategic matter to consider is to determine the domain and range of the objectPropery. Domain and range determine the classes in ontology which are related together using the objectproperty. Based on defined ObjectProperties we have following relations in i* ontology as shown in Figure 4. The relations are shown as superclass of Sys-Actor.


Ontology1402138244343.owl (http://www.semanticweb.org/ontologies/2014/5/Ontology1402138244343.owl) - [C:\Documents and Settings\Amin\ontologies\Ontology1402138244343\Onto...
File Edit Ontologies Reasoner Tools Refactor Tabs View Window Help
Ontology1402138244343.owl (http://www.semanticweb.org/ontologies/2014/5/Ontology1402138244343.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query
Asserted class hierarchy Inferred class hierarchy
Asserted class hierarchy: sys-Actor
Inferred class hierarchy: sys-Actor
Description: sys-Actor
Equivalent classes
Superclasses
Inferred anonymous superclasses
Members
Disjoint classes
start
Ontology140213824...
Screenshots
Final thesis [Compati...
i* - Wikipedia, the fr...
Protege.exe
Ontology140213824...
EN
16:47

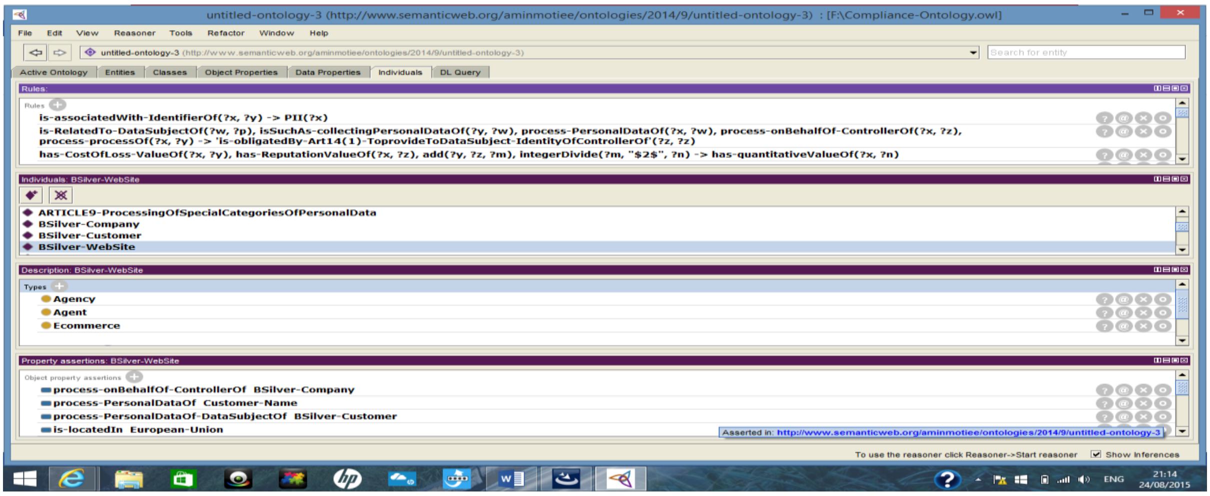
i*-Ontology
Task
SoftGoal
Open-SoftGoal
Critical-SoftGoal
Resource
Goal
Open-Goal
Critical-Goal
System
sys-Actor
Agent

Thing

i*-Ontology
has-CriticalGoalDependency-of some Critical-Goal
has-CriticalSoftGoalDependency-of some Critical-SoftGoal
has-OpenGoalDependency-of some Open-Goal
has-OpenSoftGoalDependency-of some Open-SoftGoal
has-ResourceDependency-of some Resource
has-TaskDependency-of some Task

Figure4 . Relations in i* Ontology

Having the concepts and relations, the ontology will be ready to be applied to context of any developing system. The application is performable using the *Individuals* infrastructure in protégé. Adding an individual in ontology, we can determine the class type of it and construct its relationships to other individuals using appropriate object properties. To have an example, ESilver website as an individual of *Agent*, is related to individual of *sell-ESilverProduct* as an individual of *Critical-Goal* using the objectproperty of *has-CriticalGoalDependency-of*. Other examples are shown in the figure below too.


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology Entities Classes Object Properties Data Properties Individuals DL Query
Rules:
Rules
Individuals: BSilver-WebSite
Description: BSilver-WebSite
Types
Property assertions: BSilver-WebSite
Object property assertions
Asserted in: http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3
To use the reasoner click Reasoner->Start reasoner
☑ Show Inferences
ENG
21:14
24/08/2015

```
is-associatedWith-IdentifierOf(?x, ?y) -> PII(?x)
is-RelatedTo-DataSubjectOf(?w, ?p), isSuchAs-collectingPersonalDataOf(?y, ?w), process-PersonalDataOf(?x, ?w), process-onBehalfOf-ControllerOf(?x, ?z),
process-processOf(?x, ?y) -> 'is-obligatedBy-Art14(1)-ToprovideToDataSubject-IdentityOfControllerOf'(?z, ?z)
has-CostOfLoss-ValueOf(?x, ?y), has-ReputationValueOf(?x, ?z), add(?y, ?z, ?m), integerDivide(?m, "$2$", ?n) -> has-quantitativeValueOf(?x, ?n)
```

ARTICLE9-ProcessingOfSpecialCategoriesOfPersonalData
BSilver-Company
BSilver-Customer
BSilver-WebSite

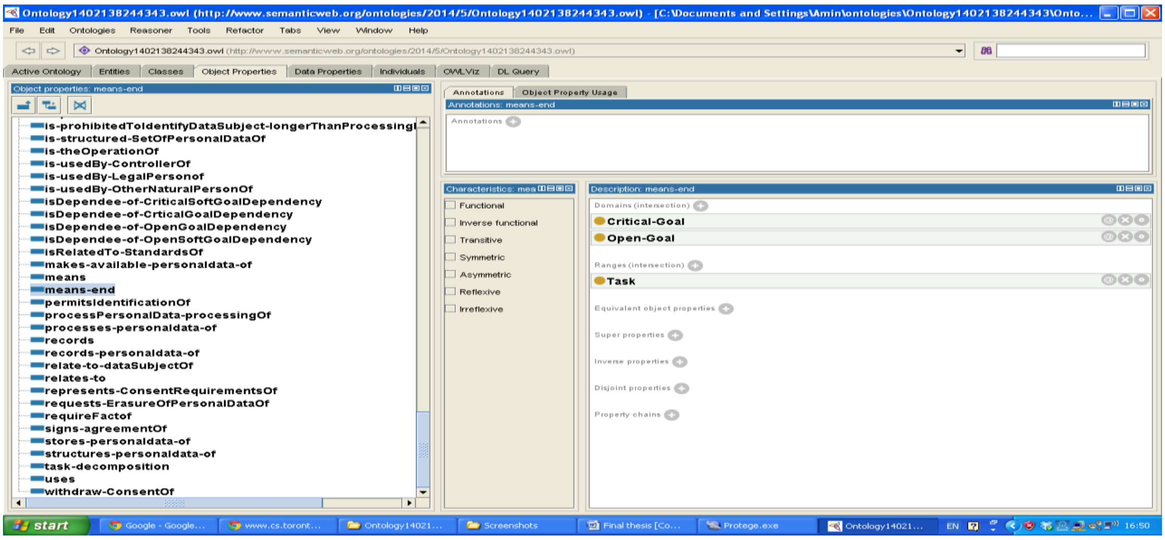
Agency
Agent
Ecommerce

process-onBehalfOf-ControllerOf BSilver-Company
process-PersonalDataOf Customer-Name
process-PersonalDataOf-DataSubjectOf BSilver-Customer
is-locatedIn European-Union

Figure5 . Individual Construction in i* Ontology

In the same way other actors of ESilver case study and their goals and tasks and resources can be constructed as well.

There are number of other relations in i* methodology which specifically define the type of refinement models of goals and tasks and resources. As the basis of i* methodology and as the requirement for system development each of goals, soft-goals and tasks should be refined to other goals, soft-goals or tasks. The refinements are categorised to different links between related classes based on their definitions and types. Sample of these relations are provided in Figure 6. this figure represents the objectproperty of *means-end* in i* ontology which relates classes of critical and open goal to the class of task. In same way the objectproperty of *Task-Decomposition* relates class of task to classes of goal, soft-goal or another task in order to specify that a task can be refined or satisfied by the later classes. Task also *contributes* in satisfaction of a soft-goal using the same objectproperty and soft-goal class (open or critical) are refined to other soft-goals using object-properties of *And* and *Or*.



Object properties: means-end

- is-prohibitedToIdentifyDataSubject-longerThanProcessingI
- is-structured-SetOfPersonalDataOf
- is-theOperationOf
- is-usedBy-ControllerOf
- is-usedBy-LegalPersonof
- is-usedBy-OtherNaturalPersonOf
- isDependee-of-CriticalSoftGoalDependency
- isDependee-of-CrticalGoalDependency
- isDependee-of-OpenGoalDependency
- isDependee-of-OpenSoftGoalDependency
- isRelatedTo-StandardsOf
- makes-available-personaldata-of
- means
- means-end
- permitsIdentificationOf
- processPersonalData-processingOf
- processes-personaldata-of
- records
- records-personaldata-of
- relate-to-dataSubjectOf
- relates-to
- represents-ConsentRequirementsOf
- requests-ErasureOfPersonalDataOf
- requireFactof
- signs-agreementOf
- stores-personaldata-of
- structures-personaldata-of
- task-decomposition
- uses
- withdraw-ConsentOf

Annotations: means-end

Annotations

Characteristics: mea

□ Functional
□ Inverse functional
□ Transitive
□ Symmetric
□ Asymmetric
□ Reflexive
□ Irreflexive

Description: means-end

Domains (intersection)
- Critical-Goal
- Open-Goal

Ranges (intersection)
- Task

Equivalent object properties

Super properties

Inverse properties

Disjoint properties

Property chains

Figure6 . Means-end Relation in i* Ontology

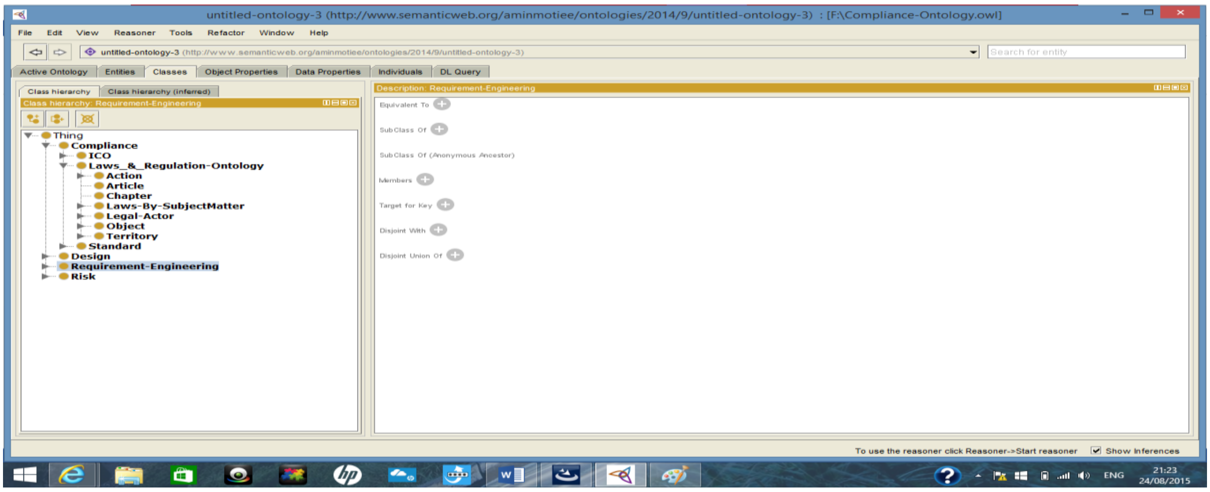
To connect individuals with means-end relation, the critical-goal of *sell-ESilverProduct* will be related to task of *browse-products* with means-end. In same way other goals and tasks can be refined to others using the mentioned relations.

○ Law & Regulation Ontology

As the second component of the proposed framework**,** we define an ontology for the legal concepts and their relations. A careful study of components of law and also the analysis of legal rules as discussed in previous sections had been an advantage to achieve this goal.

- ### Classes in Law & Regulation Ontology:

In order to provide the lists of classes in the *Legal Ontology* as the second component of the proposed framework, we have investigated through a number of concepts from the context of laws and analysed laws. Figure 7 is showing implementation of these classes in protégé.



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]

untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)

Class hierarchy: Requirement-Engineering

```
Thing
  Compliance
    ICO
    Laws_&_Regulation-Ontology
      Action
      Article
      Chapter
      Laws-By-SubjectMatter
      Legal-Actor
      Object
      Territory
    Standard
  Design
  Requirement-Engineering
  Risk
```

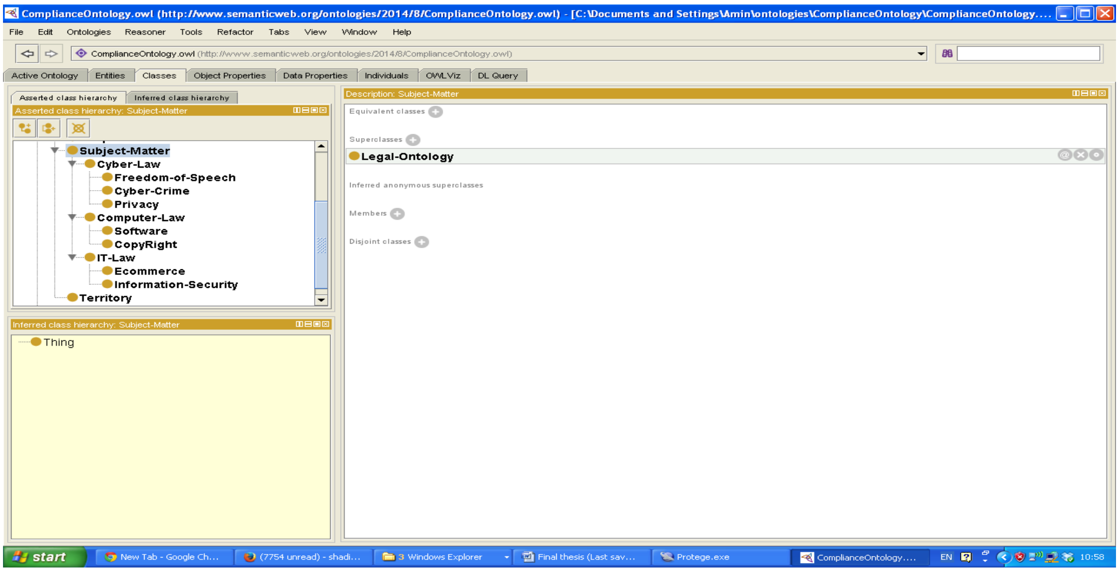
Description: Requirement-Engineering

To use the reasoner click Reasoner->Start reasoner ☑ Show Inferences

Figure7 . Law Ontology. Compliance Framework

For each of the seven classes of legal ontology as shown in image above, we have the following explanations:

1. *Subject-Matter:* this class represent the field of any considered law. As it is shown in Figure 8, it has number of subclasses which each represents an area of concern of legal system for IT matters. Figure 8 shows three main subclasses of the superclass *Subject-Matter* as *Cyber-Law*, *Computer-Law and IT-Law* and their belonged subclasses as well.



ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl) - [C:\Documents and Settings\Amin\ontologies\ComplianceOntology\ComplianceOntology....

ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl)

Asserted class hierarchy: Subject-Matter

```
Subject-Matter
  Cyber-Law
    Freedom-of-Speech
    Cyber-Crime
    Privacy
  Computer-Law
    Software
    CopyRight
  IT-Law
    Ecommerce
    Information-Security
Territory
```

Inferred class hierarchy: Subject-Matter

```
Thing
```

Description: Subject-Matter

Superclasses: Legal-Ontology

Figure8 . Law Ontology. Class of Subject-Matter

2. *Territory:* As the second class of legal ontology, we have territory of law which represent the geographical area where the law had been established for and applied to.

Talking about relation between classes, two classes of *Subject-Matter* and *Territory*, are related together through the objectproperty of *hasTerritoryOf*. In fact, different types of laws and regulations. An example is shown in Figure 9. In fact, two individuals of *Privacy-Law* and *Europe Territory* introduced as *DataProtectionRegulation2012* and *European-Union* are related together with relation “*hasTerritoryOf.*

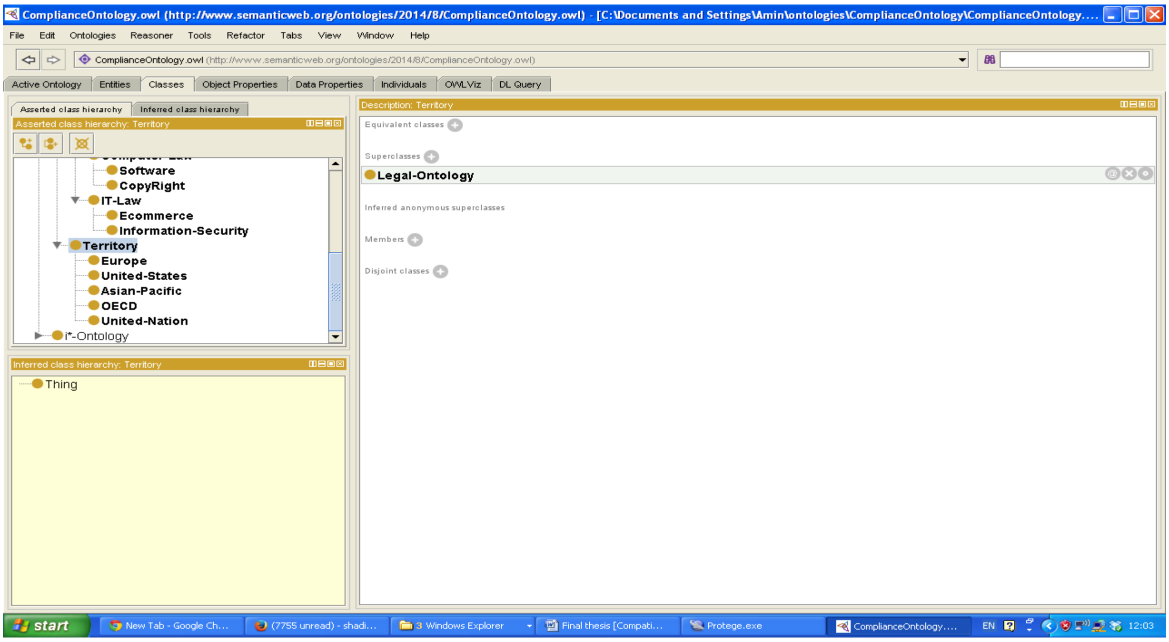

ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl) - [C:\Documents and Settings\Amin\ontologies\ComplianceOntology\ComplianceOntology....
File Edit Ontologies Reasoner Tools Refactor Tabs View Window Help
ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query
Asserted class hierarchy Inferred class hierarchy
Asserted class hierarchy: Territory
Software
CopyRight
IT-Law
Ecommerce
Information-Security
Territory
Europe
United-States
Asian-Pacific
OECD
United-Nation
i*-Ontology
Inferred class hierarchy: Territory
Thing
Description: Territory
Equivalent classes
Superclasses
Legal-Ontology
Inferred anonymous superclasses
Members
Disjoint classes
start
New Tab - Google Ch...
(7755 unread) - shadi...
3 Windows Explorer
Final thesis [Compati...
Protege.exe
ComplianceOntology....
EN
12:03

