Capturing the Basics of the GDPR in a Well-Founded Legal Domain Modular Ontology

Mirna EL GHOSH [a,1] and Habib ABDULRAB [a]

[a] *Normandie Université, INSA Rouen, LITIS, 76000 Rouen, France*

Abstract. The primary goal of the General Data Protection Regulation (GDPR) is to regulate the rights and duties of citizens and organizations over personal data protection. Implementing the GDPR is recently gaining much importance for legal reasoning and compliance checking purposes. In this work, we aim to capture the basics of GDPR in a well-founded legal domain modular ontology named OPPD (Ontology for the Protection of Personal Data). Ontology-Driven Conceptual Modeling (ODCM), ontology layering, modularization, and reuse processes are applied. These processes aim to support the ontology engineer in overcoming the complexity of the legal knowledge and developing an ontology model faithful to reality. ODCM is used for grounding OPPD in the Unified Foundational Ontology (UFO). Ontology modularization and layering aim to simplify the ontology building process. Ontology reuse focuses on selecting and reusing Conceptual Ontology Patterns (COPs) from UFO and the legal core ontology UFO-L. OPPD intends to overcome the lack of a representation of legal procedures that most ontologies encountered. The potential use of OPPD is proposed to formalize the GDPR rules by combining ontological reasoning and Logic Programming.

Keywords. GDPR, well-founded ontologies, Ontology-Driven Conceptual Modeling, ontology modularization, ontology reuse, Conceptual Ontology Patterns, Logic Programming

1. Introduction

The General Data Protection Regulation (GDPR)[2] is a European Union Regulation established in 2018 [1]. The GDPR regulates the rights and duties of citizens and organizations regarding the protection of personal data. It contains obligations concerning storing, processing, collecting, and disclosing data [2]. The implementation of GDPR is recently gaining much importance aiming to apply the Regulation in organizations [3,4,5]. Organizations seek to comply with the Regulation using technical measures to ensure that personal data processing follows GDPR [2]. In this context, a variety of approaches have been recently proposed such as AI-based [6,7,8], model-based [9], semantic annotation of text [10], and ontologies [11,12,13]. In this work, we are interested in ontologies. In

---

[1]Corresponding Author: El Ghosh Mirna, Normandie Université, INSA Rouen, LITIS, 76000 Rouen, France; E-mail: mirna.elghosh@insa-rouen.fr

[2]https://gdpr-info.eu/

the legal domain, ontologies are considered to establish the missing link between legal theory and AI & law [14]. They are defined as *generalized conceptual models of specific parts of the legal domain* [15]. They provide *stable foundations for knowledge representation* in this domain [15]. Legal ontologies have been developed and used for legal knowledge management and as knowledge bases in legal knowledge systems [16]. However, modeling legal knowledge is challenging due to the legal domain's complexity represented by regulations and legal rules. In the legal domain, legal conceptual knowledge is closely related to the language used in legal documents, which is usually considered complicated by non-experts [17]. Legal rules and standards are written, for the most part, in ordinary language containing ambiguities [18]. Specifically, we cite the incomplete definition of the law's legal concepts (e.g., consent, right, duty, etc.) [19].

To overcome these challenges, reusing foundational and/or core ontologies is recognized as a promising approach [20]. Foundational ontologies such as UFO [21], and DOLCE [22] define a range of top-level domain-independent ontological categories that form a general foundation for more elaborated domain-specific ontologies. Core ontologies such as UFO-L [23], and LKIF-Core [24] in the legal domain provide a precise definition of structural knowledge in a specific field that spans across different domain applications. Ontology reuse can also be accomplished using modeling solutions such as Ontology Patterns (OPs) [25]. OPs describe particular recurring modeling problems that arise in specific ontology development contexts, and present well-proven solutions for the problems [20]. In the legal domain, *part of the design problems can be simplified by creating or extracting conceptual ontology design patterns* [26].

In this paper, which is an extension of a prior introductory work[3], we aim to capture the essentials of GDPR in a *well-founded* legal domain ontology named OPPD (Ontology for the Protection of Personal Data). The concept of "well-founded" ontologies is addressed mainly in Guizzardi's [21] and Guarino's [27] studies. This concept means that ontologies are "faithful to reality" in the sense that *the basic primitives they are built on are sufficiently well-chosen and axiomatized to be generally understood* [27]. To Build OPPD, Ontology-Driven Conceptual Modeling (ODCM), ontology layering, modularization, and reuse processes are applied. ODCM, which is described by *applying ontological analysis based on foundational ontologies to improve the theory and practice of conceptual modeling* [28], is used for grounding OPPD in UFO. Ontology layering and modularization aim to simplify the building process. Ontology reuse focuses on selecting and reusing Conceptual Ontology Patterns (COPs) from UFO and UFO-L. Furthermore, these patterns are applied either by extension or analogy with the legal rules to build the domain content of OPPD. The intention of OPPD is to overcome the lack of a representation of legal procedures that most ontologies encountered. The potential use of OPPD is proposed to formalize GDPR rules by combining ontological reasoning and Logic Programming [29]. The rest of the paper is organized as follows. Section 2 outlines the background of this work. In Section 3, the methodology of building OPPD is presented. Section 4 describes OPPD. The ontology validation and evaluation are discussed in section 5. The ontology potential use is introduced in section 6. Section 7 analyzes the related work. Finally, sections 8 and 9 discuss and conclude the paper respectively.

---

[3]Abstract paper accepted at ICAIL's workshop (2019) - LegRegSW (Legislation and Regulation on the Semantic Web) - Available from: https://sites.google.com/view/legregsw2019/home

2. Background: UFO and UFO-L

This section outlines UFO [21] and UFO-L [23] as our study's background. UFO is a foundational ontology that employs results from formal ontology, cognitive psychology, linguistics, and philosophical logic. It is composed of three main layers: UFO-A [28] (ontology of substances), UFO-B [30] (ontology of events), and UFO-C [28] (ontology of social entities). UFO has been employed in the design of the ontologically well-founded conceptual modeling language OntoUML [21,31]. OntoUML uses the ontological constraints of UFO as modeling primitives and is specified above the UML2.0 meta-model [21]. We referred to UFO as a foundation since it comprises a rich theory of relations and complex relational properties absent in other foundational ontologies [32]. UFO has been successfully applied in many domains ranging from natural science to social domains [33]. Besides, the availability of OntoUML permits the building of ontologies by reusing the generic concepts of UFO as modeling primitives [34].

