Semantic Framework for Legally-aligned Health Data Exchanges

Beatriz Esteves[1,*], Ruben Dedecker[1], Wout Slabbinck[1], Filip Pattyn[2,3,4] and Ruben Verborgh[1]

[1]IDLab, Department of Electronics and Information Systems, Ghent University – imec, Ghent, Belgium
[2]DDCM, Department of Telecommunications and information processing, Ghent University, Ghent, Belgium
[3]Department of Pharmaceutics, Ghent University, Ghent, Belgium
[4]FAQIR, Ghent Belgium

Abstract

The emerging digitalisation of healthcare services, and in particular of the related health data they use or generate, can play a pivotal role in advancing public health initiatives, healthcare delivery, and health-related research and development. However, this digitalisation presents interoperability and data integration challenges due to the fragmentation of data sources and complexity of the involved data. Furthermore, the evolving European landscape on data protection requirements, and in particular the newly-enforceable European Health Data Space (EHDS) Regulation, also raise additional regulatory compliance requirements that must be fulfilled in order to support the primary and secondary use of health data. In this context, an assessment of legal and technical requirements that need to be tackled in order to have trustful exchanges of health data was performed. The Open Digital Rights Language (ODRL) and the Data Privacy Vocabulary (DPV) specifications emerge as promising candidates to specify such requirements as machine-readable policies, that can be acted upon by policy engines to provide access to sensitive health data. To this end, in this article, we introduce (i) an analysis of legal requirements for health data exchange, (ii) existing semantic specifications to model them as machine-readable policies, and (iii) an agreement instantiation specification and implementation. The developed health data exchange policy specification highlights the usefulness of the ODRL and the DPV specifications for modelling these requirements, while the agreement instantiation specification promotes an interoperable algorithm that can be used to generate common terms for health data exchange. Additional work is also necessary to support all requirements coming from the EHDS, as well as a benchmark that can be used to evaluate the compliance of algorithms with the agreement instantiation specification.

Keywords

Health data exchange, machine-readable policies, agreement instantiation, regulatory compliance, GDPR, EHDS

1. Introduction

The increasing digitalisation of healthcare has led to the generation of vast amounts of health-related data from multiple sources, including clinical records, wearable devices, and patient-generated data. However, the fragmentation and complexity of these data sources poses significant challenges in achieving interoperability and data integration across healthcare systems. Addressing these challenges is crucial to ensuring that health data can be effectively shared and utilized while maintaining its accuracy and accessibility across different platforms and stakeholders. Beyond interoperability, the reusability of health data plays a pivotal role in advancing public health initiatives, healthcare delivery, and health-related research and development.

In this context, ensuring that health data can be repurposed for 'altruistic' activities, such as for improving healthcare or performing scientific research for the general interest, as specified in the

OPAL'25: ODRL And Beyond: Practical Applications And Challenges For Policy-Based Access And Usage Control, colocated with the Extended Semantic Web Conference 2025, June 1–5, 2025, Portorož, Slovenia
*Corresponding author.
beatriz.esteves@ugent.be (B. Esteves); ruben.dedecker@ugent.be (R. Dedecker); wout.slabbinck@ugent.be (W. Slabbinck); filip.pattyn@faqir.eu (F. Pattyn); ruben.verborgh@ugent.be (R. Verborgh)
https://w3id.org/people/besteves (B. Esteves); https://rubendedecker.be (R. Dedecker); https://woutslabbinck.com (W. Slabbinck); https://ruben.verborgh.org (R. Verborgh)
0000-0003-0259-7560 (B. Esteves); 0000-0002-3257-3394 (R. Dedecker); 0000-0002-3287-7312 (W. Slabbinck); 0000-0002-8596-222X (R. Verborgh)

EU's Data Governance Act [1] and further specified in the newly-enforceable European Health Data Space Regulation [2], e.g., for the improvement and optimisation of personalised treatment delivery or for purposes of development of health-related products or services or training new algorithms for medical devices, is of the utmost importance and requires robust mechanisms for data governance and regulatory compliance. Moreover, both of the previously mentioned regulations build their health data processing requirements over the EU's General Data Protection Regulation (GDPR) [3], which sets the regulatory framework for the processing of personal data related to EU citizens, and categorises health data as a special category of personal data and places additional constraints to its processing. Thus, compliance with these frameworks is essential to fostering trust among stakeholders, including patients, healthcare providers, researchers, and policymakers. Furthermore, a recent case ruling [4] has broadened the definition of health data, underscoring the fact that personal data that can be used to draw inferences about the health status of the data subject can constitute health data under the broad definition of the GDPR.

