An ontology for legal reasoning on data sharing and processing between law enforcement agencies

Jérémy Bouché-Pillon, Nathalie Aussenac-Gilles, Yannick Chevalier, Pascale Zaraté

An ontology for legal reasoning on data sharing and processing between law enforcement agencies

Jeremy Bouché-Pillon[1,*], Nathalie Aussenac-Gilles[1], Yannick Chevalier[1] and Pascale Zaraté[1,2]

[1]Université de Toulouse–CNRS–IRIT–UPS 118 route de Narbonne, 31062 Toulouse Cedex 9, France
[2]Université Toulouse Capitole—IRIT–Manufacture des Tabacs, 21 Allée de Brienne, 31015 Toulouse, France

Abstract

With the advent of the digital transition,the need for control of access to information has significantly increased. In the EU in particular, Law Enforcement Agencies (LEAs) need to exchange information. In recent years, many regulations have emerged to control data processing and exchange. Texts other than the GDPR, such as the "Law Enforcement Directive (LED)", appeared to regulate specifically their processing of data. This paper aims to present an ontological representation of data sharing and processing between law enforcement agencies. After highlighting the lacking notions in existing domain ontologies like LegalRuleML, we propose an ontology that integrates the required elements for our application case. Furthermore we illustrate the validation and usage of this ontology through a rule-based reasoning mechanism for data related procedures between law enforcement agencies.

Keywords

ontology, legal knowledge, legally compliant data sharing and processing, deontic rules

1. Introduction

With the advent of the digital transition in many domains, the need for control of access to information has significantly increased. Nowadays, these controls tend to rely on an unambiguous description of data and knowledge, through ontologies and annotations of privacy or sensitivity levels. In the EU in particular, Law enforcement agencies (LEAs) need to exchange information regularly in the context of cooperation between the police forces.

In recent years, many regulations have emerged to control data processing. Among them the GDPR [1] from 2016 is the reference text that covers *"the protection of natural persons with regard to the processing of personal data and on the free movement of such data"*. Although it is relevant in most situations involving personal data, it does not apply to the processing of personal data by authorities responsible for proceedings relating to criminal offences. As a

3rd international workshop KM4LAW – Knowledge Management and Process Mining for Law, July 15–19, 2024, Enschede, Netherlands

*Corresponding author.
jeremy.bouche-pillon@irit.fr (J. Bouché-Pillon); nathalie.ausseanc-gilles@irit.fr (N. Aussenac-Gilles); yannick.chevalier@irit.fr (Y. Chevalier); pascale.zarate@irit.fr (P. Zaraté)
https://www.irit.fr/~Nathalie.Aussenac-Gilles/ (N. Aussenac-Gilles); https://www.irit.fr/~Yannick.Chevalier/ (Y. Chevalier); https://www.irit.fr/~Pascale.Zarate/ (P. Zaraté)
0000-0001-6923-9915 (J. Bouché-Pillon); 0000-0003-3653-3223 (N. Aussenac-Gilles); 0000-0002-8617-4209 (Y. Chevalier); 0000-0002-5188-1616 (P. Zaraté)

result, other regulations have emerged that regulate procedures involving the exchange and the processing of personal information as part of investigations by Law Enforcement Agencies. We will particularly focus on the three following texts whiwh were selected thanks to the contribution of a doctoral student in Law:

1. The *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* more simply called *Law Enforcement Directive (LED)* [2].
2. The *Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters* [3]. This text regulates the "European Investigation Order" (EIO) procedure in which LEAs can issue or answer to an investigation order that can involve several investigation measures such as the acquisition of evidence data.
3. The *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters* [4]. This text regulates the "European Production Order Certificate" (EPOC) and the "European Preservation Order Certificate" (EPOC-PR) procedures. These procedures allow LEAs to request or retain data originally stored in another organization.

The tables of legal provisions from the *Handbook on European data protection law - 2018 edition*[1] allowed a more precise selection of specific articles and even paragraphs in these texts.

As of now, it has become more complex and time-consuming for LEAs to assess whether the measures they would request as part of a data procedure are mandatory, permitted or prohibited under the regulations. Thus, it is meaningful to consider a framework that would provide support to LEAs and help them estimate the lawfulness of the procedures they intend to perform. Several frameworks and tools, like DAPRECO [5] are dedicated to support the GDPR, but none of them deals with decision support in relation with the above mentioned regulations.