UFO-L is a legal core ontology developed based on UFO to represent Alexy's theory of fundamental rights [35]. UFO-L defines a variety of basic legal core concepts representing, among many others, *legal roles* (e.g., Right Holder, Duty Holder, etc.), *legal relators* (e.g., Right-Duty Relator, Power-Subjection Relator, etc.), *legal moments* (e.g., Right to an Action, Duty to Act, etc.). Besides, UFO-L specifies a variety of legal patterns representing *legal relators* such as Right-Duty to an Action Relator (Figure 1).
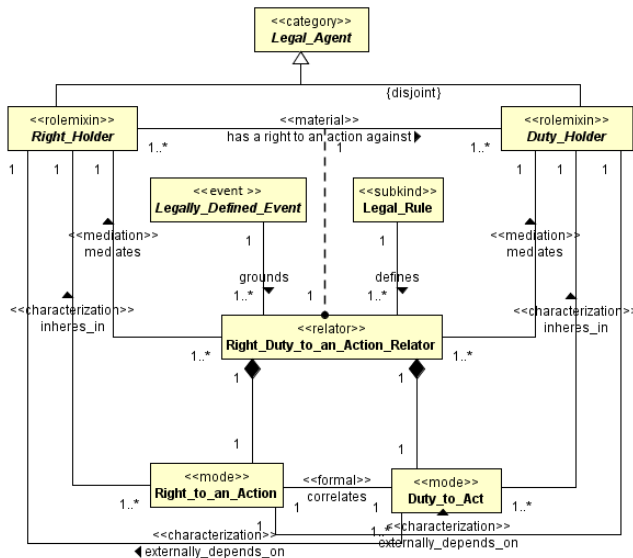

Figure 1. Right_Duty_to_an_Action_Relator represented in OntoUML (adapted from [23]).

The legal patterns aim to represent the legal relations and capture the legal roles played in the context of these relations [36]. In these patterns, legal relators, which are composed of two correlated legal moments, mediate two disjoint legal roles. Each legal moment is inherited in a legal role and externally dependent on the disjoint legal role [23]. In UFO-L, *legal moments* are based on *legal positions* in Alexy's theory. They are defined as situations in which a subject, in a legal relation, for instance, has a right or a power against another subject [34].

3. Methodology

The methodology of building OPPD, inspired by the Systematic Approach for Building Ontologies (SABiO) [25], is composed of five main phases. SABiO differs between *reference* and *operational* ontologies. The former category represents a particular kind of conceptual model developed to make the best possible description of the domain in reality [37]. The latter represents the implementation of reference models as machine-readable artifacts [25].

Ontology Specification   OPPD aims to capture the basics of the GDPR, especially the rights of natural persons (named *Data Subject*) to the protection of personal data regarding their processing by organizations (named *Controller* or *Processor*). Besides, the duties and responsibilities of organizations concerning the processing of personal data are also considered. For this purpose, we are referred to a corpus of selected articles and chapters that give rise to issues such as analysis, processing, and interpretation of personal data[4]. The corpus comprises mainly 45 articles that bear on norms. OPPD will be used to model and formalize the legal rules of the GDPR for legal reasoning or compliance checking purposes.

Ontology Requirements   They are composed of functional and non-functional. The functional, or *quality* requirements, describe the *goals for modeling* [38]. They are concerned with goals that should be achieved by the modeling process [38] and will be stated as competency questions (CQs) throughout the process. OPPD's functional requirements are: *R1*-To represent the GDPR main agents (e.g., natural persons, controller, public authorities, etc.) and objects (e.g., legal rules). *R2*-To define the essential events and situations (e.g., personal data processing, loss or destruction, infringement of regulation, etc.). *R3*-To determine the basic legal relationships and the active legal roles. Examples of legal relationships between the data subject and the controller are personal data processing, right-duty to rectify or erase data, and right-duty to withdraw consent. *R4*-To describe the legal moments that compose the legal relationships, such as the data subject's right against the controller to rectify his data. Moreover, OPPD has to fulfill the following non-functional requirements concerned with the ontology design: *R1*-The modularity of the ontology to simplify the building process. *R2*-The ontology model needs to provide a clear separation of the structural from the domain knowledge. *R3*-The ontology should be shareable and applicable for building automated applications.

Ontology Design   Aiming to simplify the building process of OPPD, we propose ontology layering that divides the ontology structure into three layers located at different granularity levels (see Figure 2). The *upper* layer, located at the most abstract level, contains domain-independent categories (e.g., agent, object, event, situation, etc.). The *core* layer includes categories commonly dependent on the legal domain (e.g., legal agent, legal rule, legal role, etc.). The *domain* layer describes the main categories of the GDPR (e.g., data subject, controller, personal data, consent, etc.). Besides, ontology modularization suggested in SABiO is applied within each layer to facilitate OPPD's building and permit reusing parts of the ontology. Three main ontology modules criteria are considered: independence, coherence and size [25]. Regarding the size, an ontology module aims to cover a sufficient understandable and graphically convenient representation of the problem addressed by this module.

---

[4]Available from: https://sites.google.com/view/legregsw2019/home

Conceptualization To develop the reference model of OPPD, a set of COPs, identified as ontology modules, are selected and reused from UFO and UFO-L to build the upper and core layers. Two main types of patterns are distinguished: *recognition* patterns defined as recurring set of concepts and relations and *template* patterns that describe a common perspective on how to solve a specific problem [39]. The recognition patterns are applied by extension for building the *static*, or *structural*, content of the domain layer. Meanwhile, the *template* patterns are applied by analogy with the legal norms for building the *dynamic*, or *procedural*, content. This phase is performed using ODCM to ground OPPD in UFO. Thus, the ontologically-founded conceptual modeling language OntoUML [21,31] is applied to represent the conceptual patterns and their application using the modeling primitives of UFO. Thereby, the OntoUML constraints for relating these primitives are respected (see Figure 2 for an example).