Given these considerations, it is imperative to develop a common framework to facilitate the interoperable and legally compliant exchange of health data. For designing such a framework, data exchange conditions must be expressed and shared amongst involved parties via interoperable, machine-readable policies that are expressive enough to address technical and legal frameworks. In this context, the usage of semantic standards, such as the Open Digital Rights Language (ODRL) [5] or the Data Privacy Vocabulary (DPV) [6], are well-suited solutions for policy expression and data protection requirement modelling, that enable a shared understanding for interpreting and enforcing health data sharing conditions. As such, we propose the definition of a framework for modelling such conditions, aligned with legal requirements from the EU's GDPR and EHDS regulation, which utilises ODRL and DPV to model requirements for health data sharing and provides an agreement instantiation algorithm that consolidates the agreed upon exchange conditions as machine-readable policies. An open-source implementation of this algorithm is also provided.

The remainder of this article is structured as follows: Section 2 describes EU-based legal provisions for health data exchange. Section 3 provides an overview of existing work for data protection-aligned policy modelling. In Section 4, we define a specification for the modelling of health data exchange conditions and an algorithm for agreement instantiation, with a respective implementation. Finally, Section 5 concludes the paper and provides pointers to future research.

2. Legal provisions for health data exchange

In this section, legal requirements to develop a framework for modeling policies are described, focusing on provisions extracted from the GDPR [3] and EHDS [2]. This is a non-exhaustive list that will be further improved with requirements for national health laws, as well as health data-related regulations from other jurisdictions. In the following paragraphs, we will explore requirements from the GDPR and EHDS.

General Data Protection Regulation Legal framework governing the processing of personal data of European Union citizens. It establishes a set of data protection principles, rights and obligations for key entities involved in data processing. These include the *data subject*, an identifiable natural person to whom the personal data pertains; the *data controller*, an entity that determines the purposes and legal basis for processing personal data; and the *data processor*, an entity that processes personal data on behalf of the controller. Additionally, Chapter III of the GDPR outlines specific rights of data subjects, such as the right to be forgotten and the right to object. Chapter IV details compliance obligations for data controllers, including the maintenance of records of processing activities and the conduction of data protection impact assessments. Furthermore, due to its sensitive nature, the processing of special

categories of personal data, such as genetic data[1] or data concerning health[2], are subject to stricter regulatory requirements, i.e., its processing is generally prohibited unless it falls under one of the legal exceptions outlined in Article 9.2 [3], such as when the data subject has given explicit consent or to protect the vital interests of the data subject.

European Health Data Space Regulation The EHDS Regulation is the first to emerge in the EU for the regulation of a common European data space. Its main goals are (i) to give individuals the solutions to access, control and share their electronic health data both at the national and European level for healthcare delivery (*primary use of data*), (ii) to enable trustful reuse of health data for research, innovation, and policy-making (*secondary use of data*), and (iii) to foster a single, interoperable market for electronic health record systems that support both primary and secondary uses of health data. In the context of primary use, patients will have the right to restrict access to all or specific parts of their electronic health data exchanged through the EHDS infrastructure, as well as an opt-out mechanism for the cross-border exchange of this data. With regard to secondary use, the processing of electronic health data, based on a permit issued by a health data access body, is permitted solely for specific purposes defined in the Regulation, e.g., public interest in the areas of public health or scientific research related to health or care sectors, and individuals who do not wish to participate have the right to opt out of such processing, unless on occasions where their data may still be utilized for certain critical public interest purposes, in which case, strict safeguards, including transparency requirements, must be met. Key entities involved in this framework include the *health data holder*[3], the *health data user*[4], and the *health data access body*[5].

In addition to the identified legal requirements, consideration for user-defined controls, e.g., ability to express the duration or frequency of a certain data exchange, and technical constraints, e.g., requirements from the used policy languages and policy enforcement mechanisms, will also be acknowledged. In this context, the following requirements were identified:

- **R1.** Ability to model policies for both data subjects/holders and data controllers/users.
- **R2.** Support legal requirements for health data exchange.
- **R3.** Define the necessity, e.g., mandatory or optional, of these requirements according to the identified legal framework.
- **R4.** Specify 'pre-defined' templates for common exchanges, e.g., patient-doctor, citizen-research organisation.
- **R5.** Generate agreements for specific health-related data exchanges between 2 parties.