To meet this requirement, we propose a framework consisting of the following components:

- an ontology to create a knowledge base; it represents all the relevant aspects of the decision-making process including the legal rules, the data sets or data collections metadata, the actors involved in the data processing and their investigation objective;
- a set of formal rules extracted from the regulations and represented thanks to the concepts and properties defined in the ontology;
- a reasoning mechanism on the knowledge base able to verify the compliance of a use case to each formal rule.

In this paper, we will focus on presenting an ontology to describe criminal aspects as well as actions taken through investigation procedures by LEAs that involve data sharing and processing. The paper is structured as follows. In Section 2 we review existing works in legal

[1] https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

knowledge representation to identify which parts of them we could reuse. We then present in Section 3 our own ontology that makes it possible to represent legal rules, investigation contexts as well as dataset content and metadata. We finally report the ontology validation and experimentation process in Section 4 before concluding (Section 5).

2. Related work

The representation of legal knowledge is an important research field in knowledge management that led to the development of several domain ontologies: PrOnto [6] that provides legal knowledge modelling of agents, data types, processing operations, rights and obligations based on the GDPR [1]; LegalRuleML [7] that extends RuleML[2] specifically for legal norms, guidelines, policies and reasoning; NRV [8] that extends LegalRuleML to express normative requirements; UFO-L [9], a well-grounded legal core ontology extending the foundational ontology UFO and focused on the representation of legal power relationships between entities. Ontology design patterns representing specific relations can be extracted from it, such as *Right-Duty to an Action* or *Power-Subjection Relations* [10]. Previous work also include formal interchange formats for rules and policies, like RIF [11], a standard for exchanging rules among rule systems; LKIF [12], a standard for representing policies, legislations and legal cases, with their arguments. Most of these works use the GDPR as reference. For instance, DAPRECO [5, 13] is a knowledge base containing the GDPR representated using LegalRuleML.

Our focus being the regulations about data exchanges between LEAs in various contexts, we want the ontology to allow to represent all the following aspects:

- The context in which procedures for data acquisition or transfer are performed, since part of this context impacts the decision-making process. For example, requesting a data transfer in a national security emergency situation will have a different answer than in a non-emergency situation.
- The characteristics of the data that would be involved in the procedure, for example whether or not some personal information is actually public.
- The terminology used in the regulations as well as the deontic notions of permission, obligation, and prohibition, which are required to represent the formal legal rules we will be using for reasoning.
- The structure of the regulations from which the formal rules are extracted as well as a way to link the formal rules to their sources.

Some of these aspects are already covered by existing works. For example, Akoma Ntoso[3] allows the representation of executive, legislative and judicial documents in a structured manner using an XML vocabulary dedicated to the legal field, notably by modeling the structure of such texts. A "source" module of LegalRuleML [7] as well as the PROV-O ontology[4] and its extension GDPRov [14] dedicated to GDPR compliance allow to represent the link between formal rules

[2] the RuleML initiative: https://www.ruleml.org
[3] https://docs.oasis-open.org/legaldocml/ns/akn/3.0
[4] https://www.w3.org/TR/prov-o/

and the source text. PROV-O also presents the advantage of representing the dates of creation and invalidation of the rules, allowing for an easy maintenance of the rule base according to the evolution of the texts of law in force. The Data Privacy Ontology (DPV)[5] [15] also allows to link processes to the applicable laws, such as the GDPR or the AI Act.

LKIF-core[6] [16] provides several useful concepts such as everything related to a Legal Agent, its Roles, the Organizations he belongs to and the Actions he performs. These concepts are reused in PrOnto [6] which also provides a Data module that meets most of our needs regarding data representation with, for example, subclasses for the different types of Sensitive Data (`BiometricData, HealthData`). DPV also provides a lot of concepts, especially regarding the context around a process. There are notably the notions of `Necessity` or `StorageCondition`.

Although the "deontic" module of LegalRuleML, or the deontic classification of rules in DPV or in the Open Digital Rights Language (ODRL)[7] could offer a good base for representing the deontic aspect of normative rules, the extension of LegalRuleML proposed by F. Gandon et. al with the Normative Requirement Vocabulary (NRV) ontology [8] provides significant supplementary concepts that allow for further characterization of a regulative statement, with classes like `Violable Requirement`.