Figure9 . Law Ontology. Class of Territory

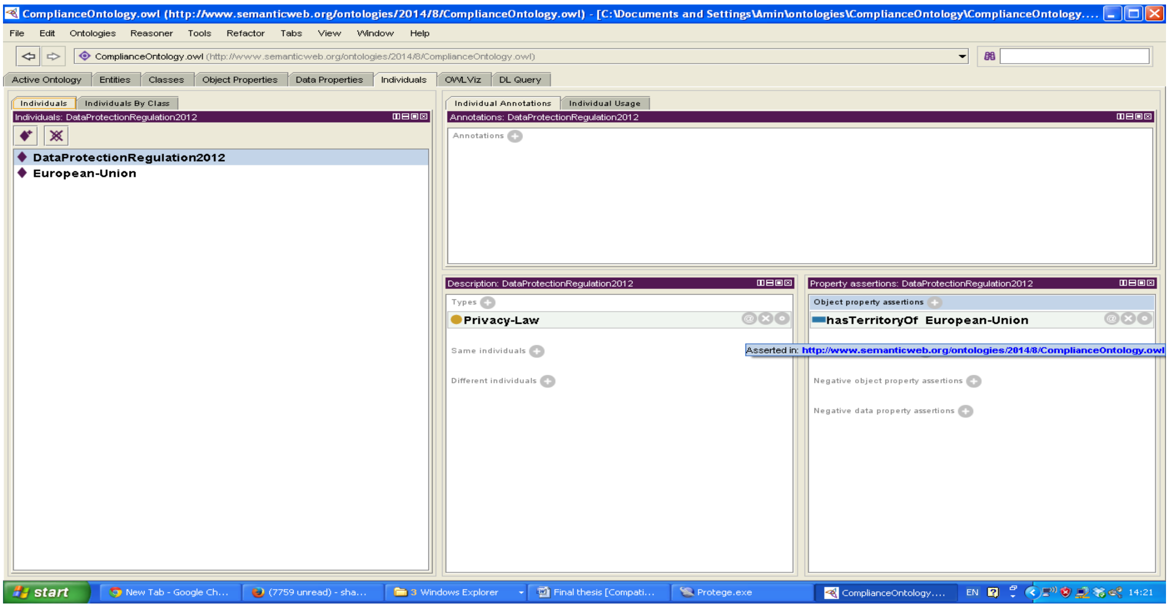
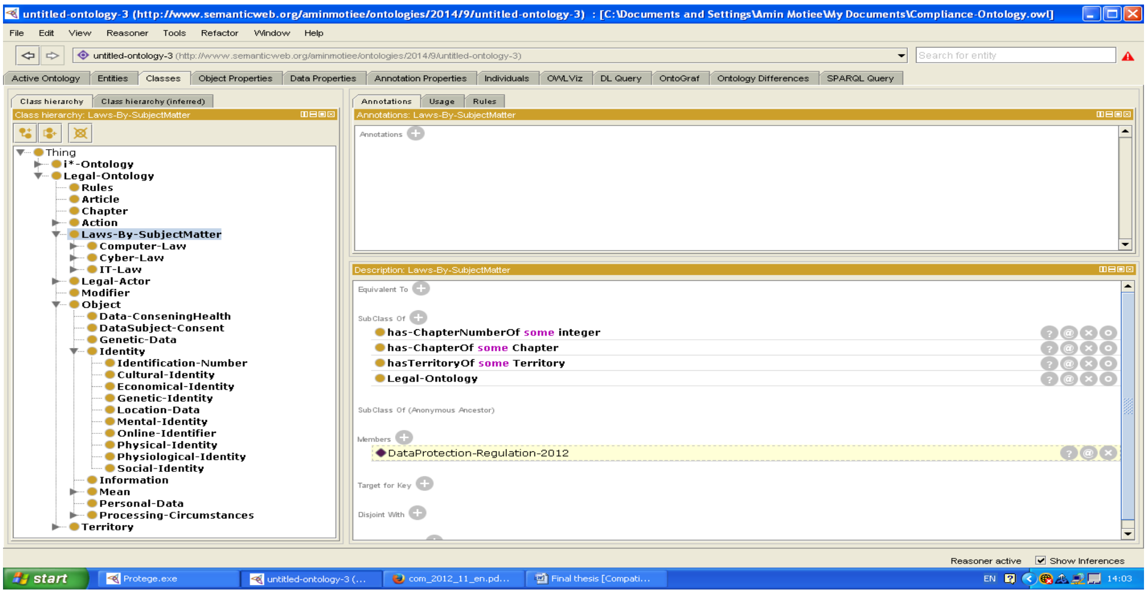

ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl) - [C:\Documents and Settings\Amin\ontologies\ComplianceOntology\ComplianceOntology....
File Edit Ontologies Reasoner Tools Refactor Tabs View Window Help
ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query
Individuals Individuals By Class
Individuals: DataProtectionRegulation2012
DataProtectionRegulation2012
European-Union
Individual Annotations Individual Usage
Annotations: DataProtectionRegulation2012
Annotations
Description: DataProtectionRegulation2012
Types
Privacy-Law
Same individuals
Different individuals
Property assertions: DataProtectionRegulation2012
Object property assertions
hasTerritoryOf European-Union
Asserted in: http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl
Negative object property assertions
Negative data property assertions
start
New Tab - Google Ch...
(7759 unread) - sha...
3 Windows Explorer
Final thesis [Compati...
Protege.exe
ComplianceOntology....
EN
14:21

Figure10 . Law Ontology. Example of Territory Relation

3. *Chapter:* This is a class in Legal Ontology which represents the same concept in law. Based on this relationship, we have two properties in ontology as *has-ChapterNumberOf* and *has-ChapterOf* connecting two classes of *Laws-BySubjectMatter* and *Chapter* as below image. As an instance we can give individual to this relation as following:

DataProtection-Regulation-2012 has-ChapterNumberOf 11

DataProtection-Regulation-2012 has-ChapterOf Controller and Processor



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]

untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)

Class hierarchy: Laws-By-SubjectMatter

```
Thing
  i*-Ontology
  Legal-Ontology
    Rules
    Article
    Chapter
    Action
    Laws-By-SubjectMatter
      Computer-Law
      Cyber-Law
      IT-Law
    Legal-Actor
    Modifier
    Object
      Data-ConseningHealth
      DataSubject-Consent
      Genetic-Data
      Identity
        Identification-Number
        Cultural-Identity
        Economical-Identity
        Genetic-Identity
        Location-Data
        Mental-Identity
        Online-Identifier
        Physical-Identity
        Physiological-Identity
        Social-Identity
      Information
      Mean
      Personal-Data
      Processing-Circumstances
    Territory
```

Annotations: Laws-By-SubjectMatter

Description: Laws-By-SubjectMatter

Equivalent To

SubClass Of
- has-ChapterNumberOf some integer
- has-ChapterOf some Chapter
- hasTerritoryOf some Territory
- Legal-Ontology

SubClass Of (Anonymous Ancestor)

Members
- DataProtection-Regulation-2012

Target for Key

Disjoint With

Reasoner active ☑ Show Inferences

Figure11 . Law Ontology. Laws-By-SubjectMatter Property

4. *Article: A* chapter of law itself consists of number of articles each focusing on a limited area of chapter subject. In same way we have properties of *has-ArticleNumberOf* and *has-ArticleOf* connecting two classes of *Chapter* and *Article*.

ChapterIV. CONTROLLER AND PROCESSOR has-ArticleNumberOf 8

ChapterIV.CONTROLLER AND PROCESSOR has-ArticleOf Responsibilit-of-Controller

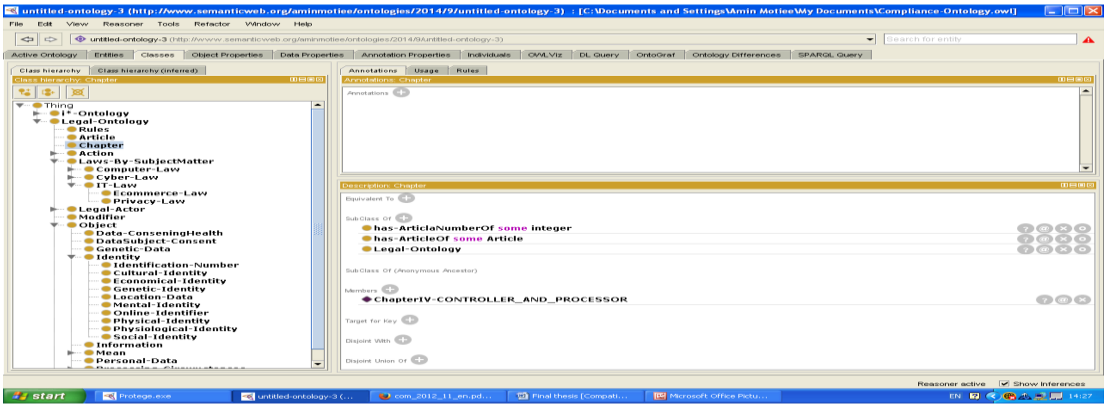


Figure12 . Law Ontology. Class of Chapter

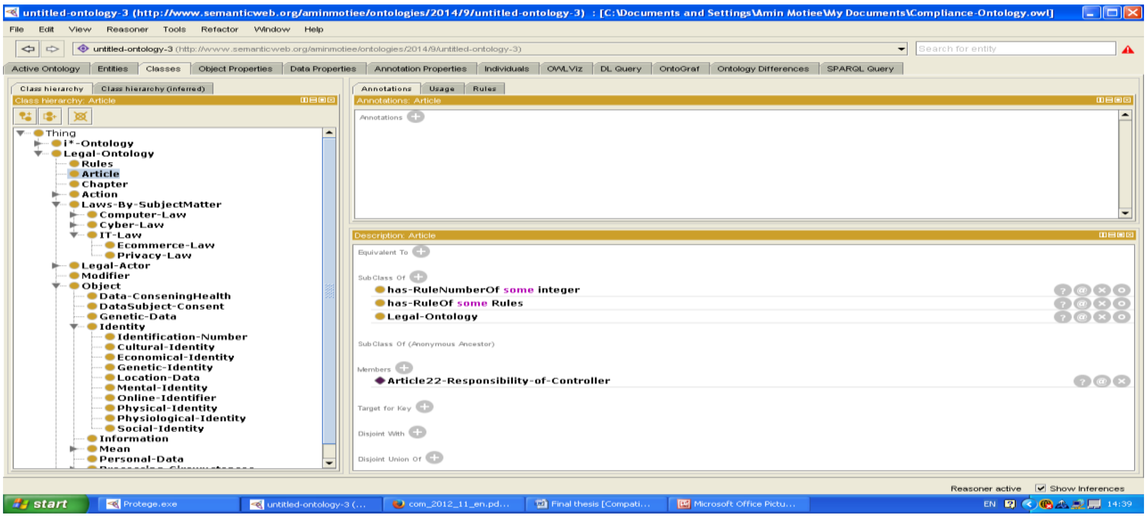


Figure13 . Law Ontology. Class of Article

5. *Rule:* the last structured organization of a law is the rule consisting of a statement where stakeholders are instructed or recommended on a right. Data property of *has-RuleNumberOf* indicates the number of rules that an article consists of. The rule itself consists of number of other components which are being discussed in following paragraphs as other classes of legal ontology.

6. *Law-Actor:* One of the main and fundamental concepts in legal ontology is the stakeholders of law. These are actually the people involved in law, the one who are obligated, permitted or prohibited on an action. In our ontology they are represented as *Law-Actor*s. When a rule of law grammatically is analysed Law-Actor is almost the subject of law who is instructed or recommended to do or not to do an action. But a Law-Actor is not always the subject of law and it can be the one the law is applied to. Figure 14 represents the list of subclasses of Law-Actor where the analysed and applying law is DataProtectionRegulation2012.

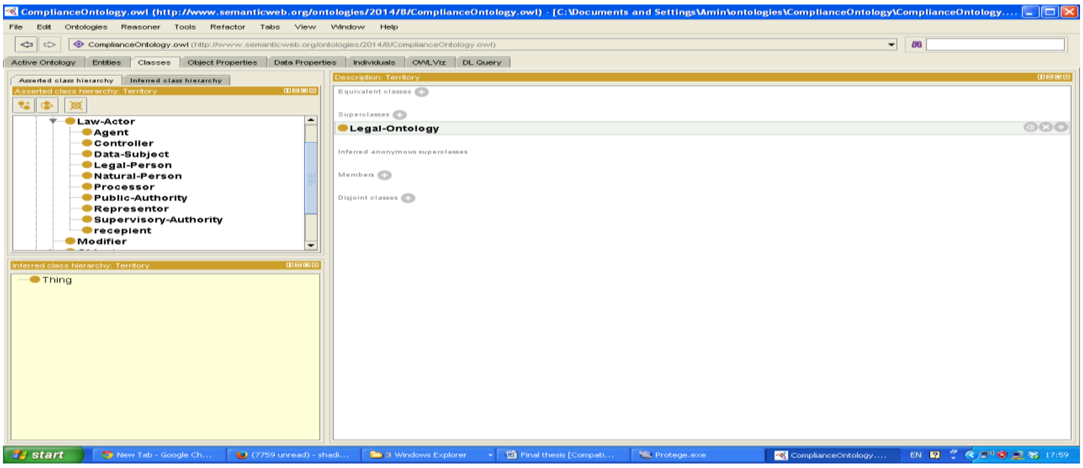

ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl) - [C:\Documents and Settings\Amin\ontologies\ComplianceOntology\ComplianceOntology....
File Edit Ontologies Reasoner Tools Refactor Tabs View Window Help
ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query
Asserted class hierarchy Inferred class hierarchy
Asserted class hierarchy: Territory
Law-Actor
Agent
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Representor
Supervisory-Authority
recepient
Modifier
Inferred class hierarchy: Territory
Thing
Description: Territory
Equivalent classes
Superclasses
Legal-Ontology
Inferred anonymous superclasses
Members
Disjoint classes
start

Figure14 . Law Ontology. Class of Law-Actor

7. *Action:* The next class to be discussed is *Action.* This represents the verbs which Law-Actors are obligated, permitted or prohibited to perform, but not limited to them. Not all of the verbs elicited from law rules have been considered here as action, but only the ones which are necessary for the mapping between i* ontology and current ontology for the purpose of law application. The rest of verbs are considered as object-properties.

8. *Object:* there are things or to be said terms discussed in rules of laws in which actions of rules are performed on them. When the rule is grammatically analysed they are almost the grammatical object of verbs, but the class of object in our ontology does not necessarily limit to this definition. It covers any touchable or non-touchable object discussed in the rules, and is almost nouns such as personal data, consent, personal data breach, time, agreement, statement and others.

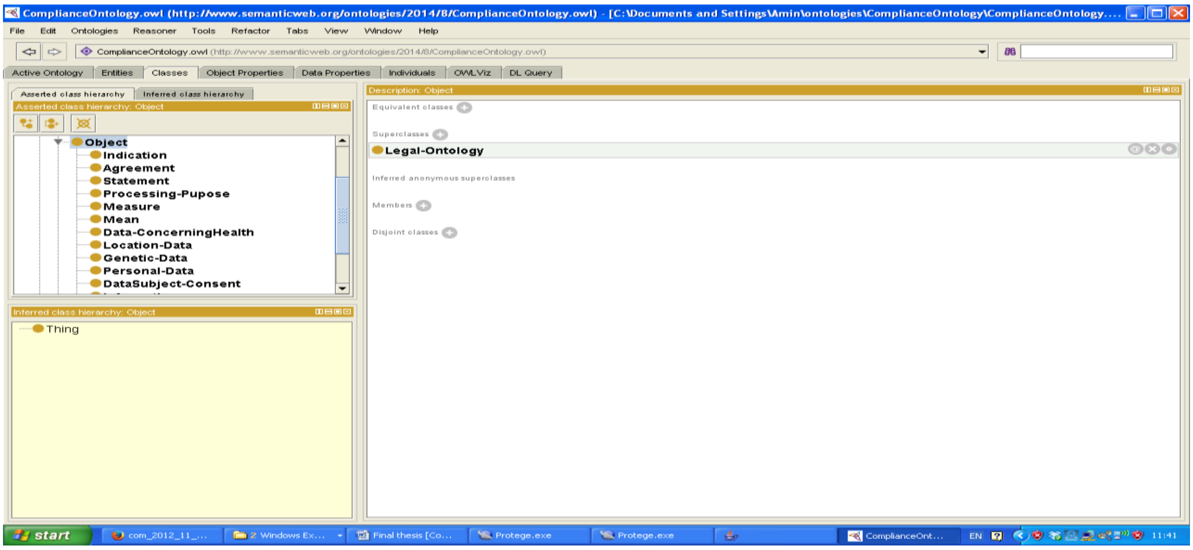

ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl) - [C:\Documents and Settings\Amin\ontologies\ComplianceOntology\ComplianceOntology....
File Edit Ontologies Reasoner Tools Refactor Tabs View Window Help
ComplianceOntology.owl (http://www.semanticweb.org/ontologies/2014/8/ComplianceOntology.owl)
Active Ontology Entities Classes Object Properties Data Properties Individuals OWLViz DL Query
Asserted class hierarchy Inferred class hierarchy
Asserted class hierarchy: Object
Object
Indication
Agreement
Statement
Processing-Pupose
Measure
Mean
Data-ConcerningHealth
Location-Data
Genetic-Data
Personal-Data
DataSubject-Consent
Inferred class hierarchy: Object
Thing
Description: Object
Equivalent classes
Superclasses
Legal-Ontology
Inferred anonymous superclasses
Members
Disjoint classes
start

Figure15 . Law Ontology. Class of Object

○ Definitions

One of the main parts of each law is an article in law which gives definition to the key terms of the law. These terms almost include the main legal actors, their actions and some critical objects of law as being defined in our ontology. Since these are the most critical concept of each law, they can be used in the process of application of law. Considering the importance of the subject of definitions in law and its application in our framework, this is essential to implement this process in our ontology. This is done by using one of the infrastructures available in Protégé called as *Rule.*

In following paragraphs, some definition of Data Protection Regulation 2012 is being represent here with the process of their conversion to the structure of rules in ontology.

