Legal Knowledge and Information Systems
M. Palmirani (Ed.)

doi:10.3233/978-1-61499-935-5-91

Legal Ontology for Modelling GDPR Concepts and Norms

Monica PALMIRANI*, Michele MARTONI*, Arianna ROSSI*, Cesare BARTOLINI**, Livio ROBALDO**

**CIRSFID, University of Bologna.*
{monica.palmirani, michele.martoni, arianna.rossi}@unibo.it

*** SnT - Interdisciplinary Centre for Security, Reliability and Trust,*
Université du Luxembourg
JFK Building, 29, Avenue J.F. Kennedy, L-1855 Luxembourg
{cesare.bartolini, livio.robaldo}@uni.lu

Abstract. This paper introduces PrOnto, the privacy ontology that models the GDPR main conceptual cores: data types and documents, agents and roles, processing purposes, legal bases, processing operations, and deontic operations for modelling rights and duties. The explicit goal of PrOnto is to support legal reasoning and compliance checking by employing defeasible logic theory (i.e., the LegalRuleML standard and the SPINDle engine).

Keywords. Semantic web, legal reasoning, legal ontology, GDPR.

1. Introduction

The GDPR (General Data Protection Regulation) is the new common framework for data protection that applies to the whole European Union and harmonizes the legal principles of its Member States that can thus be more effectively applied in the Digital Single Market. The Regulation places upon entities involved in the processing of personal data a number of obligations, among which is the obligation to assess the risks they could encounter and adapt their duties on the basis of the impact assessment (Article 35, GDPR), whereas specific measures for the safeguard of data subjects' human dignity and fundamental rights are introduced. Instruments such as audits and compliance checking are intended to ensure the application of the principles of *data protection by design* (Article 25, GDPR) during software development (ex-ante phase), but also a punctual detection of violations (ex-post phase) when they occur. Since public administrations, enterprises and non-profit organizations alike will need to observe these newly-introduced, demanding duties, semantic web and legal reasoning techniques can offer a valuable support and ease compliance.

A legal ontology that formalizes data protection norms is therefore needed and timely. This paper introduces PrOnto [21], the privacy ontology that models the GDPR main conceptual cores: data types and documents, agents and roles, processing purposes, legal bases ex Article 6 GDPR, processing operations, and deontic operations for modelling rights (Chapter 3- articles 12-23) and duties (Chapter 4- articles 24-43). This ontology considers the GDPR as a starting point, however it is meant to be extended to the concepts and relative relations of other legal frameworks (such as

Member State laws). The explicit goal of PrOnto is to support legal reasoning and compliance checking by employing defeasible logic theory (i.e., the LegalRuleML standard [5] and the SPINDle engine [12]), as opposed to exclusively execute information retrieval. This article focuses on the analysis of deontic operators in order to manage the checking of compliance with the GDPR obligations. We use the Right to Data Portability (Art. 20) for illustrating the PrOnto benefits.

2. MeLOn Methodology

PrOnto was developed through an interdisciplinary approach called MeLOn (Methodology for building Legal Ontology), which has been successfully used to develop several legal ontologies by legal experts[1]. MeLOn is explicitly designed for legal ontologies and the related difficulties encountered by the legal operators during the definition of a model of reality through ontological techniques, such as Protégé, or patterns design method or the foundational approach.

The MeLOn methodology iterates over ten steps: 1) Describe the goal of the ontology; 2) Evaluation indicators. PrOnto's criteria, based on the existing state of the art, are [6]: (i) coherence, (ii) completeness, (iii) efficiency, (iv) effectiveness, (v) usability, (vi) agreement; 3) State of the art survey: PrOnto reuses existing ontologies, ontology patterns [13][14], and other existing domain vocabularies; 4) List the whole relevant terminology, extracted from legal sources, in particular legal definitions; 5) Use usable tools (such as tables, UML diagrams and the Graffoo tool); 6) Refine and optimize: an ontology expert manually adds the axioms; 7) Test the output in terms of completeness, effectiveness and usability; 8) Evaluate the ontology: OntoClean method and SPARQL queries; 9) Publish the document with the LODE tool [20]; 10) Collect feedbacks from the community in order to reach the agreement criteria. The MeLOn methodology allows to successfully work within interdisciplinary group that include engineers, lawyers, linguists, logicians and ontologists, and to model the legal knowledge rapidly and accurately while integrating the contributions of different disciplines.

