Bridging DPV and ODRL for Legally-Oriented Usage Control in Data Spaces

Beatriz Esteves[1,*], Harshvardhan J. Pandit[2]

[1]IDLab, Department of Electronics and Information Systems, Ghent University – imec, Ghent, Belgium
[2]AI Accountability Lab (AIAL), Trinity College Dublin, Dublin, Ireland

Abstract

Data spaces increasingly require robust usage control mechanisms to ensure that data sharing complies with legal, contractual, and governance requirements while remaining interoperable across heterogeneous systems. The W3C's ODRL Information Model 2.2 provides a domain- and jurisdiction-agnostic framework for expressing permissions, prohibitions, and obligations over assets, whereas the Data Privacy Vocabulary (DPV) offers a rich, controlled vocabulary for representing privacy and data protection concepts. However, the lack of systematic alignment between legal vocabularies and enforceable policy languages hinders the creation of machine-readable, legally-oriented usage policies in data spaces. This paper addresses this gap by presenting a structured mapping between DPV and ODRL that aligns DPV concepts with ODRL constructs using RDF and SKOS properties, and provides it in a machine-readable form to support implementation. The mapping covers core correspondences such as DPV entities, processing, data, personal data, legal bases, purposes, technical and organisational measures, and risks, with ODRL parties, actions, assets, and left operands. By doing so, it enables the expression of legally grounded policies where DPV supplies semantically precise data protection terms, and ODRL provides the deontic and operational policy structure. In addition, we provide a comprehensive guidance document that specifies how DPV terms should be used within ODRL policies, including examples for constraints modelling and operator usage in accordance with ODRL profile best practices. Together, the mapping and guidance establish a reusable foundation for implementing legally-oriented, interoperable usage control policies in data spaces. They support the design of policy artefacts that are simultaneously machine-processable, semantically rich, and aligned with data protection and governance requirements, thereby contributing to more trustworthy and compliant data sharing ecosystems.

Keywords

ODRL, DPV, usage control, regulatory compliance

1. Introduction

Data spaces are emerging as a societal, legal and technical architectural paradigm at the centre of the European Commission's policy agenda for enabling trusted data sharing across organisational and sectoral boundaries [1]. Their objective is to allow participants to exchange and reuse data while maintaining control over how that data is accessed and processed. Achieving this balance between data sharing and data sovereignty requires usage control mechanisms that can express and enforce the conditions under which data may be used [2]. These conditions can be derived not only from technical but also from regulatory and contractual requirements. In this context, the Data Spaces Support Centre (DSSC) blueprint [3] highlights the importance of integrating legal and technical capabilities, specifically addressing *regulatory compliance and contractual frameworks* alongside *access and usage policies enforcement*. These building blocks together aim to ensure that the rights and obligations governing data sharing can be defined, negotiated, and enforced in an interoperable manner. Agreements between data providers and data consumers must therefore be represented in a way that supports automated interpretation, negotiation, and enforcement during the lifecycle of data transactions.

Fourth International Workshop on Semantics in Dataspaces (SDS 2026)
*Corresponding author.
beatriz.esteves@ugent.be (B. Esteves)
https://w3id.org/people/besteves (B. Esteves)
0000-0003-0259-7560 (B. Esteves)

A central challenge in this context is the representation of key agreements while preserving their legal meaning. Data sharing policies must capture permissions, prohibitions, and obligations governing data access and usage, while also reflecting constraints derived from sectoral rules, contract law and intellectual property rights, or data-related legislation. At the same time, these policies must be semantically interoperable to support the federated nature of data spaces, ensuring "that data can be accurately and consistently interpreted and used by different people and systems" [4]. Two complementary semantic specifications provide a promising foundation for addressing this challenge. The W3C Open Digital Rights Language (ODRL) standard [5] provides a general-purpose policy model for expressing rules governing the use of digital assets, including permissions, prohibitions, and obligations which can be further restricted with contextual constraints. Furthermore, ODRL is recommended in the DSSC blueprint as a standard representation for machine-readable access and usage policies within data spaces. While ODRL provides the structural framework for policy representation, it intentionally remains domain- and jurisdiction-agnostic and does not include explicit concepts related to legal compliance. The Data Privacy Vocabulary (DPV) [6], built as a 'community standard', complements ODRL by providing a rich semantic vocabulary containing taxonomies to describe legal and sectorial requirements related to data and AI regulation. Combining these two standards makes it possible to bridge the gap between legally grounded governance requirements and machine-readable policy enforcement mechanisms. In particular, the use of DPV concepts allows ODRL policies and documentation to be aligned with the terminologies of relevant laws and simplifies the process of assessing and enforcing compliance. This allows data usage policies to express legally meaningful constraints while remaining compatible with existing policy evaluation and enforcement engines. This approach aligns closely with the DSSC blueprint's vision of interoperable data spaces where legal agreements and technical enforcement mechanisms are coherently connected.