Ontology Validation and Evaluation This phase consists of (1) validating OPPD by transforming the reference model into an *operational* ontology represented using a computational language and (2) evaluating the ontology against the requirements.
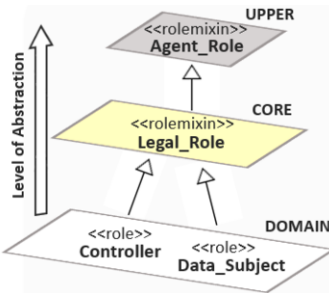

Figure 2. The layered structure of OPPD.

4. OPPD: The Reference Ontology Model

4.1. Upper and Core Layers

This section presents briefly part of the upper and core layers due to space limitation. For building the upper layer, three main COPs, considered as recognition patterns, are selected from UFO: Substance, Event and Moment.
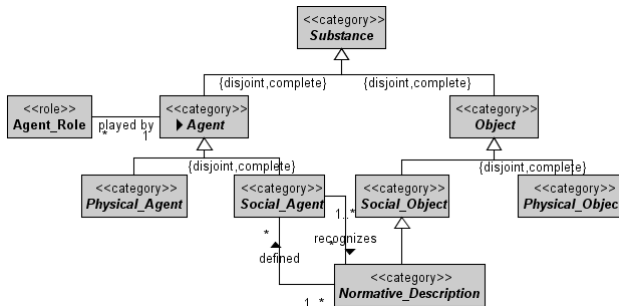

Figure 3. Substance ontology pattern (adapted from [28]).

In Figure 3, the Substance ontology pattern, which implements the functional requirement R1, is depicted. In this pattern, Substance can be Agent or Object. Normative_Description is a Social_Object recognized by at least one Social_Agent and Agent_Role is played by one Agent.

For building the core layer, different COPs are selected from UFO-L [23]. The recognition patterns are: Legal_Substance, Legal_Event, Externally_Dependent_Legal_Moment, and Legal_Relator. The template patterns are: Right_Duty_to_an_Action_Relator (Figure 1), Right_Duty_to_Omission_Relator, and Power_Subjection_Relator [23]. In Figure 4, Externally_Dependent_Legal_Moment, which implements the functional requirement R4, is depicted. In this pattern, different legal moments are considered [36]: Right (i.e., legal moment in which one may demand from another the performance of a certain conduct), Right_to_an_Action, Duty (converse moment of Right), Duty_to_Act, Legal_Power (i.e., ability to act to a power holder), Legal_Subjection (converse moment of Legal_Power), Disability (i.e., no power to create, change or extinguish a legal moment), and Immunity (converse moment of Disability).
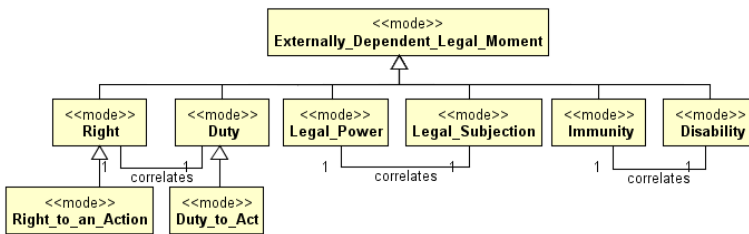

Figure 4. Externally_Dependent_Legal_Moment ontology pattern (adapted from [23]).

4.2. Domain Layer

This section addresses OPPD's domain layer developed by applying the core layer's patterns. The domain layer's static content is obtained by extending the core layer's recognition patterns. For this purpose, a list of competency questions (CQs) is outlined to fulfill the functional requirements R1 and R2, such as: (CQ1) What are the leading legal agents defined in the GDPR? (CQ2) What are the main legal objects? (CQ3) What are the critical legal events? (CQ4) What are the primary legal situations? (CQ5) What are the main legal relators? (CQ6) What are the essential legal moments? Examples of extending core layer's concepts are illustrated in Figures 5, 6, and 7. Concerning the procedural content, the core layer's template patterns are applied by analogy with the norms of the GDPR. A list of CQs is addressed for each pattern, which is considered ontology module or sub-ontology, to fulfill the functional requirements R3 and R4.

Application of Right_Duty_to_an_Action_Relator   This legal relator represents the relationship where the *Right_Holder has the right to a positive action by the Duty_Holder* [23]. The relator pattern can be applied by analogy with several legal rules such as Art. 7 (Right_Duty_to_Withdraw_Consent), Art. 15 (Right_Duty_to_Processing_Confirmation), Art. 16 (Right_Duty_to_Rectification), and Art. 82 (Right_Duty_to_Compensation).

> *Article 7. Section 3. The data subject shall have the right to withdraw his or her consent at any times [...]*

Article 15. Section 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data are being processed [...]

Article 16. The data subject shall have the right to obtain from the controller the rectification of inaccurate personal data [...]