9. 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction

Operation performed-ByProcessingMeanOf some Processing-Mean,

Operation performed-onPersonalDataOf some Personal-Data

➔ *Process (Operation)*

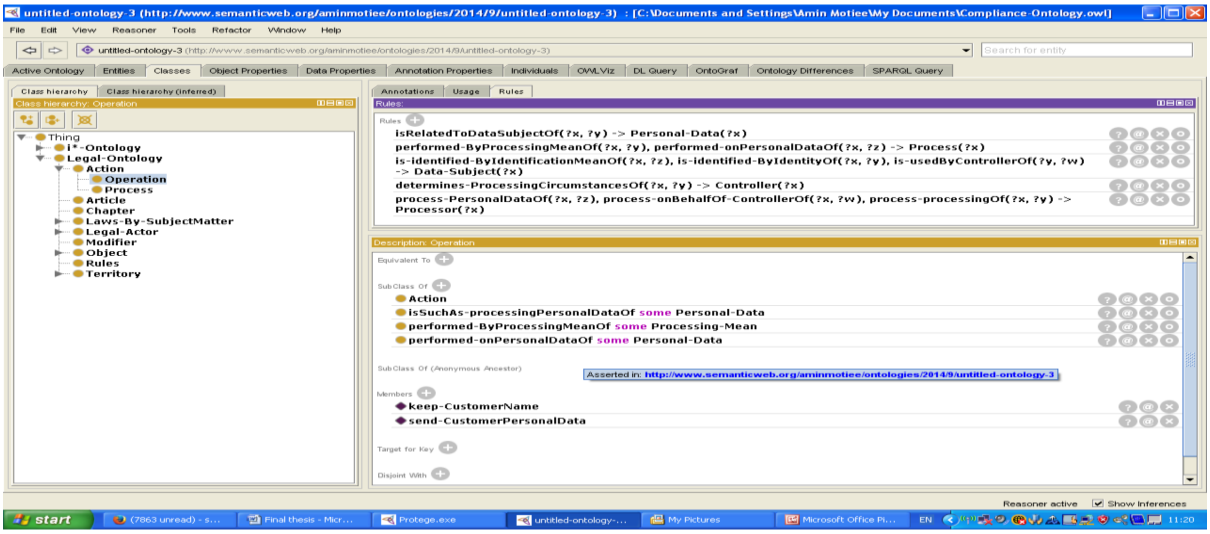
What this rule is indicating is if an operation is performed by a mean and it is performed on some personal data, the operation is a process. The following rule is others extracted from mentioned facts considering the examples of process such as collect. Same rules can be defined using other examples of process such as record:

Operation performed-ByProcessingMeanOf some Processing-Mean,

Operation performed-onPersonalDataOf some Personal-Data,

Operation is-SuchAs-collectingPersonalDataOf some Personal-Data

-> *Process (Operation)*



Rules:

```
isRelatedToDataSubjectOf(?x, ?y) -> Personal-Data(?x)
performed-ByProcessingMeanOf(?x, ?y), performed-onPersonalDataOf(?x, ?z) -> Process(?x)
is-identified-ByIdentificationMeanOf(?x, ?z), is-identified-ByIdentityOf(?x, ?y), is-usedByControllerOf(?y, ?w)
-> Data-Subject(?x)
determines-ProcessingCircumstancesOf(?x, ?y) -> Controller(?x)
process-PersonalDataOf(?x, ?z), process-onBehalfOf-ControllerOf(?x, ?w), process-processingOf(?x, ?y) ->
Processor(?x)
```

Description: Operation

Equivalent To

SubClass Of

```
Action
isSuchAs-processingPersonalDataOf some Personal-Data
performed-ByProcessingMeanOf some Processing-Mean
performed-onPersonalDataOf some Personal-Data
```

SubClass Of (Anonymous Ancestor)

Asserted in: http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3

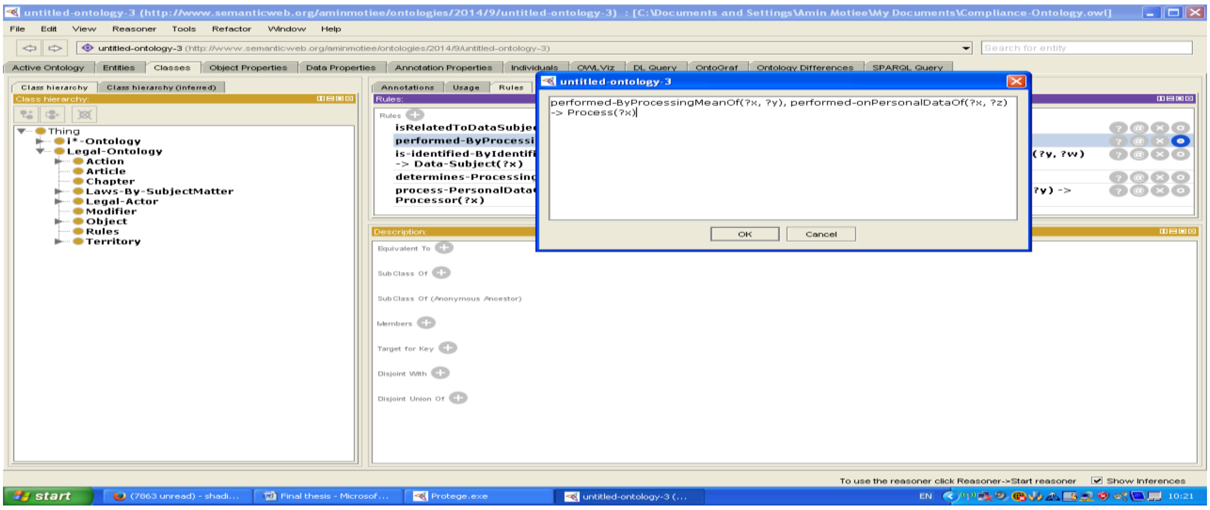
Members

```
keep-CustomerName
send-CustomerPersonalData
```

Target for Key

Disjoint With

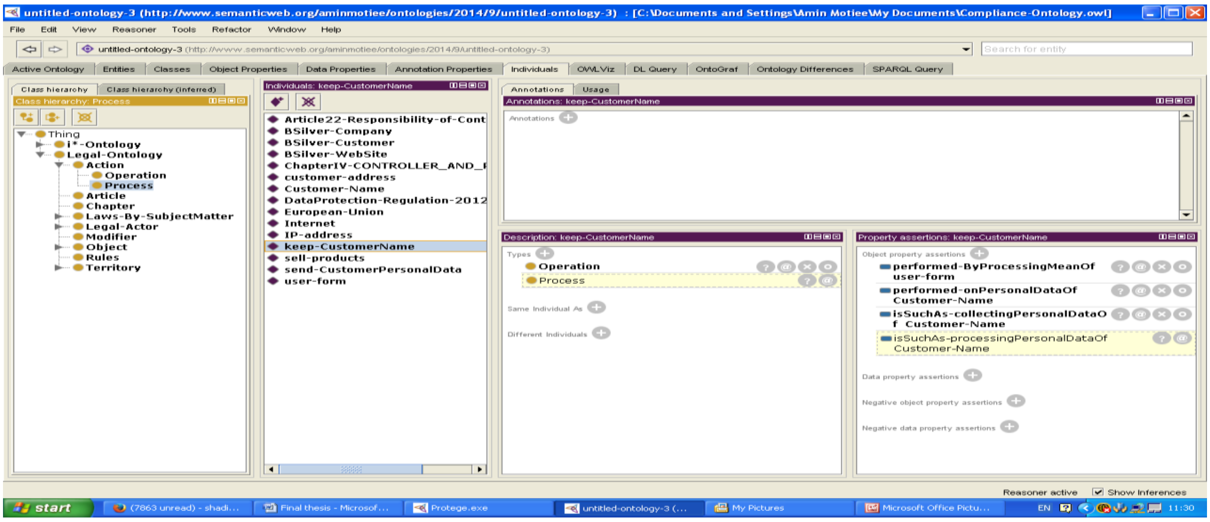
Figure16 . Law Ontology. Operation Class



```
performed-ByProcessingMeanOf(?x, ?y), performed-onPersonalDataOf(?x, ?z)
-> Process(?x)
```

Figure17 . Law Ontology. Process’ Rule

In order to check the validity of the defined rules, we give individuals to the facts of the rule and check the result as following. *Keep-CustomerName* is the individual given here as an instance of class *Operation* with defined object properties of *performed-ByProcessingMeanOf* on another individual of *Processing-Mean* as *user-form.* Running the reasoner *keep-CustomerName* will become an individual of class of *Process* too, meaning this operation is a process.



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
Active Ontology | Entities | Classes | Object Properties | Data Properties | Annotation Properties | Individuals | OWLViz | DL Query | OntoGraf | Ontology Differences | SPARQL Query
Class hierarchy | Class hierarchy (inferred)
Annotations | Usage
Reasoner active
☑ Show Inferences
start
EN 11:30

Class hierarchy: Process

- Thing
  - i*-Ontology
  - Legal-Ontology
    - Action
      - Operation
      - Process
    - Article
    - Chapter
    - Laws-By-SubjectMatter
    - Legal-Actor
    - Modifier
    - Object
    - Rules
    - Territory

Individuals: keep-CustomerName

- Article22-Responsibility-of-Cont
- BSilver-Company
- BSilver-Customer
- BSilver-WebSite
- ChapterIV-CONTROLLER_AND_I
- customer-address
- Customer-Name
- DataProtection-Regulation-2012
- European-Union
- Internet
- IP-address
- keep-CustomerName
- sell-products
- send-CustomerPersonalData
- user-form

Annotations: keep-CustomerName

Annotations

Description: keep-CustomerName

Types
- Operation
- Process

Same Individual As

Different Individuals

Property assertions: keep-CustomerName

Object property assertions
- performed-ByProcessingMeanOf user-form
- performed-onPersonalDataOf Customer-Name
- isSuchAs-collectingPersonalDataOf Customer-Name
- isSuchAs-processingPersonalDataOf Customer-Name

Data property assertions

Negative object property assertions

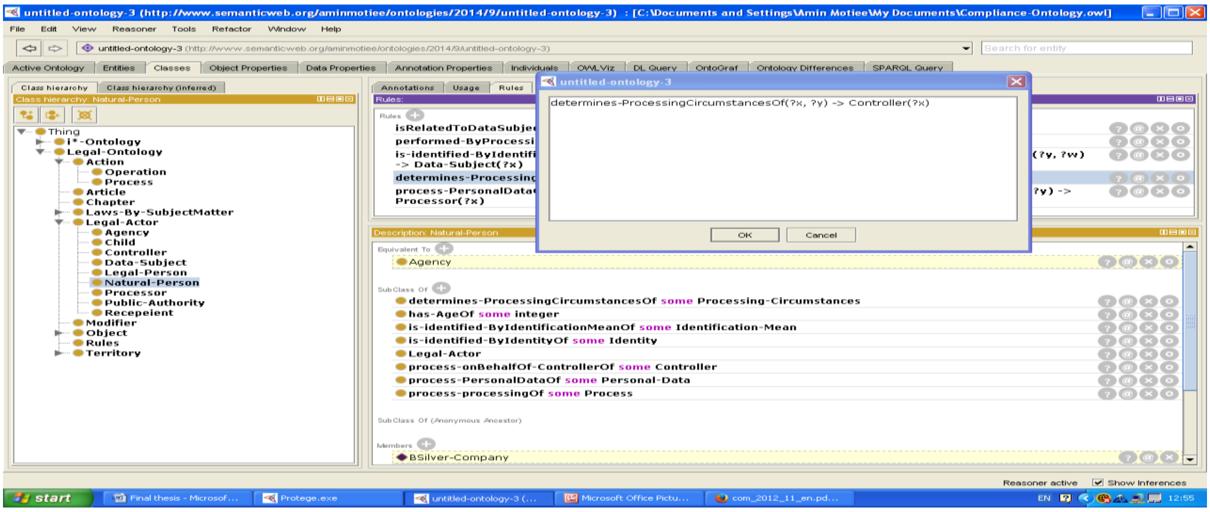
Negative data property assertions

Figure18 . Legal Ontology. Individual of Process

we are trying another definition of DataProtection-Regulation-2012 in order to clarify the discussing matter.

10. 'controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data;

In order to brief the rule, we have defined an object property of *determines-ProcessingCircumstancesOf* on two classes of *Natural-Person* and *Processing-Circumstances*. The object property of *determines-ProcessingCircumstancesOf* itself is categorized to sub-properties of *determines-ProcessingPurposeOf* and *determines-ProcessingConditionOf and determines-ProcessingMeanOf.* Same is true regarding the property *Processing-Circumstances.* In order for Reult5 to be concluded we have made ontological rules for Rules62 to Rule68. Following image represents one of the rules made in protégé:


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Annotation Properties
Individuals
OWLViz
DL Query
OntoGraf
Ontology Differences
SPARQL Query
Class hierarchy
Class hierarchy (inferred)
Class hierarchy: Natural-Person
Annotations
Usage
Rules
Rules:
Description: Natural-Person
untitled-ontology-3
OK
Cancel
Reasoner active
Show Inferences
start
Final thesis - Microsof...
Protege.exe
untitled-ontology-3 (...
Microsoft Office Pictu...
com_2012_11_en.pd...
EN
12:55

- Thing
  - i*-Ontology
  - Legal-Ontology
    - Action
      - Operation
      - Process
    - Article
    - Chapter
    - Laws-By-SubjectMatter
    - Legal-Actor
      - Agency
      - Child
      - Controller
      - Data-Subject
      - Legal-Person
      - Natural-Person
      - Processor
      - Public-Authority
      - Recepeient
    - Modifier
    - Object
    - Rules
    - Territory

Rules
isRelatedToDataSubje
performed-ByProcessi
is-identified-ByIdentifi ... (?y, ?w)
-> Data-Subject(?x)
determines-Processing
process-PersonalData ... ?y) ->
Processor(?x)

```
determines-ProcessingCircumstancesOf(?x, ?y) -> Controller(?x)
```

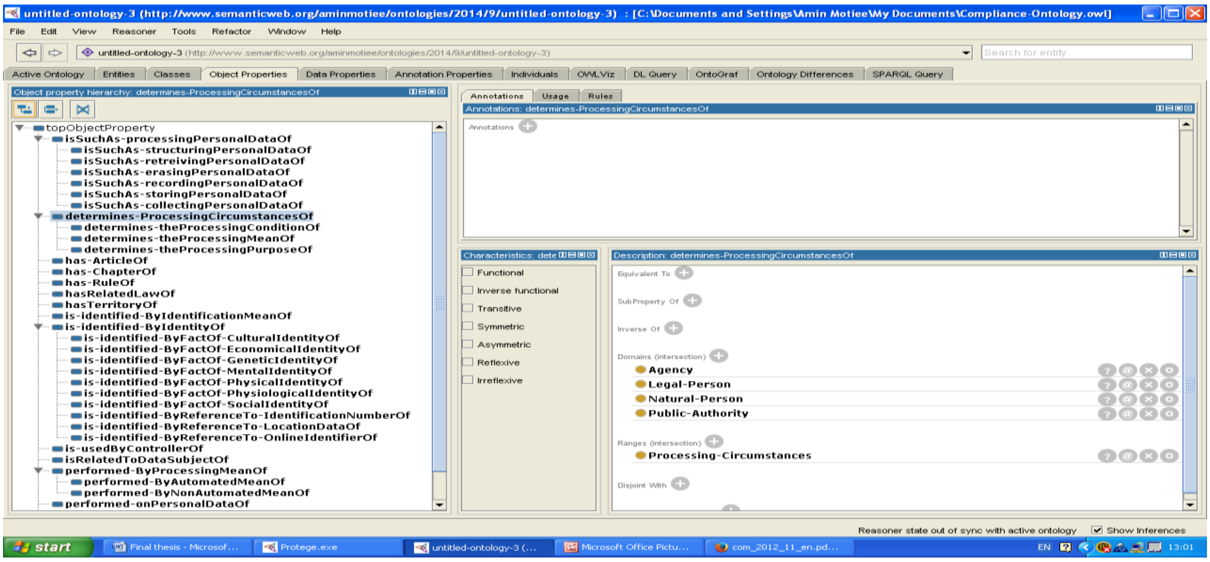
Equivalent To
- Agency

SubClass Of
- determines-ProcessingCircumstancesOf some Processing-Circumstances
- has-AgeOf some integer
- is-identified-ByIdentificationMeanOf some Identification-Mean
- is-identified-ByIdentityOf some Identity
- Legal-Actor
- process-onBehalfOf-ControllerOf some Controller
- process-PersonalDataOf some Personal-Data
- process-processingOf some Process

SubClass Of (Anonymous Ancestor)

Members
- BSilver-Company

Figure19 . Law Ontology. Controller’s Rule


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Annotation Properties
Individuals
OWLViz
DL Query
OntoGraf
Ontology Differences
SPARQL Query
Object property hierarchy: determines-ProcessingCircumstancesOf
Annotations
Usage
Rules
Annotations: determines-ProcessingCircumstancesOf
Characteristics: dete
Description: determines-ProcessingCircumstancesOf
Reasoner state out of sync with active ontology
Show Inferences
start
Final thesis - Microsof...
Protege.exe
untitled-ontology-3 (...
Microsoft Office Pictu...
com_2012_11_en.pd...
EN
13:01

- topObjectProperty
  - isSuchAs-processingPersonalDataOf
    - isSuchAs-structuringPersonalDataOf
    - isSuchAs-retreivingPersonalDataOf
    - isSuchAs-erasingPersonalDataOf
    - isSuchAs-recordingPersonalDataOf
    - isSuchAs-storingPersonalDataOf
    - isSuchAs-collectingPersonalDataOf
  - determines-ProcessingCircumstancesOf
    - determines-theProcessingConditionOf
    - determines-theProcessingMeanOf
    - determines-theProcessingPurposeOf
  - has-ArticleOf
  - has-ChapterOf
  - has-RuleOf
  - hasRelatedLawOf
  - hasTerritoryOf
  - is-identified-ByIdentificationMeanOf
  - is-identified-ByIdentityOf
    - is-identified-ByFactOf-CulturalIdentityOf
    - is-identified-ByFactOf-EconomicalIdentityOf
    - is-identified-ByFactOf-GeneticIdentityOf
    - is-identified-ByFactOf-MentalIdentityOf
    - is-identified-ByFactOf-PhysicalIdentityOf
    - is-identified-ByFactOf-PhysiologicalIdentityOf
    - is-identified-ByFactOf-SocialIdentityOf
    - is-identified-ByReferenceTo-IdentificationNumberOf
    - is-identified-ByReferenceTo-LocationDataOf
    - is-identified-ByReferenceTo-OnlineIdentifierOf
  - is-usedByControllerOf
  - isRelatedToDataSubjectOf
  - performed-ByProcessingMeanOf
    - performed-ByAutomatedMeanOf
    - performed-ByNonAutomatedMeanOf
  - performed-onPersonalDataOf

Annotations

□ Functional
□ Inverse functional
□ Transitive
□ Symmetric
□ Asymmetric
□ Reflexive
□ Irreflexive

Equivalent To

SubProperty Of

Inverse Of

Domains (intersection)
- Agency
- Legal-Person
- Natural-Person
- Public-Authority

Ranges (intersection)
- Processing-Circumstances

Disjoint With

Figure20 . Law Ontology. Subclasses of Object Property determines-ProcessingCircumstancesOf

As being seen in following image, having *ESilver-Company* as an individual of *Agent* and giving the object property of *determines-ProcessingCircumstanceof* on other individual of *sell-product* as an individual of *Processing-Purpose*, and running the reasoner of Pellet, we have E*Silver-Company* as an individual of *Controller* too.

