Using Ontologies to Model Data Protection Requirements in Workflows

Cesare Bartolini[1], Robert Muthuri[2], and Cristiana Santos[3]

[1] University of Luxembourg, Luxembourg,
cesare.bartolini@uni.lu
[2] University of Turin, Italy,
robert.kiriinya@unito.it
[3] Institute of law and technology, University of Barcelona (IDT-UAB),
cristiana.teixeirasantos@gmail.com

Abstract. Data protection, currently under the limelight at the European level, is undergoing a long and complex reform that is finally approaching its completion. Consequently, there is an urgent need to customize semantic standards towards the prospective legal framework. The aim of this paper is to provide a bottom-up ontology describing the constituents of data protection domain and its relationships. Our contribution envisions a methodology to highlight the (new) duties of data controllers and foster the transition of IT-based systems, services, tools and businesses to comply with the new General Data Protection Regulation. This structure may serve as the foundation for the design of data protection compliant information systems.

Keywords: Legal ontology; data protection; General Data Protection Regulation; compliance; business process; BPMN.

1 Introduction

The goal of the privacy and data protection domains of law is to protect the personal information of individuals (normally referred to as personal data) in a given jurisdiction. With the advent of social media and the uptake of digital technology, the availability of digital services and the soon-to-be Internet of Things have dramatically increased the amount of information collected and processed by governments and companies. Accordingly, businesses are continually developing techniques such as machine learning, big data analytics, natural language processing and applications to exploit data assets, to the detriment of new concerns of profiling, identification and re-identification risks.

The European Union (EU) is in the process of upgrading the current data protection law, which is based on the so-called Data Protection Directive (DPD), to a more modern and uniform legislation [36], in accordance with the recent technological progresses. The objective is to enhance individuals' rights, give them more control over their own data, simplify the regulatory environment for businesses, and set the foundation for the Digital Single Market [15]. The main

legislative document of the reform is the General Data Protection Regulation (GDPR), which constitutes the basis for the general protection of personal data. Although the new legislation is in its final stages, it will not be in force before 2018. The text of the GDPR is not finalized yet, and the latest official version released by the Commission dates back to early 2012[4].

A data subject is the individual to whom the personal data relate. On the other hand, a data controller is the natural or legal person who determines the purposes and means processing. The controller may delegate the actual processing to another entity called a data processor. Data Protection Authorities (DPAs) are mandated with regulating the controller and the processor while helping subjects to enforce their rights. In the light of the importance that the processing of personal data has attained over the last decade, the reform is trying to clarify and strengthen the rights of the data subjects. Correspondingly, the duties of the controller and of the processor become more burdensome and require new technical measures. As per the latest version of the GDPR, DPAs will have inquisitory powers with the possibility to levy fines as high as 5% of the annual global turnover [28]. Enterprises will thus be pressed to avoid infringements. However, most of the duties of the data controller are expressed in evaluative terms, making it difficult for the controller to know the exact extent of its obligations. For instance, the draft Regulation requires "appropriate technical and organizational measures" to ensure secure processing of personal data albeit, without further elaboration[5].

The foundations of European data protection have been laid out and evolved over several decades. Data protection involves a large number of stakeholders, including the controller, processor, data subject, recipient of transfer, national authority, legislator, auditor, and the data protection officer - a new role introduced in the draft Regulation. Additional roles which do not exist at the European level have been introduced in the legislation of some Member States. Such a context, along with the importance of the interests involved, entails a complex set of rules where each stakeholder has different powers, rights, and obligations. The technical evolution of the last decades has also significantly changed the environment in which the rules operate, blurring the distinction between the controller and the data subject [41]. Consequently, data protection in the legal domain nowadays represents a major challenge for any business or public administration involved in the processing of personal data, and a potential source of liability if its rules are not complied with correctly.

Achieving compliance is no easy task. The transition of a firm's organizational and technical measures could be eased if appropriate standards existed for it to adopt. However, no significant standards currently exist for data protection, much less in the light of the upcoming reform. Within computer science, data protection is often referred to as *privacy* and considered a subset of the security domain [32,27]. Significant differences exist between the two terms from

[4] However, versions amended by the Parliament and the Council have either been published or leaked to the general public.

[5] Article 30 of the draft Regulation

a legal perspective, although some overlapping does exist. For example, some provisions in data protection legislation require that the data processing be performed under appropriate security measures. An early-stage research [6] aims at evaluating the overlapping between the GDPR and security standards, such as the ISO 27000 family, and in particular ISO 27001:2013 [24], to measure the degree of coverage of the data protection rules a security standard would cover. This facilitates controllers to understand what is required of them when they adopt a widespread security standard relying on many years of expertise and consolidated audit firm methodologies.

Our previous work [7] defined the specific research problem, the context within which it arose, the rationale behind a potential solution, and an ontology of the data protection domain in the context of the GDPR. Its objectives were focused on the scope and extent of the duties and obligations of the data controller to facilitate compliance with the GDPR.

In this paper we illustrate the design and development of the ontology following the initial stage described therein. As a proof of concept, we introduce an approach that uses the ontology to enrich a workflow model such as a business process, with annotations that express data protection requirements. In other words, the ontology will constitute the knowledge base from which the concepts to annotate the workflow model are extracted. Such an approach can provide benefits for a number of stakeholders:

- data controllers would have a clearer view of their duties with respect to data protection in the context of their business;
- the auditors would have a first-look model to assess the GDPR compliance;
- DPAs would have a structured approach to detect potential violations.

