Fostering trust with transparency in the data economy era: an integrated ethical, legal, and knowledge engineering approach

Beatriz Esteves
beatriz.gesteves@upm.es
Ontology Engineering Group
Universidad Politécnica de Madrid
Madrid, Spain

Haleh Asgarinia
Behavioural, Management and Social Science Faculty
Universiteit Twente, Twente
Netherlands

Andres Chomczyk Penedo
Law, Science, Technology and Society Research Group
Vrije Universiteit Brussel, Brussels
Belgium

Blessing Mutiro
Castlebridge
Dublin, Ireland

Dave Lewis
Trinity College Dublin
Dublin, Ireland

ABSTRACT

Why is it hard for online users to trust service providers when it comes to their personal data? While users might give away their data when using their services, this does not mean that they necessarily trust these companies. Building trust in online services is particularly relevant as digital economy policy strategies, such as the EU Data Strategy, deposit a considerable amount of faith in the benefits of a data-driven society. To achieve this goal, transparency should be considered a necessary feature, on which trust can be built. According to scholarly literature, the more information provided to data subjects, the less power asymmetry, caused by a lack of knowledge, between them and data controllers will exist. In this respect, transparency around data processing has been, and still is, conveyed through privacy notices. But these are far from being used as helpful tools to navigate complex data-intensive environments. Technical developments, such as Solid personal datastores, provide a fertile ground for the negotiation of privacy terms between the involved parties. But to do so, it is necessary to have clear and transparent processing conditions. However, while certain specifications have been developed to accommodate for the representation of privacy terms, there is still a lack of developed solutions to address this problem. With this in mind, we propose the usage of the Privacy Paradigm ODRL Profile (PPOP), which extends ODRL and DPV to specify data processing requirements for personal datastores envisaged as key core elements of the data economy. To demonstrate the usage of PPOP, a set of policy examples will be provided, as well as a prototype implementation of a generator of machine and human-readable PPOP policies.

CCS CONCEPTS

• **Information systems → World Wide Web**; *Ontologies*; • **Security and privacy → Human and societal aspects of security and privacy**; *Access control*; *Social aspects of security and privacy*; *Privacy protections*; • **Applied computing → Law**; • **Social and professional topics → Centralization / decentralization**; *Centralization / decentralization*; *Privacy policies.*

KEYWORDS

trust, transparency, data economy, data protection, ethics, knowledge engineering, personal information management systems

ACM Reference Format:
Beatriz Esteves, Haleh Asgarinia, Andres Chomczyk Penedo, Blessing Mutiro, and Dave Lewis. 2022. Fostering trust with transparency in the data economy era: an integrated ethical, legal, and knowledge engineering approach. In *Data Economy (DE '22), December 9, 2022, Roma, Italy*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3565011.3569061

DE '22, December 9, 2022, Roma, Italy

ACM ISBN 978-1-4503-9923-4/22/12…$15.00
https://doi.org/10.1145/3565011.3569061

1 INTRODUCTION

Digital economy policymaking is currently being placed at the forefront of the political agenda, particularly in the European Union with the launch of the EU Data Strategy [4]. Therefore, (re)building trust in online services is of particular interest for both digital services' providers and users to benefit from a data-driven society. These policy developments have pushed forward an agenda around the data economy and the reliance on readily available (personal) data for its sharing and (re-)use in an interoperable manner.

Technical developments, such as Solid, also accompany this agenda and provide a fertile ground for the management of data and machine-readable renderings of the privacy terms associated with a given data processing activity. In this respect, these solutions would take users' privacy preferences and communicate them to data controllers. Given the ample possibilities that data processing entails, ontologies can provide a common framework to accommodate distinct operations and actors in a flexible manner. While certain specifications, such as the Data Privacy Vocabulary[1] (DPV) or its GDPR extension[2] (DPV-GDPR), which have been developed to accommodate for the representation of privacy terms, or the Open Digital Rights Language[3] (ODRL), which allows the expression of declarative rules over the usage of digital assets, there is a clear lack of recognized standards in this particular field. Specifically, considering the introduction of new types of entities in the data

[1] https://w3id.org/dpv
[2] https://www.w3id.org/dpv/dpv-gdpr
[3] https://www.w3.org/TR/odrl-model/, https://www.w3.org/TR/odrl-vocab/

economy, such as the data trusts or data intermediaries put forward by novel regulation as the Data Governance Act (DGA).