3. The Right to Data Portability

Chapter 3 of GDPR lists all the rights of the data subject (right to access, right to be forgotten, right to portability, right to erasure, etc.) and Chapter 4 the duties for the controller and processor (such as the obligation to notify the data breach to the data subject). PrOnto aims at modelling the deontic operators (right, obligation, prohibition, permission) but also customize the obligations and rights for the GDPR. In particular we consider the Right to Data Portability (Art. 20). The Right to Data Portability is a complex right composed basically of two obligations:

"*1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:*

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means."

[1] http://amsdottorato.unibo.it/8215/; http://amsdottorato.unibo.it/7804/; http://amsdottorato.unibo.it/7261/.

The Right to Data Portability involves the Controller that has the obligation to take some Steps (see Fig.1). A Step is executed by Actions and each Step commits LegalRules, in our case *ObligationOfPortability* The actions involved are “Provide” personal data to the data subject, and “Transmit” the same data also to other controllers. The data type is determined by the action performed by the Controller. This means that all the personal data provided by the data subject or observed are involved in this obligation. The personal data inferred, derived or stored by the Controller are not a matter of this Right[2].

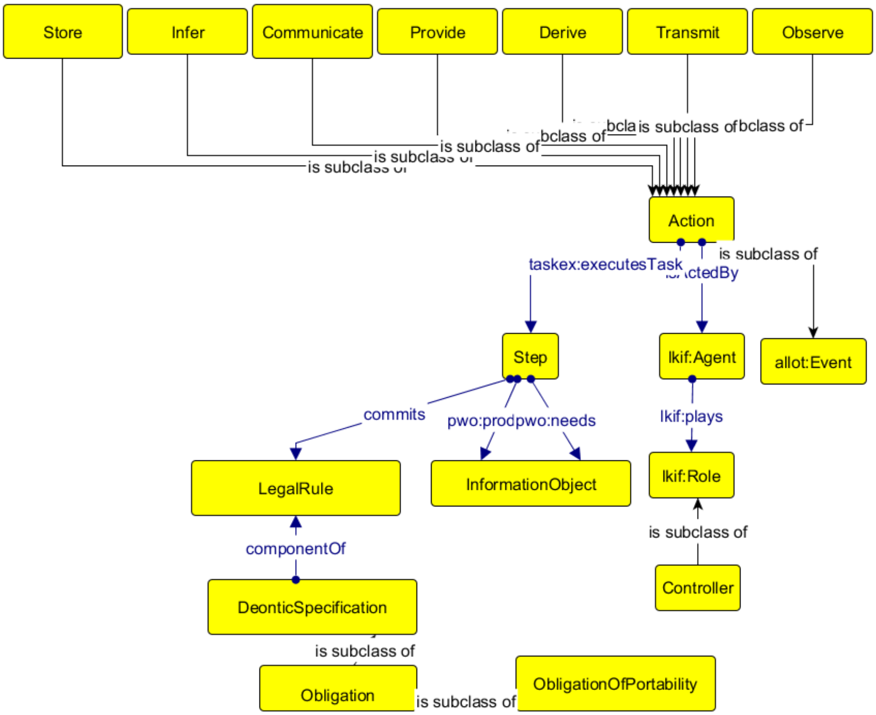

Figure 1 - Fragment of PrOnto concerning the ObligationOfPortability

4. PrOnto Modules

PrOnto is composed by modules, following the main structure of the GDPR legal principles: i) data and documents, ii) agents and roles, iii) processing purposes and legal bases; iv) data processing and workflow, risk management, and v) legal rules and deontic operators. Some documents and data refer to the data subject, which is a role of an agent (natural person). Data is processed following a given workflow, i.e., a plan of actions. When it is executed, each action assumes specific temporal parameters (e.g., interval of time of the processing), context (e.g., jurisdiction where the data processing

[2] Article 29 WP 242 rev.01 “In contrast, inferred data and derived data are created by the data controller on the basis of the data “provided by the data subject”. For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as “provided by” the data subject.”

is carried out), and value (e.g., place where the data processing is performed). The processing is lawful only if a legal basis is provided. Each processing activity involves a number of stakeholders: controller, processor, and other actors, and each has obligations or rights (for instance, data subjects have data protection rights). Such rights and obligations are linked to documents where the provisions appear, such as terms of use, information, privacy policies, consent forms.