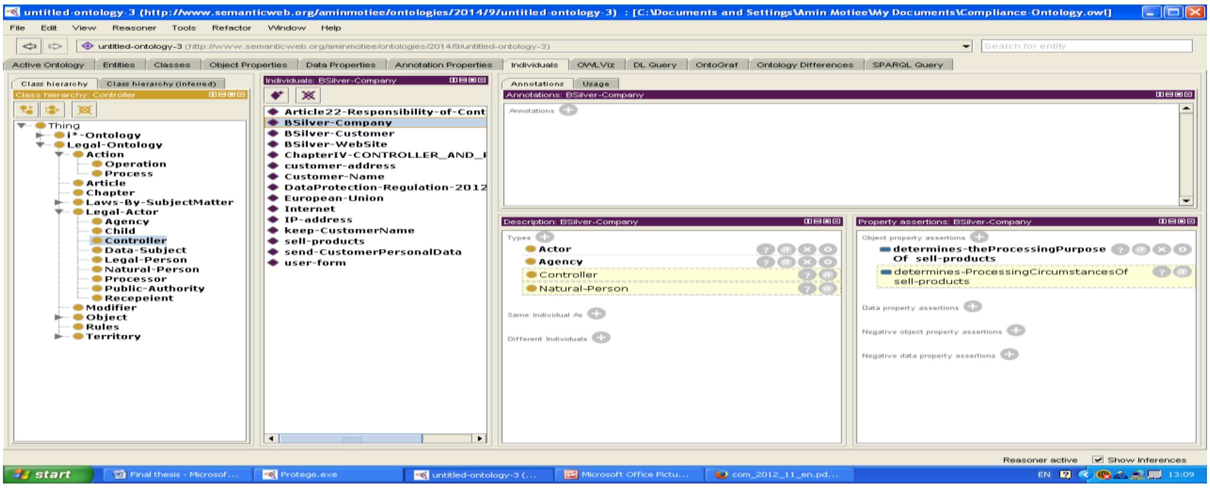

untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf Ontology Differences SPARQL Query
Class hierarchy Class hierarchy (inferred)
Class hierarchy: Controller
Thing
i*-Ontology
Legal-Ontology
Action
Operation
Process
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory
Individuals: BSilver-Company
Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_P
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form
Annotations Usage
Annotations: BSilver-Company
Annotations
Description: BSilver-Company
Types
Actor
Agency
Controller
Natural-Person
Same Individual As
Different Individuals
Property assertions: BSilver-Company
Object property assertions
determines-theProcessingPurpose Of sell-products
determines-ProcessingCircumstancesOf sell-products
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner active
Show Inferences
start
Final thesis - Microsof...
Protege.exe
untitled-ontology-3 (...
Microsoft Office Pictu...
com_2012_11_en.pd...
EN
13:09

Figure21 . Law Ontology. Individual for Controller

11. 'processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller

Same as previous processes regarding other definitions, we have the following rules in legal ontology to define the class of *Processor*.

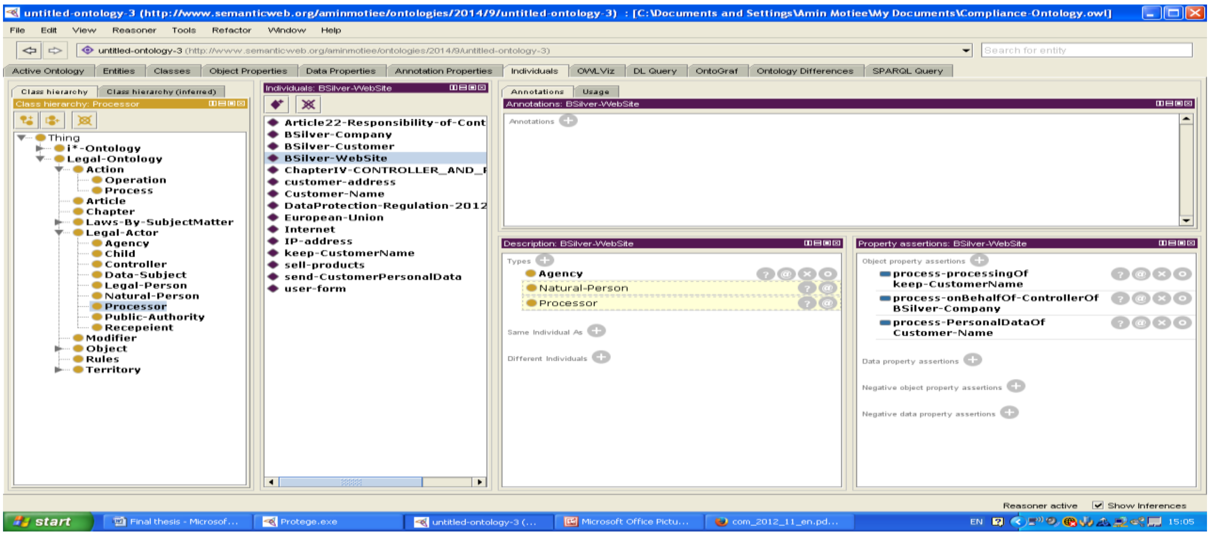
Natural-Person process-processingOf some Process,

Natural-Person process-PersonalDataOf some Personal-Data,

Natural-Person process-onBehalfOf-ControllerOf some Controller

➔ *Processor(Natural-Person)*

To give an example of processor, we consider the individual of E*Silver-website* as an *Agency* which *process-processingOf keep-CustomerName* and also *process-PersonalDataOf ESilver-CustomerName* and *process-onBehalfOf-ControllerOf ESilver-Company.* As the result we have E*Silver-website* as an individual of class of *Processor*.


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Annotation Properties
Individuals
OWLViz
DL Query
OntoGraf
Ontology Differences
SPARQL Query
Class hierarchy
Class hierarchy (inferred)
Annotations
Usage
Reasoner active
☑ Show Inferences
start
Final thesis - Microsof...
Protege.exe
untitled-ontology-3 (...
Microsoft Office Pictu...
com_2012_11_en.pd...
EN
15:05

Class hierarchy: Processor

Thing
i*-Ontology
Legal-Ontology
Action
Operation
Process
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory

Individuals: BSilver-WebSite

Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_F
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form

Annotations: BSilver-WebSite

Annotations

Description: BSilver-WebSite

Types
Agency
Natural-Person
Processor

Same Individual As

Different Individuals

Property assertions: BSilver-WebSite

Object property assertions
process-processingOf keep-CustomerName
process-onBehalfOf-ControllerOf BSilver-Company
process-PersonalDataOf Customer-Name

Data property assertions

Negative object property assertions

Negative data property assertions

Figure22 . Law Ontology. Individual for Processor

12. 'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

Such as explained in other definitions, by using of a super object property of *is-identified-ByIdentityOf* and sub class of it as *is-identified-ByReferenceTo-IdentificationNumber* or *is-identified-ByFactOf-SocialIdentityOf* and others, we were able to make following rule in protégé. The consideration is we were able to abstract above rule in following format. In fact, Fact3 and Fact4 were eliminated in this rule, regarding equality in result if these acts are used or not and for the purpose of user-friendly and ease of usage:

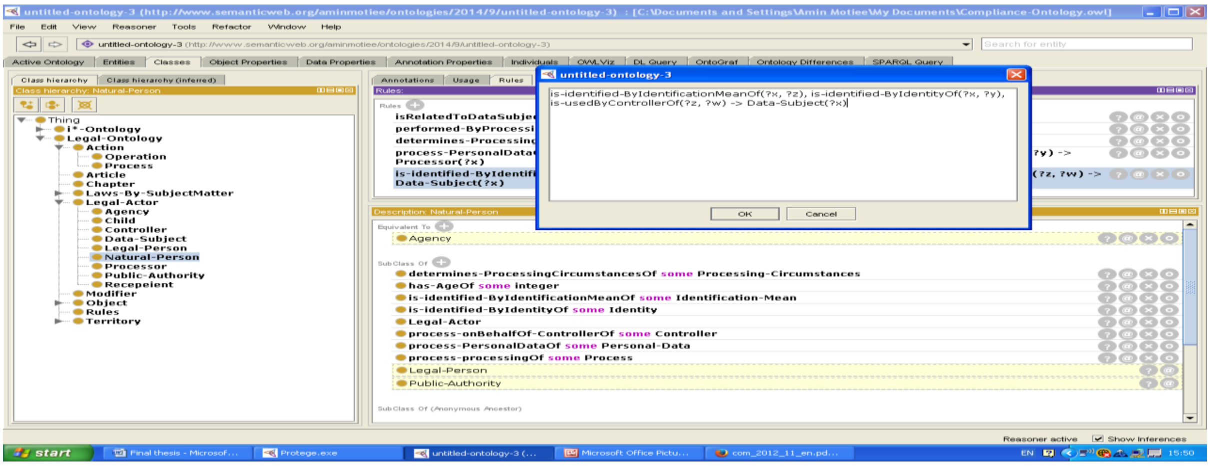
Natural-Person is-identified-ByIdentificationMeanOf some Identification-Mean,

Identification-Mean is-usedBy-ControllerOf some Controller,

Natural-Person is-Identified-ByIdentityOf some Identity

➔ *Data-Subject(Natural-Person)*

.


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf Ontology Differences SPARQL Query
Class hierarchy Class hierarchy (inferred)
Class hierarchy: Natural-Person
Thing
i*-Ontology
Legal-Ontology
Action
Operation
Process
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory
Annotations Usage Rules
Rules:
isRelatedToDataSubje
performed-ByProcessi
determines-Processinc
process-PersonalDatat
Processor(?x)
is-identified-ByIdentifi
Data-Subject(?x)
?y) ->
(?z, ?w) ->
untitled-ontology-3
OK Cancel
Description: Natural-Person
Reasoner active
Show Inferences
start
Final thesis - Microsof...
Protege.exe
untitled-ontology-3 (...
Microsoft Office Pictu...
com_2012_11_en.pd...
EN
15:50

is-identified-ByIdentificationMeanOf(?x, ?z), is-identified-ByIdentityOf(?x, ?y), is-usedByControllerOf(?z, ?w) -> Data-Subject(?x)

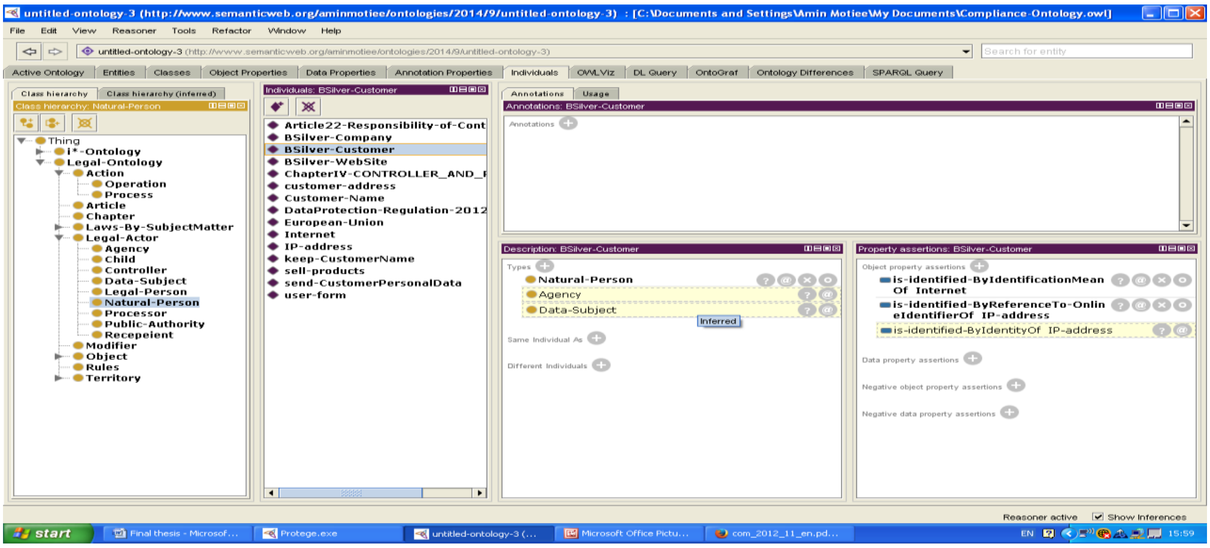
Equivalent To
Agency

SubClass Of
determines-ProcessingCircumstancesOf some Processing-Circumstances
has-AgeOf some integer
is-identified-ByIdentificationMeanOf some Identification-Mean
is-identified-ByIdentityOf some Identity
Legal-Actor
process-onBehalfOf-ControllerOf some Controller
process-PersonalDataOf some Personal-Data
process-processingOf some Process
Legal-Person
Public-Authority

SubClass Of (Anonymous Ancestor)

Figure23 . Law Ontology. Data-Subject Rule

Having individual of E*Silver-Customer* as individual of *Natural-Person* and making its relationship, we have it as a *Data-Subject*.


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf Ontology Differences SPARQL Query
Class hierarchy Class hierarchy (inferred)
Class hierarchy: Natural-Person
Thing
i*-Ontology
Legal-Ontology
Action
Operation
Process
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory
Individuals: BSilver-Customer
Annotations Usage
Annotations: BSilver-Customer
Annotations
Description: BSilver-Customer
Property assertions: BSilver-Customer
Inferred
Reasoner active
Show Inferences
start
Final thesis - Microsof...
Protege.exe
untitled-ontology-3 (...
Microsoft Office Pictu...
com_2012_11_en.pd...
EN
15:59

Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_I
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form

Types
Natural-Person
Agency
Data-Subject

Same Individual As

Different Individuals

Object property assertions
is-identified-ByIdentificationMeanOf Internet
is-identified-ByReferenceTo-OnlineIdentifierOf IP-address
is-identified-ByIdentityOf IP-address

Data property assertions

Negative object property assertions

Negative data property assertions

Figure24 . Law Ontology. Individual for Data-Subject

13. 'personal data' means any information relating to a data subject;

Information is-RelatedTo-DataSubjectOf some Data-Subject

➔ *Personal-Data(Information)*

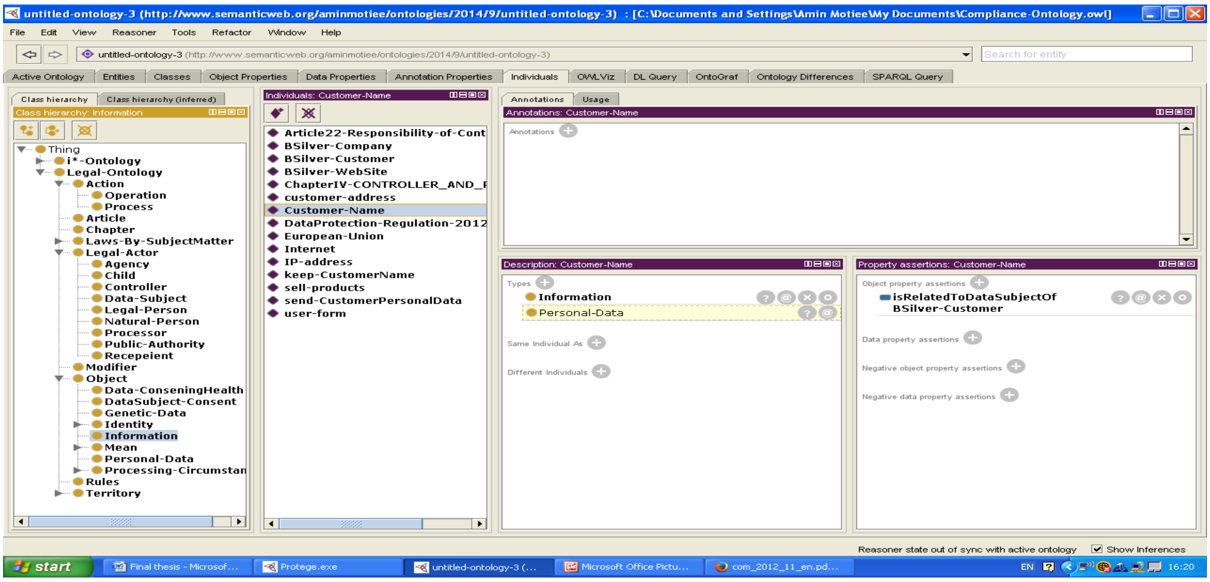

untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf Ontology Differences SPARQL Query
Class hierarchy: Information
Thing
i*-Ontology
Legal-Ontology
Action
Operation
Process
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Data-ConseningHealth
DataSubject-Consent
Genetic-Data
Identity
Information
Mean
Personal-Data
Processing-Circumstan
Rules
Territory
Individuals: Customer-Name
Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_I
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form
Annotations: Customer-Name
Description: Customer-Name
Types
Information
Personal-Data
Same Individual As
Different Individuals
Property assertions: Customer-Name
Object property assertions
isRelatedToDataSubjectOf BSilver-Customer
Data property assertions
Negative object property assertions
Negative data property assertions
Reasoner state out of sync with active ontology
Show Inferences
start
16:20

Figure25 . Law Ontology. Individual for Personal-Data

Other definition from Data Protection Regulation has been considered in our ontological model such as definitions for *Supervisory Authority*, *Child*, *Data Subject Consent*, *recipient* and others. The same process is considered for analysis of the facts and consequences of their related rules which are not mentioned in this text regarding their similarity and the limitation here.

○ Coding the Rules of Law in Legal Ontology

Rules of law are the texts which are covered under different categorisation of *Chapter* and *Article*. This may include the article regarding definition, the scope of law or the texts of law which instruct, recommend or prohibit stakeholders of some action.

Being explained before, fact or testing elements of law are the part of rule which indicates the application area of rule, to be said in detail this part specifies the conditions and scope where the obligations, permissions or prohibitions of the rule should be applied. The fact almost consists of a sentence or statement itself. Casual terms such as shall, must, may, should or shall not, indicates if the rule is instructing an obligation, permission, recommendation or prohibition. The result or Conclusion is the part which indicates what should be performed or happened if the facts are valid. And finally Exception is actually the anti-fact which specifies the condition where the rule should not be applied. The conclusion and exception of rule same as the part regarding the fact each include a statement itself which consists of other components. It was discussed before that each of mentioned facts and conclusion is constructed from number of specific elements. These elements are extracted from mentioned statements based on grammatical analysis if they are nouns or verbs. Having triple of components as *argument operator argument* and since each of these triples are statement which provides a knowledge and a fact in this field, lightened the similarity of discussed matter with knowledge representation method in ontology using triples of "*Subject objectProperty object*" as a statement. It was the basis for the idea to represent the framework with a composite ontology of framework components since the knowledge represented in other components of framework can be modelled into the ontology triple as well.