The paper is organized as follows. In section 2, we describe the related work concerning domain legal ontologies within data protection and privacy, and business processes. section 3 presents the ontology definition, explaining how to describe data protection concepts by means of ontologies and describing the ontology requirements and construction; finally, it summarizes some preliminary evaluation of the ontology. section 4 portrays a sample extension of business processes using the envisioned legal ontology. Finally, in section 5, we give a set of conclusions and future work.

2 Related Work

"Domain ontologies" in the legal field focus on a particular area of law, but their relevance is constrained by their subject-matter modeling [10] and only some have been applied beyond the prototype stage. Some of the pertinent domain ontologies are briefly mentioned in terms of their purpose, subject-matter, reusability, and availability. Despite efforts in modeling data protection domain, according to the best of our knowledge, there is no ontological representation that specifically addresses the data protection legislation in the light of the reform, the duties of data controllers and the corresponding rights of data subjects.

The LegLOPD ontology [29] was applied for the preservation of privacy in location-based services. It modeled concepts from the Spanish data protection law. The essential structure to be protected in LegLOPD is the concept of *private data*, derived from an LRI Core [8] abstract concept.

The OntoPrivacy [9] ontology modeled a glossary of keywords from the Italian Personal Data Protection Code. A bottom-up approach was used as the lexicon was the basis to build the ontology. It consisted of a domain ontology reusing top level ontologies. OntoPrivacy has been created to support a tool that allows to query the functional profile of legislative data.

The Neurona Ontologies [11] are application-oriented, and modeled the knowledge for the development of data protection compliance to offer reports regarding the correct application of security measures to data files containing personal data. Their design is based on a Data Protection Knowledge Ontology, which contains the core concepts of the system, and a Data Protection Reasoning Ontology, to assess data protection compliance. These ontologies provide legal professionals and citizens with better access to legal information, but could also support data protection and privacy compliance in organizations and administrations. However, there are several problems that make them unsuited for the purposes of the current research: the surveyed ontologies are proprietary, and their point of view is not focused on the duties of the data controller.

The Privacy by Design (PbD) approach requires that data protection measures be implemented prior to the means of processing being determined[6]. An ontology framework based on the PbD approach [26] consists of nine base ontologies, eight domain ontologies and four application specific ontologies. Another interesting approach is presented in [33]. However, that work is not focused on the obligations of the data controller, but rather on expressing the legal norms using an ontology to enforce access control policies.

The idea of using ontologies to extend notations is not novel [34,31]. It has been acknowledged in [22] that ontologies can be integrated in the Software Development Life Cycle (SDLC) in any situation where requirements in a domain are frequently used, e.g., the data protection requirements in our case. However, the proposal of this paper addresses the use of the ontology in software design not for the purposes of detailing the application domain of the software, but to specify legal constraints with which the software, or more generally the business process, must comply with. This approach will allow a more consistent interaction between the data controller, the auditors, and the DPAs to ease the transition to the GDPR.

3 An ontology for data protection rules

3.1 Ontology Engineering

Ontology Engineering refers to the set of activities that concern the ontology development process, the ontology life cycle, the methodologies for building ontologies, the tool suited and languages that support them [20]. For legal knowledge

[6] Article 23 of the GDPR, addressing the design and the implementation of a system

formalization we use the legacy guiding methodologies: METHONTOLOGY and Neon specification tasks [38] to ensure a sustainable modeling. METHONTOLOGY [17,18] is a structured method to build ontologies, also applied to legal knowledge formalization [12], carrying out the whole *ontology development* process (through the specification, conceptualization, formalization, implementation, and maintenance tasks of the ontology), and its *support activities* (knowledge acquisition, integration, evaluation and documentation), tasks that we describe below.

The ontology *specification* phase expressed in the Ontology Requirement Specification [39] facilitates the ontology development and refers to the activity of collecting the requirements that the ontology should fulfill: a) the purpose, intended scenarios of use, end-users, etc.; b) level of formality of the implemented ontology; c) scope . In particular, the Ontology Requirement Specification Document (ORSD) (1) allows the identification of the particular knowledge that should be represented in the ontology; (2) facilitates the reuse of knowledge resources by means of focusing the resource search towards the particular knowledge to be represented; and (3) permits the verification of the ontology with respect to the requirements that the ontology should fulfill.

Accordingly, our ontological commitment [14] provides a foundational structure in relation to the new data protection reform. In particular it identifies the scope and extent of the obligations of the data controller, especially in relation to the rights of the data subject.

Pursuing the context of use (users and use), this work anticipates the impact that the GDPR is likely to have on firms once it enters into force. While businesses have a legitimate interest in collecting personal data as assets to achieve their business goals, they should also comply with regulatory requirements. The chosen context envisions integration/interoperation within a business process.

