Semantic Web 15 (2024) 709–743
DOI 10.3233/SW-223009
IOS Press

Analysis of ontologies and policy languages to represent information flows in GDPR

Beatriz Esteves * and Víctor Rodríguez-Doncel
Ontology Engineering Group, Universidad Politécnica de Madrid, Spain
E-mail: beatriz.gesteves@upm.es

Editors: Michel Dumontier, Maastricht University, The Netherlands; Sabrina Kirrane, Vienna University of Economics and Business, Austria; Oshani Seneviratne, Rensselaer Polytechnic Institute, USA
Solicited reviews: Guido Governatori, NICTA Queensland, Australia; Tassilo Pellegrini, University of Alpied Sciences St. Pölten, Austria; Julian Padget, University of Bath, United Kingdom; Two Anonymous Reviewers

Abstract. This article surveys existing vocabularies, ontologies and policy languages that can be used to represent informational items referenced in GDPR rights and obligations, such as the 'notification of a data breach', the 'controller's identity' or a 'DPIA'. Rights and obligations in GDPR are analyzed in terms of information flows between different stakeholders, and a complete collection of 57 different informational items that are mentioned by GDPR is described. 13 privacy-related policy languages and 9 data protection vocabularies and ontologies are studied in relation to this list of informational items. ODRL and LegalRuleML emerge as the languages that can respond positively to a greater number of the defined comparison criteria if complemented with DPV and GDPRtEXT, since 39 out of the 57 informational items can be modelled. Online supplementary material is provided, including a simple search application and a taxonomy of the identified entities.

Keywords: Privacy policy languages, data protection ontologies, GDPR, rights, obligations

1. Introduction

Westin [96] shaped the way we define online privacy before the web existed at all. One of his two major postulates was that individuals should be able to determine to what extent information about them is communicated to others. The second of these postulates was that technological artifacts could be used to achieve this goal. His books in the late sixties and the seventies exerted significant influence on the privacy legislation that was enacted in the following years, and even today, the European General Data Protection Regulation (GDPR), which came into full effect on May 25th of 2018, owes much to his work. Any information system has data representational needs, and privacy and data protection related information systems will have to represent ideas such as 'consent' or 'the right to erasure'. If these applications are to interoperate, then the need for standard formats is clear, and the adoption of semantic-web enabled technologies that facilitate privacy-related data exchange is advantageous such as in data portability.

Machine-readable policy languages have been on the scene for some decades. Policy languages allow us to represent the will of an individual or organization to grant access to a certain resource, and they govern the operation of actual systems over actual data. They seem perfectly aligned with Alan Westin's vision and indeed several privacy-related policy languages have been defined and used in real scenarios. On the other hand, computers can also help

*Corresponding author. E-mail: beatriz.gesteves@upm.es.

in other privacy and data protection tasks different from enforcing access to personal data, and policy languages are not enough to cover every representational need. Thus, in the last few years, vocabularies and computer ontologies have appeared to formalize concepts and rules in the domain that can be used either to simply represent information as RDF, or to govern ontology-based information systems. Not all of them, however, had the GDPR specifically as their framework of reference.

This paper surveys existing policy languages, vocabularies and ontologies in the domain of privacy and data protection, and it analyses their adequacy to support GDPR-related applications. These GDPR-related applications may either support individuals to manage their personal information or to support data controllers, data processors and other stakeholders to better manage compliance with the GDPR. This joint analysis of needs (individual-oriented and company-oriented) is based on the claim that these tools may converge in a near future, and that having common vocabulary elements and common data models to refer to GDPR rights and obligations and to denote specific GDPR concepts would permit heterogeneous applications to speak in the same terms and interoperate. Taking into account this rationale, we focus on the above motivations to address the following research question: ***Are the existing policy languages and vocabularies suitable to meet the representational needs brought on by the newly applicable GDPR's rights and obligations?***.

Moreover, the main contributions of this paper are:

(i) a study of GDPR in terms of flows of information in different deontic modalities, systematized in Fig. 1, and further specified in Table 1 where the informational elements necessary for the management of each GDPR right and obligation are specified;
(ii) a survey of 22 existing vocabularies, ontologies and policy languages and their analysis in relation to that informational model; and
(iii) an online portal[1] with additional resources for the reviewed works, a REST API service to find references to specific concepts and also a lightweight ontology, the GDPR Information Flows (GDPRIF), specified to model the relationships triggered by the study on GDPR information flows.

The paper is organized as follows: Section 2 describes in detail the types of information that have to be shared between data subjects, controllers and other interested parties, as well as the main rights and obligations found in the GDPR that may be represented. Section 3 identifies related work and Section 4 systematically reviews the existing privacy-related policy languages first, and then the most salient vocabularies and ontologies in the domain. Section 5 provides an analysis of the solutions in the light of GDPR, following a systematic comparison framework, and the description of the supplementary webpage which has been published with additional resources about the reviewed solutions, a REST API service to look for specific concepts and a vocabulary with the concepts identified in Section 2. Finally, the last section synthesizes our conclusions, explicitly identifying the recommendations and possible representational needs that have to be covered.

2. Information flows in the GDPR

In the light of the established GDPR rights and obligations, a set of information flows, related to the information that needs to be exchanged between stakeholders, can be identified. These stakeholders can be classified as a (DS) data subject, a (DC) data controller, a (DP) data processor, a (Rp) recipient, a (SA) supervisory authority or a (DPO) data protection officer.

In this context, an information flow refers to the information that has to be transmitted from one stakeholder to another so that a right or obligation can be invoked and granted. For instance, if a data subject invokes its right to erasure, along with the request, there is the need to represent information related to the grounds on which the request is based, and the controller needs to transmit this information to the other controllers processing the same personal data.

Figure 1 shows a diagram of the information flows that represent the transfer of information foreseen by GDPR's rights and obligations regarding data subjects, controllers and other stakeholders. This chart is derived from an

[1] https://protect.oeg.fi.upm.es/sota/

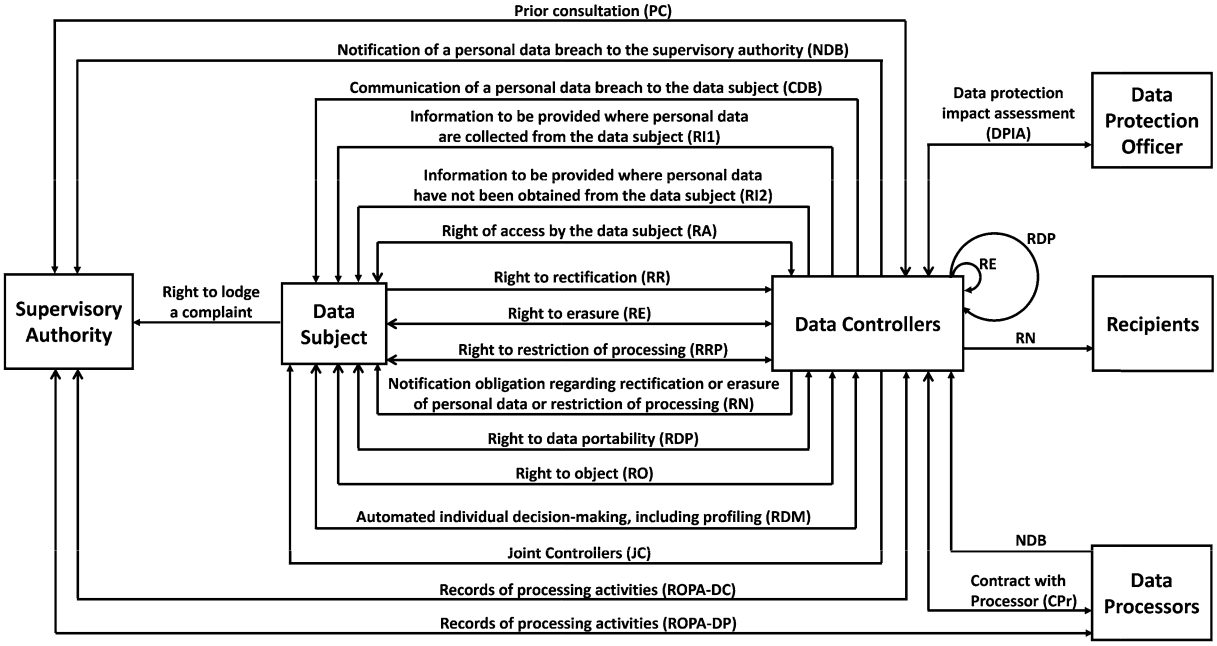

Fig. 1. GDPR's rights and obligations as information flows. The bidirectional arrows represent a right or obligation in which a request for information and respective response is expected (the open arrowhead, ➜, represents the entity waiting for the response and the closed arrowhead, ➡, the entity being requested), while the unidirectional arrows represent only a request or notification and no reply is expected (with the closed arrowhead, ➡, representing the entity being requested or notified).

analysis of Chapter's III and IV (*'Rights of the data subject'*[2] and *'Controller and processor'*,[3] respectively) of the GDPR. Each article in both chapters was manually studied to search for interactions between the aforementioned stakeholders and, when a flow of information was identified between more than one stakeholder, the respective interaction was recorded in the diagram.

Therefore, in this section, the GDPR rights and obligations that were classified as an information flow between GDPR's stakeholders are studied with the purpose of assessing which informational elements need to be represented in order to support this stream of information. A methodical study of these elements of information was manually performed for each identified information flow and systematised in Table 1. In addition, for each described item, a list of GDPR's articles where they are mentioned is also presented for readers to be able to refer to the regulation. From this list, it was therefore possible to establish mappings between each right or obligation and the respective specified informational items, which are presented in Tables 2 and 3, related to the rights of the data subject and to the responsibilities of the controllers and processors, respectively.

In particular, we shall emphasize the need to support Articles 13 and 14 of the GDPR, which describe the so-called *'right to be informed'*. According to these articles, whether personal data is collected directly from the data subject or obtained through other data sources, data controllers need to inform data subjects about any processing of personal data so that their activities are legal, fair and transparent. These articles, and the others that make up Chapter III of the GDPR, are studied here in order to understand what information data subjects are entitled to receive in the exercise of their rights and, correspondingly, what information data controllers need to disclose to be compatible with the GDPR. Sections 2.1 and 2.2 briefly describe these rights, as well as the informational items that may need to be represented.

The rights and obligations of controllers and processors, described in GDPR's Chapter IV, are also analyzed here for the same purpose of identifying which pieces of information need to be represented in order for these

[2] https://gdpr-info.eu/chapter-3/
[3] https://gdpr-info.eu/chapter-4/

Table 1

Informational items to be represented and respective identifiers (I*), which will be used to specify the informational elements necessary for the management of each right and obligation represented in Fig. 1. The GDPR articles that mention these items are also specified

I*	informational items – GDPR Article(s)	I*	informational items – GDPR Article(s)
I1	Controller identity – **13.1(a), 14.1(a), 30.1(a), 30.2(a)**	I30	Grounds to not comply with right not to be subjected to decision making – **22.2**
I2	Controller contact details – **13.1(a), 14.1(a), 30.1(a), 30.2(a)**	I31	Joint controller identity – **26, 30.1(a)**
I3	Controller's representative identity – **13.1(a), 14.1(a), 30.1(a), 30.2(a)**	I32	Joint controller contact details – **26, 30.1(a)**
I4	Controller's representative contact details – **13.1(a), 14.1(a), 30.1(a), 30.2(a)**	I33	Responsibilities of joint controllers – **26, 36.3(a)**
I5	DPO contact details – **13.1(b), 14.1(b), 30.1(a), 30.2(a), 33.3(b), 34.2, 36.3(d)**	I34	Subject-matter of the processing – **28.3**
I6	Purposes of the processing – **13.1(c), 14.1(c), 15.1(a), 28.3, 30.1(b), 35.7(a), 36.3(b)**	I35	Duration of the processing – **28.3**
I7	Legal basis of the processing – **6.1, 9.2, 13.1(c), 14.1(c)**	I36	Categories of processing – **28.3, 30.2(b)**
I8	Legitimate interests – **6.1(f), 13.1(d), 14.2(b), 35.7(a)**	I37	Categories of data subjects – **28.3, 30.1(c), 33.3(a)**
I9	Recipients / categories of recipients – **13.1(e), 14.1(e), 15.1(c), 17.2, 19, 30.1(d)**	I38	Obligations of the controller – **28.3**
I10	Transfers to third countries – **13.1(f), 14.1(f), 30.1(e), 30.2(c), 46, 47, 49.1**	I39	Obligations of the processor – **28.3**
I11	Retention period – **13.2(a), 14.2(a), 15.1(d), 30.1(f)**	I40	DPO identity – **30.1(a), 30.2(a), 33.3(b), 34.2**
I12	Data subject's rights – **13.2(b), 14.2(c), 15.1(e), 28.3**	I41	Technical and organizational security measures – **30.1(g), 30.2(d), 32.1, 35.7(d), 36.3(c)**
I13	Right to withdraw consent – **6.1(a), 9.2(a), 13.2(c), 14.2(d)**	I42	Processor identity – **30.2(a)**
I14	Right to lodge a complaint – **13.2(d), 14.2(e), 15.1(f)**	I43	Processor contact details – **30.2(a)**
I15	Statutory or contractual obligation details – **13.2(e)**	I44	Processor's representative identity – **30.2(a)**
I16	Existence of automated decision making – **13.2(f), 14.2(g), 15.1(h), 22.1, 22.4**	I45	Processor's representative contact details – **30.2(a)**
I17	Categories of personal data – **9.1, 14.1(d), 15.1(b), 28.3, 30.1(c), 33.3(a)**	I46	Nature of data breach – **33.3(a), 34.2**
I18	Source of personal data – **14.2(f), 15.1(g)**	I47	Approximate number of data subjects – **33.3(a)**
I19	Grounds to not comply with information right – **13.4, 14.5**	I48	Approximate number of personal data records – **33.3(a)**
I20	Safeguards related to the transfer to a third country – **15.2, 30.1(e), 30.2(c)**	I49	Consequences of personal data breach – **33.3(c), 34.2**
I21	Copy of personal data – **15.3, 20.1**	I50	Measures to address and mitigate data breach's effects – **33.3(d), 34.2**
I22	Request to complete incomplete personal data – **16**	I51	Systematic description of processing operations – **35.7(a)**
I23	Grounds to request erasure of data – **17.1**	I52	Assessment of the necessity and proportionality of the processing operations – **35.7(b)**
I24	Technical measures taken to erase data – **17.2**	I53	Assessment of the risks to the rights and freedoms of data subjects – **35.7(c)**
I25	Recipients contact details – **17.2, 19**	I54	Responsibilities of the controller – **36.3(a)**
I26	Grounds to not comply with right of erasure – **17.3**	I55	Responsibilities of the processors – **36.3(a)**
I27	Grounds to request restriction of processing – **18.1**	I56	Means of processing – **36.3(b)**
I28	Transfer data directly between controllers – **20.2**	I57	Data protection impact assessment (DPIA) – **35, 36.3(e)**
I29	Grounds to not comply with right to object – **21**		

stakeholders to be in compliance with the GDPR. Section 2.3 details the informational elements and respective rights and obligations that may need to be modeled.

Moreover, this study of rights and informational items will serve as a basis for the analysis of privacy-related policy languages to understand which rights and obligations can already be fully or partially formalized and for the comparison of privacy and data protection vocabularies and ontologies to perceive which can be used and extended to represent the informational items described in Table 1.

2.1. The right to be informed

Chapter III of the GDPR establishes nine fundamental rights of the data subject when it comes to the lawful processing of their personal data.

In particular, Articles 13 and 14 detail the *'Information to be provided where personal data are collected from the data subject'* (RI1) and the *'Information to be provided where personal data have not been obtained from the data subject'* (RI2), respectively. According to them, for the processing of personal data to be lawful, fair and transparent, a certain set of informational items must be provided, namely items I1 to I19 described in Table 1.

This information, and any other communications provided in the context of the provision of data subjects' rights, should be given in a concise, transparent and clear language and in an easily accessible manner. This information may also be provided with standardized icons for a more visible and intelligible overview of the intended processing.

2.2. Other data subject's rights

The data controller has the obligation to support the exercise of the data subject's rights and needs to reply with information to any requests related to the exercising of such rights within a month upon receiving the request. This period can be extended by a further two months if the data subject's request is too complex or in the case of a large number of requests. The information should be freely provided and by electronic means, unless the data subject states otherwise.

Apart from the *'right to be informed'*, already described in the previous section, the data subject is entitled to the following rights:

(RA) the *'right of access'* to the personal data being processed: data subjects have the right to receive confirmation that their data is being processed and a copy of the data in a common electronic format, as well as information about the purposes for processing, categories of the concerned personal data, their source, if not directly collected from the data subject, the recipients, the storage period, the existence of the data subject's rights as well as the right to lodge a complaint with a DPA, details of the existence of automated decision making and the security measures applied where personal data is transferred to a third party.

(RR) the *'right to rectification'*: the data subject has the right to obtain from the data controller the amendment of inaccurate personal data and, where the data is incomplete, the right to have personal data completed.