The legal core ontology UFO-L [9], an extension of the Unified Foundational Ontology (UFO) [17], allows the representation of constitutional rights concepts and 'legal relators'. Several ontology design patterns can be extracted from it, and among them the *Right-Duty to an Action Pattern* [18] and *Legal Power-Subjection Pattern* [10] that could be used to represent legal power dynamics between some of the actors involved in data exchanges between LEAs.

However, we are focusing on the representation of procedures such as the EIO [3], the EPOC and EPOC-PR [4], that respectively concern the production and preservation of electronic evidences, as well as on all the data types they involve and their characteristics. So far, they are not covered by any existing ontology. However, several ontologies can be reused to represent some aspects. For example, if the data involved belongs to datasets, then the Data Catalog Vocabulary (DCAT)[8] can be reused to represent the dataset metadata. Nor does any ontology provide all together the concepts required to represent legal rules, the dataset metadata and content, and the context of the data related procedures.

The review of existing legal models is summarized in table 1. Each ontology is evaluated on each aspect using 2 values, each on a scale between 0 and 2, and presented in this form : *2 / 1*. The first value reflects how much of the aspect is represented in the ontology, 0 meaning it is not represented at all and 2 it is represented in an elaborate way. The second value indicates the extent to which the concepts used to represent an aspect satisfies the requirements, with 0 meaning it does not correspond at all and 2 it accurately meets the requirements. In cases where an aspect is not present at all in an ontology (which would result in a *0 / 0* evaluation), we leave the corresponding cell empty.

From this study emerges that LKIF-core, LegalRuleML and DPV are the most complete candidates to be reused as basis for our ontology. These 3 ontologies cover most of the aspects

[5] https://w3c.github.io/dpv/dpv/
[6] https://github.com/RinkeHoekstra/lkif-core
[7] https://www.w3.org/TR/odrl-model/
[8] https://www.w3.org/TR/vocab-dcat-3/

Table 1
Summary of literature study

	Context of Procedures	Data Characterization	Deontic Notions	Legal Terminology	Regulation texts structure and link to rules
PrOnto	2 / 1	2 / 1	2 / 1	2 / 1	.
LegalRuleML	2 / 1	2 / 1	2 / 1	2 / 1	1 / 1
NRV	.	.	2 / 2	1 / 1	.
LKIF-Core	2 / 1	2 / 1	2 / 1	2 / 1	.
UFO-L	1 / 1	.	2 / 1	2 / 1	.
DPV	2 / 2	1 / 1	2 / 1	2 / 1	2 / 1
ODRL	1 / 1	1 / 1	2 / 1	2 / 1	1 / 1
DCAT	.	1 / 1	.	.	.
PROV-O	1 / 1	1 / 1	.	.	1 / 1
GDPRov	1 / 1	1 / 1	.	.	1 / 1
Akoma Ntoso	.	.	.	.	2 / 1

needed and provide a lot of relevant high level concepts to build upon. Moreover, a study conducted in 2017 for the design of UFO-L [9] identified LKIF as one of the legal ontologies that reuse the most foundational and core ontologies, making it a well-grounded ontology, which supports the idea of reusing LKIF as one of the basis.

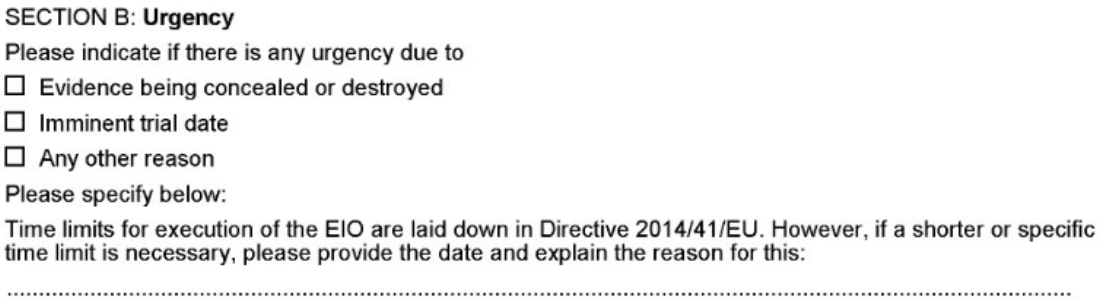
3. An ontology to represent data sharing and processing between law enforcement agencies

The construction of such an ontology has started with the manual extraction of concepts and properties from regulations. Rather than using a language model, given the (small) size of the text, text analysis was conducted manually in collaboration with a PhD student in law, who provided an expert interpretation of the rule relevance and representation.