Functional requirements are represented in the form of informal Competency Questions (CQs) that the ontology must be able to answer. A CQ [40] is a natural language sentence that expresses a pattern for a type of questions the domain experts expect an ontology to answer. The ability to answer the CQs hence becomes a functional requirement of the ontology. We extracted the CQs from external expert generated content sources declared below. For our data protection ontology, the following are CQs: 1. What are the obligations of a data controller? 2. What are the functions of a data processor? 3. What are the rights of the data subject? 4. How do the rights of the data subject relate to the obligations of the data controller and the functions of the processor? 5. How can a data subject interact and/or enforce their rights against a data controller? 6. What are the possible fines and sanctions issued in response to violations by data controllers? 7. Who supervises a data controller?

As for the knowledge acquisition phase, we elicited domain expert conceptual knowledge to support our modeling decisions. We manually harvested from

normative frameworks, particularly the DPD, the GDPR[7], and the Handbook on European data protection law [16].

Concerning non-functional requirements, this ontology is expressed in Web Ontology Language (OWL) [5] and uses Protégé [30] as the ontology development environment. A graphical depiction of the ontology is shown in Figure 1. The framework presented in this paper relies on previous efforts of the community in the field of legal knowledge representation, therefore we reuse concepts from LKIF Core and SKOS.

3.2 Describing data protection concepts

The conceptualization activity implies the organization and conversion of the informally perceived image of our domain into a semi-formal specification. Therefore, ontology components (concepts, attributes, relations, formal axioms and instances) were compiled using the sources described, and are here articulated through a task-oriented approach, to restate the informal competency questions.

A glossary of data protection terms was built and is provided together with the ontology[8].

The ontology's architecture follows the high-level partitioning structure of European data protection rules outlined by [16], and therefore it is made up of the following blocks:

1. the basic data protection principles;
2. the rules of data processing (constituting most of the duties of the data controller);
3. the data subject's rights.

An ontology entails a given level of consensus in a particular community. Within the data protection domain this includes basic data protection principles, as they have been established over the years by the Council of Europe (CoE), the EU, and the national DPAs. These serve as the foundation for our ontology. It is from these concepts that we derive and define the conceptual obligations of the data controller while contrasting them to the rights of the data subject. The result of the principles analysis is a set of ontology classes, their attributes and the relations between them.

The following is an enumeration of some of the principles, as classified under the European Data Protection Handbook [16]: lawfulness principle; purpose limitation principle (personal data must be processed for specified and lawful purposes); data quality principles (data must be adequate, relevant and not in

[7] Subject to changes in the final text - we used the official Commission text, COM(2012) 11 final. To better sharpen the scope, the ontology does not refer to decisions of courts or DPAs. The purpose is not to define a model of the legal text, but to model the requirements that the controller must meet to be compliant with the legislation.

[8] See footnote 15 *infra*.

excess in relation to the purpose of the processing, accurate, up to date); principle of data minimization, among others. A more detailed description of the principles underlying the ontology is given in [7].

The data protection principles constitute the unifying harmony underlying a controller's obligations (called *Rules* in the ontology, to ensure consistency with the knowledge sources) and data subject's rights. Since they are reifications of the general principles, in the ontology every data processing rule or data subject's right is a subclass of some principles. For example, the LawfulnessPrinciple entails a LawfulnessRule, which *is a* processing rule, and can consist of the data subject's Consent, a LegalObligation of the controller, a VitalInterest, a Contract, and so on.

To relate the data subject's rights with the corresponding rules of the controller, we define the deontic concepts in terms of correlative relations between right and rule (obligation), assuming symmetric roles. For example, the data subject's right to access corresponds to the obligation of the controller to provide means to request access to the data. To exercise the right, the data subject must perform a single access, which, by means of an object property, is defined in terms of the right to access, and is bound by a relationship with the data for which access is requested; similarly, the data subject can exercise the right to object to the processing of personal data. The objection, connected to the right to object, is related to a specific processing by a functional property called isObjected, defined in the domain of Processing. This property is also used to define the lawfulness of the processing, because personal data cannot be lawfully processed if the data subject has exercised the right to object.

Table 1 shows the hierarchy of the main concepts of the ontology.

Root Classes	**Subclasses**
Data Processing	Processing activity, Processing Mode, Lawful processing
Data Subject Right	Right to rectification, Right to object, Right to no profiling, right to portability, right to erasure
Processing Rule	Compliance, Impact Assessment, Transparent information, Security, Lawfulness Rule

Table 1. Top-level hierarchy.

Relations bind two resources (normally classes), and for each relation a *domain* and a *range* can be defined. A domain is the set of possible classes where the relation can be applied, and a range is the set of possible values of a relation. Table 2 shows the main relations in the ontology.

To formalize the ontology, a useful subset of classes were reused from LKIF Core in order to offer a solid support for the acquisition, sharing and reuse of legal knowledge. LKIF Core [23] is an established legal ontology. Our most generic concepts were linked with LKIF-Core concepts (such as the right, rule,

Relation	Domain	Range
hasObligation	Controller	Legal Obligation
notifyBreach	Controller	Data Breach
consentGrantedBy	Consent	Data Subject
AccessData	Right of Access	Personal Data

Table 2. Main relations.

legal person and natural person) using the SKOS data model[9]. Our alignment is compliant to it, but axiomatizes domain concepts of data protection, which is our priority and ontological commitment. There was therefore no need to extend the core ontology.

The main ontology metrics are summarized in Table 3.