4.1. Data and Document

In the context of data protection, personal data (Article 4.1(1)) is the object of the Regulation and the target of its protection, but data are also the information source that regulates the relations among different agents (e.g., controller, processor, etc.) using privacy policies, informed consent, contracts, codes of conduct, law, case-law, and any other legal document. Since data and documents are documental sources, the FRBR[3] ontology is employed: their representation over time can thus be modelled by following a robust design pattern that has been adopted for the publication process. Data is organized in the categories defined in the GDPR: personal data (Article 4.1(1)), non-personal data, anonymized data, pseudonymised data (Article 4.1(5)). The duties and rights depend on the type of data. For instance the DPO (Data Protection Officer) is mandatory for processing “a large scale of special categories of data” (Art. 9). This is why a specific version of data can be detected by using the time when the event occurred (e.g., a data breach event) and the dynamic versioning of the FRBR model is applied also to the class data.

4.2. Agent and Role

Agents and roles are frequently mistaken in legal ontologies. PrOnto, on the contrary, distinguishes the two classes. An agent might play multiple roles in different processing operations or contexts (e.g., a controller could act as processor or third party in relation to different data processing activities). Not only physical persons and organizations are included in the agents’ class, but also IT organizations, artificial intelligence and software, or robots. Each role is fixed in a given time period, which is linked to the time version of the dataset and the duration of the data processing. This implies that there is an event that assigns the role to an agent (e.g., designation of the processor by the controller ex Article 28, GDPR). Concerning the different roles, we have the Controller that *isRepresentedBy* a Representative in the European Union (Art. 27), *designates* a DPO and *nominates* a Processor.

4.3. Purposes and Legal Basis

Under the GDPR, personal data processing (Article 4.1(2)) is lawful only if motivated by a purpose that must be supported by a legal basis (see Article 6, GDPR, on the lawfulness of processing). This is why a lawfulness status was needed and was thus added as a Boolean data property of the PersonalDataProcessing class, whilst each personal data processing is based on a Purpose.

[3] FRBR— Functional Requirements for Bibliographic Records https://www.ifla.org/publications/functional-requirements-for-bibliographic-records

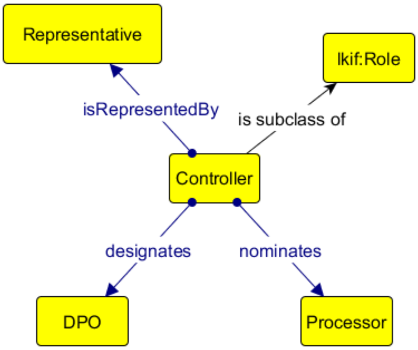

Figure 2 - Controller class and its proprieties

By modelling the knowledge in this manner, a rule engine that, for instance, is based on a rule-based language such as LegalRuleML is able to return this value after the rule reasoning process. The legal basis is also involved in the Right to Data Portability, considering that the Right is applicable only in the presence of a consent or a contract.

4.4. Data Processing

Human activities can be modelled through a workflow, i.e., a sequence of steps that takes some resources in input and produces certain outcomes. However, a workflow is composed of two parts: first a plan to do something is laid out (e.g., workflow), then the concrete sequence of actions is actually performed (e.g., execution of the workflow). This distinction is of utmost relevance in the GDPR framework: the plan (e.g., Impact Assessment Plan made by steps) is different from the real execution (e.g., the countermeasures acted in the event of a data breach), which is made up of a set of actions. Compliance checking presumes both a plan in line with the law, and countermeasures in the event of violations during the actual execution (e.g., remedies). For this goal, the Publishing Workflow Ontology (PWO) proved perfectly suitable as a basis to model the data processing ontology module because it includes both a workflow and an executed workflow. The workflow execution is composed by actions. An action [1] is a kind of event that is described by temporal parameters (e.g., interval) and contextual values (Time-indexed Value in Context - TVC). One of the values it can take is the place where the event occurs (e.g., within the EU borders) and the relevant jurisdiction (e.g., Regional competence). Other values and statuses can also be included to enrich the context description.