Article 82. Section 1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

Figure 5 presents an ontology module that defines Right_Duty_to_Compensation, realized by applying Right_Duty_to_Action_Relator by analogy with Art. 82. The following CQs are addressed for applying this pattern: (CQ1) What GDPR legal rule has been infringed? (CQ2) Who is involved in the GDPR infringement? (CQ3) What damage has resulted from the GDPR infringement? (CQ4) What personal data was affected by this damage? (CQ5) Who do the personal data identify as legal agent? (CQ6) Who is suffering from the personal data damage? (CQ7) Who has the right to compensation? (CQ8) Who is charged by the compensation?
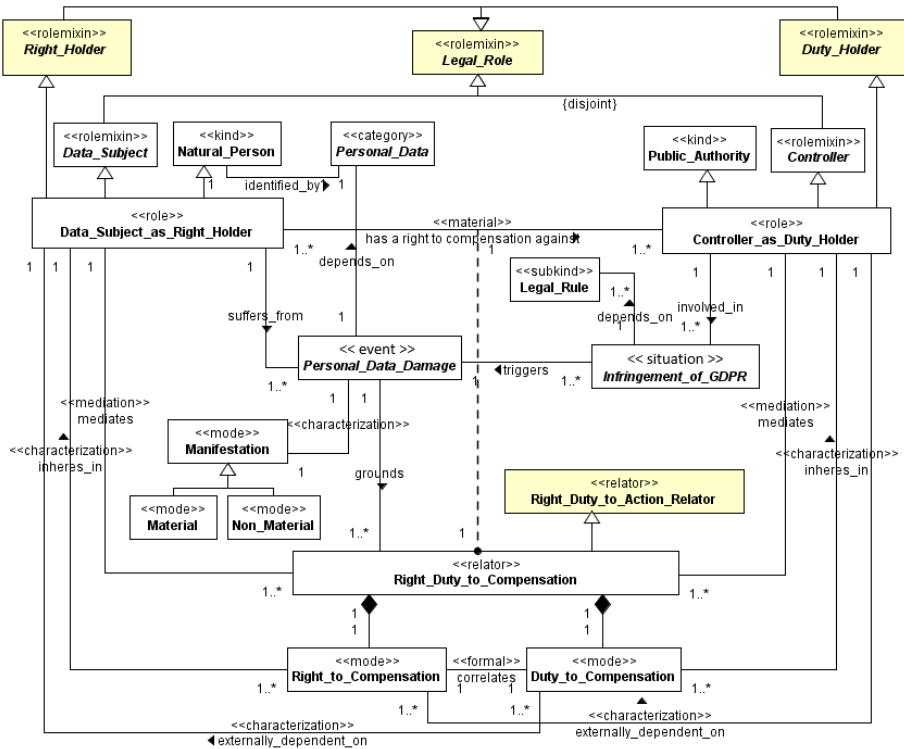

Figure 5. Right_Duty_to_Compensation represented in OntoUML.

Application of Right_Duty_to_Omission_Relator This legal relator represents the relationship where the *Right_Holder has the right to an omissive duty action by the Duty_Holder*. In other words, the Duty_Holder has a duty to refrain from acting [23]. Figure 6 depicts an ontology module, that defines Right_Duty_to_Objection_to_Processing,

achieved by applying Right_Duty_to_Omission_Relator by analogy with Art. 21. The following CQs are addressed for applying this pattern: (CQ1) For what purposes personal data processing is performed? (CQ2) On what personal data is the processing dependent? (CQ3) Who do the personal data identify? (CQ4) Who is the legal agent suffering from the processing? (CQ5) Who is involved in the personal data processing? (CQ6) Who has the right to object to personal data processing? (CQ7) Who is charged by terminating the personal data processing?

> *Article 21. Section 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing [...]*
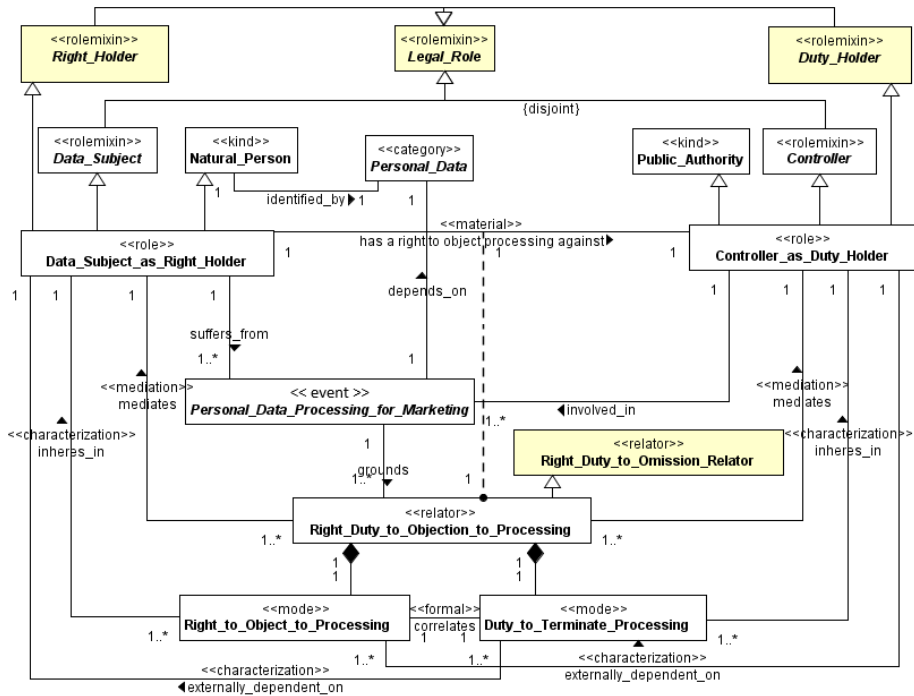

Figure 6. Right_Duty_to_Objection_to_Processing represented in OntoUML.

Application of Power_Subjection_Relator   This legal relator represents the relationship where the *Power_Holder has the competence (or the legal power) to create (change, extinguish) a legal position or a situation against the Subjection_Holder* [23]. In Figure 7, we present an ontology module, that defines Power_Subjection_to_Liabilities, obtained by applying Power_Subjection_Relator by analogy with Art. 82. The following CQs are addressed for applying this pattern: (CQ1) What GDPR legal rule has been infringed by personal data processing? (CQ2) On what personal data is the processing dependent? (CQ3) Who is involved in the personal data processing? (CQ4) What damage is caused by the GDPR infringement? (CQ5) Who is suffering from the personal data damage resulting from the infringement? (CQ6) Who has the power to define liability towards the damage? (CQ7) Who is the liable legal agent for the personal data damage? (CQ8) What legal relator was created based on the power subjection relationship?