Axiom	822
Logical axiom count	279
Class count	88
Object property count	42
Data property count	3
Individual count	16
DL expressivity	ALCHOIQ(D)
SubClassOf axioms count	114
EquivalentClasses axioms count	25
DisjointClasses axioms count	7

Table 3. Ontological components.

3.3 Evaluation

To evaluate the technical quality and consistency checking of the ontology, we used OntOlogy Pitfall Scanner! (OOPS!)[10] as pitfall detector. The results of the analysis were evaluated, and we assert no problems or inconsistencies were found in the ontology. The ontology documentation, containing the classes, properties and individuals, is available online[11], built using the Live OWL Documentation Environment (LODE) tool.

The usage of informal CQs for ontology requirements' description and its further evaluation has already been accounted [21] in ontology design methodologies. In fact, the ability to answer a CQ meaningfully can be regarded as a functional requirement that must be satisfied by the ontologies. The CQs presented in subsection 3.1 were built into a set of SPARQL Protocol and RDF Query Language (SPARQL) queries. The execution of the evaluation environ-

[9] `http://www.w3.org/2009/08/skos-reference/skos.html`.

[10] `http://oops.linkeddata.es/`.

[11] `http://www.essepuntato.it/lode/owlapi/https://raw.githubusercontent.com/guerret/lu.uni.eclipse.bpmn2/master/resources/dataprotection.owl`.

ment[12] showed that the ontology is able to answer those CQs (except #6, since the fines are not modeled in the ontology yet). For example, a SPARQL query requesting the rights of the data subject returns the following result: RightToPortability, RightToInformation, RightToObject, RightToRectification, RightOfAccess, RightToErasure, RightToNoProfiling, TransparentInformation.

4 Extending business process notation

The ontology described in section 3 can be used to aid a data controller in being compliant with the GDPR. When developing a software system, the PbD approach mentioned in section 2 means that the development cycle should address data protection. The development cycle is a workflow which can be expressed by means of formal notations such as Unified Modeling Language (UML) [25]. However, UML is domain-neutral. To express data protection, the data protection ontology would be useful: by exploiting UML's extensibility features [3], such as profiles, the expressiveness of (for example) activity or sequence diagrams can be enhanced, to specify data protection activities or requirements that a certain software routine, component, class should address.

But this is not sufficient for GDPR compliance. Many of the obligations of the GDPR involve organizational requirements as a risk assessment, and sometimes manual processing is required. Some of these activities have nothing to share with software development, but are still subject to the GDPR.

In this perspective, business processes [13] are more suited to embrace all the activities that can be subject to the GDPR, whether they are performed manually or software-based, or have a technical or organizational nature. Business processes are used to provide a description of the relationships between the various activities performed within a business, at various degrees of detail [37].

Various notations exist for specifying business processes, the most popular of which are Web Services Business Process Execution Language (WS-BPEL) [4] and Business Process Model and Notation (BPMN) [2], which have some similarities but still differ in scopes and domains [35]. They are based on an eXtensible Markup Language (XML) grammar and have extensibility features, including the possibility of using tags from different XML languages such as the OWL/XML serialization of the ontology. We chose to implement an extension of BPMN to demonstrate the possibilities offered by the present work, but the methodology is a general one that can be applied to any extensible notation.

Introducing data protection requirements by means of an ontology is a methodology that can be used in conjunction with different technologies, and it also provides a means to make heterogeneous models interoperable. In other words, the description of a workflow process might use different models at different levels e.g., UML and BPMN: if both are extended using the same ontology, the data protection requirements would be consistent, thus easing the integration and auditing of the overall workflow.

[12] The environment is available together with the Eclipse plugin described in subsection 4.1. See footnote 15 *infra*.

It would be easy to extend the methodology to use different ontologies. By using an ontology expressing the legal requirements in a specific domain (e.g., regulations for financial or healthcare services), this can be an effective method to model a clear and immediate view of the requirements in a workflow.

4.1 BPMN implementation

The proposed approach has been integrated, although at a basic level, in a BPMN 2.0 modeling tool. BPMN does not have a uniform implementation. Although it is defined as a standard, it is designed so that its implementation is platform-specific. For the purposes of the present paper, we have selected the Eclipse BPMN2 Modeler[13]. It is an Eclipse plugin which implements BPMN features using Model-Driven Engineering (MDE) techniques and the Ecore metamodel. The Eclipse version used is 4.5 (Mars).

The BPMN standard defines several different diagrams (Process, Collaboration, Choreography and Conversation) which serve different purposes. For this example, we only focused on the Process diagram, although the same methodology can be extended to all diagram types. We created an Eclipse extension plugin for BPMN, defining a new type of Task called Data Protection Task. The new task type has a distinctive graphical appearance (marked with a red icon) and supports annotations extracted from the ontology. The properties of the new Data Protection Task include a new tab which allows to introduce the annotations for data protection.

The implementation of the form to add the annotations parses through the data protection ontology using the OWL Application Programming Interface (API)[14]. Since our purpose is to offer a way to specify the activities that a data controller must perform for GDPR compliance, the reasoner selects the OWL classes that are descendants of the Rule class. This is a rough implementation, but it can be refined at the desired level, using the ontology structure or its instances, adding extra parameters and so on.