(RE) the *'right to erasure'* or *'right to be forgotten'*: the data controller has the obligation to delete personal data when it is no longer needed for the purposes which it was collected; when the data subject withdraws consent and there is no other legal basis for the processing; when the data subject objects to the processing; when said processing is unlawful; when it has to be erased to comply with a legal obligation; or when the data was collected for the provision of information society services.[4]

(RRP) the *'right to restriction of processing'* of personal data: the data subject has the right to request the ceasing of the processing when the accuracy of the data is being contested; when the processing is unlawful and the data subject does not wish to erase the data; when the purposes stated by the controller are no longer valid but the data subject needs it for any legal claims; or when the data subject objects to the processing.

(RN) the *'right to be notified'* about the rectification, erasure or restriction of processing: the data controller has the obligation of notifying the data subject and the recipients to whom the data was disclosed, as well to disclose these recipients to the data subject.

(RDP) the *'right to data portability'*: the data subject has the right to receive its data in a commonly used and machine-readable format and has the right to request that its data be transferred directly from one controller to another.

(RO) the *'right to object'* to any processing, including profiling.

(RDM) the *'right to not be subjected to automated decision-making'*, including profiling.

The informational items to be granted to the data subject in function of the established GDPR rights are represented in Table 2.

2.3. Rights and obligations of controllers and processors

Data controllers must be ready to demonstrate that their processing activities are in accordance with the GDPR and that they have in place the appropriate security measures to ensure people's right to privacy and data protection. These measures must take into account the nature, context and risks associated with each processing activity and should be embedded by design and by default in the data controllers' services.

The following rights and obligations must be observed by the data controllers and processors so that they can comply with the regulation:

[4] In GDPR's Article 4.25, 'information society service' refers to "a service as defined in point (b) of Article 1.1 of Directive (EU) 2015/1535 of the European Parliament and of the Council", meaning any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

Table 2
Informational items (I*) to be provided to the data subject, according to the rights (R*) defined under Chapter III of the GDPR

Rights (R*)	Informational items (I*)
RI1	I1 to I17, I19
RI2	I1 to I14, I16 to I19
RA	I6, I9, I11, I12, I14, I16 to I18, I20, I21
RR	I22
RE	I9, I23 to I26
RRP	I25, I27
RN	I9, I25
RDP	I21, I28
RO	I29
RDM	I30

(JC) the *'joint controllers'* responsibilities: in the case where there are two or more controllers determining the purposes and means of processing, they are joint controllers. They must determine the responsibilities of each controller in relation to the obligations generated by the data subject's rights and this information should be communicated to the data subjects.

(CPr) contract with *'processors'*: the controller can establish contracts with processors, that have in place the appropriate security measures, for the processing to be carried out on behalf of them. This processing must be governed by a contract between controller and processor, that establishes the subject-matter, duration, nature and purpose of processing, as well as the personal data types, categories of data subjects and the rights of obligations of both the data controller and the data processor. The processor can only hire a sub-processor with the authorization of the controllers.

(ROPA-DC) *'records of processing activities'* of data controllers: each controller and its representative should keep a record of the processing activities under their responsibility, which must be available to the supervisory authorities when requested.

(ROPA-DP) the *'records of processing activities'* of data processors: each processor and its representative should keep a record of the processing activities carried out on behalf of a controller, which must be available to the supervisory authorities when requested.

(NDB) the *'notification of a data breach'* to the supervisory authority: the data controller has 72 hours to notify the competent supervisory authority that a personal data breach has occurred. The processor should inform the controller without delay as soon as it is aware of the breach.

(CDB) the *'communication of a data breach'* to the data subject: the data subjects have the right to be informed about any data breach that results in a high risk to their rights and freedoms. This communication should contain at least the nature of the breach and the measures that are being taken to mitigate it.

(DPIA) the *'data protection impact assessment'*: in the case where the data controllers are going to perform an extensive evaluation of personal data based on automated processing, processing activities over special categories of data or criminal data or a systematic monitoring on a large scale, the controller should draft an assessment of the impact of the processing activities, and respective risks to the protection of personal data, with the guidance of the data protection officer.

(PC) the *'prior consultation'* right: the controller has the right to consult the supervisory authority, prior to the processing, when the DPIA illustrates that the processing activities will result in a high risk to the privacy of the data subjects if the proper measures to mitigate risks are not implemented.

The informational items that must be represented, in function of the rights and obligations of the data controllers and processors, are represented in Table 3.

Table 3
Informational items (I*) to be modelled, according to the rights and obligations of the controllers and processors, defined under Chapter IV of the GDPR

Rights / Oblig.	Informational items (I*)
JC	I31 to I33
CPr	I6, I12, I17, I34 to I39
ROPA-DC	I1 to I6, I9 to I11, I17, I20, I31, I32, I37, I40, I41
ROPA-DP	I1 to I5, I10, I20, I36, I40 to I45
NDB	I5, I17, I37, I40, I46 to I50
CDB	I5, I40, I46, I49, I50
DPIA	I6, I8, I41, I51 to I53
PC	I5, I6, I33, I41, I54 to I57

3. Related work

Some articles review the existing privacy-related policy languages, however, for the most part, they were published before the GDPR was enacted.

Kumaraguru et al. [59] provided a literature review on available privacy policy languages with the goal of developing a framework with metrics for their analysis. This framework classified languages based on the situations in which they could be used, also considering whether the policy language was user-centered or company-centered.

In 2007, Duma et al. [33] offered a scenario-based comparison of six policy languages focused on user privacy. The adopted evaluation criteria targeted the languages abilities to classify the sensitiveness of the information, to deal with resource granularity, to address access control, to support the principle of minimal information disclosure and more. Furthermore, it provides example implementations based on specific scenarios created to evaluate each specific criterion.

Moreover, Kasem-Madani and Meier [52] produced a survey focused on security and privacy policy languages. The survey's goal is to present an overview of the existing solutions as well as providing a categorization framework to facilitate the adoption of policy languages. The main categories of the framework to classify the languages are the scope, syntax, extensability, context, type (focused on issues such as security, privacy or accountability), intention of use (user-centred, enterprise-centred or both) and usability (language oriented to humans or machines).

Zhao et al. [99] produced a review focused on existing policy languages that can be used to express user's privacy preferences. The identified languages were analysed against a set of three features: the purpose of the language, i.e., if it is user or company-focused, the existence of user-friendly interface tools, and interoperability, however existing legislation on the privacy domain was not considered.

More recently, in 2018, Peixoto and Silva [84] present a framework for analyzing goal-oriented modelling languages in the context of representing requirements extracted from the GDPR, the ISO 29100 standard [49], the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [73], and other privacy-related sources. The authors focused on three particular modelling languages, i* 2.0 [32], NFR-Framework [27] and Secure-Tropos [68], that were analysed against the fourteen (extracted) privacy requirements, e.g., capability to model different types of actors, capability to model different types of personal information, or capability to model consent.

The most recent review work on privacy languages, by Leicht and Heisel [61], intends to provide a survey on languages in the context of privacy policies that can help users to easily understand them and that are compatible with data protection legislations such as the GDPR. Therefore, this framework identifies the criteria to compare the languages through the GDPR legislation. The identified criteria are system obligations, time constraints and formalization of the language.

Other review works related to the privacy and data protection domain have been published, namely overviews of access control frameworks, rights expression languages or other semantic approaches related to the representation of consent.

Kirrane et al. [56] provide an overview of access control models, such as the Mandatory Access Control (MAC), the Discretionary Access Control (DAC) and the Role Based Access Control (RBAC) models, and other RDF-based

standards and policy languages frameworks. A collection of access control requirements is proposed and are used to categorize the described frameworks accordingly.

Pellegrini et al. [85] produced a preliminary survey on Rights Expression Languages (RELs). RELs are used to define machine-readable permissions, obligations and prohibitions, and are an essential component of any Digital Rights Management (DRM) system. This work also proposed a framework to classify RELs according to their application area in the DRM domain, namely for the purpose of specifying access and trust policies, license policies and contract policies.

Pandit [78] PhD thesis describes and analyses state-of-the-art semantic-based technologies used to support and assess GDPR compliance, including privacy policy solutions, consent-related approaches and other solutions developed in the context of data privacy and data protection projects. The solutions are compared according to a set of categories, such as the representation of GDPR concepts, consent-related information or personal data handling activities, evaluation of GDPR compliance or resource accessibility.

4. Privacy and data protection languages and ontologies: A survey

In this Section, the results of the survey on privacy-related policy languages and data protection ontologies and vocabularies are described in detail. Furthermore, Section 4.1 details the methodology followed to perform the survey and Sections 4.2 and 4.3 provide a systematic description of each identified solution.

4.1. Methodology

There has been a large number of works being published on the methodologies for conducting a literature review [58,92,95]. Specifically, in 2019, Snyder [92] published an overview of different categories of reviews and provided guidelines on how to conduct and evaluate them. Three types of review methodologies are presented, namely, systematic, semi-systematic and integrative approaches, which should be chosen according with the purpose, research questions or the types of work being reviewed. In the context of this review, an integrative approach [97] was used as it is the most suitable for the purpose of discussing and synthesizing different privacy-related policy languages and data protection vocabularies in a qualitative manner and also quantitatively in the case of the discussed vocabularies. Following this approach, the search for academic publications to be included in this review, and other published documentation as this is a distinctive feature of an integrative review, was performed according to the snowballing procedure [98]. We started by researching existing survey articles connected to privacy-related policy languages and data protection vocabularies, and then performed additional research based on citation analysis, using both backward and forward snowballing methodologies, that were first introduced by Webster and Watson [95]. First, a backward snowballing approach, i.e., review the reference list of the articles to identify new papers that should be considered, was performed and then a forward approach, i.e., target new articles that cite the papers already being considered.

The collected results were reviewed and, if relevant for this analysis, included in this article. The following criteria was used to analyse and evaluate the found documentation:

- Availability of a publication to analyse.
- Only publications in English were contemplated.
- Publications only focused on access control or rights expression were left out of the review process.
- Existence of online material was not considered a prerequisite, however it allows for a better understanding of the structure and information provided by the reviewed solution.
- In the cases where the found data protection vocabularies and ontologies include access to the specification, solutions can be quantified in terms of the core classes that they implement.
- Both Pre- and Post-GDPR works are considered.

Moreover, in the cases where the identified solutions were found to be developed within the framework of a project, the main goals and research directions of said project are described through information gathered on the project's website.

Table 4
Brief description of the resources described in Section 4.2

Abbreviation (Section)	Full Name	Creators	Version	Date of publication	Last update
P3P (4.2.1)	Platform for Privacy Preferences	Cranor et al.	1.0	1998	2010
ODRL (4.2.2)	Open Digital Rights Language	Iannella et al.	2.2	2001	2019
XPref (4.2.3)	XPath-based Preference Language	Agrawal et al.	–	2003	–
AIR (4.2.4)	Accountability In RDF	Khandelwal et al.	–	2007	2009
S4P (4.2.5)	SecPAL for Privacy	Becker et al.	–	2009	2010
POL (4.2.6)	Privacy Option Language	Stefan Berthold	–	2010	2013
PPO (4.2.7)	Privacy Preference Ontology	Sacco and Passant	–	2011	2013
LegalRuleML (4.2.8)	LegalRuleML Core Specification	Palmirani et al.	1.0	2012	2021
A-PPL (4.2.9)	Accountable Policy Language	Azraoui et al.	–	2013	2016
P2U (4.2.10)	Purpose-To-Use	Iyilade and Vassileva	–	2014	–
SPL (4.2.11)	SPECIAL Usage Policy Language	Bonatti et al.	1.0	2017	2019
DPF (4.2.12)	Declarative Policy Framework	Martiny et al.	–	2018	2020
LPL (4.2.13)	Layered Privacy Language	Gerl et al.	–	2018	2019

4.2. Privacy-related policy languages

In this subsection, we aim to identify privacy-related policy languages, describing the structure and information provided by each language as well as identify its compatibility with the GDPR to describe not only rights, but also obligations. For each solution, there is an introductory summary of the language complemented by a description of its main contributions, followed by a description of the core elements of the language. When available, specific examples of use cases using the language are mentioned, as well as implementations derived from it, including details on any available reasoners that use the work. The dependencies of the solutions in previously existing works are also documented when described in the literature. In addition, if developed in the framework of a project, its main goals are briefly described. In Table 4, there is a brief description of the policy languages specified in the subsequent subsections, 4.2.1 to 4.2.13, including information about the creators of the resources, version, date of publication and date of the last known update. These solutions are analysed in chronological order in relation to the date of publication and then in relation to the date of the last update. In Fig. 2, a dependency graph, that captures the relations between languages and its dependencies and follow-up works, is presented. The described solutions were evaluated and compared according with the following criteria:

Q1. Does it model deontic concepts (e.g., permissions, obligations)?
Q2. Can it be used to model GDPR concepts, such as the informational items in Table 1?
Q3. Does it provide any taxonomies of terms to populate the identified information flows?
Q4. Does it implement any mechanisms to assist with compliance?
Q5. Does it continue to be maintained? Are new improvements being developed?
Q6. Are the resources available in an open and accessible platform?

The results and discussion of this comparison are presented in Section 5.1 and systematised on Table 6.

4.2.1. Platform for Privacy Preferences (P3P)

P3P, implemented by Cranor et al. [30], emerged as a specification for websites to disclose privacy protocols in a machine-readable format so that web user agents could easily interpret them and notify the users about the decisions based on these practices. However, these mechanisms, that allow the user to be informed about the websites' privacy policies in relation to its respective data collection, do not mean that the sites are actually implementing these policies since P3P does not provide a way to enforce them. Thus, the P3P vocabulary was not built to comply with a specific regulation but rather to specify the practices of each website.

The main contributions of the P3P specification are a P3P-based data schema for the data that the website intends to collect, a standard group of purposes, data categories and recipients and a XML standard to define privacy policies. The P3P policies are made up of general assertions and specific ones, called statements, that are related only to

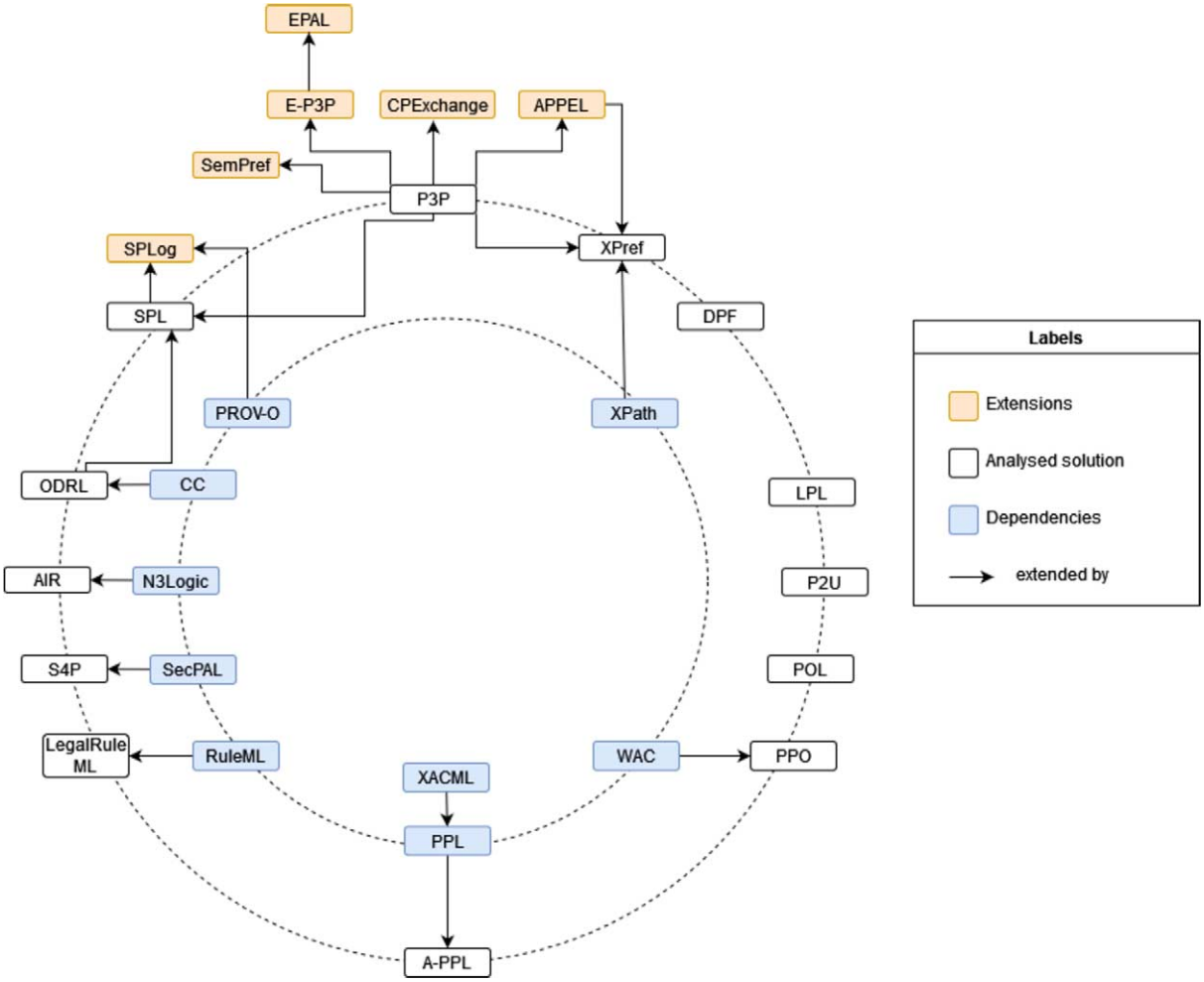

Fig. 2. Privacy-related policy languages dependency chart.

certain types of data. General assertions are constituted by the legal **entity** that applies the policy and an **access**, **disputes** and **remedies** elements. The access element expresses whether the website provides access to the data it collects. The disputes element provides a procedure for disputes on privacy practices, while the remedy element specifies the possible solutions in case a policy breach happens. In addition, each P3P statement is composed of a specific **data group**, that could contain one or more data elements, and includes **purpose**, **recipient** and **retention** elements. P3P defines a list of web relevant purposes for data processing, e.g., completion and support of the activity for which the data was provided, research and development or individual analysis. The purpose element should contain at least one purpose specification. The recipient element should specify the beneficiaries of the collected data according to the recipient types established by P3P and the retention element must reflect the retention policy that covers the statement data. Listing 1 presents a P3P policy which highlights the above described P3P elements. CatalogExample collects basic information about its users' computers and connections and also information on what pages users access, for system administration and research and development purposes, which is only used by the company and its agents and kept as long as appropriate for the stated purposes.