As such, it is necessary to rethink how trust can be developed in an environment where privacy can be understood as a social construction that individuals can create as they negotiate their relationships with others. To achieve this goal, transparency should be considered a necessary feature; enhancing transparency in the context of information disclosure encourages trustworthiness and provides good reasons for trusting. It is possible to pinpoint the importance that the EU Data Strategy has in this respect to empower individuals in the handling of their (personal) data. This policy document recognizes that '(...) there are calls to give individuals the tools and means to decide at a granular level what is done with their data (...)'. Those tools and means include consent management tools, personal information management apps, including fully decentralized solutions building on a blockchain, as well as personal data cooperatives or trusts acting as novel neutral intermediaries in the personal data economy (...)' [4]. One example of these novel technologies are personal data stores as a form of personal information management systems (PIMS) [9].

However, complex data interactions between the data subject and many other stakeholders can put a considerable amount of pressure on the individual by overloading it with decisions [12, 34]. If automation of these decisions relying on a privacy preference profile is considered, then clear transparency over the data flows is necessary to allow these preferences to match with actual practices. As such, providing those machine-readable renderings to facilitate automation on both sides can contribute to the consolidation of a model that respects and safeguards fundamental rights. This is the result of the PROTECT project, in particular of its Work Package 1.[4] As such, this contribution seeks to, relying on existing legal and ethical requirements, propose an ODRL profile capable of facilitating interactions between different entities upon transparent information on a certain data processing activity.

The paper is organized as follows: Section 2 provides an overview of existing work regarding legal, ethical and machine readable privacy policies, Section 3 describes the motivation, requirements and sources used in our approach, Section 4 introduces PPOP and gives details regarding its development and publication, Section 5 presents two examples where PPOP is used to define privacy preferences and intermediaries' transparency practices, and Section 6 concludes the paper.

2 RELATED WORK

2.1 Legal and ethical privacy notices

The risk-based approach in the GDPR implies that data controllers must adopt relevant measures to prevent or, if not possible, mitigate any harm that data subjects might suffer because of a data processing activity [20, 30]. This means that each processing activity demands a tailored set of measures decided after a thorough analysis of the situation. Authoritative bodies and legal literature have identified different types of measures [14]. Among these, information and transparency are one of the three types of safeguards that data controllers can adopt to mitigate or prevent harm.

While GDPR places a great deal of importance on transparency to the data subjects but despite this, it has come at the expense of lower ratios of data subjects actually reading them [23]. The typical privacy notice consists of a single document, usually located in an inconvenient location and relies heavily on complex and highly legal explanations [33]. In this regard, privacy notices are being used as a tool to comply with a legal requirement and not as a tool to allow data subjects to monitor how their data is used [24].

Certain supervisory authorities, such as the Agencia Española de Protección de Datos[5] or the Information Commissioner's Office[6], have published different standard privacy notice templates that can be used in a wide range of online services. However, the use of standards and templates when it comes to privacy notices might not be ethically appropriate, at least because they do not support or enhance the agency of data subjects or users for each case. Templates are compliance-focused and allow organizations can get away with burying their activities in the fine print rather than help data subjects to actually understand what is happening with their data [31]. This limits data subjects' freedom to explore and choose what happens to their data. As it shall be explored below, technical developments that allow for individual customization of data and privacy preferences are beginning to emerge and, therefore, should be preferred.

2.2 Machine-readable policies for privacy

Given this, it is possible to address the current state of the most relevant existing Semantic Web solutions for privacy-related machine-readable policy languages. The focus was placed on Semantic Web solutions since they promote interoperability and are based on open Web specifications. Recently, Esteves and Rodríguez-Doncel [19] published a review of 13 privacy-related policy languages and 9 data protection vocabularies that were analyzed in terms of their capacity to represent information described in GDPR's rights and obligations and concluded that ODRL [21], LegalRuleML [25], DPV [27] and GDPRtEXT [26] are the most adequate solutions as they can be used to fulfill a greater number of representational needs brought on by GDPR.

Moreover, there is already a body of work that uses ODRL to represent policies related to the usage of personal data or in particular connected with the GDPR. Agarwal et al. [11] provide an ODRL profile to model GDPR rights and obligations and support for the representation of information related to other legislations. De Vos et al. [17] perform automatic compliance checking using ASP rules that are based on an ODRL profile which models GDPR requirements. OAC [18] is an ODRL profile for the representation of GDPR-compliant access control policies, that can be applied for instance to the governance of access to personal data stored in Solid Pods, which uses DPV to invoke specific data protection terms.

However, through the analysis of these works, it can be concluded that there is still a gap in the representation of concepts

[4]The PROTECT project is a Marie Sklodowska-Curie ITN project funded by the European Commission with the purpose of raising up 14 early career researchers in the fields of computer science, ethics, and law so that they are able to tackle current and future issues in an interdisciplinary manner.