Figure 2 shows the interface of the extension plugin in operation and a sample application of the extended notation[15]. The example, which is built upon the official BPMN example from [1, p. 170], is not a real business process, but only aims at showing the possibilities of our approach. Some Tasks have been replaced with Data Protection Tasks. So, for example, the Handle Order activity has been annotated with the following three ontology classes:

Consent because the data subject must consent to the processing;
Security to ensure the protection of security measures;
AppropriateSafeguards because the customer's data might have to be transmitted to a vendor which might be located in a non-EU country.

[13] https://www.eclipse.org/bpmn2-modeler/
[14] `http://owlapi.sourceforge.net/`
[15] The sources are available at `https://github.com/guerret/lu.uni.eclipse.bpmn2`. The "resources" folder contains the OWL file with the ontology, the SPARQL queries and the glossary.

5 Conclusions

In this work, the authors have presented two artifacts: an ontology to model data protection requirements, and an approach for integrating it into a workflow to express the GDPR requirements within a business process by means the ontology. Our main objective is that the ontology will to assist data controllers in achieving compliance with the upcoming data protection reform. We aim to achieve this with a rigorous evaluation of the ontology and its extension to business process modelling within the data protection domain in the next phase of this research.

The ontology was modeled by a legal expert. The provisions that contain duties for the data controller and rights for the data subject have been selectively identified and built into the ontology. The granularity of the ontology is still coarse. High detail would be required in a judicial perspective, but not in the scope of the current research. However, some of the concepts expressed in the ontology appear to be generic or evaluative because they are expressed as such in the law, and not fit for direct usage. These concepts must be coordinated with knowledge from other domains. Computer security standards can partly fill these gaps, so understanding the relationship between them and the GDPR would be key to a fast transition to the new legislation.

This ontology is by definition a work in progress. It will have to be adapted to the changes in the legal text when a final version of the GDPR is released. However, in the final text, the core concepts expressed in the ontology won't drift significantly from the current ones. This structure is the basis for further refinements. It will act as a starting point which was necessary to pursue the long-term goal of verifying compliance with the GDPR. An improved version of the ontology is currently under development. It will feature a much broader and complete perspective on the GDPR, and will be designed to address many provisions not covered by the current version.

The workflow integration is an intuitive and simple way of expressing the GDPR requirements within the workflow. While not as rich and complex as some of the languages and models used in requirements engineering (such as SysML [19]), it clearly expresses the relationship between specific duties of the data controller and the workflow activities where the duties apply.

The approach presented in this work may ease the transition from the DPD to the GDPR and provide a basis for the PbD model. It can provide benefits to all end-users. Data controllers and processors will be able to determine what their duties are, on the basis of the rights of the data subject. Auditors will have a structured knowledge that can dissipate the mists of terminological uncertainties. DPAs can speed up their procedures thanks to a clearer notation. The formalization of the meaning of legal terms in an ontology could help compare the impact of the new legislation on the existing national regimes, as well as overcome linguistic differences in data protection across the EU. Also, expressing the controllers' requirements through an ontology will allow them to easily adapt designs to changes in the law and its interpretation, in a dynamic perspective.

The ontology may encompass automated classification to facilitate finding documents. Querying performance is foreseen as a future development in our

ontology, using SPARQL-DL to ascertain the corresponding rights and duties. For example, a database structured according to the ontology could be queried by data subjects to retrieve the rights and remedies in case of breaches and violations; by data controllers, to understand their obligations; by data processors, to clarify their functions.

The long-term aims of the current research focus on assessing compliance to the GDPR by means of security standards. This purpose will require development a similarly-structured ontology for security standards and a methodology to compare the degree of overlapping between the two normative bodies.

From a technical perspective, there are a number of improvements that can be investigated as well. The sample plugin introduced in section 4 could benefit from a more formal implementation using MDE, for example by defining the meta-model of the extension, integrating it with the meta-models of BPMN and OWL, and using it to generate the supporting classes.

Regardless of the underlying technologies used, the integration of the SDLC or business process notation with the data protection annotations from the ontology could also be enhanced with metrics to analyze the degree of coverage of the GDPR. Finally, when the ontology reaches a sufficient degree of maturity, a full-fledged real-world scenario will be modeled using the proposed notation.

References

1. BPMN 2.0 by example. Tech. Rep. dtc/2010-06-02, Object Management Group (June 2010)
2. Business process model and notation (BPMN). Tech. Rep. formal/2011-01-03, Object Management Group (January 2011)
3. Alhir, S.S.: Guide to Applying the UML. Springer Professional Computing, Springer New York (2002)
4. Alves, A., Arkin, A., Askary, S., Barreto, C., Bloch, B., Curbera, F., Ford, M., Goland, Y., Guízar, A., Kartha, N., Liu, C.K., Khalaf, R., König, D., Marin, M., Mehta, V., Thatte, S., van der Rijn, D., Yendluri, P., Yiu, A.: Web services business process execution language version 2.0. Tech. rep., OASIS (April 2007), `http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html`
5. Antoniou, G., van Harmelen, F.: Web Ontology Language: OWL. In: Staab, S., Studer, R. (eds.) Handbook on Ontologies, chap. 4, pp. 67–92. International Handbooks on Information Systems, Springer Berlin Heidelberg, second edn. (2004)
6. Bartolini, C., Gheorghe, G., Giurgiu, A., Sabetzadeh, M., Sannier, N.: Assessing IT security standards against the upcoming GDPR for cloud systems. In: Proceedings of the Grande Region Security and Reliability Day (GRSRD) 2015. pp. 40–42 (March 2015)
7. Bartolini, C., Muthuri, R.: Reconciling data protection rights and obligations: An ontology of the forthcoming eu regulation. In: Proceedings of the Workshop on Language and Semantic Technology for Legal Domain (LST4LD), Recent Advances in Natural Language Processing (RANLP) (September 2015), to be published.
8. Breuker, J., Hoekstra, R.: Epistemology and ontology in core ontologies: FOLaw and LRI-Core, two core ontologies for law. In: Proceedings of the Workshop on Core Ontologies in Ontology Engineering (EKAW) (October 2004)