As P3P was designed to express web services policies, A P3P Preferences Exchange Language (APPEL) by Cranor et al. [29] was developed as an extension of P3P so that users can express their preferences. Therefore both languages should be used in order to match the user's privacy preferences with the services' privacy policies. In addition, in 2000, Bohrer and Holland [18] developed the Customer Profile Exchange (CPExchange) language,

```
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
@prefix p3p: <http://www.w3.org/2002/01/P3Pv1#> .
@prefix p3prdfv1: <http://www.w3.org/2002/01/p3prdfv1#> .

<http://example.com/#forBrowsers>
  a p3p:Policy ;
  p3p:disclosure <http://example.com/PrivacyPractice.html> ;
  p3p:entity [
    p3p:business.name [ rdf:value "CatalogExample" ] ;
    p3p:business.contact-info.postal.street [
        rdf:value "4000 Lincoln Ave." ] ;
    p3p:business.contact-info.postal.city [
        rdf:value "Birmingham" ] ;
    p3p:business.contact-info.postal.stateprov [
        rdf:value "MI" ] ;
    p3p:business.contact-info.postal.country [
        rdf:value "USA" ] ;
    p3p:contact.online.email [
        rdf:value "catalog@example.com" ] ;
    p3p:contact.telephonenum.intcode [ rdf:value "1" ] ;
    p3p:contact.telephonenum.loccode [ rdf:value "248" ] ;
    p3p:contact.telephonnum.number [ rdf:value "3926753" ]
  ] ;
  p3p:access p3prdfv1:AccessClass-nonident ;
  p3p:statement [
    p3p:purposeAlways p3prdfv1:Purpose-admin,
        p3prdfv1:Purpose-develop ;
    p3p:recipientAlways p3prdfv1:Recipient-ours ;
    p3p:retention p3prdfv1:Retention-stated-purpose ;
    p3p:data
        [ rdf:predicate p3prdfv1:dynamic.clickstream ,
            p3prdfv1:dynamic.http ]
  ] .
```

Listing 1. P3P policy adapted from Example 3.1 of the P3P specification [30], which specifies the privacy policy of CatalogExample for Browsers.

an XML specification for the transfer of customer data among enterprise services, which implements P3P privacy policies applicable to the data that is being exchanged. Similarly, IBM Research's[5] Enterprise Privacy Authorization Language (EPAL) [3], and its predecessor Platform for Enterprise Privacy Practices (E-P3P) [4], were also built using P3P statements to match enterprises' privacy policies with the users' preferences. In 2006, Li et al. [62] proposed a declarative data-centric semantics and a concise and clear syntax for P3P policies to represent the association of the different P3P elements. The main objective of this language is to declare policies that can be interpreted and represented in the same manner by different user agents. Building upon this semantics, the authors proposed a preference language, SemPref, that takes into account the meaning of the privacy policy instead of its syntactical representation.

The P3P 1.0 Specification became a World Wide Web Consortium (W3C) recommendation on April 16, 2002. However, it has had a limited implementation, since its use needs to be adopted by both Web services and users and, in addition, no protocol has been implemented for these P3P policies to reflect the actual privacy practices of the sites. Its status has turned to W3C obsolete recommendation on August 30, 2018 and thereby future implementations are not recommended.

Although this specification became a W3C recommendation, its lack of adoption made it obsolete in 2018, as previously mentioned. However, the influence of P3P cannot be underestimated, as its development and implementation was the first major effort made in the area of machine-readable privacy languages. The main lessons brought by this language are therefore related to the need of having a formal semantics, to describe both the data subject and controller policies that reflect their data preferences and practices, respectively, and the need to have tools that actually enforce the policies described by the languages.

4.2.2. Open Digital Rights Language (ODRL)

The ODRL Vocabulary & Expression 2.2 [48] is a W3C recommendation since February 2018, published by the Permissions & Obligations Expression (POE) Working Group (WG), being that its first version was released in 2001. The aim of this vocabulary is to define a language that can translate natural language policies to machine-readable formats, providing information about permissions, prohibitions and duties related to an asset. This vocabulary is based on the merge of the previous work performed by the ODRL Community Group (CG), the ODRL V2.1 Com-

[5] http://www.research.ibm.com/

```
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix cc: <http://creativecommons.org/ns#> .

<http://example.com/odrl-policy>
    a odrl:Privacy ;
    odrl:permission [
        odrl:target <http://example.com/beatriz:contacts> ;
        odrl:assignee <http://example.com/beatriz> ;
        odrl:assigner <http://example.com/company-a> ;
        odrl:action odrl:use ;
        odrl:duty [
            odrl:action odrl:obtainConsent ;
            odrl:consentingParty
                <http://example.com/beatriz> ;
            odrl:consequence [
                odrl:assigner
                    <http://example.com/company-a> ;
                odrl:action odrl:delete ;
            ]
        ]
    ] .
```

Listing 2. ODRL privacy policy between Company A and Beatriz, regarding the Asset *http://example.com/beatriz:contacts*, which allows the assigner to use it under the pre-condition they obtain consent from Beatriz. If the assigner does not fulfil the duty, then the consequence will be that they will have to delete the asset.

mon Vocabulary, the ODRL V2.1 XML Encoding, the ODRL V2.1 Ontology and the ODRL V2.1 JSON Encoding. ODRL is currently supported and maintained by the ODRL CG.

Two vocabularies are used to describe ODRL: the ODRL Core Vocabulary and the ODRL Common Vocabulary. ODRL's Core Vocabulary main class is the **policy**, that allows for the identification of a particular policy using its unique identifier. Each policy may contain several **rules** – a rule is an abstract class that defines the common features of permissions, prohibitions and duties. These types of rules are used to declare that a certain action is allowed, disallowed or obligated (duty and obligation are used as synonyms in ODRL), typically in relation to an asset. The permission may also be associated with a **duty** in the case where the action is mandatory. The rules are further refined by using **constraints** to determine the conditions under which the rule is applied, e.g., to establish that a certain permission is only valid until the end of 2022. The ODRL Vocabulary also specifies a set of 49 actions for rules, of which 9 are defined by Creative Commons.[6] The **parties** (can be a group of people, an organization or an agent) that enforce the rules can take different roles, depending on their position in relation to the asset – a party that issues the rule takes on the assigner role, while the recipient of the rule is the assignee. An **asset** is an identifiable entity, such as data, software, services or even a collection of these resources, that is subject to a rule. The ODRL Common Vocabulary further specifies the policy sub-classes, the functions that can be exercised by the parties involved, the actions to which the rules apply and a set of different constraint operands, e.g., temporal, spacial, or sector, that can be specified. Of particular interest in relation to the GDPR is the privacy policy subclass. This sub-class is related to policies that express rules over assets incorporating personal data. Therefore, the privacy policies that implement the ODRL language must inform the parties involved in which way the policy is being used and also with whom and for what purpose the policy is being shared with other parties. Listing 2 implements an ODRL privacy policy which highlights the described elements above.

The representational power of ODRL has a few shortcomings, as described by Kebede et al. [53], specially when it comes to the representation of delegation, the different semantics to represent duties or the handling of conflicts. However, there are works [39,40] on the way to formalise and harmonise the semantics of ODRL policies and constraints.

ODRL has already been used in several contexts, for instance by the working groups on Open Mobile Alliance SpecWorks[7] and by the International Press Telecommunications Council (IPTC) Rights Expressions WG for the RightsML Standard, a rights expression language for the media industry.[8]

[6] https://creativecommons.org/ns#
[7] https://www.omaspecworks.org/
[8] https://www.iptc.org/std/RightsML/2.0/RightsML_2.0-specification.html

4.2.3. XPref

Agrawal et al. [1] established XPref as an alternative to APPEL, which only allows for the definition of P3P policies that are unacceptable for the user. XPref resorts to XPath (XML Path Language) 1.0 and 2.0 expressions to replace APPEL rules, making the preferences formulation more precise and less error prone. XPath 1.0, by Clark and DeRose [28], and XPath 2.0, by Berglund et al. [14], are W3C Recommendations since November 16th, 1999, and December 14th, 2010, respectively, although no further maintenance will be performed to these specifications since later versions exist and have achieved the Recommendation statute. XPath's main goal is to provide a way to navigate through the hierarchical elements present in a XML document. To accomplish this task, XPath treats a XML document as a tree of nodes and a XPath expression, when applied to the document, establishes the ordered sequence of the nodes to produce a compact path notation. The path is then comprised of expressions that return nodes, such as root, element, text, attribute, name-space, processing instruction or comment nodes.

XPref was designed so that its rules cannot only identify combinations of P3P elements which make a policy unacceptable, according to the user's preferences, but also to verify that the presented elements are specified as acceptable. XPref manages these goals maintaining the APPEL syntax and semantics and its top classes, **ruleset** and **rule**. However, the rule bodies are replaced by XPath expressions since P3P policies are XML documents and thus can be easily matched with the XPath based rules. These expressions are specified by adding a *condition* attribute to the rule, which is responsible for triggering the rule when the XPath expression provides a non-empty outcome. Thus with XPref rules, using the *behavior* attribute, it is possible to establish a preference to block or allow services according to the P3P policy elements, e.g. purposes and recipients, specified on the *condition* attribute.

4.2.4. Accountability in RDF (AIR)

Khandelwal et al. [54] implemented AIR, a declarative language to make assertions of facts and addition of rules, based on N3Logic [15], that supports rule nesting, rule reuse, and automated explanations of rule-based actions performed by the AIR reasoner. These explanations are customizable and, since they can be a source of sensitive information such as Personally Identifiable Information (PII), can be used to provide privacy, for instance, to hide actions performed under certain rules.

N3Logic is an extension of the RDF data model that aims at expressing logic rules in the web, so that the same language is used for data and logic.

AIR builds on N3Logic's built-in functions, nested graphs and contextualized reasoning, allowing the AIR rules to adopt the usage of graphs as literal values, universally or existentially quantified variables in graphs and built-in functions or operators expressed as RDF properties.

Each rule has a unique Internationalized Resource Identifier (IRI), an HTTP Uniform Resource Identifier (URI), so that it is part of the linked data cloud and can be reused. These rules are defined using the following structure: **air:if** *condition*; **air:then** *then-actions*; **air:else** *else-actions*. The action instances can be annotated through the **air:description** properties. These annotations are then incorporated by the AIR reasoner in its justifications and can be used to hide PIIs present in the rule set. Also, the rules graph format allows for the nesting of rules within the same rule set, thus providing a way to segment the conditions stated by the rule in order to only expose part of them in the justifications.

4.2.5. S4P

S4P (*SecPAL for Privacy*), developed by Becker et al. [10,11], is a language framework to express user's privacy preferences and web services data handling policies. This language was developed by Microsoft Research[9] and it is an extension of the company's previous work, SecPAL, to define the handling of PII.

SecPAL [9] is an extensible and decentralized authorization language, developed to express policies and better disclose expressiveness features such as delegation, domain-specific constraints, and negation. An authorization policy is composed of a group of assertions that have an issuer, that vouches for the assertion, the collection of conditional facts and constraints related to times, dates or addresses. Then, when requesting access to the service, this request is transformed into a series of queries, which are checked against the clauses defined to represent the system's policy, so that the decision is made. S4P extends SecPAL to treat granted rights and required obligations

[9] https://www.microsoft.com/en-us/research/

```
Alice says x may use Email for p if
    x is a eBookingService,
    where p ∈ {Confirmation, Newsletter, Stats}
Alice says x may send Email to y if
    x is a eBookingService,
    y is a TrustedPartner
Alice says x can say y is a TrustedPartner if
    x is a eBookingService
Alice says ⟨Service⟩ is a RegisteredService? ∧
    ∃t (⟨Service⟩ says ⟨Service⟩ will delete Email
        within t? ∧ t ⩽ 30 days?)
```

Listing 3. S4P example adapted from [10], which specifies the privacy preferences of Alice regarding the collection of her email address by eBooking services.

as assertions and queries and, based on these, a satisfaction checking algorithm is defined for the disclosure of PII between users and data collecting services. Therefore, services express data-handling policies as SecPAL queries, defining what is going to be their behaviour in relation to the users' PII, and the users express their preferences as SecPAL assertions, making precise what the services are permitted to do and what their obligations are towards the users' PII. The satisfaction algorithm then checks if the services data collecting activities match the behaviours permitted by the users and if the obligations defined on the users' preferences are respected by the services' policies. If the outcome of this algorithm is positive, meaning the service's policy satisfies the preferences of the user, the service can proceed with its data collecting activities. S4P also defines a data disclosure protocol to ensure that the users' preferences are regarded when their data is provided to third parties. This protocol only allows the disclosure of the user's PII if the service's policies satisfy the preferences of the user while allowing the disclosure and if the policies of the third parties are aligned with the preferences of the user.

In addition to having an XML schema for implementations, S4P has a human-readable and unambiguous syntax that allows it to be used in other applications. Listing 3 presents S4P syntax through an example where the user, Alice, specifies her privacy preferences regarding the collection of her email address. Alice allows eBooking services to use her email address for sending confirmations and newsletters, and for statistical purposes. Alice also allows the booking services to forward her email address to trusted partners, which they can define for themselves, and she is only considering using registered services which will delete her email address within a month.

4.2.6. Privacy Option Language (POL)

POL was developed by Berthold [17] in order to define privacy contracts between data controllers and data subjects, based on the concepts of financial option contracts and respective data disclosure agreements. Its framework applies the data minimization principle by automatically transforming privacy contracts into a canonical form. This canonical form allows the differences among contract compositions to be normalized and so contracts have a similar semantic structure.

In POL, each privacy contract is focused on defining the rights and obligations regarding data disclosure. As this language emerged in the financial context, contract formulations are mainly based on obligations, unless there is no trivial formulation of them. To implement these formulations, POL resorts to several modules that can also be extended. The main components defined by the language are the **syntax** module, the data-related modules for **personal data**, **purpose**, **observable** values and **time**, and the semantics modules for **management** and **human readability**. The syntax module contains the language primitives to define the POL contracts' canonical form. The data modules can then be hooked to the contracts through data support structures as simple as an attribute-value pair, such as *(eye color, brown)*, or as complex as tree-like data organizations. Specifically, the observable module specifies comparison and Boolean operators, which are available in the contract execution environment, to evaluate data retention periods for instance. The time component is useful to formalise distinct time models, i.e. event-driven time, discrete time, continuous time. The semantic modules, for management and human readability, are used to manage changes in observables, i.e. when time elapses, and to translate POL contracts into natural language, respectively. Listing 4 presents a list of POL contract examples: (1) contract c_{company}, that settles the immediate usage of personal data a_1 for purpose p_1, describes the rights and obligations of the institution that receives the data; (2) c_{user}, the negation of c_{companyA}, belongs to the user that discloses the data; (3) c_A represents a

```
(1) c_company = data a_1 p_1
(2) c_user = give c_company
(3) c_A = when (at t_A) (data a_A p_A 'or' zero)
(4) c_B = until (at t_B) (data a_B p_B 'or' zero)
```

Listing 4. POL contract examples adapted from [16].

contract in which a company has the right to use data a_A for purpose p_A at time t_A or not use it at all (represented by the zero contract); and (4) c_B in which a company may or may not use data a_B for purpose p_B until t_B and has the obligation to delete it after the t_B deadline.

This language was developed on the PETWeb II project, with the main goal of addressing societal questions in the domain of electronic identifiers. The online documentation provides application scenarios for the usage of POL.

4.2.7. Privacy Preference Ontology (PPO)

As privacy is one of the challenges of the open data era, it is of the utmost importance to define who has access to what, specially in the context of the web. In this light, the PPO [90] proposes to represent users' privacy preferences for the restriction or permission of access to specific RDF data within a RDF document. This ontology extends the Web Access Control (WAC) vocabulary [87], a taxonomy for detailing access control privileges that uses Access Control Lists (ACL) to determine which data users have access to. Its fundamental concepts are the **Read** and **Write** terms, as well as the **Control** privilege to specify and modify the ACL, although this control can only be exercised to define who can access the full RDF document and not to specify access restrictions over specific data within the document. Therefore, PPO's main goal is to offer highly granular mechanisms to regulate users' access to specific data represented as Linked Data, building on the work previously carried out by the WAC.