[5]https://www.aepd.es/en/guides-and-tools/tools/facilita-rgpd

[6]https://ico.org.uk/media/for-organisations/documents/2617435/privacy-template-v2.docx

related to privacy notices. According to the studies mentioned before, ODRL and DPV are perfect candidates to be extended for the requirements of this work as they have already been successfully used in this field of knowledge and the former is a W3C standard for the representation of policies. Furthermore, beyond maturity, DPV has the highest number of terms with taxonomies to categorize entities, personal data, purposes, processing operations, legal basis, technical and organizational measures and other contextual information, as well as specific extensions for GDPR, technology, jurisdiction and personal data categories.

3 MOTIVATION

3.1 Scope

For the development of the ODRL profile, the scope of this contribution is limited to European personal data-related regulations and ethical guidelines related to the transparency of Artificial Intelligence, given the role that automated decision making can have in the data economy but also the extensive work on building transparency technical solutions. Its main purpose is to support the specification of transparency measures in the context of data sharing activities and data-intensive flows between multiple data subjects, controllers and processors in decentralized data storage environments. This is particularly necessary as the European Commission has indicated that these technologies are still in their infancy and further development on them is necessary to harness their potential benefits [4], therefore making our proposal an adequate match for the development of web-based solutions for the digital economy.

3.2 Requirements

The following requirements were considered necessary for the development and specification of this work:

R1. Classify transparency practices of intermediary services
R2. Define access control policies for legal and ethical access to group and individual personal data stores
R3. Model safeguards for the trustworthiness of AI systems and respective rights and duties

To fulfill such requirements, a set of legal and ethical resources were comprehensively reviewed to provide terms to the defined ODRL profile, which can be used to enhance the transparency of policies specified with ODRL. Section 3.2.1 provides an overview of the used regulatory sources and Section 3.2.2 of the main sources of ethical requirements. The work was further complemented by scholarly literature on the matter when gaps were identified; a complete list of those sources can be found in the profile documentation[7].

3.2.1 Regulatory sources. As specified in Section 3.1, for this work the focus was put on the analysis of legal requirements from European legislation related to privacy and data protection. As such, in-force regulations and proposals of the European Commission were taken into account as well as existing case law and guidelines by the European Data Protection Board (EDPB). The sources used in this respect were the following: (i) GDPR[2], (ii) DGA [10], (iii) eIDAS 2 [7], (iv) DSA [6], (v) EDPB's guidelines on consent [13], (vi) Article 29 Working Party guidelines on transparency [28], and (vii) WhatsApp Ireland decision from the Irish data protection supervisory authority [16].

3.2.2 Ethical sources. A review of existing ethical guidelines related to the transparency of Artificial Intelligence was performed for the collection of requirements that our profile must fulfill. As such, the sources used in this respect were the following: (i) Ethics Guidelines for Trustworthy AI [3], (ii) Understanding artificial intelligence ethics and safety [22], (iii) Recommendation of the Council on AI [8], (iv) First draft of the recommendation on the ethics of artificial intelligence [5], and (v) European Convention on Human Rights [1]. In addition to these sources, various ethical and philosophical literature was used, which are listed in https://w3id.org/ppop#ethical-sources.

4 PRIVACY PARADIGM ODRL PROFILE

As discussed above, this work aims to provide open-source policy representation tools fit for the data sharing and platform economy that can contribute to providing transparency of these complex data flows by building bridges across the different gaps identified when reviewing the existing ethical and legal documents on the matter of this work. Besides this, a considerable gap was identified in the effective implementation of policies for a data-intensive sharing environment around personal data stores.

Therefore, we have developed an ODRL profile – the Privacy Paradigm ODRL Profile (PPOP) – which extends previous efforts, such as the OAC profile, to demonstrate concrete situations where this falls short on the representation of transparency measures and can be improved for instance in scenarios where data subjects store their data on personal data stores and want to trust in an intermediary to facilitate the sharing of their data with other entities.

Besides incorporating in a functional manner both existing machine-readable standards to render privacy terms, such as DPV or DPV-GDPR, as well as creating new classes and properties to accommodate for recent regulatory and technical developments necessary for the data/platform economy, the development of the Privacy Paradigm model would not be complete without the generation of a human-readable template of privacy notices.