3.1. Source material and competency questions

To build the ontology, we referred to the following parts of the texts mentioned in Section 1 [2, 3, 4]:

- Around 20 articles selected because they are the most relevant in the specific context of data transfer and processing. They provide explicit conditions and limitations applicable to data transfer. The involved articles are notably articles 2, 3 and 6 to 10 of [2], articles 2, 4, 5, 6, 7, 13 and 32 of [3] and articles 2 and 4 to 11 of [4].
- The forms included as appendices. These forms are the one filled by and exchanged between LEAs when performing processes such as a "European Investigation Order". For example, the section of the form allowing to indicate the urgency of a situation for an EIO is given in Figure 1.


SECTION B: **Urgency**

Please indicate if there is any urgency due to

☐ Evidence being concealed or destroyed

☐ Imminent trial date

☐ Any other reason

Please specify below:

Time limits for execution of the EIO are laid down in Directive 2014/41/EU. However, if a shorter or specific time limit is necessary, please provide the date and explain the reason for this:

.....

Figure 1: Section B of the form for an EIO [3]

The definition of *competency questions* [19] is a standard way to characterize the scope of an ontology. They express the queries to be further requested to knowledge graphs that represent data using the concepts and properties in the ontology. They reflect the users' interest. In the current project, the competency questions bear on possible issues or limitations in relation with data sharing among LEAs in the course of an investigation. Among the competency questions we defined, the main one are the following:

- Which are the data or evidences involved in a procedure? What are their types / sub-types, e.g "Sensitive Personal Data"?
- What is the situation in which a procedure takes place?
- Which are the authorities involved in a procedure and what are their roles?
- Are there people (suspects, witnesses,...) involved in a procedure and in which way are they involved?
- Which rule expresses constraints on the use of a dataset in a standard context? in an emergency context?
- What are the main features to characterise a dataset?

3.2. Overview of the Ontology

We will now detail the main concepts and classes present in the ontology to answer these questions. Currently, the ontology includes 175 classes and 98 properties. Its structure remains simple, with few additional axioms, as we have not yet formalized all the disjunctions between classes for example. We propose several top classes, each representing a different aspect of the problem, as illustrated in Appendix A:

Procedure class: its subclasses correspond to each type of procedure we are focusing on, such as the EIO and EPOC. We will search for a possibility to align our `Procedure` with classes like `Process` from LKIF-core [16];

Modality class and its sub-classes: These classes relate to the deontic aspect of regulations such as `Permission`, `Obligation` and `Prohibition`. We aligned them with the corresponding concepts from the NRV ontology [8];

Authority class: In a standard access control system, "Authorities" would be the "subjects". Since Authorities are indeed central in all the aspects of the procedures we seek to represent, this is one of the most connected top class of the ontology. For example, a procedure such as an EIO emission has an `issuing authority`, a `receiving authority`, that may or may not be `competent` to treat the request, and a `validation authority`. Besides, in case of a data acquisition request, different pieces of data may be in possession each of a specific authority, and these authorities are requested to transfer data one to another one. These authorities are by nature organizations and thus are related to concepts appearing in other ontologies like in LKIF-core for example [16];

Data class: In an access control system, "Data" would play the role of "objects" in our modeling. The numerous sub-classes of Data represent the diversity of datatypes involved in data-sharing situations. Although we noticed some similarities with concepts in the `Data` module of PrOnto [6] that we can resolve with an ontological alignment, we encountered other classifications of data. Thus, among the top sub-classes of `Data`, we consider sub-classes to make the distinction between `Sensitive Personal Data` and `Non Sensitive Personal Data` but also between `Public Data` and `Private Data` for example. We also consider particular datatypes such as `Internet Data` or `Device Content Data` that are relevant data types to be shared between LEAs.