PPO's restriction abilities apply to particular statements, to groups of statements (such as RDF graphs) and to resources, that can be particular subjects or objects within statements. The type of restriction must also be defined, as the user can either have read, write or both privileges to the data. Through the defined *hasCondition* property, certain conditions can be set to define privacy preferences in relation to specific resources, instances of particular classes or properties or even to specific values of properties. The access space should also be defined so that the requirements are met by the users to access certain resources. These requirements can be verified through a SPARQL ASK query that contains all attributes and properties that must be met by the users.

Particularly, the same authors focused in developing a specific tool for the semantic web domain, a privacy preference manager [89] based on PPO with the target of providing users with a way to specify their particular privacy choices and regulate the access to their data depending on profile characteristics such as relationships, interests or other common features. This ontology can be used to cover any social data that is modeled on RDF format or through RDF wrappers that can be applied to any major website through their API.

4.2.8. LegalRuleML

LegalRuleML is a rule interchange language applied to the legal domain, defined by the OASIS LegalRuleML Technical Committee, which achieved the OASIS Standard status in August 2021 [76]. It is a XML-schema specification that reuses and extends RuleML concepts and syntax – RuleML is an XML language for rule representation [19] – with formal features to represent and reason over legal norms, guidelines and policies. LegalRuleML's main features include the use of multiple semantic annotations to represent different legal interpretations, the modeling of deontic operators, the temporal management of rules, the authorial tracking of rules and a mapping to RDF triples.

Thus, the core elements of a LegalRuleML document are the **metadata**, the **context** and the **statements**. The metadata section contains information about the **legal source** of the norms, to ensure that they are connected with the legal text statements that specify them, and also about the **actors** and the **roles** they execute in relation to the established rules, about the **jurisdiction** and the **authorities** that create, endorse and enforce the rules and information about the **temporal parameters** that define the period of validity of the rules. The context element allows to express alternative interpretations of the source of the rule, which can change over time or according to jurisdiction, and also enables the representation of the **association** element, which connects the legal sources with the rules. The statements section encompasses the formalization of the norms, including the expression of constitutive and prescriptive

statements, overrides statements or violation-reparation statements. The **constitutive** rules represent the definitions present of the legal documents, while the **prescriptive** rules encode the deontic specifications. **Override** statements can be used to deal with incompatible rules and **violation and reparation** statements formalize the penalties applied to norm' breaches.

Particularly, in 2018, Palmirani and Governatori proposed a framework which uses LegalRuleML, Akoma Ntoso and the PrOnto ontology (described in Section 4.3.5) to model GDPR rules and check for compliance [75]. Listing 5 presents an extract of LegalRuleML's formalisation of GDPR,[10] in particular of Article 19.

4.2.9. Accountable Policy Language (A-PPL)

The A-PPL language, implemented by Azraoui et al. [5], has its origin on the A4Cloud[11] project, with the objective of applying accountability requirements to the representation of privacy policies. To accomplish this goal, the A-PPL expands PrimeLife Policy Language (PPL) by taking into account guidelines on notification, data location and retention, and auditability. PPL by Ardagna et al. [2] is an extensible privacy policy language designed within the context of the PrimeLife[12] project, based on the eXtensible Access Control Markup Language (XACML) [83], an OASIS[13] standard for access control policies. PPL's core classes to express an obligation are **triggers** and **actions**. Triggers are events that can be filtered using certain conditions and are connected to an obligation. These triggers are responsible to fire the data controller's actions, that are executed according to the data subject's authorizations. However, PPL does not cover requirements such as data location and retention rules or auditability to be in line with data handling regulations such as the GDPR.

A-PPL introduced a role attribute identifier and added the data protection authority role to the ones already modeled by PPL, the data subject, data controller and data processor. Also, two new triggers to allow or prohibit access to personal data were included. Duration and region attributes related with a particular data processing purpose are used to enforce data retention and location rules. A-PPL further extends the PPL notification system to define the recipient and the type of notification to be sent in relation to a particular action. For auditing purposes, A-PPL added a trigger to monitor the data controller and collect evidence of data-related events which are logged with parameters such as the purpose of the action, the time-stamp or the executed action on the data. Listing 6 presents an example of an A-PPL obligation to notify a data subject in case of a breach. A-PPL's ActionNotify element provides a way to notify data subjects, which is triggered in case of policy violation or loss of data.

4.2.10. Purpose-To-Use (P2U)

P2U, by Iyilade and Vassileva [51], has taken inspiration from P3P to build a policy language for the sharing of user information across different services and data consumers, resting on the principle of purpose of use. Its main focus is to provide a language for the secondary sharing and usage of data, making sure that the user's privacy is maintained. It is designed to combine information about the data sharing purpose, its retention time and, in the case the user wants to sell it, the selling price and simultaneously allows the data consumers to negotiate prices and retention periods.

This policy framework involves the interaction of the *users* (the owners of the data), the *data consumers* (services that need the data), *the data providers* (services that collect and share the data) and the *data brokers* (services that monitor the consumers' and providers' activities and execute the negotiations, among other tasks). The main elements of P2U are the **policies**, the **data provider**, the **user**, the **purposes**, the **data consumers**, the **retention**, the **data groups** and respective **data** elements. Policies are the root element of P2U, and each one needs to have an associated provider, a user and at least one purpose of use. Each policy should have a name, and optionally an attribute with the path to the human-readable policy, and the name and identifier of the data provider and user to which the policy refers. A P2U policy can specify more than one purpose for the sharing of data, along with information on how long it can be retained, with whom and the relevant data it applies to. The data consumer element has the particularity of containing an attribute, *name*, that can be set to 'public' if the data can be shared

[10] The formalisation of GDPR's provisions in LegalRuleML is at https://raw.githubusercontent.com/dapreco/daprecokb/master/gdpr/rioKB_GDPR.xml.

[11] http://www.a4cloud.eu/

[12] http://primelife.ercim.eu/

[13] Non profit organization focused on open standards for cloud, security and other areas, https://www.oasis-open.org/.

```
<lrml:LegalReference refersTo="gdprC3S3A19P1ref"
    refID="GDPR:art_19__para_1" />
<lrml:Associations key="ascs1">
    <lrml:Association>
        <lrml:appliesSource keyref="#gdprC3S3A19P1ref" />
        <lrml:toTarget keyref="#statements103" />
    </lrml:Association>
</lrml:Associations>
<lrml:Context>
    <lrml:appliesAssociations keyref="#ascs1"/>
    <lrml:inScope keyref="#statements103Formula1" />
    <lrml:inScope keyref="#statements103Formula2" />
    <lrml:inScope keyref="#statements103Formula3" />
    <lrml:inScope keyref="#statements103Formula4" />
</lrml:Context>
<lrml:Statements key="statements103">
    <lrml:ConstitutiveStatement key="statements103Formula1">
      <ruleml:Rule closure="universal">
        <ruleml:if>
          <ruleml:Exists>
            <ruleml:Var key=":a1">a1</ruleml:Var>
            <ruleml:Var key=":eor">eor</ruleml:Var>
            <ruleml:Var key=":enr">enr</ruleml:Var>
            <ruleml:Var key=":edp">edp</ruleml:Var>
            <ruleml:Var key=":w">w</ruleml:Var>
            <ruleml:Var key=":z">z</ruleml:Var>
            ...
            <ruleml:And>
              <ruleml:Atom>
                <ruleml:Rel iri="rioOnto:RexistAtTime" />
                <ruleml:Var keyref=":a1" />
                <ruleml:Var key=":t1">t1</ruleml:Var>
              </ruleml:Atom>
              <ruleml:Atom keyref=":A2570">
                <ruleml:Rel iri="rioOnto:and" />
                <ruleml:Var keyref=":a1" />
                <ruleml:Var keyref=":eor" />
                <ruleml:Var keyref=":enr" />
                <ruleml:Var keyref=":edp" />
              </ruleml:Atom>
              <ruleml:Atom>
                <ruleml:Rel iri="prOnto:DataSubject" />
                <ruleml:Var keyref=":w" />
              </ruleml:Atom>
              <ruleml:Atom>
                <ruleml:Rel iri="prOnto:PersonalData" />
                <ruleml:Var keyref=":z" />
                <ruleml:Var keyref=":w" />
              </ruleml:Atom>
              ...
            </ruleml:And>
          </ruleml:Exists>
        </ruleml:if>
        <ruleml:then>
          <ruleml:Exists>
            <ruleml:Var key=":t2">t2</ruleml:Var>
            <ruleml:And>
              <ruleml:Atom>
                <ruleml:Rel iri="rioOnto:RexistAtTime" />
                <ruleml:Var keyref=":en" />
                <ruleml:Var keyref=":t2" />
              </ruleml:Atom>
              <ruleml:Atom>
                <ruleml:After>
                  <ruleml:Var keyref=":t2" />
                  <ruleml:Var keyref=":t1" />
                </ruleml:After>
              </ruleml:Atom>
            </ruleml:And>
          </ruleml:Exists>
        </ruleml:then>
      </ruleml:Rule>
    </lrml:ConstitutiveStatement>
    <lrml:ConstitutiveStatement key="statements103Formula2">
      ...
    </lrml:ConstitutiveStatement>
    <lrml:ConstitutiveStatement key="statements103Formula3">
        ...
    </lrml:ConstitutiveStatement>
    <lrml:ConstitutiveStatement key="statements103Formula4">
        ...
    </lrml:ConstitutiveStatement>
  </lrml:Statements>
```

Listing 5. Extract of LegalRuleML formalisation of GDPR's Article 19.

```
<Obligation>
    <TriggersSet>
        <TriggerOnPolicyViolation/>
        <TriggerOnDataLost/>
    </TriggersSet>
    <ActionNotify>
        <Media>e-mail</Media>
        <Address>data-subject@example.com</Address>
        <Recipients>Data subject</Recipients>
        <Type>Policy Violation</Type>
    </ActionNotify>
</Obligation>
```

Listing 6. A-PPL example extracted from [5].

```
<POLICY discuri=http://mydatawebsite.com/privacy.html
    name="ShoppingPolicy">
    <PROVIDER name="FoodIntakeApp" provid="p6528m2" />
    <USER name="Jerry" userid="u1030050503050" />
    <PURPOSE name="Shopping Recommendations" puid="102">
        <CONSUMER name="MyShopApp" consid="c10023" />
        <RETENTION period="180" />
        <DATA-GROUP groupid="g090353" negotiable="TRUE">
            <DATA ref="#dailyfoodintake.food"
                sell="FALSE" />
            <DATA ref="#dailyfoodintake.quantity"
                sell="FALSE" />
            <DATA ref="#dailyfoodintake.hungerscale"
                sell="FALSE" />
        </DATA-GROUP>
    </PURPOSE>
</POLICY>
```

Listing 7. P2U example extracted from [51].

with any third party service. Also, the retention period of the purpose should be defined in days and a *negotiable* attribute can be detailed, which is set to false by default. The same attribute is available for the data group element. This component is composed by one or more data elements and each one can have an expiry date, which overrides the retention period, and the possibility of setting an initial price for the data in cases where the user is willing to sell it. Listing 7 presents an example of a P2U policy for secondary sharing of user's information. In the example, the data provider "FoodIntakeApp" wants to share Jerry's data with the data consumer "MyShopApp" for the purpose of shopping recommendations. The consumer can retain the data during 180 days and negotiate it with the provider.

An application scenario where a user allows the data sharing between several mobile applications is further specified in an additional publication by the same authors [50]. However this implementation does not enforce compliance of the data consumers with the policies defined by the users and does not specify any special treatment for cases dealing with sensitive data.

4.2.11. Special

The EU H2020 SPECIAL (Scalable Policy-awarE linked data arChitecture For prIvacy, trAnsparency and compLiance) project aimed to develop technology that supports today's on-going struggle between privacy and Big Data innovation, providing tools, for data subjects, controllers and processors, that facilitate the management and transparent usage of such data. Two vocabularies were produced as outcomes of this project: the SPECIAL Usage Policy Language (SPL) and the SPECIAL Policy Log Vocabulary (SPLog) [55].

A usage policy represents a set of lawful activities that can be performed in accordance with the data subject's consent. To specify these in formal terms in compliance with the GDPR, the SPL establishes five core elements: the **data** that is going to be processed, the **purpose** of such processing, a description of the **processing** itself, the **storage** information and the **recipients** of the processing results. The data storage element needs two attributes to be instantiated, as both the location and the duration of the storage need to be defined. So, in mathematical terms, the usage policy is a five-element tuple, composed of instantiations of the five core classes, that specifies an authorized operation. A general usage policy can then be defined with a union of authorized operations. The

```
ObjectIntersectionOf(
    ObjectSomeValueFrom( spl:hasData
        ObjectUnionOf(
            ex:HeartRate svd:Location ))
    ObjectSomeValueFrom( spl:hasProcessing ex:Profiling )
    ObjectSomeValueFrom( spl:hasPurpose ex:Recommendation )
    ObjectSomeValueFrom( spl:hasStorage
        ObjectIntersectionOf(
            ObjectSomeValuesFrom( spl:hasLocation
                ObjectIntersectionOf(
                    svl:OurServers svl:EU ))
            DataSomeValuesFrom(
                spl:durationInDays
                    DatatypeRestriction( xsd:integer
                        xsd:mininclusive "0"^^xsd:integer ))))
    ObjectSomeValueFrom( spl:hasRecipient spl:AnyRecipient ))
```

Listing 8. SPL general usage policy extracted from [20].

vocabularies designed to specify each of the elements on the SPL are based on previous privacy-related ontologies, such as ODRL, for the processing terms,[14] and the P3P, for the data categories,[15] recipients,[16] purposes[17] and storage duration[18] and location.[19] The vocabularies can be further extended by introducing new sub-classes to its terms [22]. Listing 8 presents an example where the auxiliary vocabularies are extended with new terms to create a usage policy (ex:HeartRate as a subclass of the personal data class svd:Health, ex:Profiling as a subclass of the processing term svpr:Analyze and ex:Recommendation as a subclass of the purpose svpu:Marketing). In this policy, heart rate and location data are used for user profiling with the purpose of creating recommendations, while the data is stored indefinitely in the servers of the data controllers in the EU and can be released to any recipients.

SPLog was designed to provide a record of the processing events related to the consent actions given by the data owners. This vocabulary builds upon **PROV-O** [60] to have information on the provenance of the log and is in line with the terms developed for the SPL vocabulary. The main concepts defined by SPLog are the **log** itself and the actual **log entries**. Each log has meta-data attached to it, such as the software agent it belongs to, and log entries that contain information about each event. The log entries can be from one of two types: policy entries – related to a consent form and related policy terms – or data events such as data processing or sharing. These entries should also contain information about the data subject involved in the event, a description, the event's content itself, time-stamps, related data-set and so on. Therefore these logs can be used to track the provenance of an event. SPLog uses the SPL vocabulary to instantiate a log entry content. This vocabulary is easily extendable and allows the grouping of events to promote scalability [57].

The SPECIAL framework was implemented in various use-cases in distinct sectors: to build personalized touristic recommendations in collaboration with *Proximus*;[20] for traffic alert notifications with *Deutsche Telekom*;[21] with *Thomson Reuters Limited*[22] to support anti-money laundering requirements.

4.2.12. Declarative Policy Framework (DPF)

DPF [65,66] is being developed by an established team under the Defense Advanced Research Projects Agency (DARPA) Brandeis programme[23] with the main goal of providing a privacy policy framework based on ontology engineering and a formal shareability theory. DPF's policy engine builds on the ontology to define policy objects which are used in the development of User Interfaces (UIs). These UIs allow non-technical users to create, validate and manage privacy policies without the need to burden them with technical formalisms of a policy language. DPF's

[14] https://specialprivacy.ercim.eu/vocabs/processing#
[15] https://specialprivacy.ercim.eu/vocabs/data#
[16] https://specialprivacy.ercim.eu/vocabs/recipients#
[17] https://specialprivacy.ercim.eu/vocabs/purposes#
[18] https://specialprivacy.ercim.eu/vocabs/duration#
[19] https://specialprivacy.ercim.eu/vocabs/locations#
[20] https://www.proximus.be/
[21] https://www.telekom.com/en
[22] https://www.thomsonreuters.com
[23] https://www.darpa.mil/program/brandeis

```
@!{NationsAllowConstrainedDiseaseStatesToRCs}
?pa [ allow_sa(?requester, ?reqData, ?time, ?constr,
        ?id, ?descr, 0) ] :-
    ?id = "NationsAllowConstrainedDiseaseStatesToRCs"^^\string,
    ?descr = "Nations share disease states w Response
        Coordinators"^^\string,
    ?pa : NationPolicyAuthority,
    ?requester : ResponseCoordinator,
    ?polData = ${ ?pa [ nation -> ?Nation ],
        ?Nation : Nation [ community -> ?Community,
            name -> ?NationName ],
        ?Community : Community [ resident -> ?Resident ],
        ?Resident : Person [ medicalInformation -> ?MedInfo ],
        ?MedInfo : DiseaseStatus [ state -> ?MedState ],
        ?Resident [ constraints -> ?constr ] },
    ?thirteenYears \is 13*365*24*60*60,
    ?time [ subtractTime(?thirteenYears) -> ?latestTime ],
    ?constr = [ ${
        ?Resident : Person [ birthDate -> ?Birthdate ],
        timeBefore(?Birthdate, ?latestTime) } ],
    implies_sharing(?polData, ?reqData, ?constr).
```

Listing 9. DPF constrained policy rule extracted from [66].

engine can also be integrated into systems supporting the management of data requests and other Privacy Enhancing Technologies (PETs).