Ultimately, the overarching goal of this work is to establish a framework for the modelling of health data exchange agreements, that enables transparent and legally compliant exchanges of health-related data between two parties, while fulfilling the requirements and concerns of all parties involved.

3. Background

In this section, we describe the selected standards and specifications for expression of policies aligned with data protection requirements. Related work on modelling health data exchanges is also identified.

[1] Defined in Article 4.13 [3] as "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question".

[2] Defined in Article 4.15 [3] as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

[3] Defined in Article 2.2(t) [2] as an entity that has the right or obligation to "process personal electronic health data for the provision of healthcare or care or for the purposes of public health, reimbursement, research, innovation, policymaking, official statistics or patient safety or for regulatory purposes" or "the ability to make available non-personal electronic health data through the control of the technical design of a product and related services".

[4] Defined in Article 2.2(u) [2] as an entity which has been given "lawful access to electronic health data for secondary use".

[5] Defined in Article 55 [2] as an entity governed by public law responsible for granting access to electronic health data for secondary use.

3.1. Specifications for policies and data protection

ODRL [5] is a W3C standard for the expression and modelling of policies related to the usage and re-usage of digital assets, including content and services. Its model allows the representation of permission, prohibition and obligation statements and includes terms to define constraints and additional duties over these rules. Amongst a set of analysed policy languages [7], ODRL emerged as a mature resource to deal with data protection law requirements, while maintaining an active engagement and development through the W3C ODRL Community Group. As a domain-agnostic language, its profiling mechanism [8] enables the incorporation of additional terms for specific domains that are not included in the core ODRL vocabulary. Furthermore, its usage for the modelling of data access and usage terms is being showcased in federated and decentralised systems, such as the newly-developed Data Spaces [9] and in Solid-based policy enforcement environments [10].

Additionally, DPV [6], a W3C specification developed by the W3C DPVCG, presents the most extensive collection of data protection-related terms, particularly when it comes to its ability to represent GDPR rights and obligations [7]. As such, DPV's comprehensive taxonomies of legally-aligned terms, including concepts to model legal entities, processing operations, purposes, or legal bases, are the ideal candidate to enrich ODRL policies to deal with such legal requirements. Moreover, DPV includes specific extensions to deal with requirements from particular laws, including an extension for the expression of concepts related to the GDPR[6] and an extension for the expression of concepts related to the EHDS[7]. When it comes to the coverage of health data-related concepts, DPV also developed an extension for the expression of concepts related to personal data categories[8], which includes a taxonomy of health data categories, and a extension for the expression of concepts related to the healthcare sector[9], which includes an extensive collection of purposes for processing data or using technologies within the context of the healthcare sector. A current effort is also being undertaken by both the W3C ODRL and DPV Community Groups to have an official ODRL profile for DPV[10], that enables the use of DPV concepts in ODRL policies while complying with the ODRL recommendations.

3.2. Related work

The Data Use Ontology (DUO)[11], a resource to represent consent codes and data use requirements developed by the Global Alliance for Genomics and Health, provides concepts to represent usage of genomic data by describing conditions for data usage through textual descriptions. To augment its usefulness in machine-readable scenarios, DUODRL [12] was developed using ODRL to instantiate DUO concepts as permissions, prohibitions, and obligations, which are employed to define the conditions for health dataset usage, specify requirements in data access requests, and facilitate the generation of data exchange agreements, through compatibility matching, between the two [11]. The usage of DPV for expressing legal concepts in a jurisdiction-agnostic manner, as well as for specific laws like the GDPR, was also explored. This work is one of the basis for the aforementioned ODRL profile for DPV.

HealthDCAT-AP[13] is a specialized extension of the DCAT Application Profile (DCAT-AP)[14], currently being developed in the context of the European-funded EHDS2 Pilot Project[15], which establishes a specification for the sharing of metadata related to catalogs, datasets, and data services in the health domain. While DCAT-AP establishes a common minimal framework to support the cross-border and cross-domain exchange of datasets and data services within the European context, HealthDCAT-AP builds upon this foundation by introducing an RDF vocabulary tailored to meet the specific requirements

[6] https://w3id.org/dpv/legal/eu/gdpr
[7] https://w3id.org/dpv/legal/eu/ehds
[8] https://w3id.org/dpv/pd
[9] https://w3id.org/dpv/sector/health
[10] https://w3id.org/dpv/mappings/odrl/
[11] http://purl.obolibrary.org/obo/duo
[12] https://w3id.org/duodrl/repo
[13] https://healthdcat-ap.github.io/
[14] https://semiceu.github.io/DCAT-AP/releases/3.0.0/
[15] https://ehds2pilot.eu/

of electronic health data, in particular related to the EHDS regulatory requirements for secondary usage of health data. Amongst other recommendations, HealthDCAT-AP promotes the usage of ODRL and DPV for the expression of policies and data protection requirements.