In this paper, we argue that ODRL and DPV together provide a suitable semantic foundation for legally-aligned policy expression in data spaces. We propose treating ODRL as the core policy framework for representing permissions, prohibitions, and obligations governing data usage, in line with the DSSC and given the mature status of ODRL as a W3C standard. We then propose using DPV as the semantic layer for modelling legal and governance concepts referenced within those policies, based on its wide coverage of EU's legal framework, extensibility for jurisdictional and sectorial applicability, as well as a lack of rigid semantics that allows wider reuse. To support this integration, we present a structured 'mapping' between DPV and ODRL that aligns DPV concepts with ODRL constructs, using RDF and SKOS properties, which allows the integration and reuse of both standards in a cohesive and semantically meaningful manner. We also provide the mapping in a machine-readable form to facilitate implementation, in accordance with ODRL profiling best practices [7]. In addition, we provide a guidance document for the use of DPV terms within ODRL policies, including examples of policies that use the developed mapping. Together, these contributions enable data space participants to express governance rules that are both legally meaningful and technically enforceable, thereby supporting scalable and interoperable policy management through automation across data space infrastructures.

In this context, our work addresses the following challenges documented by the W3C Dataspaces CG[1]: (i) *Blueprints for actors, roles and responsibilities*—our work provides the means to declare and use these concepts, with legal relevance, through existing standards; (ii) *Interoperable Policy Engines*—our work facilitates improvements to policy engines by providing a legal semantics layer, and also enables legal interoperability across data spaces through shared vocabularies; and (iii) *Schema Alignment and Semantic Data Transformation*—same as (ii), our work enables creation of schemas and vocabularies within a data space or instance, which can be reused elsewhere based on extending common interpretations through ODRL as a standard for policies and DPV as a standard for expression of legal concepts.

The remainder of this article is structured as follows: Section 2 provides an overview of applicable regulatory requirements and existing work for data protection-aligned policy modelling. Section 3 describes the developed mapping and its implementation as an ODRL profile. In Section 4, we provide examples of the application of the profile and discuss the implementation of templates to validate profile-

[1] https://w3c-cg.github.io/dataspaces/

based constraints. Finally, Section 5 concludes the paper and provides pointers to future research.

2. Background & Related Work

In this section, we provide an overview of the legal framework that must be tackled in data spaces, as well as a description of ODRL and DPV and how they have been used to tackle these regulatory requirements.

Regulatory Compliance in Data Spaces Several branches of EU law must be considered when implementing data spaces, in particular when looking at the enforcement of access and usage control. One particular area of focus is data-related legislation, in particular the General Data Protection Regulation (GDPR) [8] regarding the processing of personal data, the Data Governance Act (DGA) [9] regarding a framework to facilitate data sharing, and the Data Act [10] which establishes harmonised rules for data exchange.[2] These regulatory instruments collectively shape the legal environment in EU for data sharing and governance in data spaces. The GDPR establishes the foundational framework for the protection of personal data, defining principles such as lawfulness and purpose limitation, and providing data subject rights and obligations for data controllers, which must be respected whenever personal data is processed, including in cross-organisational data sharing scenarios typical of data spaces. The DGA aims to facilitate trustworthy data sharing by creating governance mechanisms that enable the reuse of protected public sector data, regulate data intermediation services, and promote altruistic data sharing. The Data Act complements this framework by addressing access to and sharing of data generated by connected products and services, enabling broader data portability and sharing across sectors to stimulate innovation and competition. Together, these regulations form a layered legal foundation for European data spaces: GDPR ensures protection of personal data, while the DGA and the Data Act promote trusted mechanisms and rights for data sharing and reuse, enabling interoperable and legally compliant data ecosystems. Additionally, there is sectorial legislation that should also be considered for the implementation of data spaces. For instance, the European Health Data Space (EHDS) [11] regulation establishes a common framework for the access, exchange, and reuse of electronic health data, forming the first sector-specific data space legislation under the EU data strategy. It aims to empower individuals with greater control and cross-border access to their electronic health records, while enabling the secondary use of health data for research, innovation, and policy-making purposes. Furthermore, besides data-related and sector-based legislation, other fields of law must be considered, such as intellectual property rights or competition law [3].

Access and Usage Policies Enforcement Besides being the *de facto* standard in data spaces for the expression of usage control policies, ODRL was selected since it is a W3C standard specifically designed to represent machine-readable rules governing the use of digital assets. At the core of the ODRL model [5] is the `Policy` concept, which groups one or more `Rules` that define permissions, prohibitions, or obligations. Each rule specifies an `Action` performed by a `Party` over an `Asset`, and can be further refined using `Constraints` that restrict when or how the action may occur, expressed through left operands, operators, and right operands. Rules may also include `Duties`, representing additional actions that must be fulfilled when a rule is exercised. This model allows policies such as offers, agreements, or requests to be expressed in a machine-readable and interoperable manner. However, since ODRL is both jurisdiction- and domain-agnostic, DPV [6] can be used alongside it to provide a controlled vocabulary of legal concepts — such as legal bases, legal roles, and purposes for processing data related to privacy and data protection — allowing policies to incorporate legally relevant semantics and regulatory concepts (e.g., from the GDPR). In this context, DPV is the *de facto* standard for the representation of legal requirements related to data protection, as it is an open source solution that provides the most complete set of taxonomies for this domain [12]. DPV's core specification includes

[2]The DGA and the Data Act have been proposed to be merged into a single regulation under the Digital Omnibus series of proposals. For this work, we consider them as distinct laws based on their current status.

taxonomies describing personal data categories, processing operations, and purposes for data use, as well as entities and roles such as data controllers, processors, and data subjects. Additional taxonomies describe legal concepts (e.g., laws and legal bases), technical and organisational measures, risks and risk mitigation measures, locations and jurisdictions, technologies and AI systems, and sector-specific contexts. Together, these vocabularies enable the interoperable representation of information about data processing activities and compliance requirements, which can then be incorporated into policy languages such as ODRL.