Therefore, DPF uses a defined ontology as a common data model to specify a particular domain in order to support the definition of permissive and restrictive privacy policies. Each policy rule corresponds to an allow or disallow statement that should have an identifier and a description, a Policy Authority (PA), the data requesters to whom the policy applies, and also the affected data and effectiveness time imposed by the policy. Optionally, in the case of a permissive statement, there is the possibility to define a set of constraints to establish the conditions under which the data can be shared. The PA evaluates whether a certain data request complies with the defined policies. Hence, each data request must include, in addition to the data being requested, the PA that will be consulted to grant or refuse access, and the time of the request. Then the request follows the policy engine pipeline and if there is a matching rule the engine returns the decision, the identifier and description of the analogous rule and, in the case the request is authorized, the valid conditions in which it is allowed. Since a single request can trigger multiple policy rules, the engine must be equipped to deal with conflicting decisions. To achieve this, DPF implements baselines policies and then exceptions are created to define policy rules with higher priority in relation to the data that is being shared. With this mechanism in place, this privacy framework can override decisions based on detailed constraints.

The ontologies are defined in OWL and can be translated to Flora,[24] an object-oriented reasoning system which can be used to reason with policies. To illustrate this framework, the authors provide a pandemic use-case where nation and community PAs implement data sharing policies about their residents and respective health status to monitor the disease's outbreak. Listing 9 presents an example DPF policy rule based on this use-case, where any national policy authority, ?pa, allows the nations to share their residents' disease states, ?reqData, with any response coordinators, ?requester, at a certain time, ?time, under certain constraints, ?constr. The ?polData query specifies the connection between the nations and the medical state of its residents and it is constrained by ?constr, a constraint attached to the ?Resident variable. In this constraint, the birthday of the resident is taken into account to subtract from the requested data the residents younger than thirteen.

4.2.13. Layered privacy language (LPL)

LPL [43], implemented by Gerl et al., is a human and machine-readable privacy language which aims to promote the expression and enforcement of GDPR's legal requirements related to data subject's consent, personal data provenance and retention and also to implement privacy-preserving processing activities based on the application of state-of-the-art anonymization techniques. Further work by Gerl and Pohl [45] focused on improving LPL to be able to fully represent the requirements derived from Articles 12 to 14 of the GDPR, the so-called data subject's 'Right to be informed'.

[24] http://flora.sourceforge.net/

```
dsU1=('U1','Person',publicKeyU1,'DataSource')
drC1=('C1','Legal Entity',publicKeyC1,'DataRecipient')
dsC1=('C1','Legal Entity',publicKeyC1,'DataSource')
drC2=('C2','Legal Entity',publicKeyC2,'DataRecipient')
lppdsU1−drC1=('1','LPP1','en',
    'https://company.com/privacy.html',∅,dsU1,{pU1})
pU1=('Marketing','false','true',
    'Marketing purposes, including newsletters.',
    {drC1,drC2},r1,pm,D̂1)
r1=('AfterPurpose','180 days')
D̂1={dpostal,dsalary}
dpostal=('postal-code', dGroup, 'Number', 'true',
    'Postal code of the user','QID',am1)
am1=('Suppression',{ama1,ama2,ama3,ama4},∅)
ama1=('Suppression Replacement','*')
ama2=('Suppression Direction','backward')
ama3=('Minimum Level','2')
ama4=('Maximum Level','4')
dsalary=('salary', dGroup, 'Number', 'true',
    'Monthly salary amount received by the user',
    'Sensitive',∅)
```

Listing 10. LPL policy adapted from [43].

LPL's policy structure is **purpose-based**, i.e., its core architecture is composed by a set of purposes and each purpose has associated a set of **data** types being processed and also the **recipients** of said data. The purpose element in LPL can be enriched with a human-readable description and also includes a 'required' property, which can be used to specify if a certain purpose requires the explicit consent of the data subject, and an 'optOut' property, which can be used to imply that the user has to actively deny or accept the purpose. Data elements can be used to specify which data group the data being processed belongs to and also to classify them as sensitive or explicit. In parallel with data recipients, other entities can be specified, such as controllers or the data protection officer and, additionally, information regarding the retention period, data subject's rights, legal basis and also description details related to automated decision-making activities can be detailed in LPL policies. Listing 10 presents an example LPL policy. Company dr_{C1} has a service, with a LPL privacy policy $lpp_{ds_{U1}-dr_{C1}}$, which collects and uses personal information from a user ds_{U1} for the purpose p_{U1} and, optionally, the data collected by the company could be shared with a third party recipient. In this case, a new contract has to be concluded for the data sharing, where company $C1$, ds_{C1}, is the data source and the third party $C2$, dr_{C2}, is the data recipient. 'Marketing' is the purpose for the processing, p_{U1}, of the personal data $\hat{D}_1$, which includes postal code (which is anonymised using the 'Suppression' method) and salary data that has to be deleted 180 days after the completion of the purpose.

Gerl and Meier [44] validate this language against an actual privacy policy use-case scenario in the complex healthcare domain to demonstrate its capabilities and limitations in relation to GDPR compliance. In addition, further work extends LPL with machine-readable privacy icons [42] to assess its impact on the speed and accuracy of understanding privacy policies and introduces a LPL Personal Privacy Policy User Interface [46]. This UI has the main goal of representing information related to the contents of privacy policies in order to support data subjects to give free and informed consent, which includes a policy header with a link to the human-readable policy and an overview of the purposes for processing using the aforementioned privacy icons, and a purpose section with an overview of all the purposes mentioned in the privacy policy and details regarding the identity of the controllers, data recipients, retention period and anonymisation methods.

4.3. Data protection vocabularies and ontologies

In this subsection, for each solution, we describe the data protection vocabularies and ontologies, the core classes they implement and, when available, information about use cases where their resources are applied. In addition, the dependencies of the solutions in previously existing works are also documented, when described in the literature, and, if developed in the context of a specific project, its main objectives are briefly specified. Pre-GDPR ontologies are mentioned since they can be useful to identify missing concepts and relations between terms.

In Table 5, there is a brief description of the ontologies specified in the subsequent subsections, 4.3.1 to 4.3.8 and 4.4, including information about the creators of the resources, version, date of publication and date of the last known

Table 5
Brief description of the resources described in Sections 4.3 and 4.4

Abbreviation (Section)	Full Name	Creators	Version	Date of publication	Last update
DPKO (4.3.1)	Data Protection Knowledge Ontology	Casellas et al.	–	2008	2010
DPO (4.3.2)	Data Protection Ontology	Bartolini and Muthuri	–	2015	2016
GDPRov (4.3.3)	GDPR Provenance Ontology	Pandit and Lewis	0.7	2017	2019
Cloud (4.3.4)	Cloud GDPR ontology	Elluri and Joshi	–	2018	–
PrOnto (4.3.5)	Privacy Ontology for legal reasoning	Palmirani et al.	–	2018	–
GConsent (4.3.6)	GDPR Consent ontology	Pandit et al.	0.5	2018	–
IMO (4.3.7)	Information Model Ontology	Lioudakis and Cascone	1.0	2018	–
DPV (4.3.8)	Data Privacy Vocabulary	Pandit et al.	0.2	2018	2021
GDPRtEXT (4.4)	GDPR text EXTensions	Pandit et al.	0.7	2018	2020

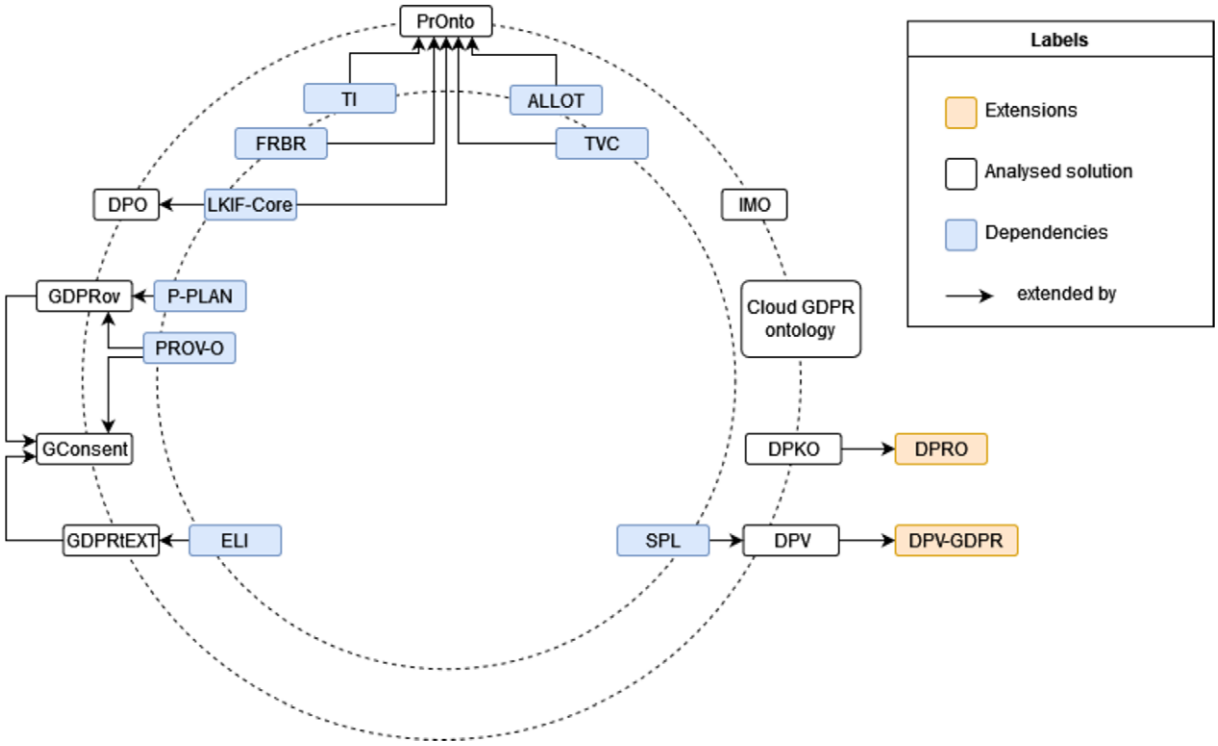

Fig. 3. Data protection vocabularies and ontologies dependency chart.

update. These solutions are analysed in chronological order in relation to the date of publication and the results of comparing the solutions in light of their ability to represent the identified informational items are discussed in Section 5.1 and systematised on Tables 7 and 8. In Fig. 3, a dependency graph, that captures the relations between the reviewed vocabularies and its dependencies, is presented.

4.3.1. NEURONA ontologies

Developed by S21SEC[25] and IDT-UAB,[26] the main focus of the NEURONA project [26] is the correctness of files containing personal data information and the measures of protection applied to them. Its legal basis was the Spanish protection of personal data regulation that was in effect prior to the GDPR enforcement in all Europe.

[25] https://www.s21sec.com/
[26] https://portalrecerca.uab.cat/en/organisations/law-and-technology-institute

The core classes implemented are the **personal data**, **consent**, **purpose** and the **data security measures**. In relation to the data class, categories such as the data regarding religion or racial origin are well defined and fall under special protection security measures. The consent should be given by the data subject in an unambiguous way and for a specific purpose. In addition, technical and organizational measures for data security should also be in place to regulate the activity of data controllers and processors. These measures should be intrinsically related to the nature of the data and should also reflect the risk associated with its unfulfillment. For this, the concept of **level of security** is introduced by the NEURONA project, a variable that can have three states: low, medium or high. For instance, a file obtained by the police without the consent of the data subjects or a file with data related to the health status of a patient should have high level measures, such as access control policies and backup procedures, associated with it.

These concepts constitute the core ontology of the project, the Data Protection Knowledge Ontology, from which the Data Protection Reasoning Ontology derives with the goal of classifying files based on its compliance with the legislation. Therefore, the NEURONA ontologies could prove useful in the context of companies that deal with great amounts of data stored in files, however, they are not publicly available for usage.

4.3.2. Data protection ontology

Bartolini and Muthuri [7] and Bartolini et al. [8] developed an ontology to deal with the new personal data rights and obligations stated by the GDPR, prior to its implementation in May 2018, using an early version of the regulation. The ontology was built focusing on the obligations of the data controller and corresponding rights of the data subject. Therefore the foundations of the ontology are the data protection principles defined in the GDPR, such as the purpose limitation, data quality or data minimization principles.

The ontology was created following the established METHONTOLOGY guide, by Fernández et al. [38], and it is based on the concepts collected from the GDPR, Data Protection Directive (DPD) and the *Handbook on European data protection law* [35], reusing concepts defined on the Legal Knowledge Interchange Format (LKIF) Core [47] and Simple Knowledge Organization System (SKOS) [67] ontologies. The core classes are the **data protection principles**, the **rules of data processing**, that constitute most of the data controller's obligations, and the **data subject's rights**, and the ontology is designed so that each data processing rule and data subject's right is connected to at least one data protection principle. For instance, data subjects have the right to access their own data, so the data controller must provide the means for their access to such data. Furthermore, this data protection ontology defines consent as a legal justification connected with the principle of trust and also specifies the special case where parents give consent in the name of the child, although the concept of consent given by delegation is left out. The several entities involved in the data usage, such as the controller, the supervisory authorities or the processor, are also modeled under the **Person** class.

The ontology has been used to extend the Business Process Model and Notation (BPMN), a language to model business processes [71], with the objective of applying data protection concepts that a data controller must follow so that its activity is GDPR compliant.

4.3.3. GDPR Provenance Ontology (GDPRov)

Based on the **PROV-O** and **P-Plan** ontologies, developed by Lebo et al. [60] and by Garijo and Gil [41], respectively, Pandit and Lewis [81] published an ontology with the objective to conceptualize the provenance of data and how the consent and processing of such data are managed in the domain of the GDPR. PROV-O is a provenance ontology, designed to define entities and the relations and activities between them in a generic and domain independent format. It is a W3C recommendation since 2013 and has already been validated in several domains, as demonstrated in the works of Belhajjame et al. [12,13]. P-Plan (Ontology for Provenance and Plans) is a necessary extension of the PROV-O ontology as the latter does not expand the concept of plan nor does it give details on the plan execution. With P-Plan extensions of the activities and corresponding steps to execute them, as well as the entities involved, it is possible to track provenance of the interaction between entities and to monitor how their activities changed over time, for instance, if there have been changes to the consent or to the data being processed.

For queries to be GDPR compliant, provenance information on consent, third party sharing, data collection, usage and storage, anonymisation of personal data and additional rights must be available. Under the GDPR, consent must be given in an explicit and unambiguous way, so that the user knows the purpose to which its data is being processed

and which entities are involved in the data life cycle workflow. GDPRov implements this through the *ConsentAgreementTemplate* class, a common template regarding consent permissions presented to the users that models how the consent is obtained. Therefore, to ensure compliance, a record must be maintained on how the consent was obtained, which processing activities were approved and in the cases where the state of the consent changes, for instance in the case of consent withdrawal, the previous consents should be recorded. Also, data collected for a specific purpose must not be used in other contexts unless the user explicitly consents to it and should only be stored as long as it is necessary. Furthermore, references to third parties with which the data is shared must be detailed to the users, along with specifications on the nature of the data that is being shared, its purpose and information about the entity and its role in the workflow. To do so, provenance meta-data on the origin, use, storage and sharing of the data must be recorded. In the cases where the data was transformed or archived, a version control system must be in place so that the provenance of the data can be tracked. As GDPR authorizes the processing of personal data without consent in the cases where the data cannot be de-anonymised, GDPRov also provides the degree of anonymisation, based on Schwartz and Solove [91]'s work, a property that can have four states: completely anonymous, pseudo-anonymous that cannot be de-anonymised by the organization with which the data was shared, pseudo-anonymous but can be de-anonymised by the organization, and not anonymous. Provenance data on the execution of rights and obligations from users and data handlers is also kept, so that the records can be checked as proof of compliance. Therefore, for each right or obligation, a plan is defined to reflect the steps involving data or consent that need to be executed when the user wants to exercise a particular right.

4.3.4. Cloud GDPR ontology

Elluri and Joshi [36] developed a GDPR compliant ontology focusing on cloud services to express the obligations of both the cloud data consumers and the cloud data providers, also taking into account the respective Cloud Security Alliance (CSA) controls defined on the *Code of Conduct for GDPR Compliance* [25].

The **stakeholders**, the **CSA controls** and the **obligations** are the core modules of this ontology. The cloud-related obligations are extracted from the GDPR and are connected to the respective articles and also to the associated CSA requirements using the implemented *hasCSAcontrol* property. These GDPR obligations are further specified taking into account which stakeholders they apply to, so there are specific obligations to be followed by cloud consumers and cloud providers and also a few that must be met by both. For instance, maintaining records of the processing activities and notifying data breaches are common obligations, while providing European Union (EU) representatives for non-EU consumers or providers is a responsibility of the consumer and hiring a Data Protection Officer (DPO) falls into the authority of the provider.