Following examples implements rules from Data Protection Regulation 2012 in our ontology model.

- *This Regulation applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.*

Therefore, having the triples constructing the statements, arguments and operators should be converted to classes and objectProperty in the legal ontology and relations between classes (arguments) using objectProperty (operators) should be build. Converting the arguments as shown above to object in ontology and the operators to objectProperty would have made some confusion for the end-user when giving individuals of the relations. For example, they may be number of different statements in law with same objectProperty as *is* or *applies* or other similar operators. The other confusion would be regarding the required process of framework to map and apply the i* ontology goals and tasks to Legal Ontology facts. For example, it is necessary to know which of i* goal or task dependencies should be mapped to the object of Process in statement of "*processor is processing personal data".* In reality and in order to map system context to Law & Regulation Ontology, it was not possible to give an individual to an objectProperty. Thefore, we had to define a class which can accept an individual for some of the operators extracted from Legal text, but not for all the operators. Therefore, we defined the class Action which can be instanced by individuals. All these reasons lead us to reshape the above modelled facts in somehow different model in Legal ontology for the aim of user-friendly as following:

1stFact. Processor isProcessing-ProcessOf some Process

2ndFact. Process is-wholly-ByAutomatedMeanOf some Automated-Mean

3rdFact. Process is-Partly-ByAutomatedMeanOf some Automated-Mean

4thFact. Process is-By-NonAutomatedMeanOf some Non-AutomatedMean

5thFact. Process form-PartOf-FilingSystemOf some Filing-System

6thFact.Process intend-toForm- PartOfFilingSystemOf some Filing-System

Conclusion. Law-By-Subject applies-to-ActionOf some Action

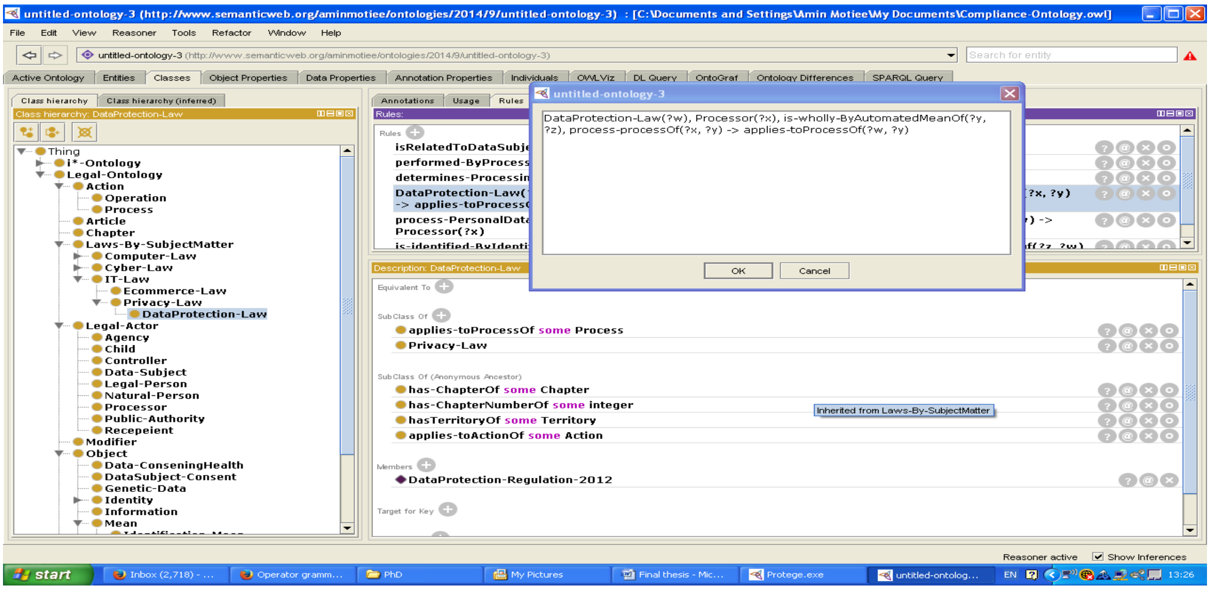
It also had been explained before that a usual functions of analysing rule of law which is performed by legal professionals and lawyers, is to rearrange the rules after their separation to their elementary components to the final rules. We are doing this process based on the AND/OR conjunction relation between the analysed elements and in a more mathematical language as following:

Since the rules above are combination of number of facts which gives a conclusion at the end and the similarity of this with the definitions of *Rule* in *Protégé*, lead us to use the infrastructure of *Rules* in Protégé in order to make the discussed rules of Data Protection Regulation 2012 or any other law.

○ Applying Ontology Rules to the Context of Developing System in i* Ontology

Having the developing system modelled by goal, task and resource dependencies in i* methodology and the analysed and rearranged rules of complying law, one of the main and strategic steps of the framework had been defined to apply and map the analysed rules to the context of developing system. This essential is being done in the ontology supporting tool by usage of the infrastructure of *individual* and the fact that an individual in ontology can have more than one *type*. Therefore, an individual which has already the type of *Goal* in i* ontology, can also have another type in Legal Ontology. In such a way the two ontologies of i* and Legal can be mapped together. Although protégé has made-in tool to map different ontology together, here it is preferred to map them together manually. The reason is first that this tool had been aimed to support and train the end-user in every step of framework rather than providing everything automatic. Second reason is that the mapping tool in ontology may make some confusion in future developing regarding the similarity of terms.

As an example, we have the goal dependency of *keep-CustomerName* in i* ontology. Having this as an individual of Process (considering the definition of Process) in Legal Ontology, and the other fact that keep-*CustomerName is-wholly-ByAutomatedMeanOf user-form*, and running the Pellet reasoner in Protégé, it will conclude that *DataProtection-Regulation-2012 applies-toProcessOf keep-CustomerName*. This is shown in figure 26.



```
DataProtection-Law(?w), Processor(?x), is-wholly-ByAutomatedMeanOf(?y,
?z), process-processOf(?x, ?y) -> applies-toProcessOf(?w, ?y)
```

Rules:

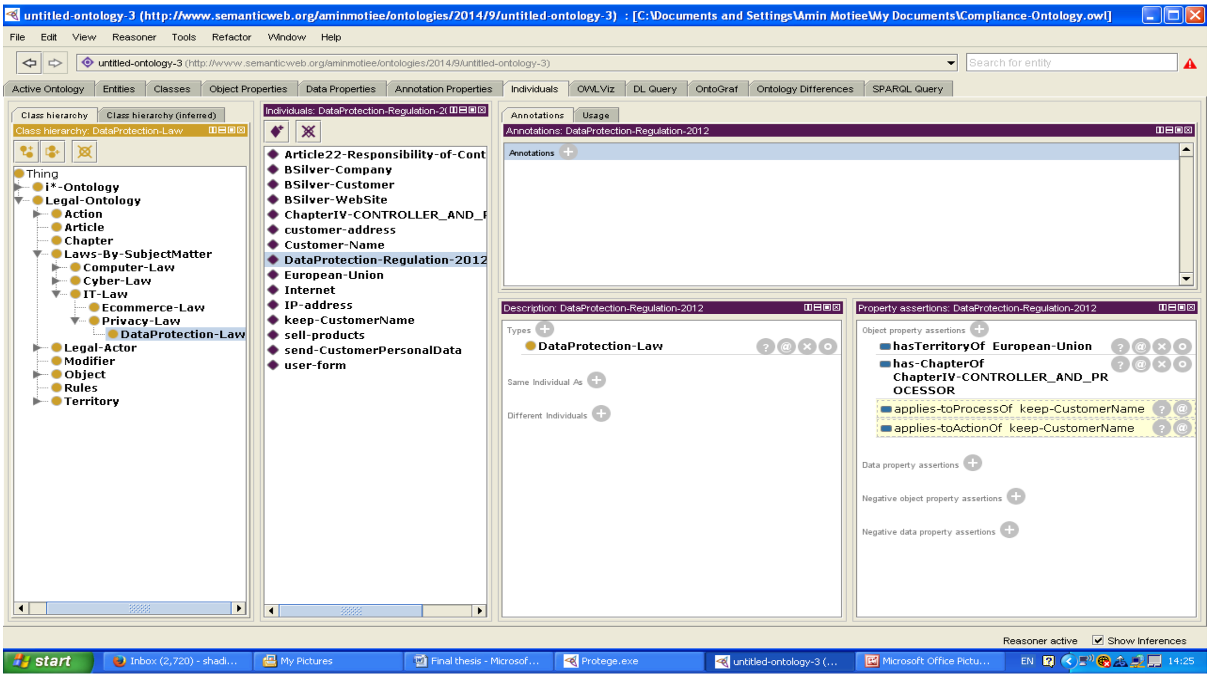
```
isRelatedToDataSubje
performed-ByProcess
determines-Processin
DataProtection-Law(                                  (?x, ?y)
-> applies-toProcess(
process-PersonalData                                 ) ->
Processor(?x)
is-identified-ByIdenti                               f(?z, ?w)
```

SubClass Of
- applies-toProcessOf some Process
- Privacy-Law

SubClass Of (Anonymous Ancestor)
- has-ChapterOf some Chapter
- has-ChapterNumberOf some integer
- hasTerritoryOf some Territory
- applies-toActionOf some Action

Members
- DataProtection-Regulation-2012

Figure26 . Legal Ontology. Data Protection-Law’s Rule



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]

Class hierarchy: DataProtection-Law

- Thing
  - i*-Ontology
  - Legal-Ontology
    - Action
    - Article
    - Chapter
    - Laws-By-SubjectMatter
      - Computer-Law
      - Cyber-Law
      - IT-Law
        - Ecommerce-Law
        - Privacy-Law
          - DataProtection-Law
    - Legal-Actor
    - Modifier
    - Object
    - Rules
    - Territory

Individuals: DataProtection-Regulation-2(

- Article22-Responsibility-of-Cont
- BSilver-Company
- BSilver-Customer
- BSilver-WebSite
- ChapterIV-CONTROLLER_AND_I
- customer-address
- Customer-Name
- DataProtection-Regulation-2012
- European-Union
- Internet
- IP-address
- keep-CustomerName
- sell-products
- send-CustomerPersonalData
- user-form

Annotations: DataProtection-Regulation-2012

Annotations

Description: DataProtection-Regulation-2012

Types
DataProtection-Law

Same Individual As

Different Individuals

Property assertions: DataProtection-Regulation-2012

Object property assertions
hasTerritoryOf European-Union
has-ChapterOf ChapterIV-CONTROLLER_AND_PROCESSOR
applies-toProcessOf keep-CustomerName
applies-toActionOf keep-CustomerName

Data property assertions

Negative object property assertions

Negative data property assertions

Figure27 . Legal Ontology. Individual for DataProtection-Regulation-2012

○ Coding Obligations, Permissions, Recommendation and Prohibitions in Legal Ontology

The main part of rules of laws is specified to number of articles and their belonging statements which order, permit, recommend or prohibit its stakeholder to perform an action. Here we illustrate the method in which these rules including the constructing elements of it (Facts, Casual term, Conclusion, Exception) are coded to the rules in Legal Ontology of our tool using some practical examples from Data Protection Regulation 2012. The facts and conclusion extracted from rules are directly copied from section5.3 regarding the analysing of laws.

Article 5

Principles relating to personal data processing

Personal data must be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject;

Therefore, we have the following ontology rule:

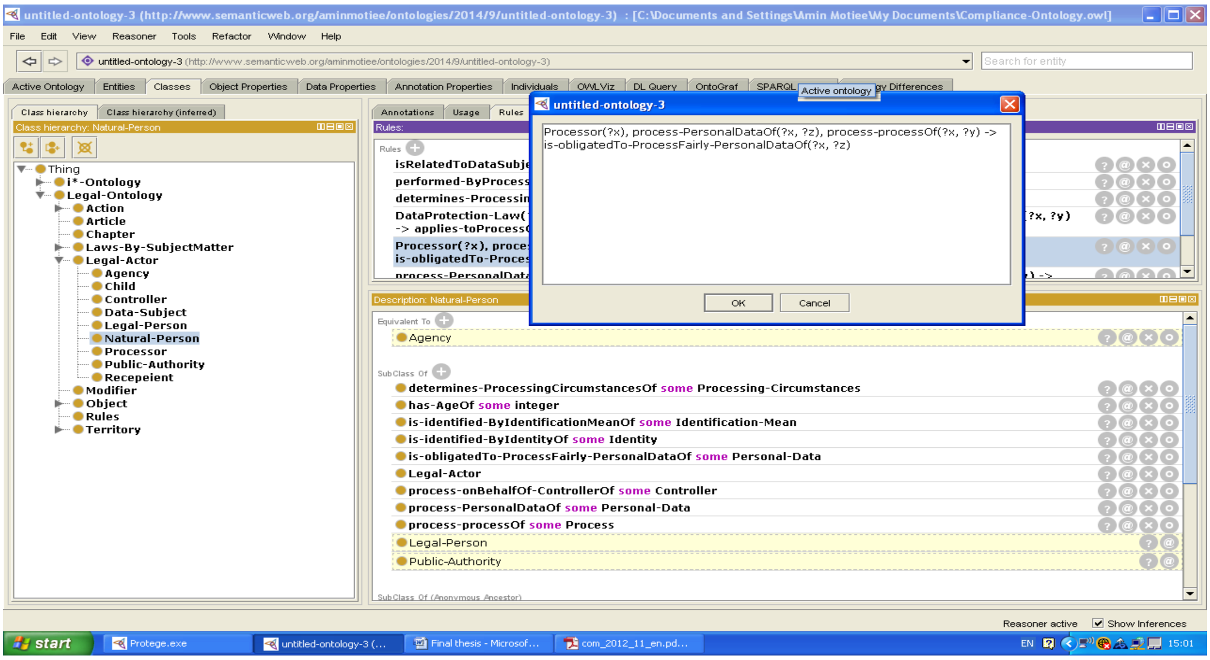
Processor process-processOf some Process,

Processor process-PersonalDataOf some Personal-Data

> *Processor is-obligatedTo-ProcessFairly-PersonalDataOf some Personal-Data*

As being seen, the rule in ontology is a bit different to in analysed laws having an extra fact which determines the processor is processing exactly which process from the context of law

(*Processor process-processOf some Process*). The reason of adding this fact to the rule in ontology is the necessity to map this rule to the context of developing system. In fact, this is determining the process in context of system where this rule be applied. We will have similar added facts to the rules being discussed in following paragraphs where similar situations apply.



Processor(?x), process-PersonalDataOf(?x, ?z), process-processOf(?x, ?y) -> is-obligatedTo-ProcessFairly-PersonalDataOf(?x, ?z)

- Thing
  - i*-Ontology
  - Legal-Ontology
    - Action
    - Article
    - Chapter
    - Laws-By-SubjectMatter
    - Legal-Actor
      - Agency
      - Child
      - Controller
      - Data-Subject
      - Legal-Person
      - Natural-Person
      - Processor
      - Public-Authority
      - Recepeient
    - Modifier
    - Object
    - Rules
    - Territory

Equivalent To

- Agency

SubClass Of

- determines-ProcessingCircumstancesOf some Processing-Circumstances
- has-AgeOf some integer
- is-identified-ByIdentificationMeanOf some Identification-Mean
- is-identified-ByIdentityOf some Identity
- is-obligatedTo-ProcessFairly-PersonalDataOf some Personal-Data
- Legal-Actor
- process-onBehalfOf-ControllerOf some Controller
- process-PersonalDataOf some Personal-Data
- process-processOf some Process
- Legal-Person
- Public-Authority

Figure28 . Law Ontology. Processor’s Rules

Article 6

Lawfulness of processing

1. Processing of personal data shall be lawful only if and to the extent that at least one

of the following applies:

(a) the data subject has given consent to the processing of their personal data for

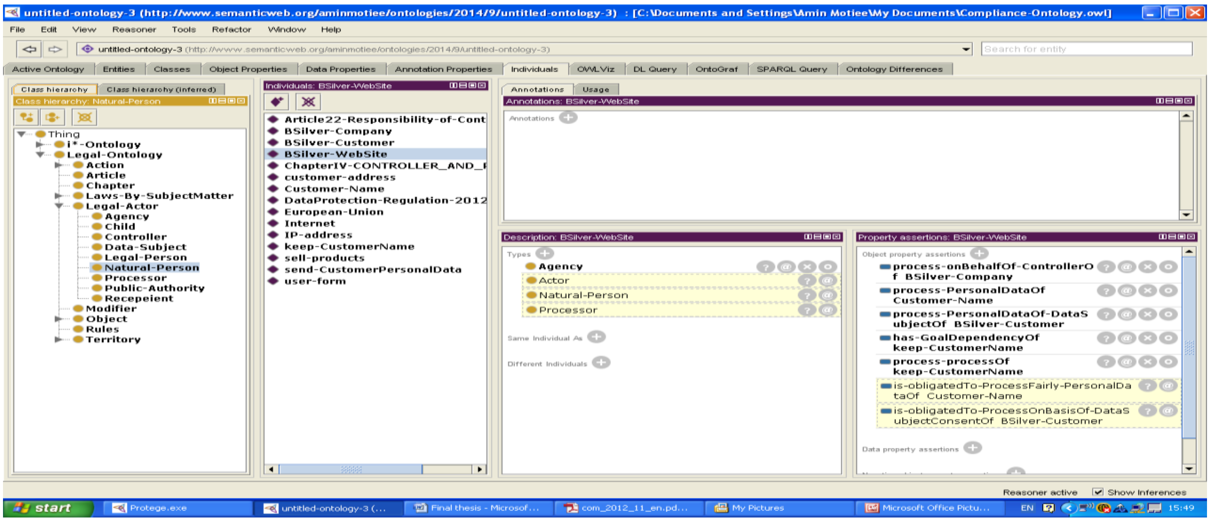
one or more specific purposes;

Processor process-processOf some Process, Processor process-PersonalDataOf some Personal-Data, Processor process-PersonalDataOf-DataSubjectOf some Data-Subject,

Processor is-obligatedTo-ProcessFairly-PersonalDataOf some Personal-Data,

➔ *Processor is-obligatedTo-ProcessOnBasisOf-DataSubjectConsentOf some Data-Subject*

The above rule is indicating the condition of this rule on previous rule of Article5 as wherever the processor is obligated to process personal data fairly, he/she is also obligated to process the personal data based on the consent from the data subject.