> *Article 82. Section 2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation [...]*
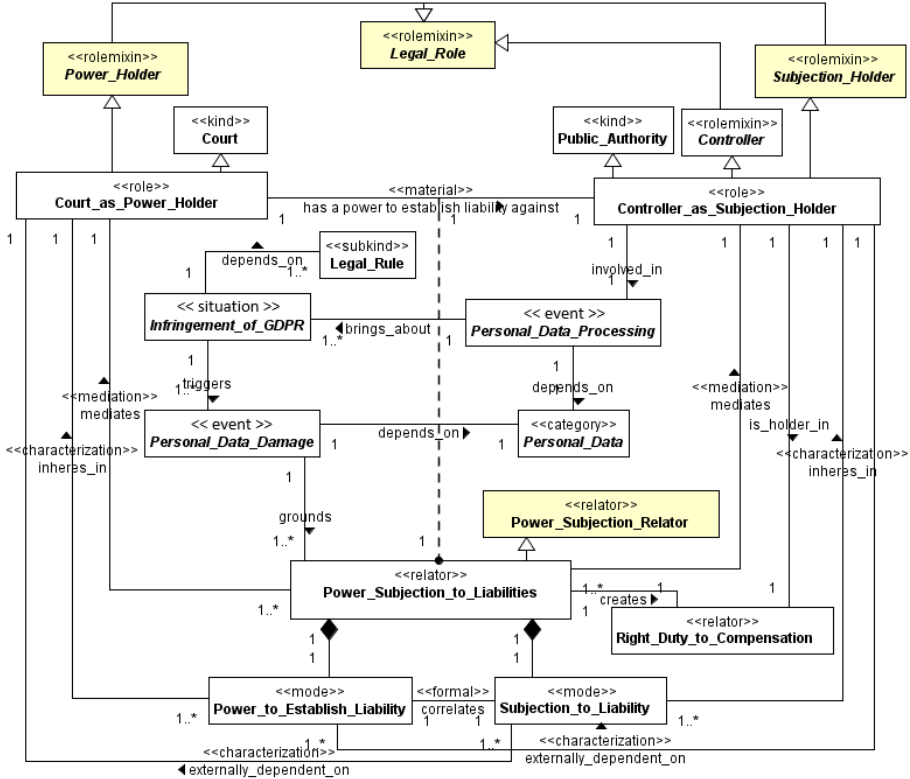

Figure 7. Power_Subjection_to_Liabilities represented in OntoUML.

5. Ontology Validation and Evaluation

In this section, we validate OPPD by transforming the reference model into an operational ontology. The ontology environment OLED [40] provides the transformation by generating the OWL code. The code generator maps OntoUML classes, associations, and attributes to OWL classes, object properties, and data properties. It considers generalization sets and their disjointness properties plus model cardinalities. The code generator transforms to SWRL[5] rules the domain constraints and cardinalities and the transitivity of material and parthood relations. The resulted operational ontology is manageable in ontology editors such as Protégé (see Figure 8 for an example). OPPD's consistency is verified using HermiT, an OWL2 inference engine[6]. The ontology, under construction, contains 89 classes, 83 subClassOf relations, 56 equivalent classes, 234 object properties, and 14 disjoint axioms.
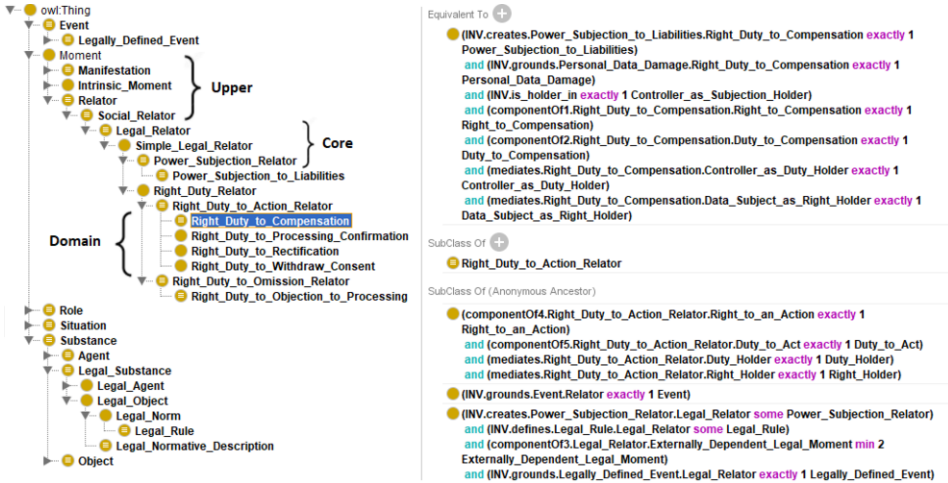
---

[5]https://www.w3.org/Submission/SWRL/

[6]http://www.hermit-reasoner.com/

Figure 8. Excerpt of OPPD (Right_Duty_to_Compensation) represented in Protégé.

Moreover, to evaluate OPPD's validity regarding its requirements, a set of SPARQL[7] queries are formalized to translate the competency questions defined in the conceptualization phase. The queries are executed to interrogate OPPD's concepts and relations using defined instances. In the following, excerpt of the SPARQL queries translated from the CQs specified for modeling Right_Duty_to_Compensation (Figure 5) is presented:

```
(CQ1) SELECT ?rule WHERE {?rule rdf:type oppd:Legal_Rule.
?infringement rdf:type oppd:Infringement_of_GDPR.
?infringement oppd:depends_on ?rule.}
(CQ2) SELECT ?controller WHERE {?controller rdf:type oppd:Controller.
?infringement rdf:type oppd:Infringement_of_GDPR.
?controller oppd:involved_in ?infringement.}
(CQ3) SELECT ?damage WHERE {?infrigement rdf:type oppd:Infringement_of_GDPR.
?infrigement oppd:triggers ?damage.}
(CQ4) SELECT ?personaldata WHERE {?damage rdf:type oppd:Personal_Data_Damage.
?damage oppd:depends_on ?personaldata.}
```

6. Ontology Use

OPPD intends to be helpful for different purposes such as data querying, information retrieval, legal reasoning, and compliance checking. In this study, we present a preliminary work that demonstrates the potential use of OPPD to formalize the GDPR legal rules for reasoning practices. Rule language such as SWRL can be used for the formalization process (e.g., [41]) yet limit the reasoning purposes since it lacks the non-monotonic features. The objective of non-monotonic reasoning is to develop reasoning systems that model how common sense is used by humans [42]. As *non-monotonic reasoning is related to Logic Programming* [43] - in the sense that they share common goals and techniques (e.g., negation as failure) - we envisaged this approach to achieve our intention to combine logic programs with ontological reasoning. Using SWI-Prolog [44] and Thea[8],

---

[7]https://www.w3.org/TR/sparql11-query/

[8]Prolog library for managing OWL2 ontologies. Available from: https://github.com/vangelisv/thea