Action class: This general class encompasses several types of actions at different levels of the data-sharing request scenario. First some actions are performed by authorities to initiate a procedure or to ensure its continuation, with classes like `EIO Emission`. We also consider all actions that can be requested through procedure forms, such as the transfer of evidences or investigation data, with for example the `Data Transmission` class. These "Actions" would be the ones appearing in a standard access control system to determine the right to access data for someone depending on the action they want to perform on them. Apart from the `Transmission` sub-class that is similar to the `Transmit` class from the `Action` module of PrOnto [6], we represent unique actions related to criminal investigations as sub-classes of `Investigation Measure` such as `Material Seizure` or `Physical Hearing`.

Regarding the properties, we mainly consider properties linking procedures to their content and the authorities involved. As such, we find:

- `asks Measure` from a `Procedure` to a `Investigation Measure` that indicates which investigation measures are required by a procedure like an EIO.
- `has Motive` from a `Procedure` to a `Ground of Justification` to express the justification behind a procedure which is essential to evaluate if the investigation measures requested are adapted and proportionate to the situation
- `would Involve` that allows to express the predicted / requested involvement of authorities, people (who could be suspects, victims, witnesses in investigation cases for example) but also of specific data in a procedure.
- All the properties linking a procedure to the authorities involved in it such as `has Issue Authority`, `has Reception Authority`, `hasCompetentAuthority` and `hasValidationAuthority`.

- We also represent the dates of emission, transmission or execution of a Procedure thanks to the data property `hasEmissionDate`, `hasTransmissionDate` and `hasExecutionDate` respectively.

Many properties characterize the actions requested in the procedures, with for example:

- In case of actions like a transmission of information, we represent its source and destination authorities with the object properties `fromTransmission` and `toTransmission`.
- Several Boolean data properties allow to indicate if an action is necessary, adapted, or even if it would cause harm to someone. An evolution of the model involves refining the representation of these properties by switching from a boolean indicator to more detailed information like who it would cause harm to.

The ontology has not yet been published since it is still being tested and validated through experimentation.

4. Validation and Experimentation

As part of the ontology validation process, we used it in a framework of decision support system for data sharing or data processing requests by LEAs. Given a set of rules from regulations and given a data sharing request (DSR), the goal is to determine if the data sharing request is permitted, prohibited or mandatory according to the law. This framework, inspired by Gandon *et. al* work about normative requirements [8], uses formal rules manually extracted from the articles used to build the ontology. The general idea is to deploy a knowledge graph from the ontology and to represent each data sharing request as a named graph that will populate the knowledge graph. Then we can reason over this graph with SPARQL queries that will add to each named graph (data sharing request) a property indicating whether or not it is compliant with one of the formal rules. For example, let's consider the first paragraph of article 6 from [3], illustrated in Figure 2.

The SPARQL query associated with this article is as follows, given the definition of `nru:Rule1` as a Permission Rule in the knowledge graph beforehand:

```
INSERT { graph ?g { nru:Rule1 nrv:hasCompliance ?g } }
WHERE  { graph ?g {
    ?action a :Emission .
    ?action :involvesProcedure ?eio .
    ?action :isNecessary "true"^^xsd:boolean .
    ?eio :asksMeasureEIO ?measure .
    ?measure :conditionsIdem "true"^^xsd:boolean .}
```

To test the framework, we manually created 20 data-sharing requests allowing to test the triggering conditions of each rule. For example, to test article 6 paragraph 1 of [3], we consider the following scenario:

> *An authority "authority_1" issues a European Investigation Order (EIO) for the authority "exec_auth_1" and with a validation authority "valid_auth_1". This EIO asks*

Article 6

Conditions for issuing and transmitting an EIO

1. The issuing authority may only issue an EIO where the following conditions have been met:

(a) the issuing of the EIO is necessary and proportionate for the purpose of the proceedings referred to in Article 4 taking into account the rights of the suspected or accused person; and

(b) the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case.

2. The conditions referred to in paragraph 1 shall be assessed by the issuing authority in each case.

3. Where the executing authority has reason to believe that the conditions referred to in paragraph 1 have not been met, it may consult the issuing authority on the importance of executing the EIO. After that consultation the issuing authority may decide to withdraw the EIO.