Previous ODRL profiles have looked at the combined usage of ODRL and DPV [13, 14, 15], however they did not provide a full overview and mapping of all existing DPV taxonomies into ODRL constructs. Furthermore, other works have used both solutions [16, 17, 18, 19, 20, 21], but failed to provide an explicit mapping of these technologies. In this context, this article fills this gap by providing a systematic consolidation and formalisation of a DPV-ODRL mapping.

3. Mapping from DPV to ODRL

The DPV-ODRL mapping described in this paper is being developed as part of the W3C DPVCG's activities[3], with the support of the W3C ODRL CG[4], and it is available at https://w3id.org/dpv/mappings/odrl, with `dpv-odrl` as the suggested prefix. Furthermore, this mapping is represented in an RDF format, as an ODRL profile, following the best practices documented in the ODRL V2.2 Profile Best Practices report [7]. This ensures compatibility with existing ODRL implementations and policy evaluation mechanisms.

3.1. Methodology

The mapping between DPV and ODRL is implemented using semantic alignment mechanisms, primarily through relations from the SKOS vocabulary[5], RDF and RDFS[6], and OWL[7]. The following alignment strategies were considered, with Table 1 providing an overview of these strategies, the semantic property used for the mapping, and examples.

- **Instantiation**: A `dpv-odrl` class is instantiated as an ODRL class
- **Specialisation**: One concept is more specific than the other
- **Hierarchy**: A strict ontology subclass relationship
- **Equivalence**: Concepts represent the same meaning
- **Approximation**: Concepts are very similar but not strictly equivalent
- **Association**: Concepts are related but not hierarchically
- **Disjointness**: Mutually exclusive concepts

Table 1
Mapping types of DPV and ODRL Concepts

Alignment	Mapping Relation	Example
Instantiation	`rdf:type`	`dpv-odrl:Entity rdf:type odrl:Party .`
Specialisation	`skos:broader`	`dpv-odrl:Recipient skos:broader odrl:recipient .`
Hierarchy	`rdfs:subClassOf`	`dpv-odrl:NDA rdfs:subClassOf odrl:Policy .`
Equivalence	`skos:exactMatch`	`dpv-odrl:Agent skos:exactMatch dpv:Agent .`
Approximation	`skos:closeMatch`	`dpv-odrl:Use skos:closeMatch odrl:use .`
Association	`skos:related`	`dpv-odrl:Duration skos:related odrl:elapsedTime .`
Disjointness	`owl:disjointWith`	`dpv-odrl:NDA owl:disjointWith (odrl:Offer, ...) .`

[3] DPVCG's mission is to develop vocabularies that support the implementation of regulations, standards, and approaches relevant to privacy and data protection, and how these are addressed in technologies, including AI.
[4] https://www.w3.org/groups/cg/odrl/
[5] http://www.w3.org/2004/02/skos/core#
[6] http://www.w3.org/1999/02/22-rdf-syntax-ns# and http://www.w3.org/2000/01/rdf-schema#
[7] http://www.w3.org/2002/07/owl#

3.2. DPV-ODRL Profile

Through the mapping described in the previous section, DPV concepts can function within ODRL policies as: *i)* parties, *ii)* actions, *iii)* assets, *iv)* left operands, *v)* rules, and *vi)* policy types. Figure 1 provides an overview of this mapping where all DPV taxonomies are mapped into one or more of the previously mentioned ODRL constructs.