OPPD, represented as OWL abstract syntax terms, is converted into a logic program. The mapping process implements Description Logic Programs (DLP) [45]. For instance, OPPD's axioms (A) are converted to the Prolog program (B).

```
(A)                                         (B)
subClassOf(Data_Subject,Legal_Role)         Legal_Role(X) :- Data_Subject(X).
classAssertion(Legal_Rule,Article_82)       Legal_Rule(Article_82).
                                            INV.mediates(X,Y) :- mediates(Y,X).
inverseProperties(INV.mediates,mediates)    mediates(X,Y) :- INV.mediates(Y,X).
```

Furthermore, the generated logic program will be used for encoding logic rules representing the procedural aspect of GDPR legal rules. For instance, the subsequent set of rules is proposed to represent Art. 82.1. (Figure 5). In this context, the isomorphism principle, stated by Bench-Capon [46], is followed to create a *well-defined correspondence* between the rules in the formal model and the rules in natural language.

```
(1) Right_Duty_to_Compensation(Z) :- Controller(X), Data_Subject(Y),
Personal_Data(P), Infringement_of_GDPR(I), involved_in(X,I),
Personal_Data_Damage(D), triggers(I,D), suffers_from(Y,D), depends_on(D,P),
Legal_Relator(Z), grounds(D,Z).
(2) mediates(Z,X) :- Right_Duty_to_Compensation(Z), Controller(X).
(3) mediates(Z,Y) :- Right_Duty_to_Compensation(Z), Data_Subject(Y).
(4) has_a_right_to_compensation_against(Y,X) :- Right_Duty_to_Compensation(Z),
Controller(X), Data_Subject(Y), mediates(Z,X), mediates(Z,Y).
```

7. Related Work

As related to this study, two main preferences are defined, the legal core ontologies and the domain ontologies representing the GDPR norms. Therefore, LKIF-Core [24] is selected being the latest validated legal core ontology preceding UFO-L. Besides, two domain ontologies are considered, PrOnto [12] as a legal domain ontology covering the GDPR norms and concepts and GConsent that represents the consent concept based on the GDPR [11].

LKIF-Core [24] is a legal core ontology implemented in OWL[9]. It is composed of 15 modules categorized into three main categories, each of which describes a set of closely related concepts from both legal and commonsense domains: (i) *Abstract Concepts* define the place, mereology, time, and spacetime; (ii) *Basic Concepts* define concepts around process, role, action, and expression; (iii) *Legal Concepts* define legal action, legal role, and norm. LKIF-Core considers the representation of *normative knowledge* which is the basis of the normative reasoning in the AI and Law research domain. It provides interpretations for the terms *obligation*, *prohibition* and *permission* [47]. By reusing LKIF-Core, the representation of the hierarchical structure of basic legal concepts is maintained. However, the main drawback is the lack of interpretation of the procedural aspect of provisions. This deficiency is admitted in the literature that *most ontologies did not have an adequate solution for legal procedures mainly because of the difficulty to find a language to express knowledge in a declarative way* [48].

---

[9]https://github.com/RinkeHoekstra/lkif-core

PrOnto [12] is a legal ontology developed for modeling the GDPR concepts and norms. Its main goal is to support legal reasoning and compliance checking by employing defeasible logic theory. PrOnto is developed using the MeLOn methodology, which iterates over ten steps. To resume, we outline five essential steps that are commonly addressed in ontology engineering approaches (as described by the authors in [12]): Describe the ontology goal; Reuse existing ontologies, design patterns, or domain vocabularies; Use usable tools (e.g., tables, UML diagrams, and the Graffoo tool); Refine and optimize the ontology with the help of an ontology expert that manually adds the axioms; Ontology evaluation. In PrOnto, concepts such as Agent and Role and relations such as *plays* are reused from LKIF-Core to represent legal roles (e.g., Controller) aiming to model obligations and rights in the GDPR (e.g., Right to Data Portability). PrOnto is composed of different modules: (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. GConsent [11] is an OWL2-DL ontology for representing information associated with consent, specifically, the given aspect of consent i.e., consent provided by the data subject. For building GConsent, the "Ontology Development 101" methodology [49] is used by applying the following phases: Gather information about consent from GDPR, articles, academic papers; Create use-cases and competency questions based on collected information; Create ontology to express information about use-cases; Ontology evaluation. The core concepts defined in GConsent are Consent, Data Subject, Personal Data, Purpose, Processing, and Status. To conclude, in PrOnto and GConsent, the representation of legal concepts and relations is established. However, an explicit description of legal procedures is not supported. The legal relations and the active legal roles are not represented in a procedural perspective required to describe the procedural aspect of the GDPR norms.

8. Discussion

This study's main contribution is developing a well-founded legal domain ontology, named OPPD, representing the essentials of the GDPR. For building OPPD, a pattern-oriented approach is applied, supported by ontology grounding, layering, modularization, and reuse processes. Conceptual Ontology Patterns are selected from the foundational ontology UFO and the legal core ontology UFO-L. These patterns are reused as ontology modules and applied either by extension or analogy with legal rules to build OPPD's domain content. Besides, the ontology-driven conceptual modeling process (ODCM) is used for grounding OPPD in UFO. In this approach, we differentiate between the ontology's reference and operational versions. The reference model of OPPD, which is independent of any computational language, is implemented in OWL and SWRL. Besides, the structural and domain knowledge in OPPD are separated. The former represents the hierarchy of concepts (e.g., Figures 3 and 4) which is distinguished from modeling the legal rules' procedural aspects (e.g., Figures 5 and 7). This distinction will support the extensibility of the ontology to include future aspects. The second contribution is that by reusing UFO-L's legal relators' patterns and applying them by analogy with the legal rules, we obtained a richly populated ontology representing the procedural aspects of these rules. This result is considerable for employing our ontology for reasoning or compliance checking purposes and is difficult to achieve by reusing other

legal core ontologies that lack the representation of legal procedures. This deficiency is admitted in the literature that most approaches have failed to support the representation of the legal relations and capture the legal roles played in the context of these relations [36]. Finally, this study has two main limitations. First, the personal data processing purposes are not considered. For instance, in Figure 6, *marketing purpose* is defined jointly with the event Personal_Data_Processing_for_Marketing. However, there is a need to distinguish the event from the event's purpose. Second, due to Prolog syntax that prevents conjunctions and disjunctions in the rule's head, a single legal rule (e.g., Art. 82.1.) is formalized using multiple logic rules (see Section 6 for an example), which may affect a more beneficial application of the isomorphism principle.
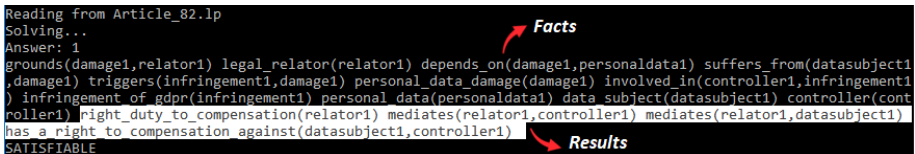
9. Conclusion