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]

Individuals: BSilver-WebSite

Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_I
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form

Description: BSilver-WebSite

Types
Agency
Actor
Natural-Person
Processor

Property assertions: BSilver-WebSite

Object property assertions
process-onBehalfOf-ControllerOf BSilver-Company
process-PersonalDataOf Customer-Name
process-PersonalDataOf-DataSubjectOf BSilver-Customer
has-GoalDependencyOf keep-CustomerName
process-processOf keep-CustomerName
is-obligatedTo-ProcessFairly-PersonalDataOf Customer-Name
is-obligatedTo-ProcessOnBasisOf-DataSubjectConsentOf BSilver-Customer

Data property assertions

Figure29 . Law Ontology. Processor’Rules

Article 7

Conditions for consent

1. The controller shall bear the burden of proof for the data subject's consent to the processing of their personal data for specified purposes

Corresponded rule in ontology is:

Processor process-processOf some Process,

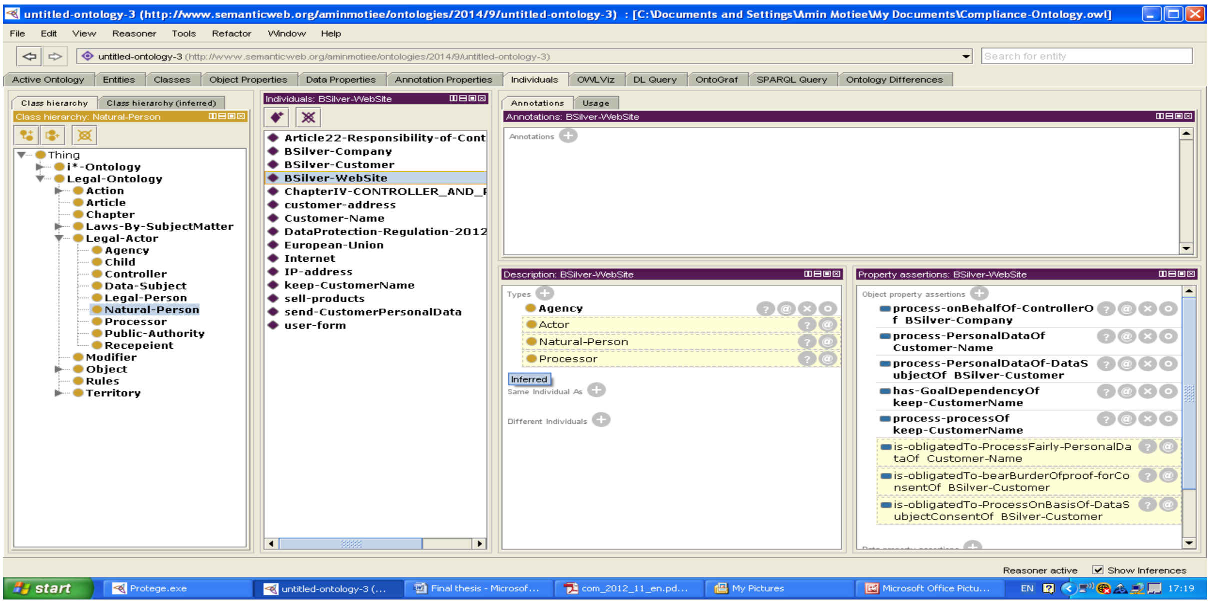
Processor process-PersonalDataOf some Personal-Data,

Process has-ProcessingPurposeOf some Processing-Purpose,

Personal-Data belong-to-DataSubjectOf some Data-Subject,

Is-obligatedTo-ProcessOnBasisOf-DataSubjectConsentOf some Data-Subject

➔ *Processor is-obligatedTo-bearTheBurdenOfProof-forConsentOf some Data-Subject*


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf SPARQL Query Ontology Differences
Class hierarchy Class hierarchy (inferred)
Class hierarchy: Natural-Person
Thing
i*-Ontology
Legal-Ontology
Action
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory
Individuals: BSilver-WebSite
Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_P
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form
Annotations Usage
Annotations: BSilver-WebSite
Annotations
Description: BSilver-WebSite
Types
Agency
Actor
Natural-Person
Processor
Inferred
Same Individual As
Different Individuals
Property assertions: BSilver-WebSite
Object property assertions
Data property assertions
Reasoner active
☑ Show Inferences
start
Protege.exe
untitled-ontology-3 (...
Final thesis - Microsof...
com_2012_11_en.pd...
My Pictures
Microsoft Office Pictu...
EN
17:19

process-onBehalfOf-ControllerOf BSilver-Company
process-PersonalDataOf Customer-Name
process-PersonalDataOf-DataSubjectOf BSilver-Customer
has-GoalDependencyOf keep-CustomerName
process-processOf keep-CustomerName
is-obligatedTo-ProcessFairly-PersonalDataOf Customer-Name
is-obligatedTo-bearBurderOfproof-forConsentOf BSilver-Customer
is-obligatedTo-ProcessOnBasisOf-DataSubjectConsentOf BSilver-Customer

Figure30 . Law Ontology. Processor’Rules

Since the title of this article indicates, this rule is a condition on consent and in fact a condition on article 6. That is the reason why we have selected the obligation in rule related to article 6 as a fact of the rule of this article, in order to apply the obligation of *bear-The BurdenOfproof* wherever the fact of the other obligation of *process-OnTheBasisOfConsent* is available.

Article 14

Information to the data subject

1. Where personal data relating to a data subject are collected, the controller shall provide the data subject with at least the following information:

(a) the identity and the contact details of the controller and, if any, of the controller's representative and of the data protection officer;

The corresponding rules in Legal ontology is:

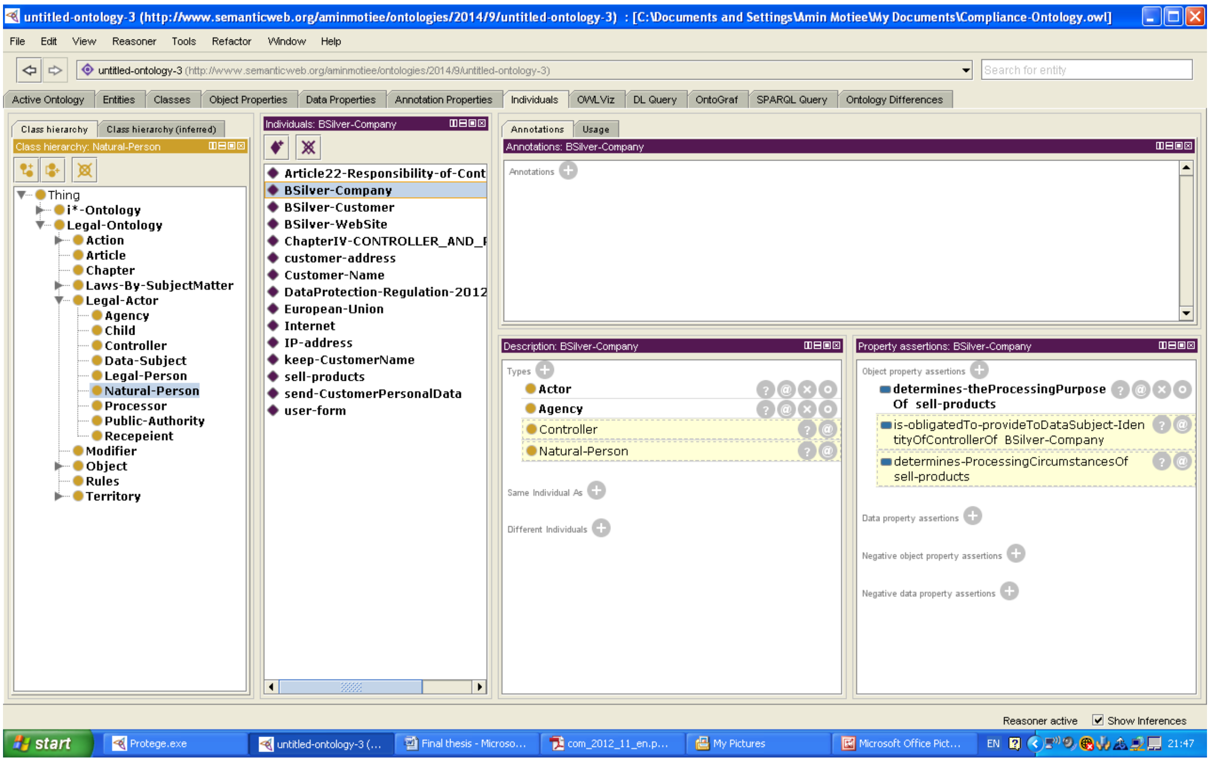
Processor process-processOf some Process,

Processor process-onBehalfOf-ControllerOf some Controller,

Process isSuchAs-collectingPersonalDataOf some Personal-Data,

Pesonal-Data isRelatedToDataSubjectOf some Data-Subject

➔ *Controller is-obligatedTo-provideToDataSubject-IdentityOfControllerOf some Controller*



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Annotation Properties
Individuals
OWLViz
DL Query
OntoGraf
SPARQL Query
Ontology Differences
Class hierarchy
Class hierarchy (inferred)
Annotations
Usage
Reasoner active
☑ Show Inferences
start
Protege.exe
untitled-ontology-3 (...
Final thesis - Microso...
com_2012_11_en.p...
My Pictures
Microsoft Office Pict...
EN
21:47

Class hierarchy: Natural-Person

- Thing
  - i*-Ontology
  - Legal-Ontology
    - Action
    - Article
    - Chapter
    - Laws-By-SubjectMatter
    - Legal-Actor
      - Agency
      - Child
      - Controller
      - Data-Subject
      - Legal-Person
      - Natural-Person
      - Processor
      - Public-Authority
      - Recepeient
    - Modifier
    - Object
    - Rules
    - Territory

Individuals: BSilver-Company

- Article22-Responsibility-of-Cont
- BSilver-Company
- BSilver-Customer
- BSilver-WebSite
- ChapterIV-CONTROLLER_AND_F
- customer-address
- Customer-Name
- DataProtection-Regulation-2012
- European-Union
- Internet
- IP-address
- keep-CustomerName
- sell-products
- send-CustomerPersonalData
- user-form

Annotations: BSilver-Company

Annotations

Description: BSilver-Company

Types
- Actor
- Agency
- Controller
- Natural-Person

Same Individual As

Different Individuals

Property assertions: BSilver-Company

Object property assertions
- determines-theProcessingPurposeOf sell-products
- is-obligatedTo-provideToDataSubject-IdentityOfControllerOf BSilver-Company
- determines-ProcessingCircumstancesOf sell-products

Data property assertions

Negative object property assertions

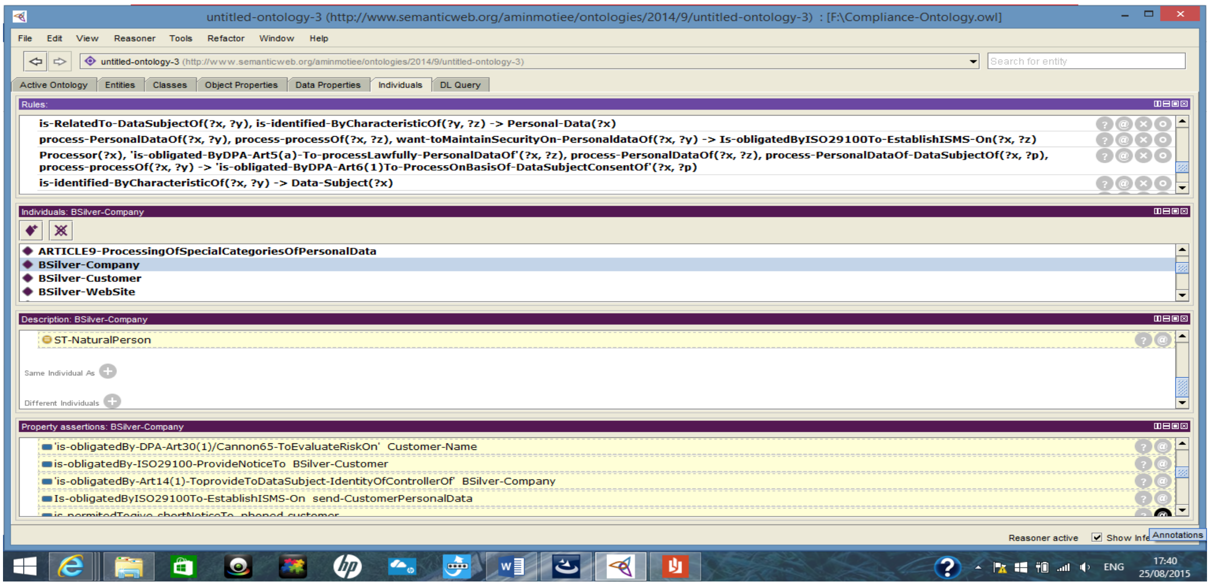
Negative data property assertions

Figure31 . Law Ontology. Controller’Rules

○ Refinement, Interpreting, Mapping and Inherit of Laws by Standard and ICO in Ontology

One of the main objective of the proposed framework in current work has been defined to refine requirements extracted from laws to more applicable requirements from authority guidelines such as standards and other resources. In case of compliance to Data Protection we used ISO 29100 and ISO 27000 series and also guidelines from ICO. In previous sections we explained how rules extracted from these resources are also mapped to similar requirements from other resources of compliance and as consequence mapped concepts inherit each other properties. In this section we implement ontological solution for the discussed materials for refinement, mapping and inheriting requirements from different ontologies. To practice the implementation of above cases, we use the same rules that has been refined and mapped in Section 5 as following:

Is-obligatedTo-EstablishISMS-On(?x,?z), Information-asset(?T)→ Is-obligated-ToIdentify (?x,?T)


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Individuals
DL Query
Reasoner active
Show Infe
Annotations
ENG
17:40
25/08/2015

Rules:

```
is-RelatedTo-DataSubjectOf(?x, ?y), is-identified-ByCharacteristicOf(?y, ?z) -> Personal-Data(?x)
process-PersonalDataOf(?x, ?y), process-processOf(?x, ?z), want-toMaintainSecurityOn-PersonaldataOf(?x, ?y) -> Is-obligatedByISO29100To-EstablishISMS-On(?x, ?z)
Processor(?x), 'is-obligated-ByDPA-Art5(a)-To-processLawfully-PersonalDataOf'(?x, ?z), process-PersonalDataOf(?x, ?z), process-PersonalDataOf-DataSubjectOf(?x, ?p),
process-processOf(?x, ?y) -> 'is-obligated-ByDPA-Art6(1)To-ProcessOnBasisOf-DataSubjectConsentOf'(?x, ?p)
is-identified-ByCharacteristicOf(?x, ?y) -> Data-Subject(?x)
```

Individuals: BSilver-Company

- ARTICLE9-ProcessingOfSpecialCategoriesOfPersonalData
- BSilver-Company
- BSilver-Customer
- BSilver-WebSite

Description: BSilver-Company

ST-NaturalPerson

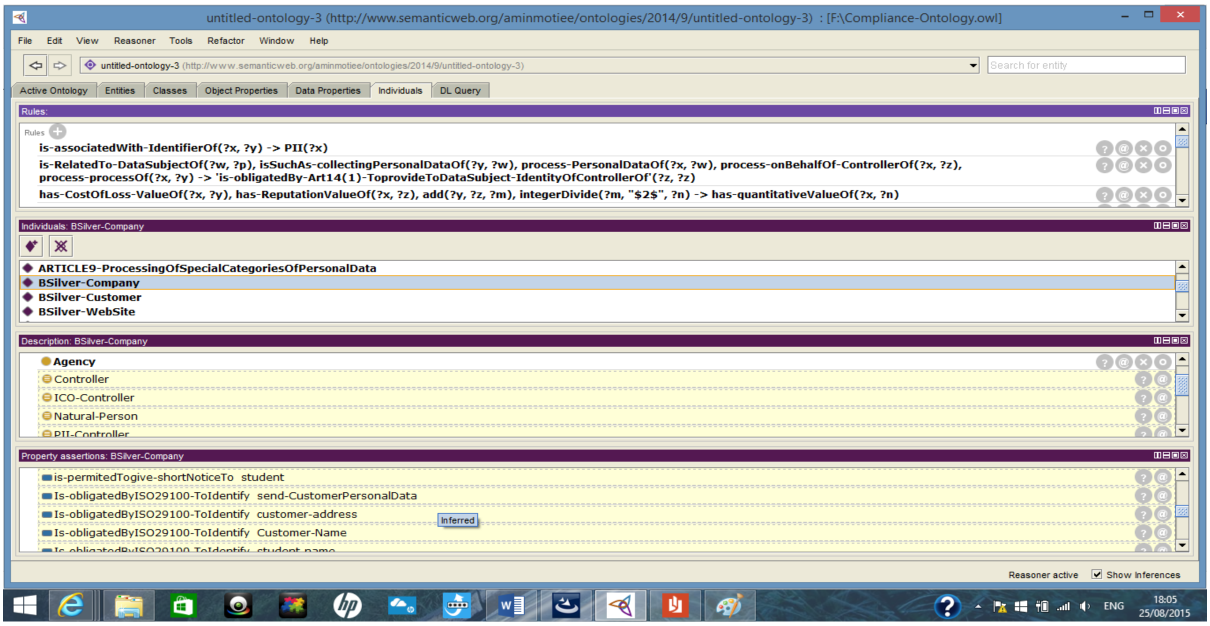
Same Individual As

Different Individuals

Property assertions: BSilver-Company

```
'is-obligatedBy-DPA-Art30(1)/Cannon65-ToEvaluateRiskOn'  Customer-Name
is-obligatedBy-ISO29100-ProvideNoticeTo  BSilver-Customer
'is-obligatedBy-Art14(1)-ToprovideToDataSubject-IdentityOfControllerOf'  BSilver-Company
Is-obligatedByISO29100To-EstablishISMS-On  send-CustomerPersonalData
```

Figure32 . Standard Ontology. Facts Refinement


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]
File
Edit
View
Reasoner
Tools
Refactor
Window
Help
untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3)
Search for entity
Active Ontology
Entities
Classes
Object Properties
Data Properties
Individuals
DL Query
Inferred
Reasoner active
Show Inferences
ENG
18:05
25/08/2015

Rules:

```
is-associatedWith-IdentifierOf(?x, ?y) -> PII(?x)
is-RelatedTo-DataSubjectOf(?w, ?p), isSuchAs-collectingPersonalDataOf(?y, ?w), process-PersonalDataOf(?x, ?w), process-onBehalfOf-ControllerOf(?x, ?z),
process-processOf(?x, ?y) -> 'is-obligatedBy-Art14(1)-ToprovideToDataSubject-IdentityOfControllerOf'(?z, ?z)
has-CostOfLoss-ValueOf(?x, ?y), has-ReputationValueOf(?x, ?z), add(?y, ?z, ?m), integerDivide(?m, "$2$", ?n) -> has-quantitativeValueOf(?x, ?n)
```

Individuals: BSilver-Company

- ARTICLE9-ProcessingOfSpecialCategoriesOfPersonalData
- BSilver-Company
- BSilver-Customer
- BSilver-WebSite

Description: BSilver-Company

- Agency
- Controller
- ICO-Controller
- Natural-Person

Property assertions: BSilver-Company

```
is-permitedTogive-shortNoticeTo  student
Is-obligatedByISO29100-ToIdentify  send-CustomerPersonalData
Is-obligatedByISO29100-ToIdentify  customer-address
Is-obligatedByISO29100-ToIdentify  Customer-Name
```