Finally, the EU is also funding the development of an European Electronic Health Record exchange Format (EHRxF)[16] to support the implementation of the EHDS Regulation, by establishing guidelines for cross-border data access and exchange and setting common technical standards for such processes. In particular, this protocol will assist patients in accessing and editing their personal health information, as well as in restricting access to specific parts of their health records, viewing who accessed their data, and asking for corrections to be made over inaccurate data.

4. Health data exchange policy framework

This section outlines a health data exchange policy framework, whose main goal is to support the modelling of policies for both data subjects/holders and data controllers/users in health data exchange scenarios, while complying with legal requirements from the EU's GDPR and EHDS. Building on the provisions described in Section 2, data subjects and holders' policies are specified as an `odrl:Policy` and data controllers and users' as an `odrl:Request`, which are subsequently used to model agreed upon conditions for a particular health data exchange. The defined specification is available at https://w3id.org/hedge.

4.1. Policies and requests modelling

Considering the requirements defined in Section 2, in Table 1, we provide a minimal set of terms to define access and usage control rules for data subjects and health data holders. The personal data, processing operation and purpose terms are considered mandatory to match the legal requirements which will be later described for data requests. Moreover, the identification of the data subject is also required for both legal and technical constraints related to policy enforcement mechanisms. Additionally, to provide these entities with further user controls, the modelling of (pseudo)anonymisation actions, e.g., as duties to be fulfilled by the data requesters to share data with other recipients, or the expression of duration and frequency constraints is also supported by this framework. Table 1 also provides a mapping of these terms to DPV and ODRL concepts and relations that can be used to model them. The applicability of each term to model the identified requirements is further refined in the specification documentation.

Table 1
Terms for defining ODRL policies for data subjects and health data holders and respective mapping into DPV and ODRL.

Term	Concept	Relation / Constraint
Data subject	URI	`odrl:assigner`
Personal data	URI / subclass of `dpv:PersonalData`	`odrl:target`
Processing operation	subclass of `odrl:Action` or `dpv:Processing`	`odrl:action`
Purpose	subclass of `dpv:Purpose`	`dpv-odrl:Purpose`
Pseudo/Anonymisation	`dpv-odrl:Pseudonymise`, `dpv-odrl:Anonymise`	`odrl:action`
Recipient	URI / subclass of `dpv:Organisation`	`dpv-odrl:Recipient`
Duration	`xsd:duration`	`dpv-odrl:Duration`
Frequency	`xsd:positiveInteger`	`dpv-odrl:Frequency`

When it comes to the definition of data controllers and health data users' policies, and building on the legal provisions from the EU's GDPR and EHDS described in Section 2, Table 2 defines a minimal set of terms that need to be expressed as access and usage control conditions. To fulfil GDPR provisions, both when it comes to the information requirements specified as a data subject right in Articles 13 and 14 [3] and the records of processing activities (RoPAs) that must be kept data controllers as defined

[16] https://ehr-exchange-format.eu/

in Article 30 [3], personal data, processing operation, purpose, legal bases, and recipient terms are considered mandatory to be modelled into concrete requests for data. Furthermore, data controllers must also be able to categorise the data subjects related to their processing activities and to identify the source of the personal data, when it does not come directly from the data subject, to fulfil these requirements. The identification of the data controller is also required for both legal and technical constraints related to policy enforcement mechanisms. Additionally, to distinguish between primary and secondary use of health data, in particular related to the exchange of personal and non-personal electronic health data regulated by the newly-enforceable EHDS Regulation, health data users must record information about the health data types they wish to use and clearly identify whether this data is being used for primary or secondary usage. Moreover, the modelling of (pseudo)anonymisation duties and the expression of duration and frequency constraints is also supported by this framework as additional user controls. Finally, modelling events or activities that are necessary for the triggering of the usage of certain legal bases, e.g., the existence of a medical emergency that supports the usage of vital interest of the data subject as the legal basis to process its personal data, should also be supported by this health data exchange policy framework. As in Table 1, Table 2 also provides a mapping of these terms to DPV and ODRL concepts and relations that can be used to model them. The applicability of each term to model the identified requirements is further refined in the specification documentation.