4.5. Deontic Operators

In order to model legal norms, deontic operators such as right, obligation, permission and prohibition are fundamental. Under the GDPR, it is also important to include violation/compliance as the status in which an obligation or a prohibition is violated or maintained. The deontic operators have temporal parameters and refer to a jurisdiction to consider those rights that are only effective in a specific domestic regulation. For all these reasons, this section of PrOnto allows to model those predicates that are necessary to implement legal rules and is an extension of the LegalRuleML metamodel, which allows the synchronization of the legal rule language modelling with the ontology.

This module also defines the relationships among deontic rules, actors' rights and obligations, obligations and permissions, and violation/compliance. This modelling allows the population of the ontology, or the creation of RDF triples, in order to perform queries such as "give me all the processing activities that have been violated by some actors in a given time". This knowledge is processed by the rule engine, but it is also transformed into individuals (e.g., materialization) of the ontology (or RDF triples) without the need to perform a query on the rule engine each time.

It is also worth noticing that, within the project DAPRECO [8], PrOnto is used to formalize GDPR in reified I/O logic [22], and in the Cloud4Eu is used with defeasible logic. In both cases formulae are connected to the concepts in PrOnto via the LegalRuleML constructs. This means that PrOnto is neutral respect the type of logic adopted.

4.6. Rights and Obligations relationships

For each obligation there is also a right connected with the data subject (Bearer). Fig. 3 shows how the ObligationOfPortability is connected to the RightToPortability using DeonticSpecification super class.

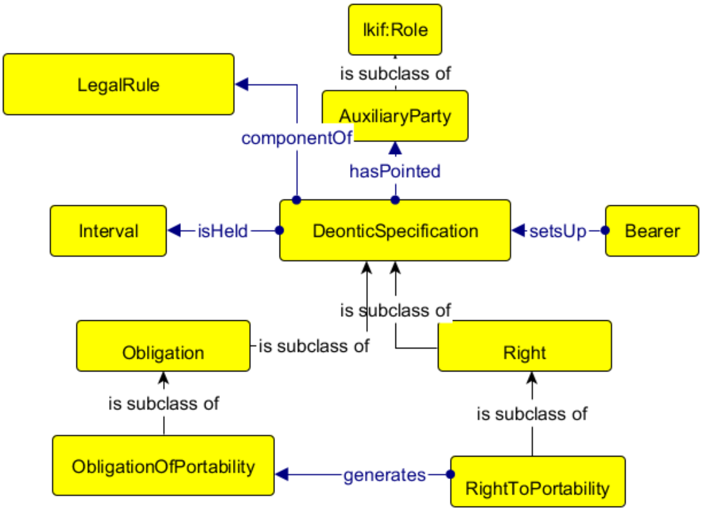

Figure 3: Right to Portability and Obligation of Portability

For implementing this fragment of ontology we have extended the LegalRuleML meta-model with several axioms. We report here some of axioms that intend to connect the right with the obligation and prohibition, and the right with the permission.

LegalRule	<owl:ObjectProperty rdf:about="https://w3id.org/ontology/pronto#componentOf"> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#DeonticSpecification"/> <rdfs:range rdf:resource="https://w3id.org/ontology/pronto#LegalRule"/>