This work was extended by Elluri et al. [37] to automate the implementation of both the GDPR and the Payment Card Industry Data Security Standard (PCI DSS) guidelines [74] to compliance. The PCI DSS legislation deals with financial data, such as the credit card number or card-holder's name. Therefore, building and maintaining a secure network, protecting card-holder's data and implementing access control measures are a few of the main requirements of the PCI DSS. As it covers a narrower scope in comparison with the GDPR, a data breach in PCI DSS automatically results in one in GDPR. Thus, the cloud-related PCI DSS requirements were used to enrich this compliance ontology and its validation was done using privacy policies from five major companies that deal with card-holder's data and PII. The ontology was also extended to include the rights of consumers, providers and end users.

4.3.5. Privacy ontology for legal reasoning – PrOnto

Palmirani et al. [77] presented in 2018 the first draft of PrOnto, a privacy ontology with the purpose to model the relationships between agents, processing activities, data categories and deontic specifications present on the GDPR. With the goal to support legal reasoning and compliance with the GDPR and other future regulations, PrOnto takes advantage of various other ontologies previously developed. The **LKIF Core** ontology, developed by Hoekstra et al. [47], was used to model the different classes of agents (controller, processor,...) described in the GDPR as well as the several roles that can be assigned to them.

The **Functional Requirements for Bibliographic Records (FRBR)** ontology by Byrum et al. [24] is used to model legal documents as sources of information, that regulate the different relationships between the agents documented in the text, and to register changes in their representation over time. The FRBR model together with the **A Light Legal Ontology On Top level classes (ALLOT)** ontology, developed by Barabucci et al. [6], are used to

model the relationship between the document and the data within, according to the Akoma Ntoso[27] guidelines. Other ontologies, such as the **Time-indexed Value in Context (TVC)** [86] and the **Time Interval (TI)** [72], are used to connect time-dependant events with specific roles that emerge in certain contexts.

PrOnto was built upon five core modules: **documents and data**, **agents and roles**, **processing and workflow**, **legal rules and deontic formula**, and **purposes and legal bases**. The GDPR document is used as the source of information, from which the main data categories are defined: judicial and sensitive data (personal data) and anonymous and legal person data (non-personal data). The agent and role classes are clearly distinguished as the agent refers to the entity (person, organization, software,...) while the role class intends to characterize the activity of the agent (data processor, data controller, supervisory authority,...). Furthermore, an agent can be involved in different roles depending on the context. The processing activity is modulated through a workflow of actions that should be well placed in terms of the context and time in which each event occurs. This workflow has several associated properties that are defined in the text, e.g., transparency, fairness, lawfulness, and is prepared to deal with eventual data breaches and consequent counter measures. Each processing activity should be performed with a purpose and be committed to a legal rule, which is composed of deontic specifications (prohibitions, rights, permissions and obligations) to check if the activity being executed is in compliance or violation of the GDPR.

This ontology was tested on several use-cases: eGovernment services in the cloud, school services and also in the MIREL project[28] and DAPRECO[29] [88] projects.

4.3.6. GConsent

In the Article 6 of the GDPR, the legal basis for the lawful processing of personal data are settled, consent being one of them that should be freely given in a specific, informed and unambiguous way. Information about the consent must be collected and stored, as well as maintaining a log of any changes that may be requested over time, and should be available for all parties involved – data subject, data controller and processor and the authorities.

In this context, Pandit et al. [79] created the GConsent ontology based on the guidelines defined by Noy and McGuinness [69]. The GDPR was the main source adopted to collect information about consent, though other legal authorities' guidelines and reports were used, such as the guidelines on consent published by the European Data Protection Board [34]. However, this ontology only conceptualizes consent in the domain within Article 4.11 of the GDPR, so special cases where other forms of consent are allowed, such as children's personal data or scientific research, are not covered by this model. As GConsent aims at not only capturing the concept of consent, but also to represent its state, context and provenance, existing vocabularies on this subject, such as PROV-O [60], GDPRov [81] and GDPRtEXT [80], are reused.

The core classes are the **data subject**, **personal data**, **purpose** and **processing**, as well as the **consent** and the **status**. GConsent represents a step further in relation to other ontologies that conceptualized consent since it not only defines the 'given consent' concept, but also classifies other states of consent as valid or invalid for processing. Consent status can be one of the following: expired, invalidated, not given, refused, requested, unknown and withdrawn, and in these cases will be invalid for processing, or explicitly given, given by delegation and implicitly given and will be valid. To represent the context in which the consent was obtained, information about the location, the time of creation and the medium is recorded, as well as about the expiry of the consent and the entity that granted it. Also, the authors plan to extend the ontology to deal with the spacial and temporal representation of processing activities, such as data storage or sharing, and continue to provide new use-cases to motivate the community's adoption of this model.

4.3.7. BPR4GDPR – compliance ontology

The BPR4GDPR (Business Process Re-engineering and functional toolkit for GDPR compliance) project started at May of 2018 and was running until April 2021. It is a European Union's H2020 innovation programme with the main goal of providing a framework to reinforce the implementation of GDPR-compliant measures inside organizations at diverse scales and in several domains [23].

[27] XML vocabulary with the primary objective of providing information about the top level classes (person, event, locations,...) in legal or legislative documents.

[28] http://www.mirelproject.eu/

[29] https://www.fnr.lu/projects/data-protection-regulation-compliance/

The Compliance Ontology, described on BPR4GDPR's deliverable D3.1 by Lioudakis and Cascone [63], is based on the BPR4GDPR's Information model, that aims to define the entities and respective roles that are involved in the organization processes' life-cycles. Its core classes are the **data types**, the **roles** assigned to users inside the organizations, the **operations** and **operation containers**, the **machine types** that host the operations, the **organization types**, the **events** and **contexts** in which they happened and the **purposes** for which operations are executed. The roles class is related to the responsibilities that are assigned to the user in the context of the organization and its instances can be implemented hierarchically according to the detail level of the data and connected through the *isA* property. This hierarchical structure is valid for most classes in the ontology. The data processing activities are implemented through the operations class, which have associated the *hasInput* and *hasOutput* properties that allow to connect the operations with the data that is processed and the one that is generated and respective states (i.e. plain or anonymised). These operations can be grouped in an operation container – a class that groups processing activities in contexts where they usually work together, for instance, in the management of a database, in which functions such as create, read, update or delete are commonly used. The roles and operations classes should always be connected with an instance of the purpose class. The events class, that aims at capturing all processing activities, a data breach or the revoke of consent, has associated the context class to instantiate specific cases and provide temporal and spatial details, among others.

Using this ontology, BPR4GDPR defines a policy instantiating its purpose, context, action, pre-action and pos-action. The action reflects the activity permitted, prohibited or obliged by the policy, while the pre-action and pos-action indicate the actions that must take place before and after the main action. In turn, each action is specified by the user's role, data, operation and the organization where it takes place.

BPR4GDPR is implementing services in three use-cases: for governmental services in the social security and healthcare domains with IDIKA S.A.;[30] for automotive management with CAS Software AG;[31] and for cloud-supported real state agencies with Innovazioni Tecnologiche.[32]

4.3.8. Data privacy vocabularies

The Data Privacy Vocabulary (DPV) was introduced by the W3C Data Privacy Vocabularies and Controls Community Group (DPVCG)[33] in 2018 when the GDPR came into force. This W3C CG was one of the first outputs from a W3C workshop on data privacy controls, that took place in Vienna in April 2018, with the objective of defining priorities for the standardization of this domain [21]. Initially, the group searched for relevant vocabularies that attempted to address data privacy and, in particular, the GDPR. From this state-of-the-art review, a few conclusions emerged: there is a need for vocabularies to describe personal data and the purposes for the processing of said data, as well as vocabularies to coordinate privacy legislations. The methodology used to develop the vocabulary was based on the **NeOn** methodology by Suárez-Figueroa et al. [94] and the **SPECIAL Usage Policy Language** [93] was the core ontology used to model the processing, purpose, recipient and personal data category classes. New concepts were added to the vocabulary after being discussed and agreed upon by the CG. As a result of this process, a first version of the base vocabulary was published with the following main classes: **personal data categories**, **processing**, **purposes**, **legal basis**, **technical and organizational measures** and **legal entities**, including **data subject** and **child**, **recipients**, **data controller**, **data processor** and **third party** [82]. A second and third versions of the base vocabulary were released in 2021; the **risk**, **right** and **data subject right** classes were added to the base vocabulary and the previously existing classes were extended with new terms. Moreover, new legal entities, including **authority** and **data protection authority**, **vulnerable data subject**, **data sub-processor**, **data protection officer** and **representative**, were added to the vocabulary, as well as new purpose and legal basis sub-classes. DPV's classes are further developed as sub-vocabularies, making it possible for them to be used independently.[34]

The personal data categories are split into top level classes such as financial or social data, which are further specified, and classes for sensitive and derived data are also present as required by the GDPR. The top level categories

[30] http://www.idika.gr/
[31] https://www.cas.de/en/homepage.html
[32] https://www.innovazioni-tecnologiche.com/en/index.aspx#about
[33] https://www.w3.org/community/dpvcg/
[34] http://www.w3.org/ns/dpv#

are adapted from the **EnterPrivacy** taxonomy by Cronk [31]. The purpose vocabulary is composed of 64 suggested purpose sub-classes, which are topped by classes such as R&D or Service Provision, that can be extended to specify other GDPR purposes not yet conceptualized. The purpose category can be further constrained to specific contexts or business sectors. In relation to the processing categories, DPV covers the terms defined in the Article 4.2 of the GDPR, providing 40 processing categories. Properties related to the origin of the data being processed or the logic used in automated decision making algorithms are available to check compliance with the GDPR. Technical and organizational measures, such as the pseudo-anonymisation and encryption of the data, must be in place so that the processing of personal data is in line with the GDPR. These categories of measures are usually accompanied by a comment to describe the measure or the standardized practices to follow. The consent legal basis is further specified in the DPV with the withdrawal, provision and expiry concepts, based on **GConsent** [79] and **Consent Receipt** [64].

The CG also developed a GDPR extension for DPV, the DVP-GDPR vocabulary.[35] DVP-GDPR covers all the legal bases specified on the GDPR Articles 6 and 9 for the processing of personal data and also the legal bases for the transfer of personal data to third countries defined on Articles 45, 46 and 49. This vocabulary also models 12 GDPR rights of the data subjects.

The work to improve and extend the DPV vocabularies, as well as to provide more examples of application scenarios, is ongoing at time of writing.

4.4. GDPR as a linked open data resource

Pandit et al. [80] developed **GDPRtEXT**, a linked open data resource that provides a way to connect GDPR concepts with the specific sections, chapters, articles or points of the GDPR text. GDPRtEXT is an extension of the **European Legislation Identifier (ELI)**, an ontology developed for the identification of European, national and regional legislation through URI templates [70]. Extending the properties defined by ELI, GDPRtEXT provides a way to link the correlated chapters, sections, articles or points. The ontology was developed using the *"Ontology Development 101"* guide by Noy and McGuinness [69] and the SKOS vocabulary was used to describe the GDPR terms.

The main terms represented in this ontology are the specific **entities** mentioned in the regulation's text, the **rights** and **obligations** of the entities, the **principles** and the **activities** which specify processes and actions defined in the GDPR, such as reporting a data breach, exercising rights or demonstrating consent. These terms are connected to the relevant points in the GDPR text using the *rdfs:isDefinedBy* property.

GDPRtEXT's documentation also contains two example use-cases where it was used for GDPR compliance reports and also to link obligation concepts with the previous data protection regulation, the DPD.

5. Discussion

5.1. Analysis of existing resources

Using Table 6 as a reference, it is possible to compare the policy languages described in Section 4.2 in relation to their capacity of assisting with the representation of the rights and obligations described in Section 2. In this Table, the languages are sorted in descending order by the number of supported criteria, then alphabetically, if necessary, to improve readability.

Although these languages do not specifically mention the rights and obligations discussed in Section 2, they can be used to represent a few of the items of information mentioned by them, which is why they are classified as capable of partially representing GDPR concepts and principles (Q2 criterion in Table 6). Therefore, most of the analysed languages can be used to partially model the GDPR representational needs identified in Section 2, apart from AIR, PPO and XPref. Listings 1 to 10 provide examples of how to encode a particular privacy policy aspect for

[35] http://www.w3.org/ns/dpv-gdpr#

Table 6
Comparison of the analysed privacy policy languages according to the defined criteria, described on Section 4.2

	Q1	Q2	Q3	Q4	Q5	Q6
LegalRuleML	Yes	Partially	No	Yes	Yes	Yes
ODRL	Yes	Partially	Yes	No	Yes	Yes
SPL	No	Partially	Yes	Yes	No	Yes
A-PPL	Yes	Partially	No	Yes	No	No
DPF	Yes	Partially	No	Yes	Unknown	No
P3P	No	Partially	Yes	No	No	Yes
AIR	No	No	No	Yes	No	Yes
LPL	No	Partially	No	Yes	Unknown	No
S4P	No	Partially	No	Yes	No	No
P2U	No	Partially	No	No	No	No
POL	No	Partially	No	No	No	No
PPO	No	No	No	No	No	No
XPref	No	No	No	No	No	No

each language identified as capable of partially representing concepts present in the rights and obligations described in Section 2.

However, only ODRL, SPL and P3P provide taxonomies to populate the identified information flows and solely LegalRuleML, ODRL, A-PPL and DPF model deontic concepts such as permissions or obligations. LegalRuleML, SPL, A-PPL, DPF, AIR, LPL and S4P also mention in their literature the existence of reasoning mechanisms or other tools, which are based on the implemented languages, to assist with compliance, and in some cases access to such tools are provided. From the described languages, solely LegalRuleML and ODRL continue to be actively maintained and developed, and only LegalRuleML, ODRL, SPL, P3P and AIR have the resources available for reuse on the Web.

In particular, LegalRuleML and ODRL stand out from other languages as they have resources to respond positively to a greater number of the established comparison criteria.

Since the majority of the policy languages were developed before the GDPR came into full effect, they do not model concepts such as the legal basis for processing or the rights of the data subject. In this context, the ontologies and vocabularies in the domain of privacy and data protection as well as the GDPRtEXT ontology, described in the previous sections and compared in Tables 7 and 8, are of particular interest to cover these gaps on the representation of informational items. When available, the name of the class that can be used to model the respective informational item is detailed, as well as the number of sub-classes which can be used to more specifically define the term. The cases in which there is still no specific concept to represent the informational item, yet there are terms that can be extended to accomplish it, are marked with an asterisk. Informational items I15, I19, I24, I26, I28 to I30, I33, I34, I46 to I48, I51, I52 and I54 to I56 are not represented in either Table 7 or 8 since they are not modeled by any of the analyzed ontologies.

DPO, GDPRov, PrOnto, DPV and GDPRtEXT can be used to partially populate a great deal of the informational items required by the *'right to be informed'* (RI1 and RI2) and the other GDPR rights and obligations. However, we must highlight DPV and GDPRtEXT since they represent, at least partially, 31 and 25 informational items, respectively, out of the 57 described in Table 1. Furthermore, these vocabularies are the ones that have the largest number of sub-classes to specifically define the respective informational items.

Most of the ontologies and vocabularies presented are obsolete or without new developments in recent years, with BPR4GDPR's IMO, GDPRov, GConsent, DPV and GDPRtEXT being the only ones that continue to be improved. Moreover, of all the covered vocabularies, only DPKO, IMO and PrOnto do not have open and accessible resources.

Taking into account the performed analysis, it can be concluded that LegalRuleML, ODRL, DPV and GDPRtEXT are resources that can be easily extended to support the discussed representational needs of GDPR rights and obligations. As an example, Listing 11 combines ODRL, DPV and GDPRtEXT with a few new terms to describe a *communication of a data breach* (CDB) obligation. This example describes the need of a certain controller to inform

Table 7

Representation of the informational items I1 to I57 in the DPKO, DPO, GDPRov, Cloud and PrOnto ontologies. The names of the classes which can be used to specify a particular item are depicted in the table, as well as their respective number of sub-classes. The informational items which cannot be fully represented by the current ontology terms are illustrated with an asterisk

	DPKO	DPO	GDPRov	Cloud	PrOnto
I1		Controller	Controller		*
I3			ControllerRepresentative		
I6	*	Purpose			Purpose (10)
I7	*	LegalJustification (6)			
I8		LegitimateInterest			
I9		Recipient (2)			*
I10			*		
I11					*
I12		DataSubjectRight (7)	Process (10)		Right (8)
I16		AutomatedProcessing	*		
I17	*	PersonalData	PersonalData (3)		PersonalData (7)
I20		*			
I21			ProvideCopyOfPersonalData		
I22			RectifyData		
I31			JointController		
I36					Action (13)
I37		DataSubject (1)			
I38		*	*	*	*
I39		*		*	*
I40		DataProtectionOfficer	DPO		*
I41	*	Measures (2)			
I42		Processor	Processor		*
I44			ProcessorRepresentative		
I57		*	*		

a specific data subject in the case of a personal data breach event. A data controller keeping these obligations in this structured form can more easily fulfill them if the event actually happens.