Figure33 . Standard Ontology. Obligation Refinement

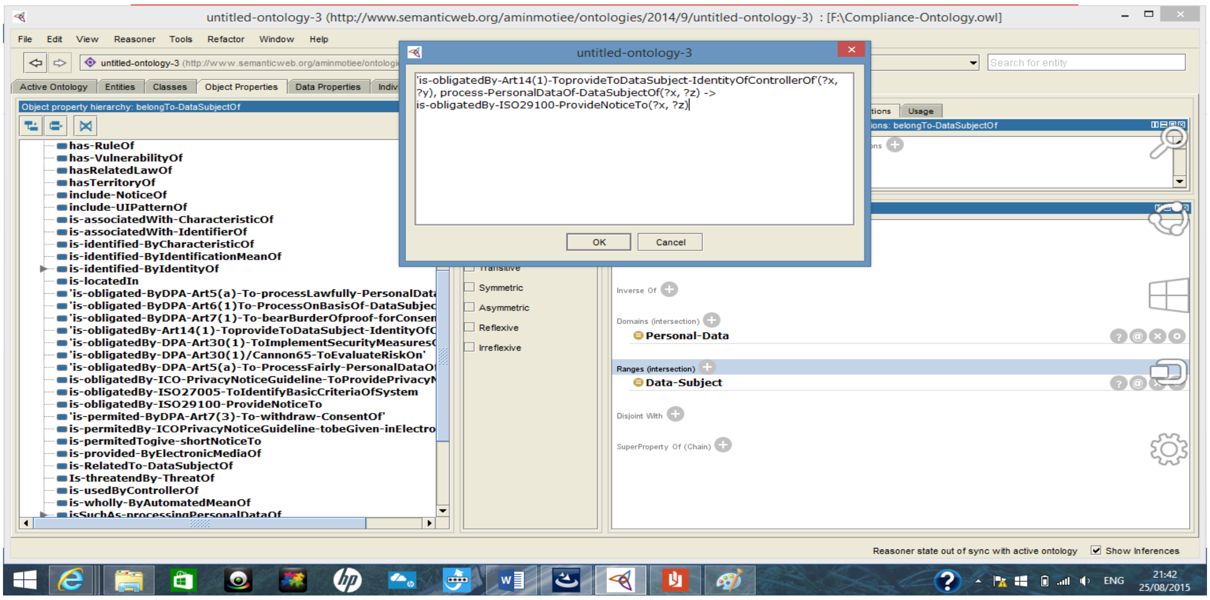
Following rules has been selected to practice refinement of GDPR and standard by ICO guidelines:

'is-obligatedBy-Art14(1)-ToprovideToDataSubject-IdentityOfControllerOf'(?x, ?y), process-PersonalDataOf-DataSubjectOf(?x, ?z) -> is-obligatedBy-ISO29100-ProvideIdentityIn-NoticeTo(?x, ?z)

Processing-Personaldataof(?x,?y), process-processOf(?x,?z), belongTo(?y,?w) → is-obligatedBy-ICO-ToprovideInPrivacyNotice-IdentityOfController(?x,?x) OR

Is-obligatedBy-ICO-ToprovideInPrivacyNotice-IdentityOfController(?x,?x), Privacy-notice(?k) → Is-permittedTO-takePositiveAction-forNoticeOf(?x,?k)

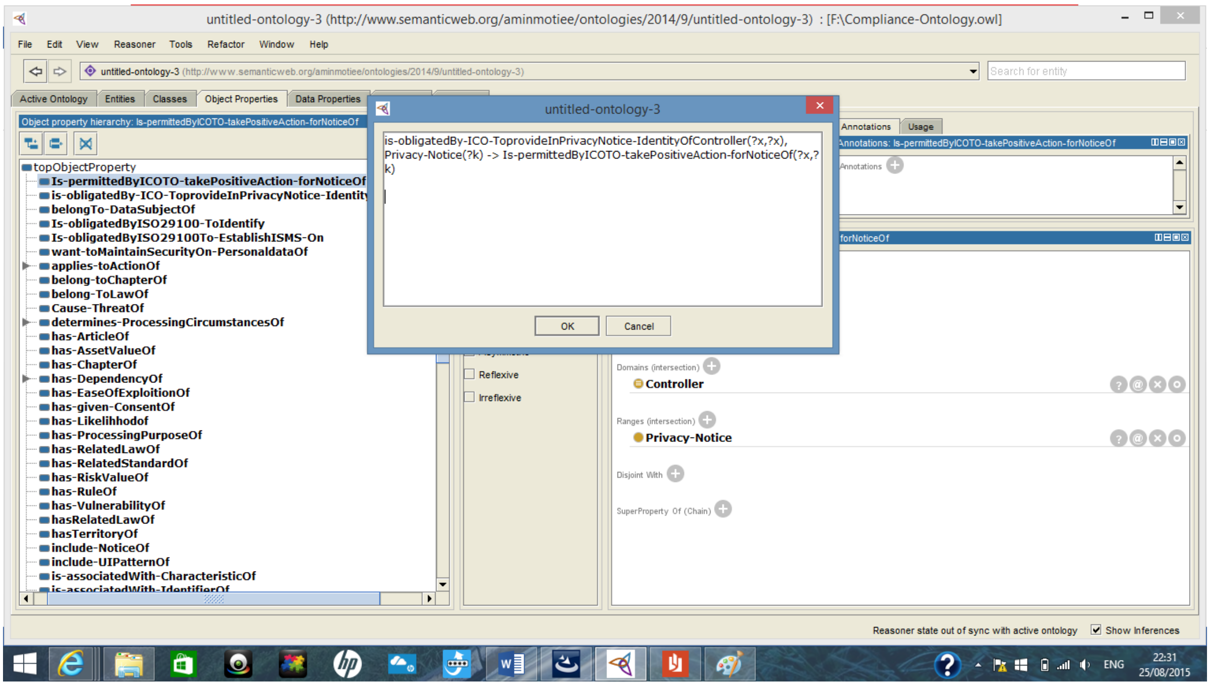
Is-permittedTO-takePositiveAction-forNoticeOf (?x,?k) → Is-permittedTo-sendByEmail-NoticeOf(?x,?k)



```
'is-obligatedBy-Art14(1)-ToprovideToDataSubject-IdentityOfControllerOf'(?x,
?y), process-PersonalDataOf-DataSubjectOf(?x, ?z) ->
is-obligatedBy-ISO29100-ProvideNoticeTo(?x, ?z)
```

has-RuleOf
has-VulnerabilityOf
hasRelatedLawOf
hasTerritoryOf
include-NoticeOf
include-UIPatternOf
is-associatedWith-CharacteristicOf
is-associatedWith-IdentifierOf
is-identified-ByCharacteristicOf
is-identified-ByIdentificationMeanOf
is-identified-ByIdentityOf
is-locatedIn
'is-obligated-ByDPA-Art5(a)-To-processLawfully-PersonalDat
'is-obligated-ByDPA-Art6(1)To-ProcessOnBasisOf-DataSubjec
'is-obligated-ByDPA-Art7(1)-To-bearBurderOfproof-forConsen
'is-obligatedBy-Art14(1)-ToprovideToDataSubject-IdentityOfC
'is-obligatedBy-DPA-Art30(1)-ToImplementSecurityMeasures(
'is-obligatedBy-DPA-Art30(1)/Cannon65-ToEvaluateRiskOn'
'is-obligatedBy-DPA-Art5(a)-To-ProcessFairly-PersonalDataO
is-obligatedBy-ICO-PrivacyNoticeGuideline-ToProvidePrivacyN
is-obligatedBy-ISO27005-ToIdentifyBasicCriteriaOfSystem
is-obligatedBy-ISO29100-ProvideNoticeTo
'is-permited-ByDPA-Art7(3)-To-withdraw-ConsentOf'
is-permitedBy-ICOPrivacyNoticeGuideline-tobeGiven-inElectro
is-permitedTogive-shortNoticeTo
is-provided-ByElectronicMediaOf
is-RelatedTo-DataSubjectOf
Is-threatendBy-ThreatOf
is-usedByControllerOf
is-wholly-ByAutomatedMeanOf
isSuchAs-processingPersonalDataOf

Figure34 . Standard Ontology. Obligation Refinement



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]

Object property hierarchy: Is-permittedByICOTO-takePositiveAction-forNoticeOf

topObjectProperty
Is-permittedByICOTO-takePositiveAction-forNoticeOf
is-obligatedBy-ICO-ToprovideInPrivacyNotice-Identity
belongTo-DataSubjectOf
Is-obligatedByISO29100-ToIdentify
Is-obligatedByISO29100To-EstablishISMS-On
want-toMaintainSecurityOn-PersonaldataOf
applies-toActionOf
belong-toChapterOf
belong-ToLawOf
Cause-ThreatOf
determines-ProcessingCircumstancesOf
has-ArticleOf
has-AssetValueOf
has-ChapterOf
has-DependencyOf
has-EaseOfExploitionOf
has-given-ConsentOf
has-Likelihhodof
has-ProcessingPurposeOf
has-RelatedLawOf
has-RelatedStandardOf
has-RiskValueOf
has-RuleOf
has-VulnerabilityOf
hasRelatedLawOf
hasTerritoryOf
include-NoticeOf
include-UIPatternOf
is-associatedWith-CharacteristicOf
is-associatedWith-IdentifierOf

untitled-ontology-3

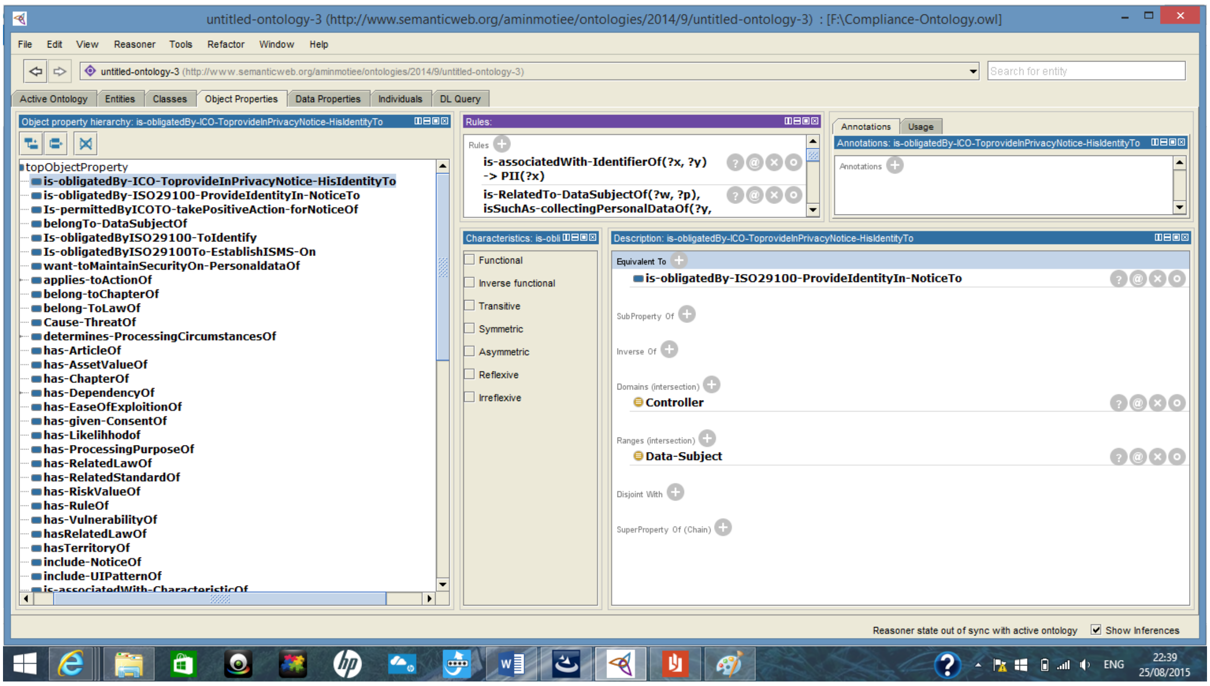
is-obligatedBy-ICO-ToprovideInPrivacyNotice-IdentityOfController(?x,?x),
Privacy-Notice(?k) -> Is-permittedByICOTO-takePositiveAction-forNoticeOf(?x,?k)

Annotations: Is-permittedByICOTO-takePositiveAction-forNoticeOf

Domains (intersection)
Controller

Ranges (intersection)
Privacy-Notice

Figure35 .ICO Ontology. Refinement Obligation



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]

Object property hierarchy: is-obligatedBy-ICO-ToprovideInPrivacyNotice-HisIdentityTo

topObjectProperty
is-obligatedBy-ICO-ToprovideInPrivacyNotice-HisIdentityTo
is-obligatedBy-ISO29100-ProvideIdentityIn-NoticeTo
Is-permittedByICOTO-takePositiveAction-forNoticeOf
belongTo-DataSubjectOf
Is-obligatedByISO29100-ToIdentify
Is-obligatedByISO29100To-EstablishISMS-On
want-toMaintainSecurityOn-PersonaldataOf
applies-toActionOf
belong-toChapterOf
belong-ToLawOf
Cause-ThreatOf
determines-ProcessingCircumstancesOf
has-ArticleOf
has-AssetValueOf
has-ChapterOf
has-DependencyOf
has-EaseOfExploitionOf
has-given-ConsentOf
has-Likelihhodof
has-ProcessingPurposeOf
has-RelatedLawOf
has-RelatedStandardOf
has-RiskValueOf
has-RuleOf
has-VulnerabilityOf
hasRelatedLawOf
hasTerritoryOf
include-NoticeOf
include-UIPatternOf
is-associatedWith-CharacteristicOf

Rules:

is-associatedWith-IdentifierOf(?x, ?y) -> PII(?x)
is-RelatedTo-DataSubjectOf(?w, ?p), isSuchAs-collectingPersonalDataOf(?y,

Annotations: is-obligatedBy-ICO-ToprovideInPrivacyNotice-HisIdentityTo

Characteristics: is-obli

□ Functional
□ Inverse functional
□ Transitive
□ Symmetric
□ Asymmetric
□ Reflexive
□ Irreflexive

Description: is-obligatedBy-ICO-ToprovideInPrivacyNotice-HisIdentityTo

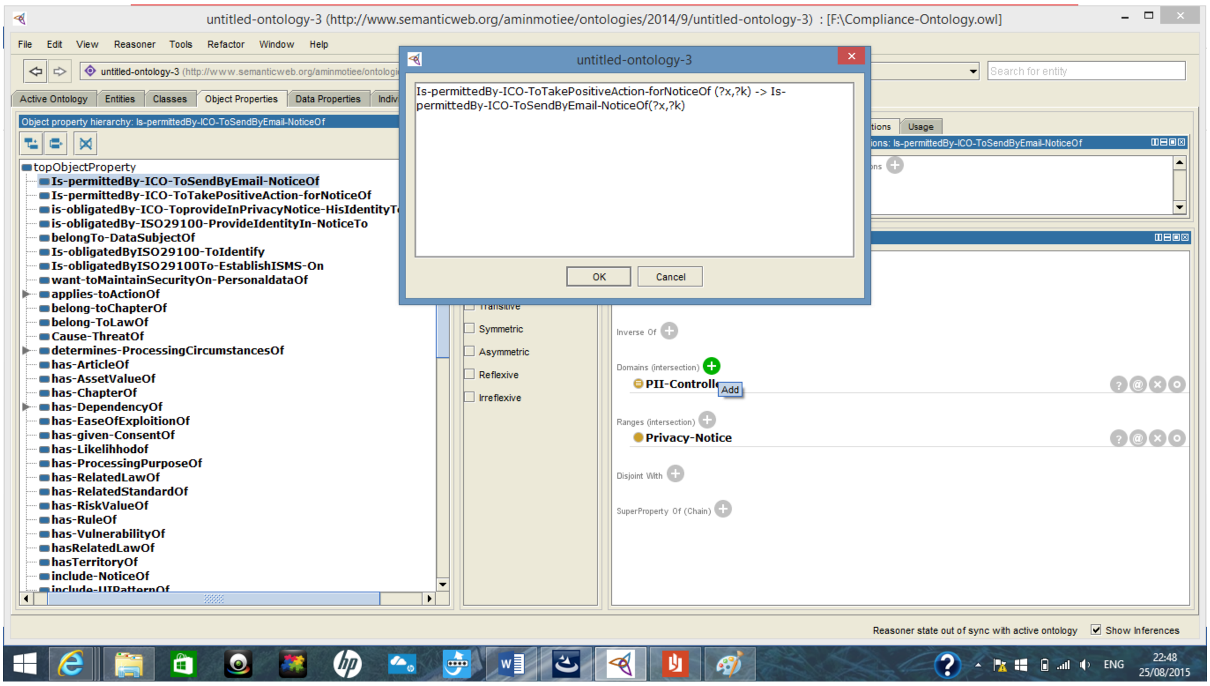
Equivalent To
is-obligatedBy-ISO29100-ProvideIdentityIn-NoticeTo

Domains (intersection)
Controller

Ranges (intersection)
Data-Subject

Figure36 . ICO Ontology. Obligation Equivalency

Figure 36 shows how we were able to equivalent two object properties of two Obligations together. As a consequence, any other rights such as Permissions that are concluded from one Obligation, automatically will be concluded from the other Obligation too. In other word, an obligation from ISO 29100 will result to some permissions in ISO 29100 (Refinement).



untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [F:\Compliance-Ontology.owl]

untitled-ontology-3

```
Is-permittedBy-ICO-ToTakePositiveAction-forNoticeOf (?x,?k) -> Is-permittedBy-ICO-ToSendByEmail-NoticeOf(?x,?k)
```

Object property hierarchy: Is-permittedBy-ICO-ToSendByEmail-NoticeOf

```
topObjectProperty
  Is-permittedBy-ICO-ToSendByEmail-NoticeOf
  Is-permittedBy-ICO-ToTakePositiveAction-forNoticeOf
  is-obligatedBy-ICO-ToprovideInPrivacyNotice-HisIdentityT
  is-obligatedBy-ISO29100-ProvideIdentityIn-NoticeTo
  belongTo-DataSubjectOf
  Is-obligatedByISO29100-ToIdentify
  Is-obligatedByISO29100To-EstablishISMS-On
  want-toMaintainSecurityOn-PersonaldataOf
▶ applies-toActionOf
  belong-toChapterOf
  belong-ToLawOf
  Cause-ThreatOf
▶ determines-ProcessingCircumstancesOf
  has-ArticleOf
  has-AssetValueOf
  has-ChapterOf
▶ has-DependencyOf
  has-EaseOfExploitionOf
  has-given-ConsentOf
  has-Likelihhodof
  has-ProcessingPurposeOf
  has-RelatedLawOf
  has-RelatedStandardOf
  has-RiskValueOf
  has-RuleOf
  has-VulnerabilityOf
  hasRelatedLawOf
  hasTerritoryOf
  include-NoticeOf
  include-UIPatternOf
```

ons: Is-permittedBy-ICO-ToSendByEmail-NoticeOf

□ Transitive
□ Symmetric
□ Asymmetric
□ Reflexive
□ Irreflexive

Inverse Of

Domains (intersection)
PII-Controll

Ranges (intersection)
Privacy-Notice

Disjoint With

SuperProperty Of (Chain)