Table 2
Terms for defining ODRL requests, respective mapping into DPV and ODRL, and their necessity according to the identified legal requirements. *** is used to identity terms that currently cannot be modelled with ODRL or DPV.

Term	Concept	Relation / Constraint	Law
Data controller	URI	`odrl:assignee`	GDPR
Data subject (type)	URI / subclass of `dpv:HumanSubject`	`odrl:assigner`	GDPR
Personal data	subclass of `dpv:PersonalData`	`odrl:target`	GDPR
Personal electronic health data	subclass of `pd:MedicalHealth`	`odrl:target`	EHDS
Non-personal electronic health data	***	`odrl:target`	EHDS
Processing operation	subclass of `odrl:Action` or `dpv:Processing`	`odrl:action`	GDPR
Purpose	subclass of `dpv:Purpose`	`dpv-odrl:Purpose`	GDPR
Primary/Secondary use	***	***	EHDS
Legal basis	subclass of `dpv:LegalBasis`	`dpv-odrl:LegalBasis`	GDPR
Pseudo/Anonymisation	`dpv-odrl:Pseudonymise`, `dpv-odrl:Anonymise`	`odrl:action`	GDPR
Recipient	URI / subclass of `dpv:Organisation`	`dpv-odrl:Recipient`	GDPR
Data source	subclass of `dpv:DataSource`	`dpv-odrl:DataSource`	GDPR
Duration	`xsd:duration`	`dpv-odrl:Duration`	GDPR
Frequency	`xsd:positiveInteger`	`dpv-odrl:Frequency`	GDPR
Events	***	`odrl:event`	GDPR

Examples of policies modelled with this specification are available at https://w3id.org/hedge. The specification also identifies possible future improvements. Beyond the previously specified terms to be modelled as ODRL policies and requests that represent the health data conditions of all parties involved in a certain exchange, further consideration must be taken into the legal requirements for health data holders coming from EHDS Regulation. In particular, terms to define primary and secondary use of data, as well as to model personal and non-personal electronic health data concepts, are still missing from DPV. Moreover, in applicable cases, data controllers must also be able to specify the existence of joint data controllers and data processors in their data request policies. In terms of additional user controls, data subjects and health data holders must also be able to specify distinct usage conditions for retrospective and prospective data. For technical interoperability, the alignment of this specification with the HealthDCAT-AP and EHRxF protocols is also a must.

4.2. Agreement instantiation

Building on the previous section, the work of Slabbinck et al. [12] was leveraged as the basis for the creation of an agreement instantiation specification and implementation. This specification defines an algorithm to derive a health data sharing agreement, from a concrete request, that fulfills both the the data subject or holder policies, as well as the requester's terms. To align with the previously mentioned work on interoperable policy engines [12], data subjects and holders' policies are modelled as an `odrl:Policy` and data controllers and users' requests as `odrl:Requests`. In conjunction with contextual information modelled as the state of the world (SoTW), these policies are evaluated to establish the activation state of their rules and gather this output in compliance reports. Considering these reports, an `odrl:Agreement` policy can be generated that defines the agreed conditions for data exchange. The several steps of the algorithm to define such an agreement are defined as follows:

- Validate the proper modelling of the `odrl:Policy`, `odrl:Request` and SoTW information.
- Convert compact policies into their atomic equivalents.
- Remove the rules that are not relevant for the request.
- Reference the ODRL request that triggered the agreement instantiation and the policies from the data subject/holder.
  - The policies associated with the data subject/holder data exchange conditions should only be directly accessible by them to mitigate privacy concerns.
  - Data subjects/holders should be able to set these policies as public if that is their wish.
- Instantiate the concrete assigner and assignee of the agreement.
- Include relevant rules with concrete actions, targets and constraints.

This specification is available at https://w3id.org/force/policy-instantiation, including examples of instantiated agreements. The specification and the proof of concept implementation, available at https://w3id.org/force/policy-instantiation/poc, represent a first step towards having automatic agreement generation for Web-based data exchanges.