Figure 2: Article 6 of DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT

> *for a specific investigation measure: the seizure of materiel from a certain "Arthur Watts" living at "address_01" to prevent a proof destruction. The EIO also indicates that it is "necessary".*

We express this DSR as a named graph in RDF format, by populating the ontology to form a knowledge base, which we present here using the TriG syntax:

```
<*named graph uri*> {
    :EIO_emission_01
        a :ProcedureEmission;
        :involvesProcedure :EIO_01;
        :hasIssueAuthorityEIO :authority_1;
        :hasExecutionAuthorityEIO :exec_auth_1;
        :hasValidationAuthorityEIO :valid_auth_1;
        :isNecessary "true"^^xsd:boolean.

    :EIO_01
        a :EIO;
        :asksMeasureEIO :measure_01.

    :measure_01
        a :InvestigationMeasure;
        a :MaterialSeizure;
        :hasJustificationMeasure :risk_of_evidence_alteration;
        :involvesPersonMeasure :Arthur_Watts;
        :involvesLocationMeasure :address_01.      }
```

The reasoning engine, here a SPARQL endpoint, matches the conditions of the SPARQL request and the RDF triples in the named graph. Then, with all the conditions met, a new

triple is added to the named graph to indicate that the DSR it represents complies with "Rule1", meaning that the requested procedure shall be permitted.

5. Conclusion and Future Work

This paper presented a new ontology usable in a decision-making support framework dedicated to data management between law enforcement agencies. This ontology captures the specific elements needed to represent legal rules, the context of data-related procedures among LEAs as well as the involved dataset metadata. We showed how it can be used in a rule-based reasoning engine to determine the compliance of procedures involving data sharing and processing in LEAs like EIO and EPOC to regulations.

Future work includes validating the ontology thanks to methods like OOPS! [9] and OQuaRE [20] to ensure its correctness. After generating the ontology documentation and metadata, we will make it available online. Another short term perspective will be to improve the ontology reusability by splitting it into meaningful modules as well as by adding alignments with domain and core ontologies.

Since the legal text selection that we conducted in this study, these legal texts have been updated and new texts have been voted. For example, [4] has not been a proposal since last year, and the text that should be considered in its stead is *Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings* [21]. There are also *Directive (EU) 2023/977 of the European Parliament and of the Council of 10 May 2023 on the exchange of information between the law enforcement authorities of Member States and repealing Council Framework Decision 2006/960/JHA* [22] and *Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings* [23] that seems to cover aspects of the application case.

Testing other frameworks of rule-based reasoning is also part of future work to develop a full decision support system. We are planning to use a formalism based on the LKIF [12] format together with the CARNEADES inference engine [24] to generate argument graphs explaining the system decisions. The final goal would be to compare the results obtained through these different frameworks.

Acknowledgments

The work in this paper is partially funded by the H2020 project STARLIGHT[10] ("Sustainable Autonomy and Resilience for LEAs using AI against High priority Threats") that received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101021797. We would also like to thank Ronan PONS, PhD student in Law, who assisted this work by providing his insight as legal expert.

[9] https://oops.linkeddata.es
[10] https://www.starlight-h2020.eu/

References

[1] EUR-Lex, Regulation - 2016/679 - en - gdpr - eur-lex.europa.eu., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679, 2016. Last changed: 04/05/2016, Last Accessed: 04/04/2024.

[2] EUR-Lex, 2016/680 - en - law enforcement directive; led - eur-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L0680, 2016. Last changed: 04/05/2016, Last Accessed: 04/04/2024.

[3] EUR-Lex, Directive - 2014/41 - en - eur-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041, 2014. Last change: 13/03/2022, Last Accessed: 04/04/2024.

[4] EUR-Lex, 52018pc0225 - en - eur-lex - european union, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018PC0225, 2018. Last Accessed: 04/04/2024.

[5] L. Robaldo, C. Bartolini, M. Palmirani, A. Rossi, M. Martoni, G. Lenzini, Formalizing gdpr provisions in reified i/o logic: The dapreco knowledge base, Journal of Logic, Language and Information 29 (2019) 401 – 449. URL: https://api.semanticscholar.org/CorpusID:213350734.

[6] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, L. Robaldo, Pronto: Privacy ontology for legal reasoning, in: International Conference on Electronic Government and the Information Systems Perspective, Springer International Publishing, Cham, 2018, pp. 139–152. URL: https://api.semanticscholar.org/CorpusID:52047214.