9. Cappelli, A., Lenzi, V.B., Sprugnoli, R., Biagioli, C.: Modelization of domain concepts extracted from the Italian privacy legislation. In: Proceedings of the 7^{th} International Workshop on Computational Semantics (IWCS-7) (January 2007)
10. Casellas, N.: Legal Ontology Engineering Methodologies, Modelling Trends, and the Ontology of Professional Judicial Knowledge, Law, Governance and Technology Series, vol. 3. Springer Netherlands (2011)
11. Casellas, N., Nieto, J.E., Roig, A.M.n.A., Torralba, S., Reyes, M., Casanovas, P.: Ontological semantics for data privacy compliance: The NEURONA project. In: Proceedings of the Intelligent Privacy Management Symposium. pp. 34–38 (March 2010)
12. Corcho, O., Fernández-López, M., Gómez-Pérez, A., López-Cima, A.: Building legal ontologies with METHONTOLOGY and WebODE. In: Benjamins, V.R., Casanovas, P., Breuker, J., Gangemi, A. (eds.) Law and the Semantic Web, Lecture Notes in Computer Science, vol. 3369, pp. 142–157. Springer Berlin Heidelberg (2005)
13. Davenport, T.H., Short, J.E.: The new industrial engineering: Information technology and business process redesign. Sloan Management Review 31(4), 11–27 (Summer 1990)
14. Davis, R., Shrobe, H., Szolovits, P.: What is a knowledge representation? AI Magazine 14(1), 17–33 (Spring 1993)
15. European Commission: A digital single market strategy for Europe. `http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN` (May 2015)
16. European Union Agency for Fundamental Rights: Handbook on European data protection law (April 2014)
17. Fernández, M., Gómez-Pérez, A., Juristo, N.: METHONTOLOGY: From ontological art towards ontological engineering. In: Proceedings of the Ontological Engineering AAAI-97 Spring Symposium Series. pp. 33–40 (March 1997)
18. Fernández López, M., Gómez-Pérez, A., Pazos Sierra, J., Pazos Sierra, A.: Building a chemical ontology using methontology and the ontology design environment. IEEE Intelligent Systems 14(1), 37–46 (January–February 1999)
19. Friedenthal, S., Moore, A., Steiner, R.: A practical guide to SysML: the systems modeling language. Morgan Kaufmann, third edn. (2014)
20. Gómez-Pérez, A., Fernández-López, M., Corcho, O.: Ontological Engineering: With Examples from the Areas of Knowledge Management, e-Commerce and the Semantic Web. Advanced Information and Knowledge Processing, Springer London (2004)
21. Grūninger, M., Fox, M.S.: The role of competency questions in enterprise engineering. In: Rolstadås, A. (ed.) Benchmarking - Theory and Practice, pp. 22–31. IFIP Advances in Information and Communication Technology, Springer US (1995)
22. Hesse, W.: Ontologies in the software engineering process. In: Lenz, R., Hasenkamp, U., Hasselbring, W., Reichert, M. (eds.) Proceedings of the 2^{nd} GI-Workshop on Enterprise Application Integration (EAI). pp. 3–15 (June 2005)
23. Hoekstra, R., Breuker, J., Di Bello, M., Boer, A.: LKIF Core: Principled ontology development for the legal domain. In: Breuker, J., Casanovas, P., Klein, M.C., Francesconi, E. (eds.) Law, Ontologies and the Semantic Web: Channelling the Legal Information Flood, Frontiers in Artificial Intelligence and Applications, vol. 188, pp. 21–52. IOS Press (January 2009)
24. International Organization for Standardization: ISO/IEC 27001 – Information technology – Security techniques – Information security management systems – Requirements, second edn. (October 2013)