5. Conclusions and Future Work

The exchange of health-related data brings many interoperability challenges that need to be overcome in order to the envisioned European Health Data Space to emerge as a scalable and legal compliant platform for individuals, healthcare providers, governments and many other entities to share electronic health data in a trustful manner. As such, the analysis of health data exchange requirements provided in this article, and in particular of the identification of mandatory requirements from the GDPR and EHDS Regulation, represents a step forward for both data subjects and holders, as well as data controllers and users, towards the adoption of a common specification to define health data exchange conditions as machine-readable policies. Using the proposed health data exchange policy framework and the developed agreement instantiation algorithm, these entities can model and generate agreements for Web-based health data exchanges, while considering legal requirements.

As future work, a complete mapping and integration of EHDS Regulation concepts to the DPV's EHDS extension is required, as well as a refinement of the alignment betwen DPV, DPV's health sector extension and DPV's EHDS extension. Building on this, the proposed health data exchange policy framework can be extended to cover a wider range of use cases and extended to also cover requirements from national health laws or other jurisdictions. A benchmark of policies to evaluate the compliance of agreement instantiation algorithms with the defined specification should also be developed. Moreover, the proof of concept implementation of the agreement instantiation algorithm should be extended to support all the terms defined in the proposed health data exchange policy framework.

Acknowledgments

This research was funded by SolidLab Vlaanderen (Flemish Government, EWI and RRF project VV023/10) and by the imec.icon project PACSOI (HBC.2023.0752), which was co-financed by imec and VLAIO and brings together the following partners: FAQIR Foundation, FAQIR Institute, MoveUP, Byteflies, AContrario, and Ghent University – IDLab.

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly in order to: Grammar and spelling check. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] 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), Official Journal of the European Union L 152 (2022) 1–44. URL: http://data.europa.eu/eli/reg/2022/868/oj/eng.

[2] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (2025). URL: http://data.europa.eu/eli/reg/2025/327/oj/eng.

[3] 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), Official Journal of the European Union L 119 (2016) 1–88. URL: http://data.europa.eu/eli/reg/2016/679/oj.

[4] Urteil des Gerichtshofs (Große Kammer) vom 4. Oktober 2024. ND gegen DR., 2024. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62023CJ0021.

[5] R. Iannella, S. Villata, ODRL Information Model 2.2 – W3C Recommendation 15 February 2018, 2018. URL: https://www.w3.org/TR/odrl-model/.

[6] H. J. Pandit, B. Esteves, G. P. Krog, P. Ryan, D. Golpayegani, J. Flake, Data Privacy Vocabulary (DPV) – Version 2.0, in: The Semantic Web – ISWC 2024, 2024, pp. 171–193. doi:10.1007/978-3-031-77847-6_10.

[7] B. Esteves, V. Rodríguez-Doncel, Analysis of ontologies and policy languages to represent information flows in GDPR, Semantic Web 15.3 (2024) 709–743. doi:10.3233/SW-223009.

[8] M. Steidl, ODRL Profile Best Practices – Draft Community Group Report 28 July 2023, 2023. URL: https://w3c.github.io/odrl/profile-bp/.

[9] A. Eitel, C. Jung, R. Brandstädter, A. Hosseinzadeh, S. Bader, C. Kühnle, P. Birnstill, G. Brost, Gall, F. Bruckner, N. Weißenberg, B. Korth, Usage Control in the International Data Spaces, Position Paper Version 3.0, 2021. doi:10.5281/ZENODO.5675884.

[10] Slabbinck, Wout and Rojas Melendez, Julian Andres and Esteves, Beatriz and Verborgh, Ruben and Colpaert, Pieter, Enforcing Usage Control Policies in Solid using Rule-Based Web Agents, in: Esteves, Beatriz and Hofmann, Jan and Schmid, Sebastian (Ed.), Proceedings of the Posters and Privacy Session of the Solid Symposium 2024, volume 3947, CEUR, 2024, pp. 109–117. URL: https://ceur-ws.org/Vol-3947/short15.pdf.

[11] H. J. Pandit, B. Esteves, Enhancing Data Use Ontology (DUO) for Health-Data Sharing by Extending it with ODRL and DPV, Semantic Web Journal (2024). doi:10.3233/SW-243583.

[12] Wout Slabbinck, Julián Andrés Rojas, Beatriz Esteves, Pieter Colpaert, Ruben Verborgh, Interoperable Interpretation and Evaluation of ODRL Policies, in: Accepted for publication at ESWC 2025, 2025.