Legal ontologies are considered the missing link between legal theory and AI & law. They provide stable foundations for knowledge representation in the legal domain. However, their development is challenging due to the complexity of the legal knowledge. This study demonstrated that applying a pattern-based approach supported by ontology reuse, modularization, and layering processes is a practical strategy to overcome the existing difficulties. The support processes aimed to simplify the ontology development by reusing conceptual patterns from the foundational ontology UFO and the legal core ontology UFO-L. Besides, ODCM is used for grounding OPPD in UFO. As a result, we obtained OPPD, a well-founded legal domain ontology with a significant ontological expressiveness. OPPD is validated by implementing the ontology in OWL and evaluated using SPARQL queries translated from the defined CQs. Finally, preliminary work to formalize GDPR legal rules by integrating OPPD and Prolog is presented. In further works, we will proceed with the ontology development to address other legal aspects such as consent, immunities to liabilities, and processing purposes. Furthermore, OPPD's *semantic accuracy* will be assessed by computing different structural measures (e.g., depth, average depth, depth variance, etc.) [50]. Concerning the reasoning over the formalized logic rules, it will be maintained using Answer Set Programming (ASP) [51]. ASP solvers binding to SWI-Prolog are required to solve logic programs (see Figure 9).

Figure 9. An example of solving the logic program representing Art. 82.1.

References

[1] EU-Commission. General Data Protection Regulation. Official Journal of the European Communities. 2018.

[2] Teixeira GA, Silva M, Pereira R. The critical success factors of GDPR implementation: a systematic literature review. Digital Policy, Regulation and Governance. 2019;21(4):402-418.

[3]   Romanou A. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise, Computer Law & Security Review. 2018;34:99-110.

[4]   Lopes IM, Guarda T, Oliveira P. EU General Data Protection Regulation Implementation: An Institutional Theory View. Proceedings of WorldCIST'19, New Knowledge in Information Systems and Technologies. Advances in Intelligent Systems and Computing; vol. 930. Springer, Cham; 2019. p. 383-393.

[5]   Tikkinen-Piri C, Rohunen A, Markkula J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law and Security Review. 2018;34(1):134-153.

[6]   Kingston, J. Using artificial intelligence to support compliance with the general data protection regulation. Artificial Intelligence and Law. 2017;25:429-443. doi: 10.1007/s10506-017-9206-9.

[7]   Torre D. An AI-assisted Approach for Checking the Completeness of Privacy Policies Against GDPR. Proceedings of IEEE 28th International Requirements Engineering Conference (RE), Zurich, Switzerland; 2020. p. 136-146; doi: 10.1109/RE48521.2020.00025.

[8]   Brkan M. AI-supported decision-making under the general data protection regulation. Proceedings of the 16th edition of the International Conference on Artificial Intelligence and Law; 2017. p. 3-8.

[9]   Torre D, Soltana G, Sabetzadeh M, Briand LC, Auffinger Y, Goes P. Using Models to Enable Compliance Checking Against the GDPR: An Experience Report. Proceedings of ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems (MODELS); Munich, Germany; 2019. p. 1-11. doi: 10.1109/MODELS.2019.00-20.

[10]   Zeni N, Kiyavitskaya N, Mich L, Cordy J, Mylopoulos J. GaiusT: supporting the extraction of rights and obligations for regulatory compliance. Requirements Eng. 2015;20:1–22.

[11]   Pandit HJ, Debruyne C, O'Sullivan D, Lewis D. GConsent - A Consent Ontology based on the GDPR. Proceedings of 16th European Semantic Web Conference (ESWC); 2019.

[12]   Palmirani M, Martoni M, Rossi A, Bartolini C, Robaldo L. Legal Ontology for Modelling GDPR Concepts and Norms. In Monica Palmirani, editor, Legal Knowledge and Information Systems - JURIX 2018: The Thirty-first Annual Conference, Groningen, The Netherlands; 2018 December 12-14; IOS Press; 2018. p. 91-100.

[13]   Bonatti PA, Ioffredo L, Petrova IM, Sauro L, Siahaan I. Real-time reasoning in OWL2 for GDPR compliance. Artificial Intelligence. 2020 jan;289. doi:arxiv-2001.05390.

[14]   Valente A, and Breuker J. Ontologies: The missing link between legal theory and AI & law. In: H. Prakken, A.J. Muntjewerff, and A. Soeteman, editors. Proceedings of Legal Knowledge Based Systems Jurix 1994; Lelystad: Vermande; 1994.

[15]   Mommers L. Application of a knowledge-based ontology of the legal domain in collaborative workspaces. Proceedings of the 9th international conference on Artificial intelligence and law; 2003. p. 70-76.

[16]   Benjamins VR, Casanovas P, Breuker J, Gangemi A. Law and the Semantic Web: Legal Ontologies, Methodologies, Legal Information Retrieval and Applications. Springer; 2005.

[17]   Francesconi E, Tiscornia D. Building Semantic Resources for Legislative Drafting: The DALOS Project. Computable Models of the Law. LNCS; Springer-Verlag Berlin, Heidelberg; 2008. p. 56-70.

[18]   Dove I. Legal Expert Systems: The End of Jurisprudence?. The Journal of Legal Studies in Business. 1996.