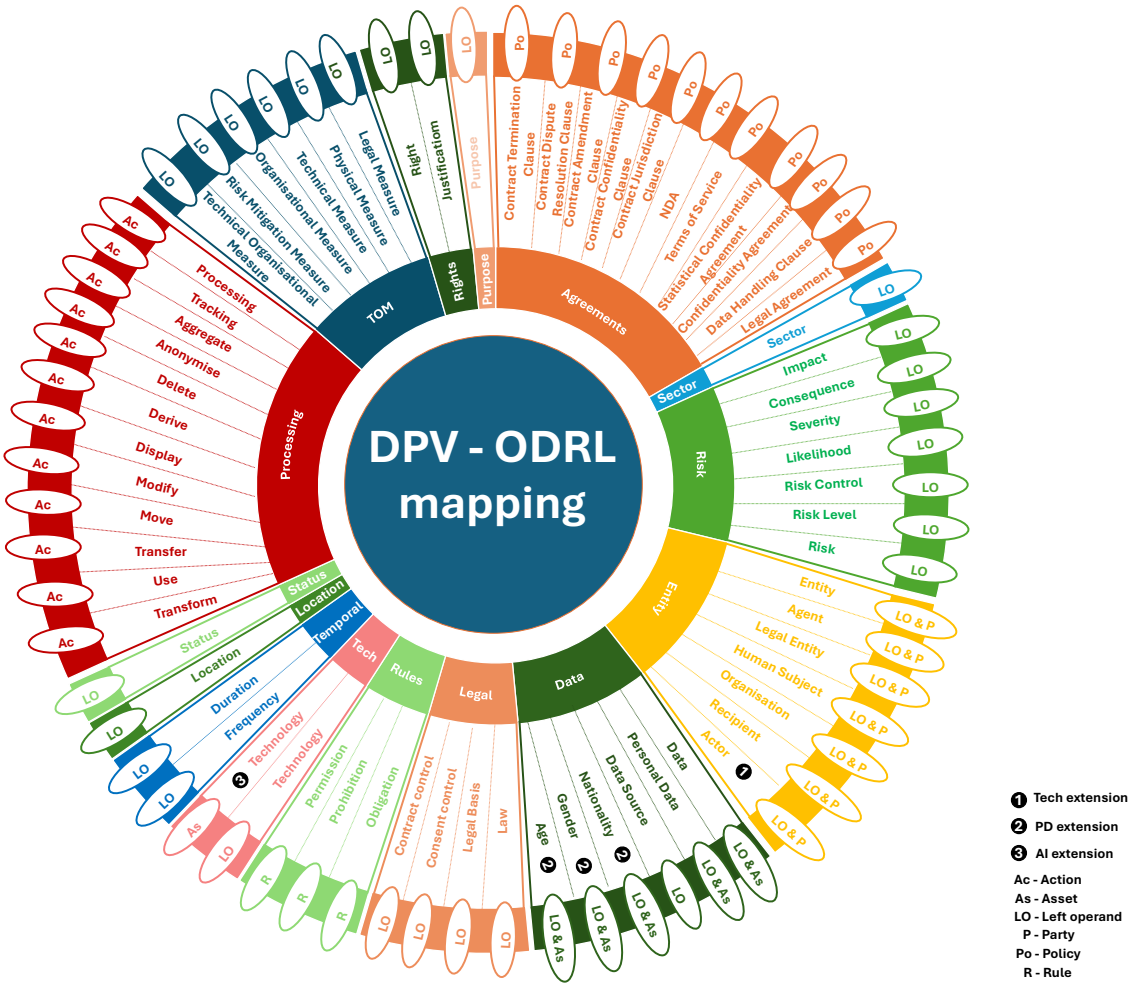

Figure 1: Overview of DPV-ODRL mapping: the inner layer groups the terms by taxonomy, the middle layer contains the mapped DPV terms, and the outer layer contains the mapping to ODRL constructs. The following labels were used to represent ODRL constructs: 'Ac' represents Action concepts, 'As' Asset concepts, 'LO' Left Operands, 'P' Party concepts, 'Po' Policy types, and 'R' Rules. Terms from DPV's extensions, e.g., Tech, PD, and AI, were also included in the mapping.

Entities and Legal Roles DPV defines entities and legal roles representing stakeholders involved in data processing activities, such as individuals, organisations, institutions, or authorities. As such, they can be mapped as `odrl:Party` instances and used as `odrl:assigner` or `odrl:assignee` of ODRL policies. Furthermore, due to the hierarchical structure of DPV, certain entity concepts can be used as left operands to filter ODRL party collections. For example, when a party collection contains multiple human subjects of different types, the use of `dpv-odrl:HumanSubject` as the left operand and `dpv:Patient` as the right operand enables the specification of an ODRL policy that applies exclusively to subjects of this particular type. Listing 1 provides an example of a DPV-ODRL mapping for entity concepts. In this case, `dpv-odrl:Recipient`, the equivalent to `dpv:Recipient`, is instantiated as a `odrl:Party` and as a `odrl:LeftOperand`, and has a narrower scope than `odrl:recipient`, i.e., the right operand of

`odrl:recipient` is not restricted to a particular vocabulary, while `dpv-odrl:Recipient` should require a `dpv:Entity` as the right operand.

```
dpv-odrl:Recipient a odrl:Party, odrl:LeftOperand, skos:Concept ;
      skos:exactMatch dpv:Recipient ;
      skos:broader odrl:recipient .
```

Listing 1: DPV-ODRL mapping for the Recipient concept.

Processing Operations DPV processing concepts describe operations that may be performed on data, such as aggregation, deletion, transformation, or transfer. These operations naturally correspond to ODRL actions and can therefore be used to define permitted, prohibited or mandatory activities within policies. Furthermore, a few DPV processing terms closely correspond to existing ODRL actions, allowing them to be related using the `skos:closeMatch` — Table 2 contains an overview of these terms. Listing 2 provides an example of a DPV-ODRL mapping for a processing operation. In this case, `dpv-odrl:Use`, the equivalent to `dpv:Use`, is instantiated as an `odrl:Action` and has a similar ODRL concept, i.e., `odrl:use`.

```
dpv-odrl:Use a odrl:Action, skos:Concept ;
      skos:exactMatch dpv:Use ;
      skos:closeMatch odrl:use .
```

Listing 2: DPV-ODRL mapping for the Use concept.

Table 2
Mapping of DPV processing operations to ODRL actions.