Due to the use of English as the main working language in the project, a template from a native English-speaking authority was selected as the basis for this work. While the Irish Data Protection Commissioner lacks such a template, the Information Commissioner's Office, the UK data protection supervisory authority, does have one that was produced before Brexit. Therefore, this work extends the UK template with the terms captured by the Privacy Paradigm, which is described in the PPOP ontology, to provide a more transparent notice of the personal data processing practices of organizations. The templates are available at https://github.com/besteves4/ppop/tree/main/templates.

4.1 Ontology development and evaluation

For the development of the profile, the LOT methodology [29] was followed and, to determine its extent, formal competency questions (CQ) were made using the methodology described by Suárez-Figueroa et al. [32]. The collected requirements are presented in an abbreviated Ontology Requirement Specification Document (ORSD), available at https://w3id.org/ppop#orsd.

[7] https://w3id.org/ppop#references

Table 1: CQs derived from regulatory and ethical sources and respective concepts

Competency Questions	Main concepts
What measures were taken into account to improve the transparency of an AI system? To what extent did you safeguard the trustworthiness of the system under harsh conditions?	Measure, TransparencyMeasure, SafeguardForTrustworthiness
How to ensure that the decisions of the system do not have discriminatory or inequitable impacts on the lives of the people they affect? How to ensure that the users are able to make free and informed decisions while enforcing their rights? Is there any applicable exemption to the legal obligations of a company regarding data subject rights?	Right, GroupRight, DataSubjectRight, OrganisationDuty, RightExemption
Who are the new stakeholders involved in the data sharing economy?	Group, DataSharingEntity, DataTrustProvider
Which technologies can be used to return control over data to the users?	Technology, PIMS

Based on the related work and motivation described in Sections 2 and 3, it was concluded that there is a gap in the existing work, particularly when trying to approach this phenomenon of intensive data sharing flows in an interdisciplinary manner. In this context, ODRL can provide an already validated model to represent policies related to the use of data resources and, when aligned with DPV, it can be applied to define data sharing preferences aligned with data protection requirements. Therefore, these two vocabularies were used as the foundation of the PPOP ontology.

Once the requirements were specified and using the terms generated through the preparation of competency questions, the Chowlk Visual Notation tool [15] was used to generate the first version of the ontology's diagram and RDF specification. After the generation of the first version of the ontology, the created terms were evaluated against a set of concrete data sharing scenarios[8], derived from previous work conducted in the PROTECT project. From this evaluation, a new set of terms was added to the ontology and the ORSD, more specifically the CQs, was updated accordingly. PPOP's applicability was also evaluated by modeling concrete example use cases (examples available in Section 5) and by using the OntOlogy Pitfall Scanner (OOPS!)[9]. As a final evaluation, a complete review of the terms, and their definitions, was performed by the legal and ethical experts present in this work and each term was connected with the relevant legal and ethical legislation, guidelines and other literature.

4.2 Ontology overview

The profile online documentation and RDF serializations can be found at https://w3id.org/ppop. Since a few regulatory sources, e.g., eIDAS 2 and DSA, are still proposals for regulation, and as such subject to change, PPOP's terms and requirements will need to be revised and updated at the time of publication of the final text of the mentioned regulations. Additionally, other relevant documents published by supervisory authorities, case law and other ethical guidelines or publications might be useful to update and improve the quality of the ontology. Table 1 contains a list of the main competency questions and respective derived concepts – a complete list of all considered CQs is available in the online documentation.

In Figure 1, the main concepts of the PPOP ontology are depicted. As mentioned before, PPOP reuses concepts from the ODRL Access Control (OAC) profile, mainly to represent information related to legal entities, personal data categories, processing activities and purposes for processing – these particular taxonomies include a very large collection of terms that stem from DPV. PPOP also extended DPV's technology, safeguard, processing context and rights concepts with new terms and introduces a taxonomy of organization duties.

Regarding entities, PPOP included 8 new terms that extend DPV's Entity taxonomy, to reflect the new stakeholders involved in personal data sharing activities, coming from the DGA, eIDAS 2 and DSA. These include terms to specify data intermediaries such as data sharing service providers and data altruism organizations, as well as data holder, data user and data trust entities. The concept of "Group" was also added to represent a collection of individuals who share a common purpose, for instance regarding the processing of their personal data. A diagram and the complete definition of each term, and respective legal and ethical sources, are available at https://w3id.org/ppop#x3-1-entities. The "Technology" terms that were added to PPOP to model PIMS, such as personal data stores and identity wallets,[10] and their definition and respective legal source, are available at https://w3id.org/ppop#x3-2-technologies. These terms are particularly important to be able to specify the technology used in conjunction with the service provider and the location of the data.