5.2. *Supplementary material*

In order to complement the description of privacy languages, ontologies and vocabularies presented on Section 4 of this paper, an online portal[36] has been published with additional resources. For each solution, there is a brief description of the language or ontology and also links to additional documentation and available RDF serializations. There is more information about the authors of the solutions, when it was first created and last updated, about the projects or the research groups where it was developed and, when available, examples of implementations that are using it. The webpage's source code is also preserved as a Zenodo resource, at *https://doi.org/10.5281/zenodo.5148947*, and its public repository can be accessed by the community at *https://github.com/besteves4/SotAResources* for further development.

This webpage also includes a REST API service to find references to specific concepts in the collection of ontologies and languages that have been identified in the context of this paper. The main objective of this service is to give users a platform where they can search for ontologies that model processing activities such as 'derive' or 'disclose' or a language that can be used to represent the *'right to erasure'*.

[36] https://protect.oeg.fi.upm.es/sota/

Table 8
Representation of the informational items I1 to I57 in the GConsent, IMO, DPV and GDPRtEXT ontologies. The names of the classes which can be used to specify a particular item are depicted in the table, as well as their respective number of sub-classes. The informational items which cannot be fully represented by the current ontology terms are illustrated with an asterisk

	GConsent	IMO	DPV	GDPRtEXT
I1	DataController	DataController	DataController	Controller
I2			hasContact	
I3			Representative	ControllerRepresentative
I4			hasContact	
I5			hasContact	
I6	Purpose	Purposes	Purpose (64)	
I7	*		LegalBasis (34)	LawfulBasisForProcessing (14)
I8			A6-1-f	LegitimateInterest
I9	*		Recipient (4)	*
I10			*	CrossBorderTransfer
I11	*	*	*	RecordDataRetentionPeriod
I12			DataSubjectRight (12)	Rights (10)
I13	*		A7-3	
I14			A77	
I16			AutomatedDecisionMaking	AutomatedProcessing
I17		DataTypes (52)	PersonalDataCategory (170)	PersonalData (5)
I18			DataSource	InfoAboutSourceOfData
I20			*	
I21				ProvideCopyOfPersonalData
I23				RightOfErasure (2)
I25			hasContact	
I27				RightToRestrictProcessing (3)
I31				JointController
I32			hasContact	
I35			*	
I36	Processing (18)	Operations (40)	Processing (40)	DataActivity (9)
I37	DataSubject (1)	DataSubject	DataSubject (2)	DataSubject
I38				ControllerObligation (11)
I39				ProcessorObligation (14)
I40		DataProtectionOfficer	DataProtectionOfficer	DPO
I41			TechnicalOrganisationalMeasure (48)	
I42		DataProcessor	DataProcessor (2)	Processor
I43			hasContact	
I44			Representative	ProcessorRepresentative
I45			hasContact	
I49				*
I50				*
I53			Risk	
I57			DPIA	*

Furthermore, we specify a lightweight ontology, the GDPR Information Flows (GDPRIF),[37] in order to model the relationships between GDPR stakeholders, informational items, GDPR rights and obligations and also to specify information about the flows of information and about the events that trigger the rights and obligations. GDPRIF's

[37] https://w3id.org/gdprif

```
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .
@prefix dpv: <http://www.w3.org/ns/dpv#> .
@prefix gdprtext: <https://w3id.org/GDPRtEXT#> .
@prefix gdprif: <https://w3id.org/gdprif#> .

gdprif:communicateDataBreach
    rdfs:comment "Data controller A informs Beatriz
        Esteves about the existence of a personal data breach";
    rdfs:seeAlso gdprtext:NotifyDataSubjectOfBreach ;
    odrl:obligation [
        odrl:informedParty [
            a dpv:DataSubject, odrl:Party ;
            dpv:hasName "Beatriz Esteves" .
        ] ;
        odrl:informingParty _:ControllerA ;
        odrl:assignee _:ControllerA ;
        odrl:action odrl:inform ;
        odrl:target gdprif:I5, gdprif:I40, gdprif:I46,
            gdprif:I49, gdprif:I50 ;
        odrl:constraint [
            a odrl:Constraint ;
            odrl:leftOperand odrl:event ;
            odrl:operator odrl:eq ;
            odrl:rightOperand gdprif:PersonalDataBreach ;
        ] .
    ] .

_:ControllerA
    a dvp:DataController, odrl:Party ;
    dpv:hasName "Controller A" .
```

Listing 11. Communication of a personal data breach to a data subject.

documentation is also stored in a public repository.[38]

6. Conclusions

There is a strong need to develop technologies to support individuals to manage their personal information and at the same time there is a need to support companies to better manage compliance. Having common vocabulary elements and common data models to refer to these rights and to denote specific GDPR concepts would favor data subjects and data controllers to speak in the same terms, and would ease the interoperability between different types of tools. Not only companies may have information systems to manage the individuals' consent and abide the law: other software systems can also help individuals to manage the consent they are constantly giving. In particular: data subjects can control the access to their personal data in distributed stores; as recommended by the Opinion 9/2016 of the European Data Protection Supervisor on Personal Information Management Systems (PIMS). Conversely, data controllers can make sure they have complied with their obligations about (i) informing the data subjects and (ii) responding to the data subjects' requests. For example, having a categorization of the types of information that an individual should receive would enable automatic labeling tools analyzing existing text communications. Aligning ontologies and vocabularies with the GDPR (or other equivalent norms in other territories) would greatly favor interoperability of the privacy-related tools both on the side of the individuals and on the side of the companies.

This paper has analyzed the value of existing policy languages, vocabularies and ontologies to support these interoperability needs, and has concluded that LegalRuleML, ODRL, DPV and GDPRtEXT are mature resources, ready to be used for representing privacy-related rights and obligations, with an explicit link to the current version of the GDPR text. Points in favor of these solutions are the fact that they are open access, have good documentation and, in the case of ODRL and LegalRuleML, they are a W3C recommendation for digital rights management and a OASIS Standard for representing legal rules, respectively. In the specific case of DPV and GDPRtEXT, together they already allow representing, at least partially, most of the informational items necessary to adequately represent both rights and obligations, so these solutions prove to be the most appropriate options to be extended to cover all representational needs. Furthermore, beyond maturity, these solutions can formalise the highest number of information flows and can represent the most informational items required by the GDPR. An example of using

[38] https://github.com/besteves4/gdprif

these resources to specify the obligation to report a data breach is given to support this conclusion. In terms of future work, we intend to create ODRL-DPV-GDPRtEXT rules for each of the rights and obligations found in GDPR, as this exceeds the ambitions of this paper, but would favor its quick adoption.

Acknowledgements

This research has been supported by European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 813497 (PROTECT).

References

[1] R. Agrawal, J. Kiernan, R. Srikant and Y. Xu, XPref: A preference language for P3P, *Computer Networks* **48**(5) (2005), 809–827, https://linkinghub.elsevier.com/retrieve/pii/S1389128605000095. doi:10.1016/j.comnet.2005.01.004.

[2] C.A. Ardagna, L. Bussard, S.D.C.D. Vimercati, G. Neven, S. Paraboschi, E. Pedrini, F.-S. Preiss, D. Raggett, P. Samarati, S. Trabelsi and M. Verdicchio, PrimeLife Policy Language, Technical Report, 2009.

[3] P. Ashley, S. Hada, G. Karjoth, C. Powers and M. Schunter, Enterprise Privacy Authorization Language (EPAL 1.2), 2003, https://www.w3.org/Submission/2003/SUBM-EPAL-20031110/.

[4] P. Ashley, S. Hada, G. Karjoth and M. Schunter, E-P3P privacy policies and privacy authorization, in: *Proceeding of the ACM Workshop on Privacy in the Electronic Society – WPES'02*, ACM Press, 2002, pp. 103–109, http://portal.acm.org/citation.cfm?doid=644527.644538. ISBN 978-1-58113-633-3. doi:10.1145/644527.644538.

[5] M. Azraoui, K. Elkhiyaoui, M. Önen, K. Bernsmed, A.S. De Oliveira and J. Sendor, A-PPL: An Accountability Policy Language, Research Report, 2014, http://www.eurecom.fr/en/publication/4372/download/rs-publi-4372.pdf.

[6] G. Barabucci, L. Cervone, A. Di Iorio, M. Palmirani, S. Peroni and F. Vitali, *Managing semantics in XML vocabularies: an experience in the legal and legislative domain*, 2010, http://www.balisage.net/Proceedings/vol5/html/Barabucci01/BalisageVol5-Barabucci01.html. ISBN 978-1-935958-01-7. doi:10.4242/BalisageVol5.Barabucci01.

[7] C. Bartolini and R. Muthuri, Reconciling data protection rights and obligations: An ontology of the forthcoming EU regulation, in: *Workshop on Language and Semantic Technology for Legal Domain*, 2015.

[8] C. Bartolini, R. Muthuri and C. Santos, Using ontologies to model data protection requirements in workflows, in: *New Frontiers in Artificial Intelligence*, M. Otake, S. Kurahashi, Y. Ota, K. Satoh and D. Bekki, eds, Lecture Notes in Computer Science, Vol. 10091, Springer International Publishing, 2017, pp. 233–248, http://link.springer.com/10.1007/978-3-319-50953-2_17. ISBN 978-3-319-50952-5, 978-3-319-50953-2. doi:10.1007/978-3-319-50953-2_17.

[9] M. Becker, C. Fournet and A. Gordon, Design and Semantics of a Decentralized Authorization Language, in: *20th IEEE Computer Security Foundations Symposium (CSF'07)*, IEEE, 2007-07, pp. 3–15, http://ieeexplore.ieee.org/document/4271637/. ISSN: 1063-6900. ISBN 978-0-7695-2819-9. doi:10.1109/CSF.2007.18.

[10] M.Y. Becker, A. Malkis and L. Bussard, A Framework for Privacy Preferences and Data-Handling Policies, Technical Report, Microsoft Research, 2009, https://www.microsoft.com/en-us/research/wp-content/uploads/2009/09/A-Framework-for-Privacy-Preferences-and-Data-Handling-Policies-2009-09-28.pdf.

[11] M.Y. Becker, A. Malkis and L. Bussard, S4P: A Generic Language for Specifying Privacy Preferences and Policies, Technical Report, Microsoft Research, 2010, https://www.microsoft.com/en-us/research/wp-content/uploads/2010/04/main-1.pdf.

[12] K. Belhajjame, J. Zhao, D. Garijo, M. Gamble, K. Hettne, R. Palma, E. Mina, O. Corcho, J.M. Gómez-Pérez, S. Bechhofer, G. Klyne and C. Goble, Using a suite of ontologies for preserving workflow-centric research objects, *Journal of Web Semantics* **32** (2015), 16–42, https://linkinghub.elsevier.com/retrieve/pii/S1570826815000049. doi:10.1016/j.websem.2015.01.003.

[13] K. Belhajjame, J. Zhao, D. Garijo, A. Garrido, S. Soiland-Reyes, P. Alper and O. Corcho, A workflow PROV-corpus based on taverna and wings, in: *Proceedings of the Joint EDBT/ICDT 2013 Workshops on – EDBT'13*, ACM Press, 2013, p. 331, http://dl.acm.org/citation.cfm?doid=2457317.2457376. ISBN 978-1-4503-1599-9. doi:10.1145/2457317.2457376.

[14] A. Berglund, S. Boag, D. Chamberlin, M.F. Fernández, M. Kay, J. Robie and J. Siméon, XML Path Language (XPath) 2.0 (Second Edition), 2010, https://www.w3.org/TR/xpath20/.

[15] T. Berners-Lee, D. Connolly, L. Kagal, Y. Scharf and J. Hendler, N3Logic: A logical framework for the World Wide Web, in: *Theory and Practice of Logic Programming*, Vol. 8, 2008-05, pp. 249–269, https://www.cambridge.org/core/product/identifier/S1471068407003213/type/journal_article. doi:10.1017/S1471068407003213.

[16] S. Berthold, Towards a formal language for privacy options, in: *Privacy and Identity 2010: Privacy and Identity Management for Life*, S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes and G. Zhang, eds, IFIP Advances in Information and Communication Technology, Vol. 352, Springer, Berlin, Heidelberg, 2011, pp. 27–40, https://link.springer.com/chapter/10.1007.

[17] S. Berthold, The Privacy Option Language – Specification & Implementation, Research Report, Faculty of Health, Science and Technology, Karlstad University, 2013, http://kau.diva-portal.org/smash/get/diva2:623452/FULLTEXT01.pdf.

[18] K. Bohrer and B. Holland, Customer Profile Exchange (CPExchange) Specification, Technical Specification, 2000.

[19] H. Boley, A. Paschke, T. Athan, A. Giurca, N. Bassiliades, G. Governatori, M. Palmirani, A. Wyner, A. Kozlenkov and G. Zou, Specification of RuleML 1.02, 2017, http://wiki.ruleml.org/index.php/Specification_of_RuleML_1.02.
[20] P. Bonatti, S. Kirrane, I.M. Petrova, L. Sauro and E. Schlehahn, The SPECIAL Usage Policy Language version 1.0, 2019, https://ai.wu.ac.at/policies/policylanguage/.
[21] P.A. Bonatti, B. Bos, S. Decker, J.D. Fernandez, S. Kirrane, V. Peristeras, A. Polleres and R. Wenning, Data Privacy Vocabularies and Controls: Semantic Web for Transparency and Privacy, in: *Semantic Web for Social Good (SWSG2018) ISWC2018*, CEUR Workshop Proceedings, 2018.
[22] P.A. Bonatti, S. Kirrane, I. Petrova, L. Sauro and E. Schlehahn, *Policy Language V2 – Deliverable D2.5, Project Deliverable*, 2018, https://www.specialprivacy.eu/images/documents/SPECIAL_D25_M21_V10.pdf.
[23] BPR4GDPR, Business Process Re-engineering and functional toolkit for GDPR compliance, 2018, https://www.bpr4gdpr.eu/.
[24] J. Byrum, S. Jouguelet, D. McGarry, N. Williamson, M. Witt, T. Delsey, E. Dulabahn, E. Svenonius and B. Tillett, Functional Requirements for Bibliographic Records, Technical Report, 2009, https://www.ifla.org/publications/functional-requirements-for-bibliographic-records.
[25] C.S.A.-P.L.A.W. Group, Code of Conduct for GDPR Compliance, 2017, https://downloads.cloudsecurityalliance.org/assets/research/gdpr/CSA_Code_of_Conduct_for_GDPR_Compliance.pdf.
[26] N. Casellas, J.-E. Nieto, A. Meroño, A. Roig, S. Torralba, M. Reyes and P. Casanovas, *Ontological Semantics for Data Privacy Compliance: The NEURONA Project, in: 2010 AAAI*, Spring Symposium, Intelligent Information Privacy Management, AAAI, 2010, pp. 34–38, https://ddd.uab.cat/pub/artpub/2010/137891/aaaisprsymser_a2010n1iENG.pdf.
[27] L. Chung, B.A. Nixon, E. Yu and J. Mylopoulos, The NFR framework in action, in: *Non-Functional Requirements in Software Engineering*, International Series in Software Engineering, Springer US, 2000, pp. 15–45. ISBN 978-1-4615-5269-7. doi:10.1007/978-1-4615-5269-7_2.
[28] J. Clark and S. DeRose, XML Path Language (XPath) Version 1.0, 1999, https://www.w3.org/TR/1999/REC-xpath-19991116/.
[29] L. Cranor, M. Langheinrich and M. Marchiori, A P3P Preference Exchange Language 1.0 (APPEL1.0), 2002, https://www.w3.org/TR/2002/WD-P3P-preferences-20020415/.
[30] L. Cranor, M. Langheinrich, M. Marchiori, M. Presler-Marshall and J. Reagle, Specification, 2002, Publication Title: W3C Recommendation 16 April 2002 obsoleted 30 August 2018, https://www.w3.org/TR/P3P/.
[31] R.J. Cronk, Categories of personal information, 2017, Publication Title: Enterprivacy Consulting Group, https://enterprivacy.com/2017/03/01/categories-of-personal-information/.
[32] F. Dalpiaz, X. Franch and J. Horkoff, *iStar 2.0 Language Guide*, 2016, http://arxiv.org/abs/1605.07767.
[33] C. Duma, A. Herzog and N. Shahmehri, Privacy in the semantic web: What policy languages have to offer, in: *Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07)*, 2007, pp. 109–118. doi:10.1109/POLICY.2007.39.
[34] E.D.P. Board, Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1, 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.
[35] E.U.A. for Fundamental Rights, *Handbook on European data protection law*, Re-ed. edn, Handbook / FRA, European Union Agency for Fundamental Rights, Publ. Office of the Europ. Union [u.a.], 2014, OCLC: 931804500. ISBN 978-92-871-9934-8, 978-92-9239-461-5.
[36] L. Elluri and K.P. Joshi, A knowledge representation of cloud data controls for EU GDPR compliance, in: *2018 IEEE World Congress on Services (SERVICES)*, IEEE, 2018, pp. 45–46, https://ieeexplore.ieee.org/document/8495788/. ISBN 978-1-5386-7374-4. doi:10.1109/SERVICES.2018.00036.
[37] L. Elluri, A. Nagar and K.P. Joshi, An Integrated Knowledge Graph to Automate GDPR and PCI DSS Compliance, in: *2018 IEEE International Conference on Big Data (Big Data)*, IEEE, 2018-12, pp. 1266–1271. ISBN 978-1-5386-5035-6, https://ieeexplore.ieee.org/document/8622236/. doi:10.1109/BigData.2018.8622236.
[38] M. Fernández, A. Gómez-Pérez and N. Juristo, Methontology: From ontological art towards ontological engineering, in: *Proceedings of the Ontological Engineering AAAI-1997 Spring Symposium Series*, 1997, pp. 33–40.
[39] N. Fornara and M. Colombetti, Operational semantics of an extension of ODRL able to express obligations, in: *Multi-Agent Systems and Agreement Technologies*, F. Belardinelli and E. Argente, eds, Lecture Notes in Computer Science, Springer International Publishing, 2018, pp. 172–186. ISBN 978-3-030-01713-2. doi:10.1007/978-3-030-01713-2_13.
[40] N. Fornara and M. Colombetti, Using semantic web technologies and production rules for reasoning on obligations, permissions, and prohibitions, *AI Communications* **32**(4) (2019), 319–334, https://content.iospress.com/articles/ai-communications/aic190617. doi:10.3233/AIC-190617.
[41] D. Garijo and Y. Gil, Augmenting PROV with plans in P-PLAN: Scientific processes as linked data, in: *CEUR Workshop Proceedings*, 2012.
[42] A. Gerl, Extending Layered Privacy Language to Support Privacy Icons for a Personal Privacy Policy User Interface, 2018. doi:10.14236/ewic/hci2018.177.
[43] A. Gerl, N. Bennani, H. Kosch and L. Brunie, LPL, towards a GDPR-compliant privacy language: Formal definition and usage, in: *Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVII*, A. Hameurlain and R. Wagner, eds, Lecture Notes in Computer Science, Springer, 2018, pp. 41–80. ISBN 978-3-662-57932-9. doi:10.1007/978-3-662-57932-9_2.
[44] A. Gerl and B. Meier, Privacy in the Future of Integrated Health Care Services – Are Privacy Languages the Key?, in: *2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2019, pp. 312–317. ISSN: 2160-4894. doi:10.1109/WiMOB.2019.8923532.
[45] A. Gerl and D. Pohl, in: *Critical Analysis of LPL According to Articles 12–14 of the GDPR*, 2018, pp. 1–9. doi:10.1145/3230833.3233267.
[46] A. Gerl and F. Prey, LPL Personal Privacy Policy User Interface: Design and Evaluation (2018), Publisher: Gesellschaft für Informatik e.V., http://dl.gi.de/handle/20.500.12116/16908. doi:10.18420/MUC2018-WS08-0540.