	</owl:ObjectProperty>
isViolatedBy it defines the relationship between obligation/prohibition and violation	<owl:ObjectProperty rdf:about="https://w3id.org/ontology/pronto#isViolatedBy"> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Obligation"/> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Prohibition"/> <rdfs:range rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Violation"/> </owl:ObjectProperty>
isFulfilledBy	<owl:ObjectProperty rdf:about="https://w3id.org/ontology/pronto#isFulfilledBy"> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Obligation"/> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Prohibition"/> <rdfs:range rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Compliance"/> </owl:ObjectProperty>
Relationship between obligation and permission	<owl:ObjectProperty rdf:about="https://w3id.org/ontology/pronto#implies"> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Obligation"/> <rdfs:range rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Permission"/> </owl:ObjectProperty>
Relationship between prohibition and obligation	<owl:ObjectProperty rdf:about="https://w3id.org/ontology/pronto#isAKindOf"> <rdfs:domain rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Prohibition"/> <rdfs:range rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Obligation"/> </owl:ObjectProperty>
Right as a subclass of Permission	<owl:Class rdf:about="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Right"> <rdfs:subClassOf rdf:resource="http://docs.oasis-open.org/legalruleml/ns/v1.0/metamodel#Permission"/> </owl:Class>

Table 1 – Some axioms of the extension of the LegalRuleML ontology

4.7. Duties and Violation

Finally, the Steps are connected with LegalRuleML that is the deontic part of the ontology, capable to model and perform reasoning with right, obligation, permission, prohibition. The violation is connected with the obligation/prohibition that is violated and the compliance states when the obligation is complied with. In this way, we are able to detect the steps that create violations of some obligations and the connected risks, along with the related measures (see Fig. 4).

5. Evaluation

The evaluation is carried out inside the Cloud4EU European project PCP, that intends to provide legal compliance checking systems for eGovernment services that are delivered across the cloud. We are currently in the phase of testing PrOnto on three different scenarios related to school services. PrOnto is also used inside the MIREL European project and the DAPRECO Luxembourgish project.

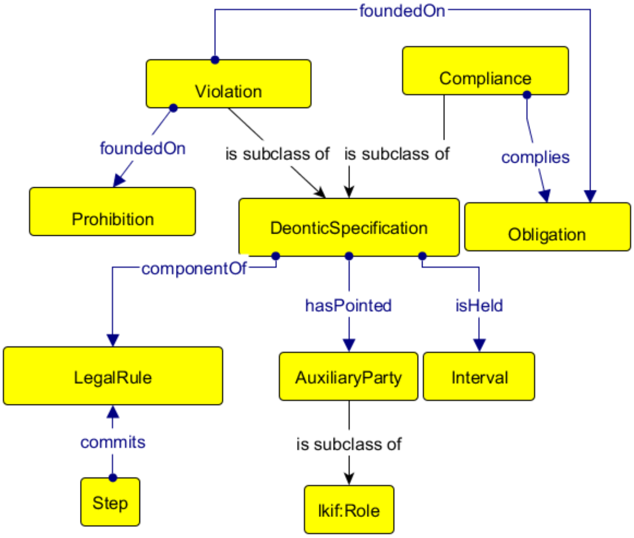

Figure 4: Violation, Compliance and Obligation, Prohibition

6. Related Work

A few privacy ontologies with specific goals [4]; [11]; have been designed, for instance the HL7 privacy ontology [13] for electronic health records. Other ontologies were created to ensure secure messaging among Internet of Things devices, whilst others are meant to manage data flows in the linked open data environment or on the blockchain. UsablePrivacy and PrivOnto [16] are more oriented to provide linguistic instruments in order to define glossary and taxonomy for the privacy domain, basically starting from the bottom-up annotation of the privacy policies (crowdsourcing annotation). GDPRtEXT [18] provides a list of concepts present in the GDPR text without really entering the modelling of the norms and the legal axioms (e.g., the actions performed by the processor, the obligations of the controller and the rights of the data subject). Morover GDPRtEXT does not foster FRBR information for managing versioning of the legal text over the time and consequently the changes of the legal concepts due to modifications in the legal system. GDPRov aims to describe the provenance of the consent and data lifecycle in the light of the Linked Open Data principles such as Fairness and Trust [17]. The SPECIAL Project[4] aims to provide tools for checking compliance in privacy domain. However, no ontology with foundational concepts, patterns, deontic operators and privacy principles has been designed to support legal

[4] https://www.specialprivacy.eu/

reasoning and check compliance yet. ODRL provides predicates and classes for managing obligations, permission, prohibitions, but several parts of the deontic logic are missing (e.g., right and penalty classes). ODRL is good for modelling simple policies capable to be searchable in SPARQL, but it is quite limited to manage the complex organization of the legal rules (e.g., exception in the constitutive rules or in the prescriptive rule). PrOnto is more exhaustive in this field. In order to do so, rights and obligations must be modelled through deontic operators. Moreover, actors and processing operations described in the normative prescriptions must also be included.
This is why PrOnto considers and reuses existing ontologies and follows ontology design patterns [21]: ALLOT [7], FRBR [15], LKIF we use in particular lkif:Agent to model lkif:Organization, lkif:Person and lkif:Role [9], the Publishing Workflow Ontology (PWO) [10]; Time-indexed Value in Context (TVC) and Time Interval [19].