The term "Measure" is defined as "Any action deployed by an entity involved in a data processing activity, due to the existence of a legal obligation, to guarantee and protect that the personal data involved shall not be affected in any way and, consequently, cause harm to the data subject" and is intended to be a superclass for DPV's technical and organizational measures and to the transparency measure term which is also an addition brought by PPOP. In addition, the term "safeguard for trustworthiness" was added as a subclass of DPV's safeguard term to specify subclasses of this term such as safeguards for explainability or safeguards for general safety. A diagram and the complete definition of each

[8]The human and machine-readable renderings of the developed scenarios are described in detail at https://w3id.org/ppop#examples
[9]https://oops.linkeddata.es/

[10]These terms were suggested for inclusion in the DPV's vocabularies and the PIMS and IdentityWallet terms were included in the DPV-TECH extension – https://w3id.org/dpv/dpv-tech.

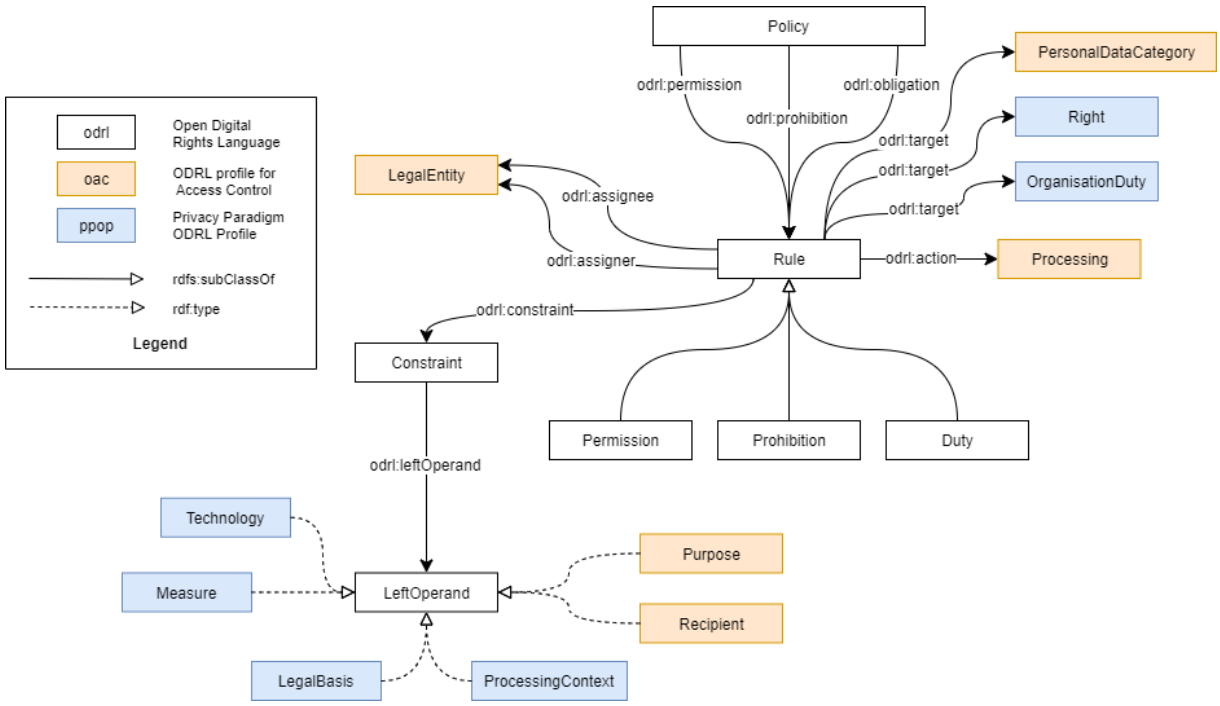

Figure 1: Main concepts of the PPOP ontology

new term, and respective legal and ethical sources, are available at https://w3id.org/ppop#x3-3-measures.

A new set of terms to describe individual and group rights was added to PPOP by extending DPV and DPV-GDPR's rights taxonomy. A collection of data subject's rights exemptions, described in the GDPR, was also included in PPOP. Diagrams and the complete definition of each right and right exemption term, and respective legal and ethical sources, are available at https://w3id.org/ppop#x3-4-rights and at https://w3id.org/ppop#x3-5-right-exemptions. As for duties of organizations, the terms explainability, traceability, auditability and accuracy were added to PPOP, which can be connected with the previously described safeguards to describe how they can be implemented organisation-wise. A diagram and the definition of each duty, and respective legal and ethical sources, are available at https://w3id.org/ppop#x3-6-duties.