25. Jacobson, I., Booch, G., Rumbaugh, J.: The Unified Software Development Process. Addison-Wesley, Reading, Massachussetts (1999)
26. Kost, M., Freytag, J.C., Kargl, F., Kung, A.: Privacy verification using ontologies. In: Proceedings of the Sixth International Conference on Availability, Reliability and Security (ARES). pp. 627–632 (August 2011)
27. Massacci, F., Prest, M., Zannone, N.: Using a security requirements engineering methodology in practice: The compliance with the Italian data protection legislation. Tech. rep., University of Trento (November 2003)
28. Mikkonen, T.: Perceptions of controllers on EU data protection reform: A Finnish perspective. Computer Law & Security Review 30(2), 190–195 (April 2014)
29. Mitre, H.A., González-Tablas, A.I., Ramos, B., Ribagorda, A.: A legal ontology to support privacy preservation in location-based services. In: Meersman, R., Tari, Z., Herrero, P. (eds.) On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, Lecture Notes in Computer Science, vol. 4278, pp. 1755–1764. Springer Berlin Heidelberg (2006)
30. Noy, N.F., Sintek, M., Decker, S., Crubézy, M., Fergerson, R.W., Musen, M.A.: Creating semantic web contents with Protégé-2000. IEEE Intelligent Systems 16(2), 60–71 (March–April 2001)
31. Paulheim, H., Probst, F.: Ontology-enhanced user interfaces: A survey. International Journal on Semantic Web & Information Systems 6(2), 36–59 (April 2010)
32. Pfleeger, C.P., Pfleeger, S.L.: Security in Computing. Prentice Hall, Upper Saddle River, NJ, USA, fourth edn. (October 2006)
33. Rahmouni, H.B., Solomonides, T., Casassa Mont, M., Shiu, S.: Privacy compliance and enforcement on European healthgrids: an approach through ontology. Philosophical Transactions of the Royal Society A 368(1926), 4057–4072 (September 2010)
34. Rebstock, M., Fengel, J., Paulheim, H.: Ontologies-Based Business Integration. Business Information Systems, Springer-Verlag Berlin Heidelberg (2008)
35. Recker, J.C., Mendling, J.: On the translation between BPMN and BPEL: Conceptual mismatch between process modeling languages. In: Latour, T., Petit, M. (eds.) The 18^{th} International Conference on Advanced Information Systems Engineering. Proceedings of Workshops and Doctoral Consortium. pp. 521–532. Namur University Press (June 2006)
36. Reding, V.: The upcoming data protection reform for the European Union. International Data Privacy Law (November 2010)
37. Reijers, H.A.: Design and Control of Workflow Processes: Business Process Management for the Service Industry, Lecture Notes in Computer Science, vol. 2617. Springer-Verlag Berlin Heidelberg (2003)
38. Suárez-Figueroa, M.C., Gómez-Pérez, A., Motta, E., Gangemi, A. (eds.): Ontology Engineering in a Networked World. Springer Berlin Heidelberg (2012)
39. Suárez-Figueroa, M.C., Gómez-Pérez, A., Villazón-Terrazas, B.: How to write and use the ontology requirements specification document. In: Meersman, R., Dillon, T., Herrero, P. (eds.) On the Move to Meaningful Internet Systems: OTM 2009. Lecture Notes in Computer Science, vol. 5871, pp. 966–982. Springer Berlin Heidelberg (November 2009)
40. Uschold, M., Gruninger, M.: Ontologies: principles, methods and applications. The Knowledge Engineering Review 11(2), 93–136 (June 1996)
41. Van Alsenoy, B., Ballet, J., Kuczerawy, A., Dumortier, J.: Social networks and web 2.0: are users also bound by data protection regulations? Identity in the Information Society 2(1), 65–79 (December 2009)