7. Conclusions and Future Work

The existing privacy ontologies presented in the state of the art (e.g., HL7 for eHealth, PPO for Linked Open Data, ODRL for modelling rights, etc.) do not integrate deontic logic models that can be used for legal reasoning. PrOnto aims at the integration of different levels of semantic representation for multiple goals: 1) document and data modelling can support information retrieval in the Semantic Web, in particular with Linked Open Data (e.g., SPARQL queries); 2) workflow and processing modelling can represent helpful tools to plan privacy policies, but also BPMN modelling can be useful in system design (e.g., privacy-by-design); rights and obligations are necessary modules to enable automated legal reasoning that employ rule languages (e.g., LegalRuleML and compliance checking); 3) and finally, human-centered approaches can allow the visualization and the presentation of data protection principles and concepts in different contexts and directed to different audiences.
The research described in these pages has a long-term goal. Our intention is that of continuing the modelling and optimization of the formal model of the ontology, but also to evaluate it with a number of use-cases. In the meantime, we deem fundamental a discussion about the ontology within a large community, in order to establish consensus and to place such results in a standardization body for future governance (e.g., OASIS, W3C). In the future, it will also become necessary to develop specific profiles, one for each specific national law or even by thematic domain (e.g., Privacy in IoT, Privacy in AI, etc.).

Acknowledgements

This work was partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 690974 “MIREL: MIning and REasoning with Legal texts”, and by Luxembourg National Research Fund (FNR) CORE project C16/IS/11333956 “DAPRECO: DAta Protection REgulation COmpliance”.

References

[1] Abrams, M., 2014. The Origins of Personal Data and its Implications for Governance. SSRN Electron. J. https://doi.org/10.2139/ssrn.2510927

[2] Article 29 Working Party, 2018. Guidelines on Personal data breach notification under Regulation 2016/679 (No. wp250rev.01).

[3] Article 29 Working Party, 2017. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (No. wp248rev.01).

[4] Ashley, K.D., 2017. Artificial intelligence and legal analytics: new tools for law practice in the digital age. Cambridge Univ Press, Cambridge New York Melbourne Delhi Singapore.

[5] Athan, T., Governatori, G., Palmirani, M., Paschke, A., Wyner, A., 2015. LegalRuleML: Design Principles and Foundations, in: Faber, W., Paschke, A. (Eds.), Reasoning Web. Web Logic Rules. Springer International Publishing, Cham, pp. 151–188. https://doi.org/10.1007/978-3-319-21768-0_6

[6] Bandeira, J., Bittencourt, I.I., Espinheira, P., Isotani, S., 2016. FOCA: A Methodology for Ontology Evaluation. Eprint ArXiv.

[7] Barabucci, G., Cervone, L., Di Iorio, A., Palmirani, M., Peroni, S., Vitali, F., 2010. Managing semantics in XML vocabularies: an experience in the legal and legislative domain. Balisage Ser. Markup Technol. 5. https://doi.org/10.4242/balisagevol5.barabucci01

[8] Bartolini, Cesare, Andra Giurgiu, Gabriele Lenzini, and Livio Robaldo. 2016. Towards legal compliance by correlating standards and laws with a semi-automated methodology. In BNCAI, volume 765 of Communications in Computer and Information Science, pages 47{62. Springer.

[9] Breuker, J., Hoekstra, R., Boer, A., van den Berg, K., Sartor, G., Rubino, R., Wyner, A., Bench-Capon, T., Palmirani, M., 2007. OWL Ontology of Basic Legal Concepts (LKIF-Core) (Deliverable No. 1.4). IST-2004-027655 ESTRELLA: European project for Standardised Transparent Representations in order to Extend Legal Accessibility.