ODRL Concept	DPV Concept	Mapping Type
odrl:acceptTracking	dpv:Tracking	skos:closeMatch
odrl:aggregate	dpv:Aggregate	skos:closeMatch
odrl:anonymize	dpv:Anonymise	skos:closeMatch
odrl:delete	dpv:Delete	skos:closeMatch
odrl:derive	dpv:Derive	skos:closeMatch
odrl:display	dpv:Display	skos:closeMatch
odrl:modify	dpv:Modify	skos:closeMatch
odrl:move	dpv:Move	skos:closeMatch
odrl:transfer	dpv:Transfer	skos:closeMatch
odrl:transform	dpv:Transform	skos:closeMatch
odrl:use	dpv:Use	skos:closeMatch

Data and Technologies In ODRL, assets represent the resources targeted by policies. On the other hand, DPV provides a comprehensive taxonomy for describing data, including categories of personal and non-personal data, as well as a Personal Data Categories extension[8], which provides additional concepts to represent different types of personal data, e.g., social, demographic, financial, or health-related data categories. These concepts can therefore be mapped to ODRL assets, but can also be used as left operands to refine asset or party collections to specific data types or demographic groups, e.g., to allow only the usage of health-related data from a personal data catalog, or to restrict the usage of a certain asset to parties which are over 18. Furthermore, DPV provides technology-related concepts that can be used to denote the use of any technological resources, including AI systems. These concepts can also be used as assets within ODRL policies to specify conditions governing the use of such resources. Furthermore, DPV's Technology[9] and AI Technology[10] extensions introduce additional technological concepts that can be employed as assets or as further constraints in ODRL policies. For example, a policy may specify that a given asset may only be used for training an AI model.

[8] https://w3id.org/dpv/pd
[9] https://w3id.org/dpv/tech
[10] https://w3id.org/dpv/ai

Contextual and Governance-related Constraints The majority of DPV taxonomies yet to be discussed in this section are mapped as ODRL left operands to further constrain ODRL policies. The following list provides an overview of these taxonomies and their utility to restrict ODRL policies:

- **Purpose:** Purpose limitation is a central principle in many data protection frameworks, particularly the GDPR. DPV includes an extensive taxonomy of purposes, which can be integrated into ODRL policies to constrain data or technology usage to a particular purpose or set of purposes. This alignment enables the expression of policies such as allowing the use of a dataset exclusively for research or restricting its use to statistical analysis.
- **Technical and Organisational Measures:** Data protection regulations frequently require the implementation of safeguards such as encryption, authentication mechanisms, or organisational controls. DPV models such safeguards as technical and organisational measures (TOMs), which can be used as constraints within ODRL policies for, e.g., permitting access to a dataset only when multi-factor authentication is implemented.
- **Legal and Jurisdictional Constraints:** DPV location concepts can restrict asset usage to specific locations or jurisdictions, supported by the Location[11] extension that contains concepts to represent countries and regions based on ISO 3166. Additionally, DPV provides concepts for representing applicable laws and legal bases for processing activities, with the Legal[12] extensions supporting the modelling of laws and authorities across jurisdictions.
- **Time-based Context:** Temporal aspects of policies, including duration and frequency of usage, can also be represented through DPV concepts. These mappings allow policies to define how long data may be used or how often certain operations may occur. Furthermore, these DPV concepts can be related to a few ODRL left operands in a non-hierarchical way, e.g., `dpv:Duration` is related to `odrl:elapsedTime`. Listing 3 provides the DPV-ODRL mapping for duration, where `dpv-odrl:Duration`, the equivalent to `dpv:Duration`, is instantiated as an `odrl:LeftOperand` and has related ODRL concepts, i.e., `odrl:elapsedTime` and `odrl:count`.
- **Rights and Risks:** DPV includes concepts representing risks, rights, and justifications associated with processing activities. They can be used to justify the exercising of a certain right, e.g., a data subject wants to exercise their right to erasure given that the processing of their personal data is no longer required, or to restrict the use of assets when risk levels exceed certain thresholds.
- **Sector and Status:** DPV sector concepts can be used to permit or restrict asset usage based on the application domain. The AI Act[13] extension provides sector-related concepts, such as education and employment, to represent these domains. Additionally, DPV status concepts can indicate the state of processes or activities, enabling policies to constrain asset usage based on conditions such as the status of given consent.

A detailed list of these mappings is available at https://w3id.org/dpv/mappings/odrl and can be observed in Figure 1.

```
dpv-odrl:Duration a odrl:LeftOperand, skos:Concept ;
   skos:exactMatch dpv:Duration ;
   skos:related odrl:elapsedTime, odrl:count .
```

Listing 3: DPV-ODRL mapping for the Duration concept.

Rules and Agreements DPV rule concepts align with the core rule types in ODRL. Permissions, prohibitions, and obligations can therefore be represented consistently across both vocabularies. Listing 4 provides an example of a DPV-ODRL mapping for a rule. In this case, `dpv-odrl:Obligation` is equivalent to `dpv:Obligation`, and closely matches `odrl:Duty`. Additionally, DPV contractual clauses and legal agreements can be represented as subclasses of ODRL policies. Examples include confidentiality agreements, non-disclosure agreements (NDA), and data handling clauses. Listing 5

[11] https://w3id.org/dpv/loc
[12] https://w3id.org/dpv/legal
[13] https://w3id.org/dpv/legal/eu/aiact

provides the DPV-ODRL mapping for the NDA concept. In this case, dpv-odrl:NDA, equivalent to dpv:NDA, is a subclass of odrl:Policy, and mutually exclusive from all ODRL policies and also from those defined in the DPV-ODRL profile. The latter condition is required by the ODRL Profile Mechanism [7] for the definition of additional policy subclasses.

```
dpv-odrl:Obligation skos:exactMatch dpv:Obligation ;
      skos:closeMatch odrl:Duty .
```