5 USING PPOP IN THE DATA ECONOMY ERA

The development of PPOP allows for the integration of recent legal developments, in particular the DGA, with technological tools, such as Solid, in a cohesive manner, improving on previous efforts, such as the OAC profile which only addressed GDPR requirements. In order to assess the ontology's expressiveness and for the purpose of demonstrating it in a practical concrete situation, a cohort of case studies was selected. By deploying the profile using the developed terms to model concrete use-case scenarios, it is possible to argue that these use cases serve as validation that the ontology requirements have been met. In this context, Section 5.1 discusses a use case where PPOP is used to draft an access control policy for family data stored on a personal data store and Section 5.2 demonstrates PPOP's ability to model transparency practices and safeguards. More examples are available in the profile documentation. In addition, a prototype implementation of a generator of machine and human-readable PPOP policies, based on the profile ontology and the privacy notice template, is available at https://besteves4.github.io/ppop-gen/.

5.1 Family Pod

In this scenario, represented in Listing 1, a family, with two parents and two children, has created a policy to allow the use of their medical health data (represented as target data of the policy in `odrl:target oac:MedicalHealth`), that is stored on their family Pod, for the purpose of research and development (represented in the policy as the `ex:RD-purpose` constraint with `odrl:rightOperand dpv:ResearchAndDevelopment`) and to have a data-sharing service provider as a data intermediary. Since the data in the Pod can belong to any of the four members of the family, the assigner of the policy is a `ppop:Group` which is composed by both the parents and the children, where the parents are data holders and act as data holders for the children (represented in the policy with the property `ppop:isDataHolderFor`). The family also wishes to have a `ppop:DataSharingServiceProvider` to act as a data intermediary for the use of the data for the specified purposes. Through this example, PPOP's ability to deal with requirement R2 is demonstrated. Moreover, through the use of PPOP, it is possible for a family to express privacy preferences associated with the exercise of other rights and performance of legal duties, such as those arising from legal custody over children and dependent family members.

```
PREFIX rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>
PREFIX dc: <http://purl.org/dc/terms/>
PREFIX odrl: <http://www.w3.org/ns/odrl/2/#>
PREFIX oac: <https://w3id.org/oac#>
PREFIX ppop: <https://w3id.org/ppop#>
PREFIX dpv: <https://w3id.org/dpv#>
PREFIX ex: <https://example.com/>

ex:family-pod a odrl:Policy ;
    odrl:profile ppop:, oac: ; dc:issued "2022-02-22" ;
    odrl:uid <https://pod-provider/familyA/policy1> ;
    odrl:permission [
        odrl:assigner ex:family-pool ;
        odrl:assignee [ a ppop:DataSharingServiceProvider ] ;
        odrl:target oac:MedicalHealth ;
        odrl:action [
            rdf:value oac:Use ;
            odrl:refinement [ odrl:and (ex:RD-purpose, ex:tech) ] ] ] .
ex:RD-purpose odrl:leftOperand oac:Purpose ;
    odrl:operator odrl:isA ;
    odrl:rightOperand dpv:ResearchAndDevelopment .
ex:tech odrl:leftOperand ppop:Technology ;
    odrl:operator odrl:isA ;
    odrl:rightOperand ex:PersonalDataStore .
ex:PersonalDataStore a ppop:PersonalDataStore ;
    dpv:hasStorage [ dpv:hasLocation <https://pod-provider/familyA/> ] .
ex:family-pool a ppop:Group ;
    ppop:hasVoluntaryMembership ex:Parent1, ex:Parent2 ;
    ppop:hasNonVoluntaryMembership ex:Child1, ex:Child2 .
ex:Parent1 a ppop:DataHolder, dpv:DataSubject ;
    ppop:isDataHolderFor ex:Child1, ex:Child2, ex:Parent1 .
ex:Parent2 a ppop:DataHolder, dpv:DataSubject ;
    ppop:isDataHolderFor ex:Child1, ex:Child2, ex:Parent2 .
ex:Child1 a dpv:Child .
ex:Child2 a dpv:Child .
```

Listing 1: Family sharing policy related to its health data.