[7] M. Palmirani, G. Governatori, A. Rotolo, S. Tabet, H. Boley, A. Paschke, Legalruleml: Xml-based rules and norms, in: Rule-Based Modeling and Computing on the Semantic Web: 5th International Symposium, RuleML 2011–America, Ft. Lauderdale, FL, Florida, USA, November 3-5, 2011. Proceedings, Springer, 2011, pp. 298–312.

[8] F. Gandon, G. Governatori, S. Villata, Normative requirements as linked data, in: JURIX 2017-The 30th international conference on Legal Knowledge and Information Systems, 2017, pp. 1–10.

[9] C. Griffo, Ufo-l: A core ontology of legal concepts built from a legal relations perspective, in: DC3K, Doctoral Consortium on Knowledge Discovery, Knowledge Engineering, Knowledge Management, 2015, pp. 13–20. URL: https://api.semanticscholar.org/CorpusID:53593399.

[10] C. Griffo, J. P. A. Almeida, J. A. Lima, T. Prince Sales, G. Guizzardi, Legal powers, subjections, disabilities, and immunities: Ontological analysis and modeling patterns, Data & Knowledge Engineering 148 (2023) 102219. URL: https://www.sciencedirect.com/science/article/pii/S0169023X23000794. doi:https://doi.org/10.1016/j.datak.2023.102219.

[11] M. Kifer, Rule interchange format: The framework, in: D. Calvanese, G. Lausen (Eds.), Web Reasoning and Rule Systems, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 1–11.

[12] T. F. Gordon, G. Governatori, A. Rotolo, Rules and norms: Requirements for rule interchange languages in the legal domain, in: International Workshop on Rules and Rule Markup Languages for the Semantic Web, Springer, 2009, pp. 282–296.

[13] L. Robaldo, C. Bartolini, G. Lenzini, The DAPRECO knowledge base: Representing the GDPR in LegalRuleML, in: Proceedings of the Twelfth Language Resources and Evaluation Conference, European Language Resources Association, Marseille, France, 2020, pp. 5688–5697. URL: https://aclanthology.org/2020.lrec-1.698.

[14] H. J. Pandit, D. Lewis, Modelling provenance for gdpr compliance using linked open data vocabularies, in: Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) co-located with ISWC 2017, CEUR-WS volume 1951, 2017. URL: https://ceur-ws.org/Vol-1951/PrivOn2017_paper_6.pdf.
[15] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data privacy vocabulary (dpv) – version 2, 2024. arXiv:2404.13426.
[16] R. Hoekstra, J. Breuker, M. Di Bello, A. Boer, The lkif core ontology of basic legal concepts, International Journal of High Performance Computing Applications - IJHPCA (2007) 43–63.
[17] G. Guizzardi, A. Benevides, C. Fonseca, D. Porello, J. Almeida, T. Prince Sales, Ufo: Unified foundational ontology, Applied Ontology (2022). doi:10.3233/AO-210256.
[18] C. Griffo, J. Castello, Ontology of healthcare compliance based on just culture paradigm, in: workshop RELATED'21: Relations in the Legal Domain, @ International Conference on Artificial Intelligence and Law 2021, June 21–25, 2021, Sao Paulo, SP, Ceur-ws vol-2896, 2021, pp. 25–43. URL: https://ceur-ws.org/Vol-2896/RELATED_2021_paper_3.pdf.
[19] M. Uschold, M. Gruninger, Ontologies: principles, methods and applications, The Knowledge Engineering Review 11 (1996) 93–136. doi:10.1017/S0269888900007797.
[20] A. Duque-Ramos, J. T. Fernández-Breis, M. Iniesta-Moreno, M. Dumontier, M. E. Aranguren, S. Schulz, N. Aussenac-Gilles, R. Stevens, Evaluation of the oquare framework for ontology quality, Expert Syst. Appl. 40 (2013) 2696–2703. URL: https://doi.org/10.1016/j.eswa.2012.11.004. doi:10.1016/J.ESWA.2012.11.004.
[21] EUR-Lex, Regulation - 2023/1543 - en - eur-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543, 2023. Last Accessed: 19/06/2024.
[22] EUR-Lex, Directive - 2023/977 - en - eur-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023L0977, 2023. Last Accessed: 19/06/2024.
[23] EUR-Lex, Directive - 2023/1544 - en - eur-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023L1544, 2023. Last Accessed: 19/06/2024.
[24] T. F. Gordon, Combining rules and ontologies with carneades, in: Proceedings of the 5th International RuleML2011@ BRF Challenge, CEUR Workshop Proceedings, Citeseer, 2011, pp. 103–110.