Listing 4: DPV-ODRL mapping for the Obligation concept.

```
dpv-odrl:NDA a rdfs:Class, skos:Concept ;
   skos:exactMatch dpv:NDA ;
   rdfs:subClassOf odrl:Policy ;
   owl:disjointWith odrl:Agreement, odrl:Offer, odrl:Privacy, odrl:Request, odrl:Ticket, odrl:Assertion,
      dpv-odrl:ContractConfidentialityClause, dpv-odrl:ContractDisputeResolutionClause,
      dpv-odrl:ContractJurisdictionClause, dpv-odrl:ContractTerminationClause,
      dpv-odrl:TermsOfService, dpv-odrl:DataHandlingClause, dpv-odrl:LegalAgreement,
      dpv-odrl:ConfidentialityAgreement, dpv-odrl:StatisticalConfidentialityAgreement .
```

Listing 5: DPV-ODRL mapping for the NDA concept.

3.3. Usage of ODRL Operators

Besides specifying the mapping between DPV and ODRL, when defining the DPV-ODRL profile, the usage of ODRL operators for each left operand should also be included in the left operand specification. For this, the skos:note property can be used to associate a certain left operand with a note on the operators that must be used with said left operand. Listing 6 provides an example of such a specification. In this case, the dpv-odrl:LegalBasis left operand can only be used with the odrl:isA, odrl:eq, and odrl:neq operators. Section 4.1 will provide details on how to implement this specification.

```
dpv-odrl:LegalBasis a odrl:LeftOperand, skos:Concept ;
      skos:exactMatch dpv:LegalBasis ;
      skos:example "A legal basis can be consent, legitimate interest, contract performance or
          jurisdiction-specific legal basis such as the ones provided in GDPR Article 6."@en ;
      skos:note """Only the odrl:isA, odrl:eq and odrl:neq MUST be used. Example:
        ex:legalBasisConstraint a odrl:Constraint ;
            odrl:leftOperand dpv-odrl:LegalBasis ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:Consent .
        indicates that the legal basis for the processing should be an instance of dpv:Consent."""@en .
```

Listing 6: Note specification for the usage of operators with the Legal Basis left operand.

4. Usage Guidelines

In addition to the DPV-ODRL mapping described in the previous section, we provide a guidance document at https://w3id.org/dpv/guides/dpv-odrl with examples of ODRL policies that use the developed mapping and conform with the ODRL standard. In this section, we reproduce a few of these examples to showcase the usefulness of this work to tackle legal compliance enforcement in data spaces.

Listing 7 provides an example of a DPV-ODRL policy, where a data holder allows the usage of a certain asset, i.e., ex:research-dataset, only for the purpose of dpv:ResearchAndDevelopment and only for data users which are classified as dpv:AcademicScientificOrganisation.

```
ex:policy-partycollection a odrl:Agreement ;
   odrl:uid ex:policy-partycollection ;
   odrl:profile dpv-odrl:;
   odrl:permission [
      odrl:assigner ex:data-holder ;
      odrl:assignee [
         a odrl:PartyCollection ;
         odrl:source ex:entities ;
         odrl:refinement [
            odrl:leftOperand dpv-odrl:Entity ;
            odrl:operator odrl:isA ;
```

```
        odrl:rightOperand dpv:AcademicScientificOrganisation ] ] ;
    odrl:target ex:research-dataset ;
    odrl:action dpv-odrl:Use ;
    odrl:constraint [
      odrl:leftOperand dpv-odrl:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:ResearchAndDevelopment ] ] .
```

Listing 7: Purpose-restricted agreement with a party collection refinement.

Listing 8 provides an example of a DPV-ODRL policy, where a data subject allows the usage of elements of a certain asset collection, i.e., `ex:data-catalog`, that are instances of health record data, i.e., `pd:HealthRecord`.

```
ex:policy-assetcollection a odrl:Policy ;
  odrl:uid ex:policy-assetcollection ;
  odrl:profile dpv-odrl:;
  odrl:permission [
    odrl:target [
      a odrl:AssetCollection ;
      odrl:source ex:data-catalog ;
      odrl:refinement [
        odrl:leftOperand dpv-odrl:PersonalData ;
        odrl:operator odrl:isA ;
        odrl:rightOperand pd:HealthRecord ] ] ;
    odrl:assigner ex:data-subject ;
    odrl:action dpv-odrl:Use ] .
```

Listing 8: Policy with a DPV-ODRL-based asset collection refinement on personal data type.

Listing 9 contains an example specifying an agreement between a data subject and a data controller, where the data controller has the obligation to delete the data subject data, given that the latter exercised their GDPR right to erasure, i.e., `eu-gdpr:A17`, supported by a non-necessity justification, i.e., `eu-gdpr:JustificationA17NonNecessity`, which can be used in such a request when the involved personal data is no longer necessary in relation to the purposes for which it was initially collected or otherwise processed.

```
ex:policy-right-erasure-justification a odrl:Agreement ;
  odrl:uid ex:policy-right-erasure-justification ;
  odrl:profile dpv-odrl:;
  odrl:obligation [
    odrl:assigner ex:subject ;
    odrl:assignee ex:controller ;
    odrl:target ex:subject-data ;
    odrl:action dpv-odrl:Delete ;
    odrl:constraint [
      odrl:leftOperand dpv-odrl:Right ;
      odrl:operator odrl:eq ;
      odrl:rightOperand eu-gdpr:A17 ], [
      odrl:leftOperand dpv-odrl:Justification ;
      odrl:operator odrl:eq ;
      odrl:rightOperand eu-gdpr:JustificationA17NonNecessity ] ] .
```

Listing 9: Obligation-based policy for the exercising of a right and related justification.