[10] Gangemi, A., Peroni, S., Shotton, D., Vitali, F., 2017. The Publishing Workflow Ontology (PWO). Semantic Web 8, 703–718. https://doi.org/10.3233/SW-160230

[11] Gharib, M., Giorgini, P., Mylopoulos, J., 2017. Towards an Ontology for Privacy Requirements via a Systematic Literature Review, in: Mayr, H.C., Guizzardi, G., Ma, H., Pastor, O. (Eds.), Conceptual Modeling. Springer International Publishing, Cham, pp. 193–208. https://doi.org/10.1007/978-3-319-69904-2_16

[12] Governatori, G., Hashmi, M., Lam, H.-P., Villata, S., Palmirani, M., 2016. Semantic Business Process Regulatory Compliance Checking Using LegalRuleML, in: Blomqvist, E., Ciancarini, P., Poggi, F., Vitali, F. (Eds.), Knowledge Engineering and Knowledge Management. Springer International Publishing, Cham, pp. 746–761. https://doi.org/10.1007/978-3-319-49004-5_48

[13] Health Level Seven International, 2015. HL7 Specification: Clinical Quality Common Metadata Conceptual Model, Release 1 (HL7 Informative Document).

[14] Hitzler, P., Gangemi, A., Janowicz, K., Krisnadhi, A., Presutti, V. (Eds.), 2016. Ontology engineering with ontology design patterns: foundations and applications, Studies on the semantic web. IOS Press, Amsterdam Berlin.

[15] IFLA Study Group on the Functional Requirements for Bibliographic Records, 1996. Functional Requirements for Bibliographic Records, IFLA Series on Bibliographic Control. De Gruyter Saur.

[16] Oltramari, A., Piraviperumal, D., Schaub, F., Wilson, S., Cherivirala, S., Norton, T.B., Russell, N.C., Story, P., Reidenberg, J., Sadeh, N., 2016. Privonto: A semantic framework for the analysis of privacy policies. Semantic Web (1-19).

[17] Pandit H.J., Lewis D., 2017. Modelling Provenance for GDPR Compliance using Linked Open Data Vocabularies, Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) co-located with the 16th International Semantic Web Conference (ISWC 2017), http://ceur-ws.org/Vol-1951/PrivOn2017_paper_6.pdf.

[18] Pandit H.J., Fatema K., O'Sullivan D., Lewis D., 2018. GDPRtEXT - GDPR as a Linked Data Resource. In: Gangemi A. et al. (eds) The Semantic Web. ESWC 2018. Lecture Notes in Computer Science, vol 10843. Springer, Cham.

[19] Peroni, S., Palmirani, M., Vitali, F., 2017. UNDO: The United Nations System Document Ontology, in: d'Amato, C., Fernandez, M., Tamma, V., Lecue, F., Cudré-Mauroux, P., Sequeda, J., Lange, C., Heflin, J. (Eds.), The Semantic Web – ISWC 2017. Springer International Publishing, Cham, pp. 175–183. https://doi.org/10.1007/978-3-319-68204-4_18

[20] Peroni, S., Shotton, D., Vitali, F., 2012. The Live OWL Documentation Environment: A Tool for the Automatic Generation of Ontology Documentation, in: ten Teije, A., Völker, J., Handschuh, S., Stuckenschmidt, H., d'Acquin, M., Nikolov, A., Aussenac-Gilles, N., Hernandez, N. (Eds.), Knowledge Engineering and Knowledge Management.

[21] Monica Palmirani, Michele Martoni, Arianna Rossi, Cesare Bartolini, Livio Robaldo: PrOnto: Privacy Ontology for Legal Reasoning. EGOVIS2018, 7th International Conference, EGOVIS 2018, Regensburg, Germany, September 3-5, 2018, Proceedings. LNCS 11032, Springer, pp. 139-152 (2018)

[22] Robaldo, L. and X. Sun. 2017. Reifed input/output logic: Combining input/output logic and reification to represent norms coming from existing legislation. The Journal of Logic and Computation, Vol. 7