5.2 Transparency and safeguards for trustworthiness

In this scenario, represented in Listing 2, a data intermediary published a policy related to the use of work history data from their users (represented as target data of the policy in `odrl:target oac:WorkHistory`). The intermediary's transparency practices are reflected in this policy: no price is charged for the service (represented with the property `ppop:hasChargePrice` set to false) and the data is not converted to other formats (represented with the property `ppop:convertsData` set to false). The intermediary also states its duty to implement a `ppop:SafeguardForExplainability` measure in its service to provide details on how the data is being used to its users. Through this example, PPOP's ability to deal with requirements R1 and R3 is demonstrated.

```
ex:transparency-policy a odrl:Policy ;
    odrl:profile ppop:, oac: ;
    odrl:uid <https://application.com/policy1> ;
    dc:issued "2022-03-13" ;
    odrl:target oac:WorkHistory ;
    odrl:action oac:Use ;
    odrl:assignee ex:data-intermediary ;
    odrl:duty [
        odrl:action [
            rdf:value ppop:implement ;
            odrl:refinement [
                odrl:leftOperand ppop:Measure ;
                odrl:operator odrl:isA ;
                odrl:rightOperand ppop:SafeguardForExplainability ] ] ] .
ex:data-intermediary a ppop:DataIntermediary ;
    ppop:hasChargePrice "false" ;
    ppop:convertsData "false" .
```

Listing 2: Modeling transparency practices and safeguards for trustworthiness.

6 CONCLUSION AND FUTURE WORK

The Privacy Paradigm's main goal was to achieve the development of two elements, both technical and legal: the Privacy Paradigm ODRL Profile and the Privacy Paradigm notice template. These elements are intended for use in tandem in order to facilitate the communication of privacy preferences between data subjects and data controllers in the data/platform economy.

While the Privacy Paradigm constitutes a considerable improvement that has bridged in a practical manner existing gaps between the three different fields mentioned previously, there remains considerable work to be done beyond our current contribution. First and foremost, some of the regulatory proposals still need to be passed by the relevant European bodies, which could have an impact on their current wording. Secondly, the technical landscape of PIMS technologies is ever-evolving and widespread adoption of them can present new challenges not identified by this work, which should also be monitored to adjust as necessary the proposed Privacy Paradigm ODRL Profile.

In terms of future work, the legal impact of upcoming regulations related to the creation of Common Data Spaces for the healthcare, financial and other industry sectors needs to be considered in order to have an ontology that supports group, collective and collaborative control of data sharing and reuse to enable trust and can also be used by data controllers to deliver 'fit-for-purpose' advice when making choices in the platform economy. The profile should also be evaluated in real case scenarios where people can define their personal data sharing preferences. PPOP's ethical research can also be extended to preserve group rights to privacy by mitigating privacy risks against groups caused by the processing of aggregated data and disclosure of information.

While the determination of privacy preferences can be seen as putting a further burden on data subjects, they are not alone in this task. The emergence of entities such as data cooperatives, as defined under the DGA, would help users in assessing their data choices. Besides this, data controllers have an obligation to process data in a lawful manner. Data controllers, in turn, are further pressed by decisions from supervisory authorities and case law from courts that precise how this general duty needs to be complied with. Moreover, other laws, such as the Digital Markets Act and Digital Services Act, also steer data controllers' actions towards a more proactive and protective approach concerning data subjects. In this sense, more and more interactions between users and service providers can be expected in the short term, which would benefit from tools, such as PPOP, that could manage such an abundance of actions.

ACKNOWLEDGMENTS

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

REFERENCES

[1] 1950. European Convention on Human Rights.

[2] 2016. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[3] 2020. The Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment. https://data.europa.eu/doi/10.2759/002360

[4] 2020. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: a European Strategy for Data.

[5] 2020. First Draft of the Recommendation on the Ethics of Artificial Intelligence.

[6] 2020. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN

[7] 2021. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity COM/2021/281 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

[8] 2021. Recommendation of the Council on Artificial Intelligence.

[9] 2021. TechDispatch #3/2020 - Personal Information Management Systems. https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en

[10] 2022. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). http://data.europa.eu/eli/reg/2022/868/oj/eng Legislative Body: CONSIL, EP.

[11] Sushant Agarwal, Simon Steyskal, Franjo Antunovic, and Sabrina Kirrane. 2018. Legislative compliance assessment: framework, model and GDPR instantiation. In *Annual Privacy Forum*. Springer, 131–149.

[12] Omri Ben-Shahar and Carl E. Schneider. 2014. *More Than You Wanted to Know: The Failure of Mandated Disclosure*. Princeton University Press. https://doi.org/10.1515/9781400850389

[13] European Data Protection Board. 2020. Guidelines 05/2020 on consent under Regulation 2016/679 Version 1.1. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

[14] Andrés Chomczyk Penedo. 2022. *56 Reasonable Safeguards*. Edward Elgar Publishing Ltd., United Kingdom, 318–322.