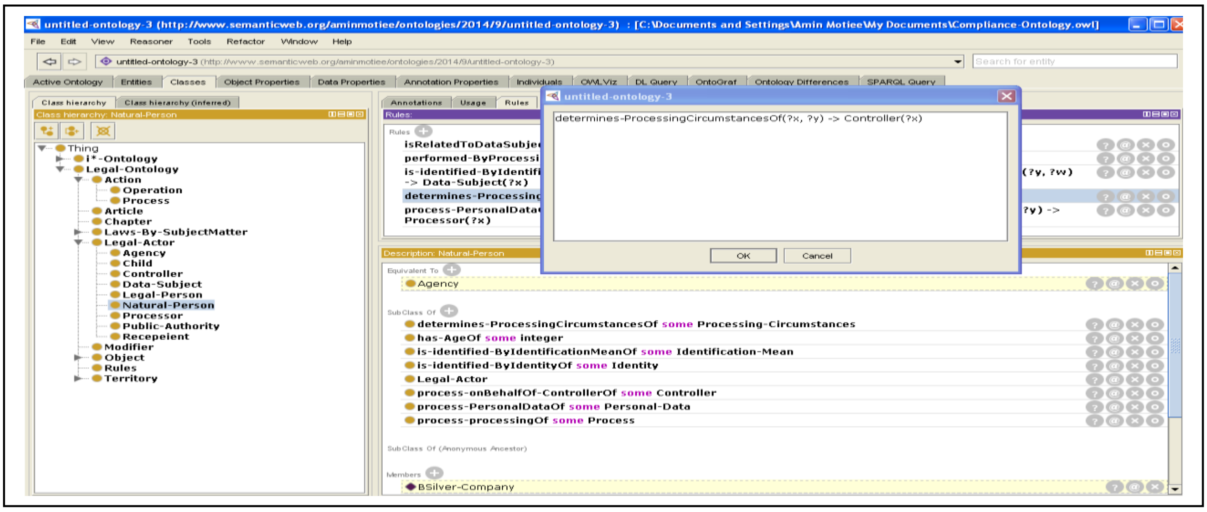
Reasoner state out of sync with active ontology ☑ Show Inferences

Figure37 . ICO Ontology. Permission Refinement

In this section we were able to represent implementation of some of the ontological rules which we could built and analyse from Data Protection Regulation. Later we showed how these rules can be refined, mapped or inherit from rules of other ontologies of our framework such as standard and ICO. Using the implemented automated tool, the concept of our theatrical framework are applied. This application is exactly based on the concepts from Figure 37 which illustrates the model of our framework. Using this tool, the user can extract compliance knowledge, instance concepts with real world scenarios from developing IT systems or even any business process and conclude compliance solutions.

- ### Legal Reasoning for ESilver Case Study

In order to perform the legal reasoning task, we need to individual each of the Law Ontology classes with variables (instances) from i* Ontology (if founded). As it can be seen in Figure 38 and 39, E*Silver-website* and ESilver-company are both individuals of *Agency* in Law Ontology as well. Therefore, running the ontology reasoner any Rule defined for the class of Agency with depicted relationships as being derived for ESilver-website and ESilver-company will be applicable for these individuals. As the result ESilver-company will also become a controller and ESilver-website as a processor. See Figure 38 and 39 for these definitions. Being a controller, any Rule defined for a controller will also apply on ESilver-company if it has the facts defined on those rules as its relationship.


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf Ontology Differences SPARQL Query
Class hierarchy: Natural-Person
Thing
i*-Ontology
Legal-Ontology
Action
Operation
Process
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory
Annotations Usage Rules
untitled-ontology-3
OK
Cancel

Rules:

- isRelatedToDataSubje
- performed-ByProcessi
- is-identified-ByIdentifi … (?y, ?w) -> Data-Subject(?x)
- determines-Processing
- process-PersonalData … ?y) -> Processor(?x)

determines-ProcessingCircumstancesOf(?x, ?y) -> Controller(?x)

Description: Natural-Person

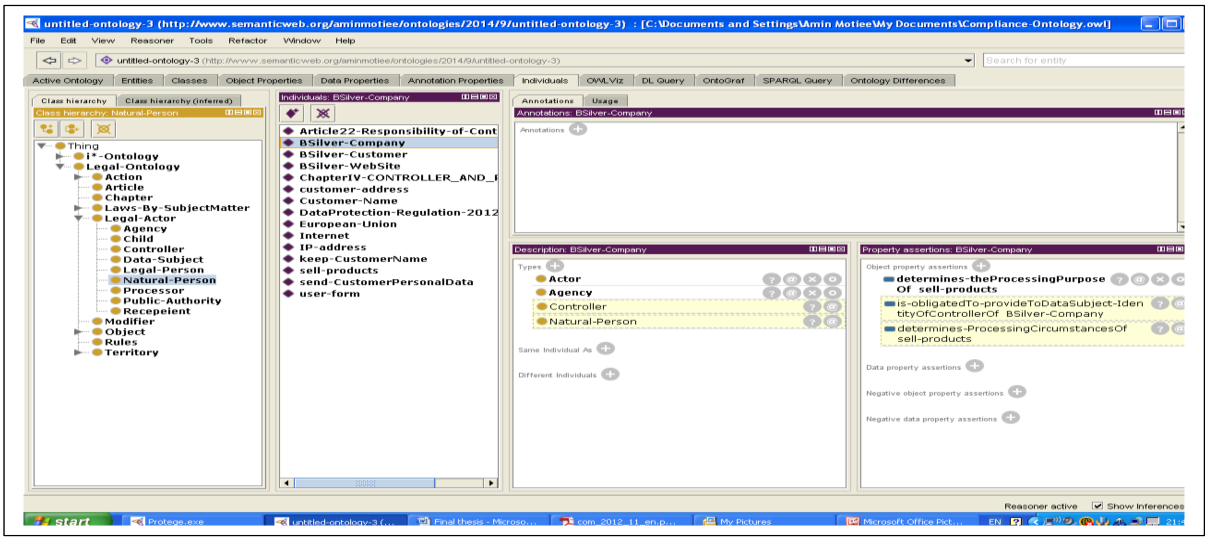
Equivalent To
- Agency

SubClass Of
- determines-ProcessingCircumstancesOf some Processing-Circumstances
- has-AgeOf some integer
- is-identified-ByIdentificationMeanOf some Identification-Mean
- is-identified-ByIdentityOf some Identity
- Legal-Actor
- process-onBehalfOf-ControllerOf some Controller
- process-PersonalDataOf some Personal-Data
- process-processingOf some Process

SubClass Of (Anonymous Ancestor)

Members
- BSilver-Company

Figure38 . Controller Rule


untitled-ontology-3 (http://www.semanticweb.org/aminmotiee/ontologies/2014/9/untitled-ontology-3) : [C:\Documents and Settings\Amin Motiee\My Documents\Compliance-Ontology.owl]
File Edit View Reasoner Tools Refactor Window Help
Active Ontology Entities Classes Object Properties Data Properties Annotation Properties Individuals OWLViz DL Query OntoGraf SPARQL Query Ontology Differences
Class hierarchy: Natural-Person
Thing
i*-Ontology
Legal-Ontology
Action
Article
Chapter
Laws-By-SubjectMatter
Legal-Actor
Agency
Child
Controller
Data-Subject
Legal-Person
Natural-Person
Processor
Public-Authority
Recepeient
Modifier
Object
Rules
Territory
Individuals: BSilver-Company
Article22-Responsibility-of-Cont
BSilver-Company
BSilver-Customer
BSilver-WebSite
ChapterIV-CONTROLLER_AND_I
customer-address
Customer-Name
DataProtection-Regulation-2012
European-Union
Internet
IP-address
keep-CustomerName
sell-products
send-CustomerPersonalData
user-form
Annotations Usage
Annotations: BSilver-Company
Annotations
Reasoner active
Show Inferences
start
Protege.exe
untitled-ontology-3 (...
Final thesis - Microso...
com_2012_11_en.p...
My Pictures
Microsoft Office Pict...
EN

Description: BSilver-Company

Types
- Actor
- Agency
- Controller
- Natural-Person

Same Individual As

Different Individuals

Property assertions: BSilver-Company

Object property assertions
- determines-theProcessingPurposeOf sell-products
- is-obligatedTo-provideToDataSubject-IdentityOfControllerOf BSilver-Company
- determines-ProcessingCircumstancesOf sell-products

Data property assertions

Negative object property assertions

Negative data property assertions

Figure39 . E-Silver-website Processor

APPENDIX V. RDF REPRESENTATION OF KN-SOPD ONTOLOGIES

CLASS	PROPERTY
<rdfs: Class rdf:id= "Actor"> <rdfs: Subclassof rdf:resource="i*/> </rdf: Class> <rdfs:Class rdf:about= "Goal"> <rdfs:Subclassof rdf:resource=i*/> </rdfs:Class> <rdfs:Class rdf:about="Soft-goal"> <rdfs:SubClassOf rdf:resource: "Goal"/> </rdf:Class> <rdf:Class rdf:about="Hard-goal"> <rdf:SubClassof rdf:resource= "Goal"/> </rdf:Class> <rdfs:Class rdf:id= "Task"> <rdfs:Subclassof rdf:resource= "i*> </rdf:Class> <rdfs:class rdf:id= "Resource"> <rdfs:Subclassof rdf:resource= "i*"> </rdf:Class> <rdfs: Class rdf:id= "System"> <rdfs: Subclassof rdf:resource="i*/> </rdf: Class	<rdfs:Property rdf:id="has-GoalDependencyOf"> <rdfs:domain rdf:resource="Actor"> <rdfs:range rdf:resource="Goal"> </rdfs:Property> <rdfs:Property rdf:id="has-TaskDependencyOf"> <rdfs:domain rdf:resource="Actor"> <rdfs:range rdf:resource="Goal"> </rdfs:Property> <rdfs:Property rdf:id="has-ResorceDependencyOf"> <rdfs:domain rdf:resource="Actor"> <rdfs:range rdf:resource="Goal"> </rdfs:Property> <rdfs:Property rdf:id="means-end"> <rdfs:domain rdf:resource="Goal"> <rdfs:range rdf:resource="Task"> </rdfs:Property> <rdfs:Property rdf:id="AND"> <rdfs:domain rdf:resource="Goal"> <rdfs:range rdf:resource="Goal"> </rdfs:Property> <rdfs:Property rdf:id="OR"> <rdfs:domain rdf:resource="Goal"> <rdfs:range rdf:resource="Goal"> </rdfs:Property>

	<rdfs:Property rdf:id="decomposed"> <rdfs:domain rdf:resource="Task"> <rdfs:range rdf:resource="Goal"> </rdfs:Property>

Table2 .i* Ontology in RDF Language

CLASS	PROPERTY
<rdfs: Class rdf:id= "Web-Application"> <rdfs: Subclassof rdf:resource="Developing-System*/> </rdf: Class> <rdfs: Class rdf:id= "Information-Worker"> <rdfs: Subclassof rdf:resource="Developing-System*/> </rdf: Class> <rdfs: Class rdf:id= "Educational-Software"> <rdfs: Subclassof rdf:resource="Developing-System*/> </rdf: Class> <rdfs: Class rdf:id= "Entertainment-Software"> <rdfs: Subclassof rdf:resource="Developing-System*/> </rdf: Class>	<rdfs:Property rdf:id="has-PatternOf"> <rdfs:domain rdf:resource="Developing-System"> <rdfs:range rdf:resource="Pattern"> </rdfs:Property> <rdfs:Property rdf:id="Comply-with"> <rdfs:domain rdf:resource="Deveoping-Systm"> <rdfs:range rdf:resource="Laws-By-Subject"> </rdfs:Property>

Table3 .Design Ontology in RDF Language

CLASS	PROPERTY
<rdfs: Class rdf:id= "-Law-By-Subject"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class> <rdfs: Class rdf:id= "IT-Law"> <rdfs: Subclassof rdf:resource=" Subject-of-Law "/> </rdf: Class> <rdfs: Class rdf:id= "Computer-Law"> <rdfs: Subclassof rdf:resource="Subject-of-Law*/> </rdf: Class> <rdfs: Class rdf:id= "Cyber-Law"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class> <rdfs: Class rdf:id= "Chapter"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class> <rdfs: Class rdf:id= "Article"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class> <rdfs: Class rdf:id= "Rule"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class> <rdfs: Class rdf:id= "Legal-Actor"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/>	<rdfs:Property rdf:id="has-TerritoryOf"> <rdfs:domain rdf:resource="Law-By-Subject"> <rdfs:range rdf:resource="Territory"> </rdfs:Property> <rdfs:Property rdf:id="has-ChapterOf"> <rdfs:domain rdf:resource=" Law-By-Subject"> <rdfs:range rdf:resource="Chapter"> </rdfs:Property> <rdfs:Property rdf:id="has-ArticleOf"> <rdfs:domain rdf:resource=" Chapter"> <rdfs:range rdf:resource="Article"> </rdfs:Property> <rdfs:Property rdf:id="has-RuleOf"> <rdfs:domain rdf:resource=" Article"> <rdfs:range rdf:resource="Rule"> </rdfs:Property> <rdfs:Property rdf:id="Does"> <rdfs:domain rdf:resource=" Actor"> <rdfs:range rdf:resource="Object"> </rdfs:Property> <rdfs:Property rdf:id="is-ObligatedTo-do">

</rdf: Class> <rdfs: Class rdf:id= "Action"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class> <rdfs: Class rdf:id= "Object"> <rdfs: Subclassof rdf:resource="Laws&Regulation*/> </rdf: Class>	<rdfs:domain rdf:resource=" Actor"> <rdfs:range rdf:resource="Object"> </rdfs:Property> <rdfs:Property rdf:id="is-PermittedTo-do"> <rdfs:domain rdf:resource=" Actor"> <rdfs:range rdf:resource="Object"> </rdfs:Property> <rdfs:Property rdf:id="is-ProhibitedTo-do"> <rdfs:domain rdf:resource=" Actor"> <rdfs:range rdf:resource="Object"> </rdfs:Property>

Table4 Law Ontology in RDF Language

CLASS	**PROPERTY**
</rdf: Class> <rdfs: Class rdf:id= "Purpose"> <rdfs: Subclassof rdf:resource="Risk*/> </rdf: Class> <rdfs: Class rdf:id= "ISMS"> <rdfs: Subclassof rdf:resource="Pupose*/> </rdf: Class> <rdfs: Class rdf:id= "Legal-Complince"> <rdfs: Subclassof rdf:resource="Purpose*/> </rdf: Class> <rdfs: Class rdf:id= "Context">	<rdfs:Property rdf:id="has-BasicCriteriaOf> <rdfs:domain="Purpose" rdf:resource="Basic-Criteria"> </rdf:Property> <rdfs:Property rdf:id="has-AssetOf"> <rdfs:domain rdf:resource=" Basic-Criteria"> <rdfs:range rdf:resource="Asset"> </rdfs:Property> <rdfs:Property rdf:id="has-AssetOf"> <rdfs:domain rdf:resource=" Scope&Boundary"> <rdfs:range rdf:resource="Asset">

<rdfs: Subclassof rdf:resource="Risk*/> </rdf: Class> <rdfs: Class rdf:id= "Basic-Criteria"> <rdfs: Subclassof rdf:resource="Context*/> </rdf: Class> <rdfs: Class rdf:id= "Risk-Evaluation-Citeria"> <rdfs: Subclassof rdf:resource="Basic-Criteria*/> </rdf: Class> <rdfs: Class rdf:id= "Impact-Criteria"> <rdfs: Subclassof rdf:resource="Basic-Criteria*/> </rdf: Class> <rdfs: Class rdf:id= "Risk-Assesment"> <rdfs: Subclassof rdf:resource="Risk*/> </rdf: Class> <rdfs: Class rdf:id= "Asset"> <rdfs: Subclassof rdf:resource="Risk-Assesment*/> </rdf: Class> <rdfs: Class rdf:id= "Threat"> <rdfs: Subclassof rdf:resource="Risk-Assesment*/> </rdf: Class> <rdfs: Class rdf:id= "Vulnerability"> <rdfs: Subclassof rdf:resource="Risk-Assesment*/> </rdf: Class>	</rdfs:Property> <rdfs:Property rdf:id="has-ValueOf"> <rdfs:domain rdf:resource=" Asset"> <rdfs:range rdf:resource="Value"> </rdfs:Property> <rdfs:Property rdf:id="has-LikelihoodOf"> <rdfs:domain rdf:resource="Threat "> <rdfs:range rdf:resource="Value"> </rdfs:Property> <rdfs:Property rdf:id="has-VulnerabilityOf"> <rdfs:domain rdf:resource=" Asset"> <rdfs:range rdf:resource="Vulnerability"> </rdfs:Property> <rdfs:Property rdf:id="has-ControlOf"> <rdfs:domain rdf:resource=" Threat"> <rdfs:range rdf:resource="Control"> </rdfs:Property> <rdfs:Property rdf:id="has-ControlOf"> <rdfs:domain rdf:resource=" Vulnerability"> <rdfs:range rdf:resource="Control"> </rdfs:Property> <rdfs:Property rdf:id="is-exploidBy"> <rdfs:domain rdf:resource=" Vulnerability">

<rdfs: Class rdf:id= "Value"> <rdfs: Subclassof rdf:resource="Risk-Assesment*/> </rdf: Class> <rdfs: Class rdf:id= "Primary-Assest"> <rdfs: Subclassof rdf:resource="Asset*/> </rdf: Class> <rdfs: Class rdf:id= "Information"> <rdfs: Subclassof rdf:resource="Primary-Asset*/> </rdf: Class> <rdfs: Class rdf:id= "Business-Process"> <rdfs: Subclassof rdf:resource="Primary-Asset*/> </rdf: Class> <rdfs: Class rdf:id= "Negligible"> <rdfs: Subclassof rdf:resource="Value*/> </rdf: Class> <rdfs: Class rdf:id= "Very-Low"> <rdfs: Subclassof rdf:resource="Value*/> </rdf: Class> <rdfs: Class rdf:id= "Control"> <rdfs: Subclassof rdf:resource="Risk-Treatment*/> </rdf: Class>	<rdfs:range rdf:resource="Threat> </rdfs:Property>

Table5 Risk Ontology in RDF Language

PUBLICATIONS

1.“To Comply Software and IT System Development with Related Laws”. The CAiSE Doctorial Consortium. 2011

2. “Extracting Security Requirements from Relevant Laws and Regulations”. Research Challenges in Information System Conference (RCIS) 2012.

3. “A Meta-model for Legal Compliance and Trustworthiness of Information Systems”. CAiSE 2012

4. “A High-Level Ontology for a Software Development Compliance Framework”. Big Data Security 2015

5. “An Ontology Based Approach to Analyse Compliance Requirements in Software Development “. ICSEA 2015