Finally, we provide a policy catalog at https://github.com/besteves4/SDS2026-DPV-ODRL-mapping that contains an example policy for each mapped concept. In the long term, these examples will be integrated and maintained by the W3C's DPVCG in its 'Examples' report available at https://w3id.org/dpv/examples.

4.1. SHACL Shapes for Constraint Validation

Beyond specifying examples, the guidance document recommends the usage of SHACL[14] shapes to validate DPV-ODRL-based policies. While such shapes already exist to validate core ODRL constructs[15], the same exercise is needed for the policies described in this work, in particular to validate the usage of

[14] https://www.w3.org/TR/shacl/

[15] See https://github.com/oeg-upm/licensius/blob/master/odrlapi/src/main/resources/shapes.ttl

constraints, as previously discussed in Section 3.3. In this context, the ODRL vocabulary has a set of 12 defined constraint operators to express the relation between left and right operands. Given that multiple operators can be used to restrict this relation, the left operand and operator usage should be refined for each left operand, e.g., the `odrl:isA` operator should not be used with the `dpv-odrl:Frequency` left operand. Listing 10 provides a template for a SPARQL-based SHACL constraint that can be used to detect the usage of an invalid operator for a given left operand.

```
ex:ConstraintShapeTemplate a sh:NodeShape ;
   sh:targetClass odrl:Constraint ;
   sh:sparql [
      a sh:SPARQLConstraint ;
      sh:message "Invalid operator for given left operand." ;
      sh:prefixes odrl:;
      sh:select """
            SELECT $this WHERE {
                $this odrl:leftOperand <LEFT_OPERAND> .
                $this odrl:operator ?op .
                FILTER(?op NOT IN (<ALLOWED_OPERATORS>))
            }
        """ ;
   ] .
```

Listing 10: Template shape to detect the usage of an invalid operator for a given left operand.

4.2. Limitations

While this work provides a structured and comprehensive mapping between DPV and ODRL, several limitations must be acknowledged.

First, the contribution primarily focuses on conceptual alignment and specification artefacts, including example policies and a SHACL-based validation template. However, it does not yet include a systematic implementation and evaluation within realistic data space environments. As such, the proposed profile has not been empirically assessed in operational settings involving interoperable policy engines or real-world data sharing scenarios. Building on the latter, the policy examples provided throughout the article serve an illustrative purpose but are not validated within concrete data space scenarios. While they demonstrate how DPV concepts can be embedded within ODRL policies, they do not account for challenges that may arise in real deployments, such as policy conflicts, negotiation workflows, or integration with existing enforcement mechanisms. As a result, the applicability of these examples to complex, multi-party data sharing environments remains to be validated. Finally, it is important to consider that DPV is an actively evolving vocabulary that is continuously extended to cover new data-related regulations, sector-specific requirements, and emerging technologies. While this extensibility is a strength, it also introduces a moving target for the proposed mapping. Hence, changes or additions to DPV – such as new legal concepts, jurisdictions, or domain-specific extensions – may require ongoing updates to the DPV-ODRL alignment to maintain completeness and consistency.

5. Conclusions and Future Work

This article presents a structured integration of the Data Privacy Vocabulary with the Open Digital Rights Language to enable the representation of legally grounded, machine-readable usage control policies in data spaces. By defining a comprehensive mapping between DPV taxonomies and ODRL constructs, and formalising it as an interoperable ODRL profile, the work bridges the gap between legal semantics and enforceable policy representations. The resulting approach allows policies to capture permissions, prohibitions, and obligations enriched with domain-specific concepts such as purposes, legal bases, risks, and technical measures, thereby supporting the expression of compliance requirements derived from data protection legislation. Overall, this contribution provides a reusable and extensible foundation for aligning legal, organisational, and technical perspectives in the design of trustworthy and interoperable data sharing ecosystems.

Future work will focus on the implementation and evaluation of this profile within interoperable ODRL policy engines [22] to support automated policy interpretation, validation, and enforcement across heterogeneous data space infrastructures. This includes extending existing ODRL engines to natively support DPV-based semantics and integrating SHACL-based validation mechanisms for constraint checking. Additionally, further research is needed to assess scalability and interoperability across different data space implementations, as well as to explore integration with data negotiation protocols and trust frameworks. These efforts will contribute to operationalising the proposed profile and advancing practical, standards-based solutions for legally compliant usage control in real-world data spaces.

Funding Acknowledgments

This research was funded 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. This publication is also partially based upon work from COST Action CA23147 GOBLIN – Global Network on Large-Scale, Cross-domain and Multilingual Open Knowledge Graphs, supported by COST (European Cooperation in Science and Technology, https://www.cost.eu). Harshvardhan J. Pandit is part of the AI Accountability Lab, which has been funded under the AI Collaborative, an Initiative of the Omidyar Group; the Bestseller Foundation; the AI Security Institute (AISI), and the John D. and Catherine T. MacArthur Foundation; and is part of the ADAPT Centre for Digital Media Technology that is funded by Research Ireland through the Research Centres Programme and is co-funded under the European Regional Development Fund (ERDF) through Grant 13/RC/2106_P2, and has received funding through the RECITALS project funded by the European Commission's Horizon research and innovation programme under grant agreement No.101168490.