A. Overview of the ontology

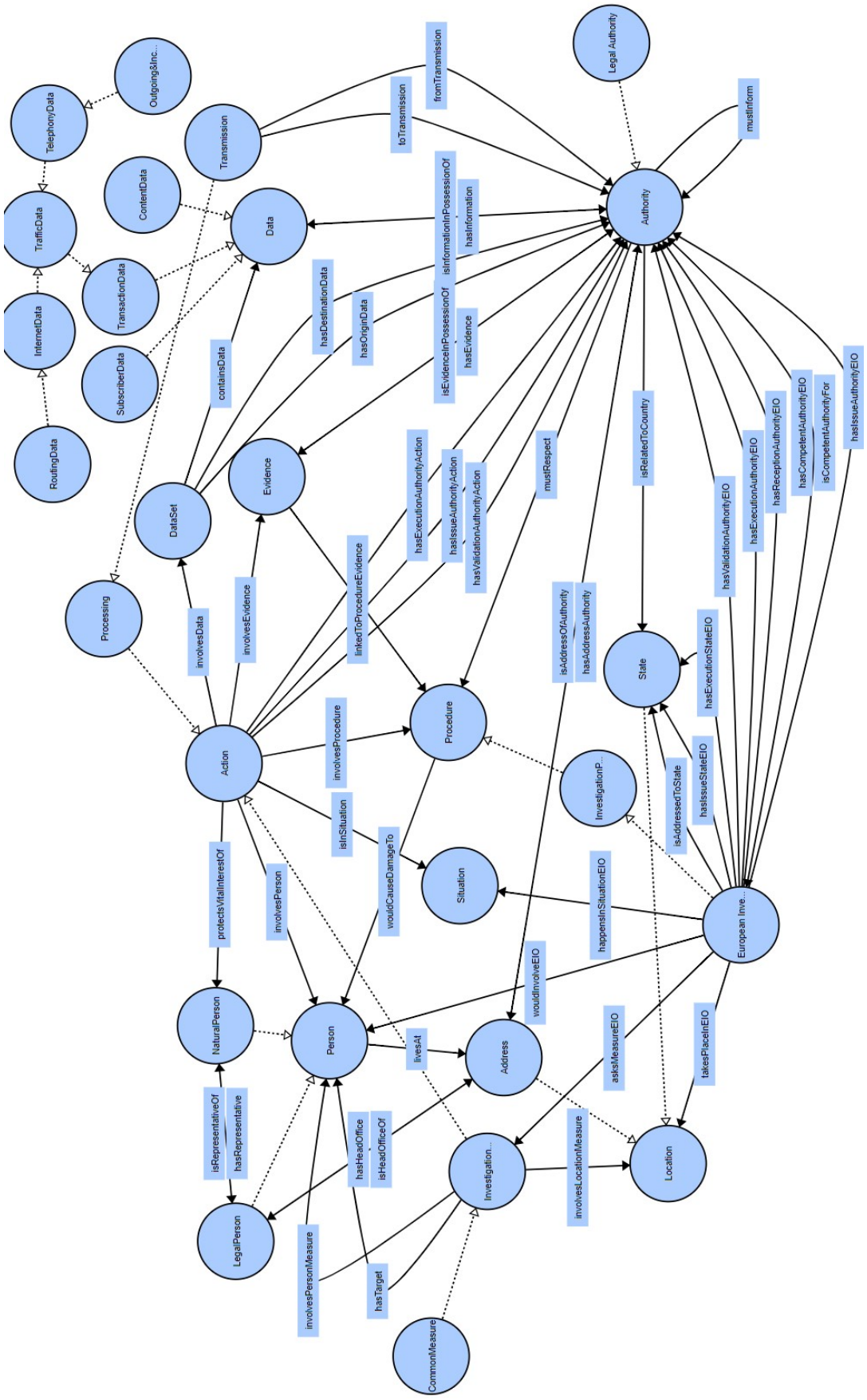


Figure 3: Overview of the ontology core elements