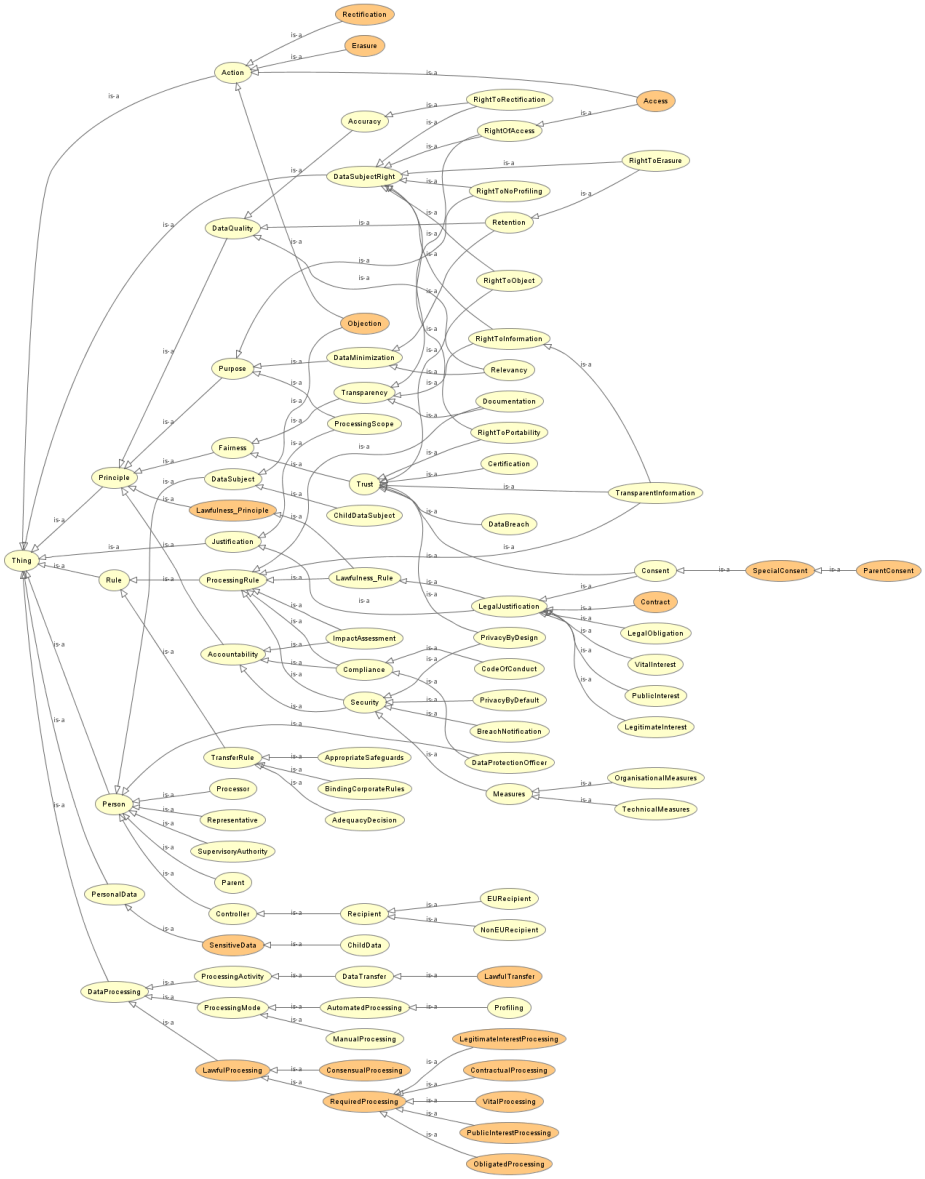
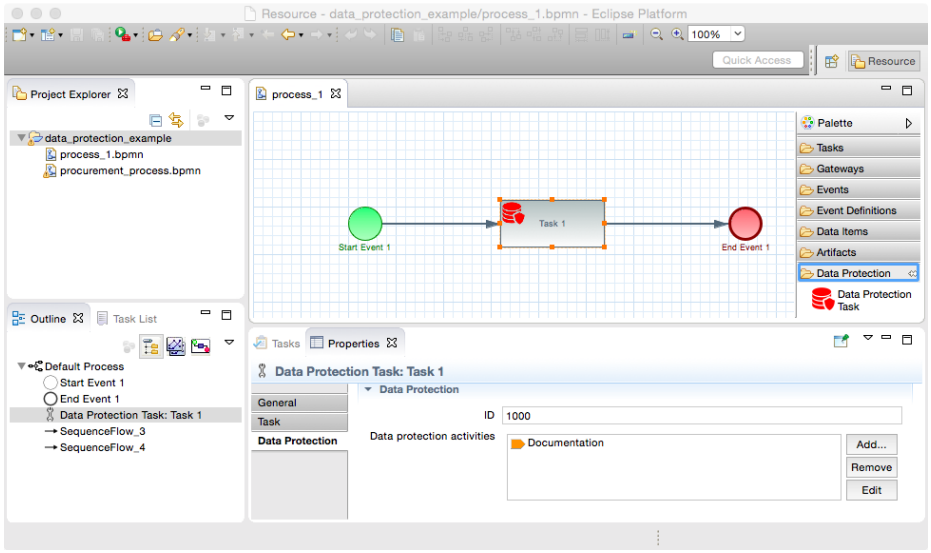
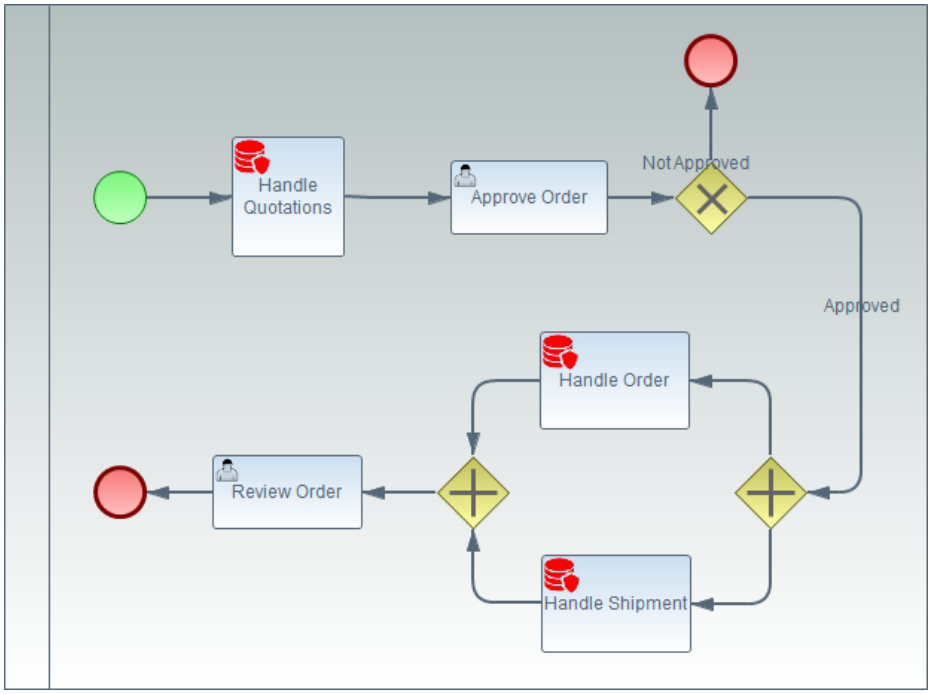


Fig. 1. Schema of the data protection ontology.



(a) The BPMN extension plugin.



(b) Procurement process example.

Fig. 2. The data protection ontology extension plugin.