[15] Serge Chávez-Feria, Raúl García-Castro, and María Poveda-Villalón. 2021. Converting UML-Based Ontology Conceptualizations to OWL with Chowlk. In *ESWC22*. 44–48.

[16] Data Protection Commission. 2021. WhatsApp Ireland Limited - IN-18-12-2. https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf

[17] Marina De Vos, Sabrina Kirrane, Julian Padget, and Ken Satoh. 2019. ODRL Policy Modelling and Compliance Checking. In *Rules and Reasoning*. 36–51.

[18] Beatriz Esteves, Harshvardhan J. Pandit, and Víctor Rodríguez-Doncel. 2021. ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid. In *EuroS&PW 2021*. 298–306. https://doi.org/10.1109/EuroSPW54576.2021.00038

[19] Beatriz Esteves and Víctor Rodríguez-Doncel. 2022. Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR. *Semantic Web J* (2022).

[20] Raphaël Gellert. 2018. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review* 34, 2 (2018), 279–288. https://doi.org/10.1016/j.clsr.2017.12.003

[21] Renato Iannella and Serena Villata. 2018. *ODRL Information Model 2.2*. https://www.w3.org/TR/odrl-model/

[22] David Leslie. 2019. Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector. https://doi.org/10.5281/ZENODO.3240529

[23] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. 2020. The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies* 1 (2020), 47–64. https://doi.org/10.2478/popets-2020-0004

[24] Jayashree Mohan, Melissa Wasserman, and Vijay Chidambaram. 2019. Analyzing GDPR Compliance Through the Lens of Privacy Policy. In *DMAH Poly 2019* (Cham). 82–95. https://doi.org/10.1007/978-3-030-33752-0_6

[25] Monica Palmirani, Guido Governatori, Tara Athan, Harold Boley, Adrian Paschke, and Adam Wyner. 2021. *LegalRuleML Core Specification Version 1.0*. https://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/os/legalruleml-core-spec-v1.0-os.html

[26] Harshvardhan J. Pandit, Kaniz Fatema, Declan O'Sullivan, and Dave Lewis. 2018. GDPRtEXT - GDPR as a Linked Data Resource. In *The Semantic Web* (Cham) *(Lecture Notes in Computer Science, Vol. 10843)*, Aldo Gangemi, Roberto Navigli, Maria-Esther Vidal, Pascal Hitzler, Raphaël Troncy, Laura Hollink, Anna Tordai, and Mehwish Alam (Eds.). Springer International Publishing, 481–495. https://doi.org/10.1007/978-3-319-93417-4_31

[27] Harshvardhan J. Pandit, Axel Polleres, Bert Bos, Rob Brennan, Bud Bruegger, Fajar J. Ekaputra, Javier D. Fernández, Roghaiyeh Gachpaz Hamed, Elmar Kiesling, Mark Lizar, Eva Schlehahn, Simon Steyskal, and Rigo Wenning. 2019. 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* (Cham), Hervé Panetto, Christophe Debruyne, Martin Hepp, Dave Lewis, Claudio Agostino Ardagna, and Robert Meersman (Eds.), Vol. 11877. Springer International Publishing, 714–730. https://doi.org/10.1007/978-3-030-33246-4_44

[28] Article 29 Data Protection Working Party. 2018. Guidelines on Transparency under Regulation 2016/679. https://ec.europa.eu/newsroom/article29/items/622227

[29] María Poveda-Villalón, Alba Fernández-Izquierdo, and Raúl García-Castro. 2019. Linked Open Terms (LOT) Methodology. https://doi.org/10.5281/zenodo.2539305

[30] Claudia Quelle. 2018. Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-based Approach. *Eur. j. risk regul.* 9, 3 (2018), 502–526. https://doi.org/10.1017/err.2018.47

[31] Neil Richards and Woodrow Hartzog. 2017. Trusting Big Data Research. *DePaul Law Review* 66 (2017).

[32] Mari Carmen Suárez-Figueroa, Asunción Gómez-Pérez, and Mariano Fernández-López. 2012. The NeOn Methodology for Ontology Engineering. In *Ontology Engineering in a Networked World*. 9–34. https://doi.org/10.1007/978-3-642-24794-1_2

[33] Arnout Terpstra, Alexander P. Schouten, Alwin de Rooij, and Ronald E. Leenes. 2019. Improving privacy choice through design: How designing for reflection could support privacy self-management. *First Monday* 24 (2019). https://doi.org/10.5210/fm.v24i7.9358

[34] Carissa Véliz. 2020. *Privacy is Power*. https://www.penguin.co.uk/books/442343/privacy-is-power-by-carissa-veliz/9780552177719