[47] R. Hoekstra, J. Breuker, M. Di Bello and A. Boer, The LKIF core ontology of basic legal concepts, in: *Proceedings of the Workshop on Legal Ontologies and Artificial Intelligence Techniques (LOAIT 2007)*, 2007, pp. 43–63.
[48] R. Iannella, M. Steidl, S. Myles and V. Rodríguez-Doncel, ODRL Vocabulary & Expression 2.2, 2018, Publication Title: W3C Rec., https://www.w3.org/TR/odrl-vocab/.
[49] ISO Technical Committee: ISO/IEC JTC 1/SC 27, ISO/IEC 29100:2011, Technical Report, 2011, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/51/45123.html.
[50] J. Iyilade and J. Vassileva, A framework for privacy-aware user data trading, in: *User Modeling, Adaptation, and Personalization*, S. Carberry, S. Weibelzahl, A. Micarelli and G. Semeraro, eds, Series Title: Lecture Notes in Computer Science., Vol. 7899, Springer, Berlin Heidelberg, 2013, pp. 310–317, http://link.springer.com/10.1007/978-3-642-38844-6_28 ISBN 978-3-642-38843-9, 978-3-642-38844-6. doi:10.1007/978-3-642-38844-6_28.
[51] J. Iyilade and J. Vassileva, P2U: A Privacy Policy Specification Language for Secondary Data Sharing and Usage, in: *2014 IEEE Security and Privacy Workshops*, IEEE, 2014-05, pp. 18–22, http://ieeexplore.ieee.org/document/6957279/. ISBN 978-1-4799-5103-1. doi:10.1109/SPW.2014.12.
[52] S. Kasem-Madani and M. Meier, *Security and Privacy Policy Languages: A Survey, Categorization and Gap Identification*, 2015, http://arxiv.org/abs/1512.00201.
[53] M.G. Kebede, G. Sileno and T.V. Engers, *A critical reflection on ODRL*, in: *AICOL 2021* Volume, 2020, to appear.
[54] A. Khandelwal, J. Bao, L. Kagal, I. Jacobi, L. Ding and J. Hendler, Analyzing the AIR language: A semantic web (production) rule language, in: *Web Reasoning and Rule Systems*, P. Hitzler and T. Lukasiewicz, eds, Lecture Notes in Computer Science, Vol. 6333, Springer, Berlin Heidelberg, 2010, pp. 58–72, http://link.springer.com/10.1007/978-3-642-15918-3_6. ISBN 978-3-642-15917-6, 978-3-642-15918-3. doi:10.1007/978-3-642-15918-3_6.
[55] S. Kirrane, J.D. Fernández, W. Dullaert, U. Milosevic, A. Polleres, P.A. Bonatti, R. Wenning, O. Drozd and P. Raschke, A scalable consent, transparency and compliance architecture, in: *The Semantic Web: ESWC 2018 Satellite Events*, A. Gangemi, A.L. Gentile, A.G. Nuzzolese, S. Rudolph, M. Maleshkova, H. Paulheim, J.Z. Pan and M. Alam, eds, Lecture Notes in Computer Science, Vol. 11155, Springer International Publishing, 2018, pp. 131–136, http://link.springer.com/10.1007/978-3-319-98192-5_25. ISBN 978-3-319-98191-8, 978-3-319-98192-5. doi:10.1007/978-3-319-98192-5_25.
[56] S. Kirrane, A. Mileo and S. Decker, Access control and the resource description framework: A survey, *Semantic Web* **8**(2) (2016), 311–352. doi:10.3233/SW-160236.
[57] S. Kirrane, U. Milosevic, J.D. Fernández, A. Polleres and J. Langens, *Transparency Framework V2 – Deliverable D2.7, Project Deliverable*, 2018, https://www.specialprivacy.eu/images/documents/SPECIAL_D27_M23_V10.pdf.
[58] B. Kitchenham and P. Brereton, A systematic review of systematic review process research in software engineering, *Information and Software Technology* **55**(12) (2013), 2049–2075, https://www.sciencedirect.com/science/article/pii/S0950584913001560. doi:10.1016/j.infsof.2013.07.010.
[59] P. Kumaraguru, J. Lobo, L. Cranor and S.B. Calo, A Survey of Privacy Policy Languages, *World Wide Web Internet And Web Information Systems* (2007).
[60] T. Lebo, S. Sahoo and D. McGuinness, PROV-O: The PROV Ontology, 2013, https://www.w3.org/TR/prov-o/.
[61] J. Leicht and M. Heisel, A survey on privacy policy languages: Expressiveness concerning data protection regulations, in: *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*, IEEE, 2019, pp. 1–6, https://ieeexplore.ieee.org/document/8962144/. ISBN 978-1-72812-856-6. doi:10.1109/CMI48017.2019.8962144.
[62] N. Li, T. Yu and A. Antón, A semantics-base approach to privacy languages, *Computer Systems: Science & Engineering – CSSE* **21** (2006).
[63] G. Lioudakis and D. Cascone, *Compliance Ontology – Deliverable D3.1, Project Deliverable*, 2019, https://www.bpr4gdpr.eu/wp-content/uploads/2019/06/D3.1-Compliance-Ontology-1.0.pdf.
[64] M. Lizar and D. Turner, Consent Receipt Specification v1.1.0, Technical Report, 2017, https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification.
[65] K. Martiny and G. Denker, Partial Decision Overrides in a Declarative Policy Framework, in: *2020 IEEE 14th International Conference on Semantic Computing (ICSC)*, IEEE, 2020-02, pp. 271–278, https://ieeexplore.ieee.org/document/9031488/. ISBN 978-1-72816-332-1. doi:10.1109/ICSC.2020.00056.
[66] K. Martiny, D. Elenius and G. Denker, Protecting Privacy with a Declarative Policy Framework, in: *2018 IEEE 12th International Conference on Semantic Computing (ICSC)*, IEEE, 2018-01, pp. 227–234, http://ieeexplore.ieee.org/document/8334462/. ISBN 978-1-5386-4408-9. doi:10.1109/ICSC.2018.00039.
[67] A. Miles and S. Bechhofer, *SKOS Simple Knowledge Organization System Reference*, 2009, https://www.w3.org/TR/skos-reference/.
[68] H. Mouratidis and P. Giorgini, Secure tropos: A security-oriented extension of the tropos methodology, in: *International Journal of Software Engineering and Knowledge Engineering*, Vol. 17, Publisher: World Scientific Publishing Co., 2007, pp. 285–309. doi:10.1142/S0218194007003240.
[69] N.F. Noy and D.L. McGuinness, *Ontology Development 101: A Guide to Creating Your First Ontology*, 2001.
[70] O. of Publications on Eur-Lex, EU Vocabularies – European Legislation Identifier (ELI), 2017, https://op.europa.eu/en/web/eu-vocabularies/eli.
[71] O.M.G. (OMG), Business Process Model and Notation (BPMN) Version 2.0, Specification, 2011, http://www.omg.org/spec/BPMN/2.0.
[72] ODPA, Ontology Design Patterns.org (ODP) – Time interval ontology, http://www.ontologydesignpatterns.org/cp/owl/timeinterval.owl.
[73] OECD, The OECD Privacy Framework, Technical Report, 2013, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[74] P.S.S. Council, Payment Card Industry (PCI) Data Security Standard – Version 3.2.1, 2018, https://www.pcisecuritystandards.org/document_library.

[75] M. Palmirani and G. Governatori, Modelling legal knowledge for GDPR compliance checking, in: *Legal Knowledge and Information Systems*, Vol. 313, IOS Press, 2018, pp. 101–110. doi:10.3233/978-1-61499-935-5-101.

[76] M. Palmirani, G. Governatori, T. Athan, H. Boley, A. Paschke and A. Wyner, LegalRuleML Core Specification Version 1.0 – OASIS Standard, 2021-08-30, https://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/os/legalruleml-core-spec-v1.0-os.html.

[77] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini and L. Robaldo, PrOnto: Privacy ontology for legal reasoning, in: *Electronic Government and the Information Systems Perspective (EGOVIS 2018)*, A. Kő and E. Francesconi, eds, Lecture Notes in Computer Science, Vol. 11032, Springer International Publishing, 2018, pp. 139–152, http://link.springer.com/10.1007/978-3-319-98349-3_11. ISBN 978-3-319-98348-6, 978-3-319-98349-3. doi:10.1007/978-3-319-98349-3_11.

[78] H.J. Pandit, Representing Activities associated with Processing of Personal Data and Consent using Semantic Web for GDPR Compliance, 2020.

[79] H.J. Pandit, C. Debruyne, D. O'Sullivan and D. Lewis, GConsent – a consent ontology based on the GDPR, in: *The Semantic Web*, P. Hitzler, M. Fernández, K. Janowicz, A. Zaveri, A.J.G. Gray, V. Lopez, A. Haller and K. Hammar, eds, Lecture Notes in Computer Science, Vol. 11503, Springer International Publishing, 2019, pp. 270–282, http://link.springer.com/10.1007/978-3-030-21348-0_18. ISBN 978-3-030-21347-3, 978-3-030-21348-0. doi:10.1007/978-3-030-21348-0_18.

[80] H.J. Pandit, K. Fatema, D. O'Sullivan and D. Lewis, GDPRtEXT – GDPR as a linked data resource, in: *The Semantic Web*, A. Gangemi, R. Navigli, M.-E. Vidal, P. Hitzler, R. Troncy, L. Hollink, A. Tordai and M. Alam, eds, Lecture Notes in Computer Science, Vol. 10843, Springer International Publishing, 2018, pp. 481–495, http://link.springer.com/10.1007/978-3-319-93417-4_31. ISBN 978-3-319-93416-7, 978-3-319-93417-4. doi:10.1007/978-3-319-93417-4_31.

[81] H.J. Pandit and D. Lewis, Modelling provenance for GDPR compliance using linked open data vocabularies, in: *Society, Privacy and the Semantic Web – Policy and Technology (PrivOn 2017), Co-Located with ISWC 2017*, 1951, http://ceur-ws.org/Vol-1951/PrivOn2017_paper_6.pdf.

[82] H.J. Pandit, A. Polleres, B. Bos, R. Brennan, B. Bruegger, F.J. Ekaputra, J.D. Fernández, R.G. Hamed, E. Kiesling, M. Lizar, E. Schlehahn, S. Steyskal and R. Wenning, Creating a vocabulary for data privacy: The first-year report of data privacy vocabularies and controls community group (DPVCG), in: *On the Move to Meaningful Internet Systems: OTM 2019 Conferences*, H. Panetto, C. Debruyne, M. Hepp, D. Lewis, C.A. Ardagna and R. Meersman, eds, Series Title: Lecture Notes in Computer Science., Vol. 11877, Springer International Publishing, 2019, pp. 714–730, http://link.springer.com/10.1007/978-3-030-33246-4_44. ISBN 978-3-030-33245-7, 978-3-030-33246-4. doi:10.1007/978-3-030-33246-4_44.

[83] B. Parducci, H. Lockhart and E. Rissanen, eXtensible Access Control Markup Language (XACML) Version 3.0, 2013, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

[84] M.M. Peixoto and C. Silva, Specifying privacy requirements with goal-oriented modeling languages, in: *Proceedings of the XXXII Brazilian Symposium on Software Engineering, SBES'18*, Association for Computing Machinery, 2018, pp. 112–121. ISBN 978-1-4503-6503-1. doi:10.1145/3266237.3266270.

[85] T. Pellegrini, A. Schönhofer, S. Kirrane, A. Fensel, O. Panasiuk, V. Mireles-Chavez, T. Thurner, M. Dörfler and A. Polleres, A genealogy and classification of rights expression languages – preliminary results, in: *Proceedings of the 21st International Legal Informatics Symposium*, 2018, pp. 243–250.

[86] S. Peroni, The semantic publishing and referencing ontologies, in: *Semantic Web Technologies and*, Legal Scholarly Publishing, Law, Governance and Technology Series, Vol. 15, Springer, Cham, 2014, pp. 121–193. ISBN 978-3-319-04776-8.

[87] R.W.W.C. Group, WebAccessControl, 2019, Publication Title: W3C Wiki, https://www.w3.org/wiki/WebAccessControl.

[88] L. Robaldo, C. Bartolini and G. Lenzini, The DAPRECO knowledge base: Representing the GDPR in LegalRuleML, in: *Proceedings of the 12th Conference on Language Resources and Evaluation (LREC 2020)*, 2020, pp. 5688–5697.

[89] O. Sacco and A. Passant, A privacy preference manager for the social semantic web, in: *Proceedings of the 2nd Workshop on Semantic Personalized Information Management: Retrieval and Recommendation, SPIM2011*, 2011, pp. 42–53. ISBN 16130073.

[90] O. Sacco and A. Passant, *A Privacy Preference Ontology (PPO) for Linked Data*, 2011, http://ceur-ws.org/Vol-813/ldow2011-paper01.pdf.

[91] P.M. Schwartz and D.J. Solove, PII 2.0: Privacy and a New Approach to Personal Information, Technical Report, 2012.

[92] H. Snyder, Literature review as a research methodology: An overview and guidelines, *Journal of Business Research* **104** (2019), 333–339, https://www.sciencedirect.com/science/article/pii/S0148296319304564. doi:10.1016/j.jbusres.2019.07.039.

[93] SPECIAL, Home – SPECIAL, 2019, https://www.specialprivacy.eu/.

[94] M.C. Suárez-Figueroa, A. Gómez-Pérez and M. Fernández-López, The NeOn methodology for ontology engineering, in: *Ontology Engineering in a Networked World*, M.C. Suárez-Figueroa, A. Gómez-Pérez, E. Motta and A. Gangemi, eds, Vol. 2, Springer, Berlin Heidelberg, 2012, pp. 9–34, https://doi.org/10.1007/978-3-642-24794-1_2. ISBN 978-3-642-24794-1. doi:10.1007/978-3-642-24794-1_2.

[95] J. Webster and R.T. Watson, Analyzing the past to prepare for the future: Writing a literature review, *MIS Quarterly* **26**(2) (2002), xiii–xxiii, https://www.jstor.org/stable/4132319.

[96] A.F. Westin, Special report: Legal safeguards to insure privacy in a computer society, *Communications of the ACM* **10**(9) (1967), 533–537. doi:10.1145/363566.363579.

[97] R. Whittemore and K. Knafl, The integrative review: Updated methodology, *Journal of Advanced Nursing* **52**(5) (2005), 546–553. doi:10.1111/j.1365-2648.2005.03621.x.

[98] C. Wohlin, *Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering*, ACM, 2014, http://urn.kb.se/resolve?urn=urn:nbn:se:bth-6463.

[99] J. Zhao, R. Binns, M. Van Kleek and N. Shadbolt, Privacy languages: Are we there yet to enable user controls? in: *Proceedings of the 25th International Conference Companion on World Wide Web, WWW'16 Companion, International World Wide Web Conferences Steering Committee*, 2016, pp. 799–806. ISBN 978-1-4503-4144-8. doi:10.1145/2872518.2890590.