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] E. Farrell, M. Minghini, A. Kotsev, J. Soler-Garrido, B. Tapsall, M. Micheli, M. Posada, S. Signorelli, A. Tartaro, J. Bernal, M. Vespe, M. Di Leo, B. Carballa-Smichowski, R. Smith, S. Schade, K. Pogorzelska, L. Gabrielli, D. De Marchi, European data spaces: Scientific insights into data sharing and utilisation at scale, Technical Report, Publications Office of the European Union, 2023. URL: https://data.europa.eu/doi/10.2760/400188.

[2] 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.

[3] Data Spaces Support Centre, Summary of the DSSC Blueprint Version 3.0, 2026. URL: https://assets.dssc.eu/rsc/papers/Blueprint%20V3%20Summary.pdf.

[4] S. Steinbuss, A. H. Almeida, W. van den Berg, S. G. Berwanger, S. B. Arechabala, I. Fernandez, G. G. Inchaurza, P. Klinker, V. Lähteenoja, A. Müller, M. Stornebrink, A. Turkmayali, P. Kivimäki, P. Calvez, P. Koen, Semantic Interoperability in Data Spaces, Position Paper Version 1.1, 2025. doi:10.5281/zenodo.17630664.

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

[8] 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), 2016. URL: http://data.europa.eu/eli/reg/2016/679/oj.

[9] 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), 2022. URL: http://data.europa.eu/eli/reg/2022/868/oj/eng.

[10] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), 2023. URL: http://data.europa.eu/eli/reg/2023/2854/oj.

[11] 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.

[12] 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.

[13] B. Esteves, H. J. Pandit, V. Rodríguez-Doncel, ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid, in: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), 2021, pp. 298–306. doi:10.1109/EuroSPW54576.2021.00038.

[14] 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.

[15] D. Golpayegani, B. Esteves, H. J. Pandit, D. Lewis, AIUP: an ODRL Profile for Expressing AI Use Policies to Support the EU AI Act, in: 20th International Conference on Semantic Systems, 2024. URL: https://ceur-ws.org/Vol-3759/paper17.pdf.

[16] B. Esteves, R. Dedecker, W. Slabbinck, F. Pattyn, R. Verborgh, Semantic Framework for Legally-aligned Health Data Exchanges, in: OPAL'25: ODRL And Beyond: Practical Applications And Challenges For Policy-Based Access And Usage Control, colocated with the Extended Semantic Web Conference 2025, 2025. URL: https://ceur-ws.org/Vol-3977/OPAL2025-9.pdf.

[17] B. Esteves, H. Asgarinia, A. C. Penedo, B. Mutiro, D. Lewis, Fostering trust with transparency in the data economy era: an integrated ethical, legal, and knowledge engineering approach, in: Proceedings of the 1st International Workshop on Data Economy, Association for Computing Machinery, 2022, pp. 57–63. doi:10.1145/3565011.3569061.

[18] I. Plaza-Ortiz, A. Munoz-Arcentales, J. Salvachua, C. Aparicio, G. Huecas, E. Barra, Authentication and authorization in Data Spaces: A relationship-based access control approach for policy specification based on ODRL, in: ODRL and Beyond: Practical Applications and Challenges for Policy-based Access and Usage Control (OPAL 2025), co-located with the Extended Semantic Web Conference 2025 (ESWC 2025), 2025. URL: https://ceur-ws.org/Vol-3977/OPAL2025-3.pdf.

[19] E. I. Papagiannakopoulou, N. L. Dellas, G. V. Lioudakis, M. N. Koukovini, A. Mousas, Semantic conflict resolution for access and usage control, in: NeXt-generation Data Governance workshop 2025 (NXDG 2025), co-located with SEMANTiCS'25: International Conference on Semantic Systems, 2025. URL: https://ceur-ws.org/Vol-4064/NXDG25-paper4.pdf.

[20] S. Yumusak, S. Gheisari, J. O. Salas, S. A. Moqurrab, L.-D. Ibáñez, G. Konstantinidis, Data Sharing Negotiation and Contracting, in: Posters, Demos, and Industry Tracks at ISWC 2024, 2024. URL: https://ceur-ws.org/Vol-3828/paper39.pdf.

[21] M. De Vos, S. Kirrane, J. Padget, K. Satoh, ODRL Policy Modelling and Compliance Checking, in: P. Fodor, M. Montali, D. Calvanese, D. Roman (Eds.), Rules and Reasoning, Springer International Publishing, 2019, pp. 36–51. doi:10.1007/978-3-030-31095-0_3.

[22] W. Slabbinck, J. Rojas Meléndez, B. Esteves, P. Colpaert, R. Verborgh, Interoperable Interpretation

and Evaluation of ODRL Policies, in: E. Curry, M. Acosta, M. Poveda-Villalón, M. van Erp, A. Ojo, K. Hose, C. Shimizu, P. Lisena (Eds.), The Semantic Web, Springer Nature Switzerland, 2025, pp. 192–209. doi:10.1007/978-3-031-94578-6_11.