[19]   Gardner A. Book Review. An Artificial Intelligence Approach To Legal Reasoning. MIT Press; 1987. p. 223-233.

[20]   Falbo R, Guizzardi G, Gangemi A, Presutti V. Ontology Patterns: Clarifying Concepts and Terminology. Proceedings of WOP; 2013. p. 14-26.

[21]   Guizzardi G. Ontological Foundations for Structural Conceptual Models. Telematica-Instituut/CTIT. 2005.

[22]   Borgo S, Masolo C. Ontological foundations of DOLCE; Theory and Applications of Ontology: Computer Applications. Springer; 2010.

[23]   Griffo C. UFO-L, A Core Ontology of Legal Aspects Building Under the Perspective of Legal Relations. Federal University of Espirito Santo. 2018.

[24]   Hoekstra R, Breuker J, Di Bello M, Boer A. LKIF Core: Principled Ontology Development for the Legal Domain. Proceedings of the 2009 conference on Law, Ontologies and the Semantic Web: Channelling the Legal Information Flood; IOS Press; 2009. p. 21-52.

[25]   Falbo R. SABiO: Systematic Approach for Building Ontologies. 2014.

[26]   Gangemi A. Design Patterns for Legal Ontology Constructions. Proceedings of the 2nd Workshop on

Legal Ontologies and Artificial Intelligence Techniques; USA; 2007.

[27] Guarino N, Oberle D, Staab S. What is an Ontology? In: Staab S, Studer R, editors. Handbook on Ontologies. International Handbooks on Information Systems. Springer, Berlin, Heidelberg; 2009. doi: 10.1007/978-3-540-92673-3_0

[28] Guizzardi G, Falbo R, Guizzardi RS. Grounding software domain ontologies in the unified foundational ontology (UFO): The case of the ode software process ontology. Proceedings of the 1th Iberoamerican Workshop on Requirements Engineering and Software Environments; 2008.

[29] Kowalski R. Predicate logic as a programming language. Proceedings of IFIP Congress 74; 1974; p. 569–574.

[30] Guizzardi G. Towards Ontological Foundations for the Conceptual Modeling of Events. Proceedings of ER 2013; Springer, Heidelberg; 2013. p. 327-341.

[31] Guizzardi G, Fonseca CM, Benevides AB, Almeida JPA, Porello D, Sales TP. Endurant Types in Ontology-Driven Conceptual Modeling: Towards OntoUML 2.0. Proceedings of ER 2018; 2018.

[32] Guizzardi G, Wagner G, Falbo R, Guizzardi R S. Towards Ontological Foundations for Conceptual Modeling: The Unified Foundational Ontology (UFO) Story. Applied Ontology. 2015;10(3-4):259-271.

[33] Falbo R, Baiao F, Lopes M, Guizzardi G. The Role of Foundational Ontologies for Domain Ontology Engineering: An Industrial Case Study in the Domain of Oil and Gas Exploration and Production. International Journal of Information System Modeling and Design. 2010;1:1-22.

[34] Griffo C, Almeida J, Guizzardi G. Towards A Legal Core Ontology Based On Alexy's Theory of Fundamental Rights. Proceedings of ICAIL Multi-Lingual Workshop on AI and Law (MWAIL); 2015.

[35] Alexy R. A Theory of Constitutional Rights. Oxford University Press; 2009.

[36] Griffo C, Almeida J, Guizzardi G. Conceptual Modeling of Legal Relations. Proceedings of ER 2018, Conceptual Modeling; 2018. p. 169-183.

[37] Guizzardi G. On Ontology, ontologies, Conceptualizations, Modeling Languages and (Meta)Models. Proceedings of Databases and Information systems; 2007. p. 18-39.

[38] Guizzardi G, Proper HA. On Understanding the Value of Domain Modeling. Proceedings of 15th International Workshop on Value Modelling and Business Ontologies (VMBO 2021); 2021.

[39] Gangemi A, Presutti V. Ontology Design Patterns. Handbook on Ontologies; Springer, Heidelberg. 2009.

[40] Guerson J, Sales TP, Guizzardi G, Almeida JPA. OntoUML Lightweight Editor: A Model-Based Environment to Build, Evaluate and Implement Reference Ontologies. Proceedings of 19th IEEE EDOC; 2015.

[41] El Ghosh M, Abdulrab H. Ontology-Based Liability Decision Support in the International Maritime Law. Proceedings of the 33rd International Conference on Legal Knowledge and Information Systems (JURIX); 2020. p. 273-276.

[42] Minker J. An overview of nonmonotonic reasoning and logic programming. The Journal of Logic Programming. 1993;17(2-4):95-126.

[43] Gelfond M, Leone N. Logic programming and knowledge representation—The A-Prolog perspective. Artificial Intelligence. 2002;138:3–38.

[44] Wielemaker J, Schrijvers T, Triska M, Lager T. SWI-Prolog. Theory and Practice of Logic Programming. 2010;12(1-2):67-96.

[45] Grosof BN, Horrocks I, Volz R, Decker S. Description logic programs: combining logic programs with description logic. Proceedings of the 12th international conference on World Wide Web; 2003. p. 48–57.

[46] Bench-Capon TJM, Coenen FP. Isomorphism and legal knowledge based systems. Artificial Intelligence and Law. 1992;1:65–86. doi: 10.1007/BF00118479.

[47] Breuker J, Valente A, Wikels R. Legal Ontologies in Knowledge Engineering and Information Management. Artificial Intelligence and Law. 2004;12:241-277.

[48] Visser PR, Bench-Capon TJ. A comparison of two legal ontologies. Working papers of the First International Workshop on Legal Ontologies; University of Melbourne, Australia. 1997.

[49] Noy NF, McGuinness DL. Ontology Development 101: A Guide to Creating Your First Ontology. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880; 2001.

[50] Sanchez D, Batet M, Martinez M, Domingo-Ferrer J. Semantic variance: An intuitive measure for ontology accuracy evaluation. Engineering Applications of Artificial Intelligence. 2015;39:89-99.

[51] Erdem E, Gelfond M, Leone N. Applications of Answer Set Programming. AI Magazine. 2016;37(3):53-68. doi: 10.1609/aimag.v37i3.2678.