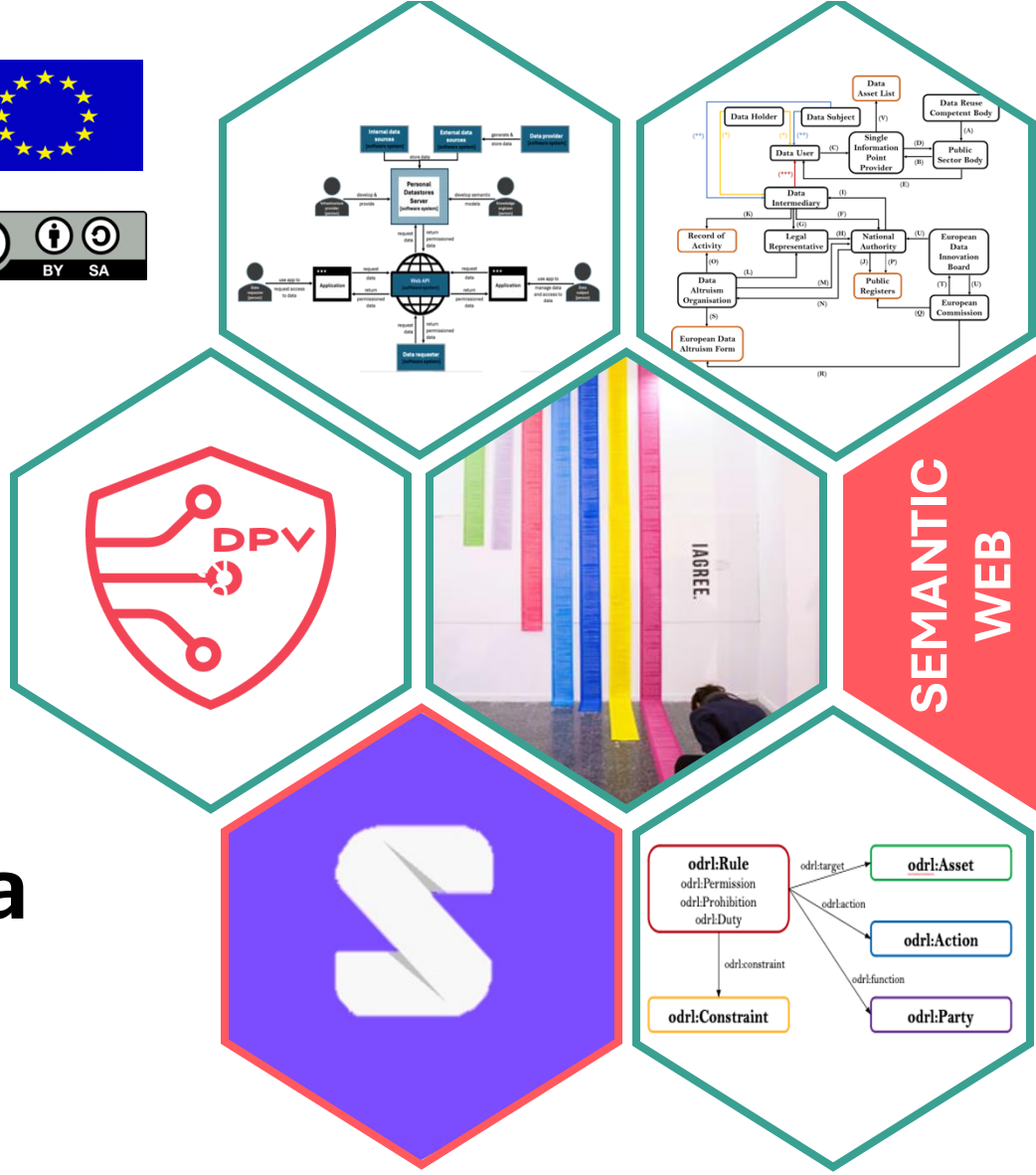
Beatriz Esteves

MSc in Biomedical Engineering

Semantic Representation of Privacy Terms and Policy-based Algorithms for Decentralised Data Environments



Supervisors

Ontology Engineering Group
Universidad Politécnica de Madrid

Dr. Víctor Rodríguez Doncel

ADAPT Centre
Trinity College Dublin

Dr. David Lewis

beatriz.esteves@ugent.be

in/beatriz-esteves-032249156/

besteves4

MY STORY

I want to update my address!

But I want to update it only once!

Government
Doctors
Banks
Insurance

THESIS OVERVIEW

A Introduction

B State of the art

C Vocabularies for personal data stores

D Legal challenges

E Policy-based algorithms

F Exploring the DGA

G Conclusion

SEMANTIC WEB

A Introduction

A1 – Motivation

A2 – Definitions

A3 – Objectives and Research questions

B State of the art

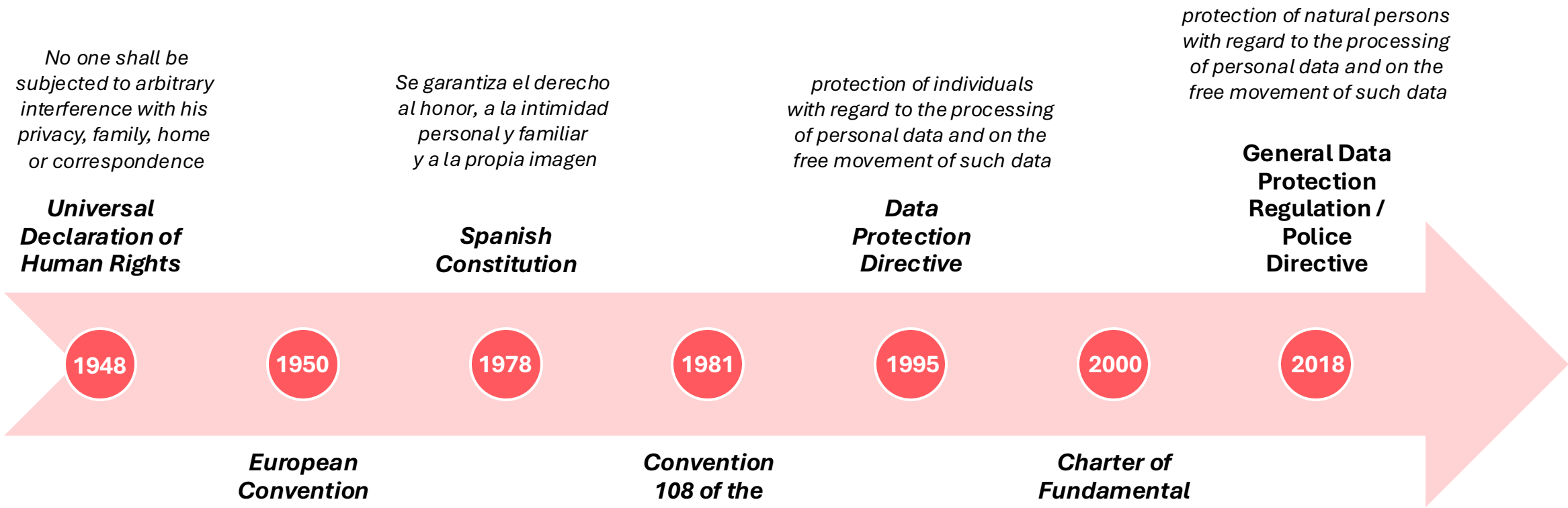
C Vocabularies for personal data stores

D Legal challenges

E Policy-based algorithms

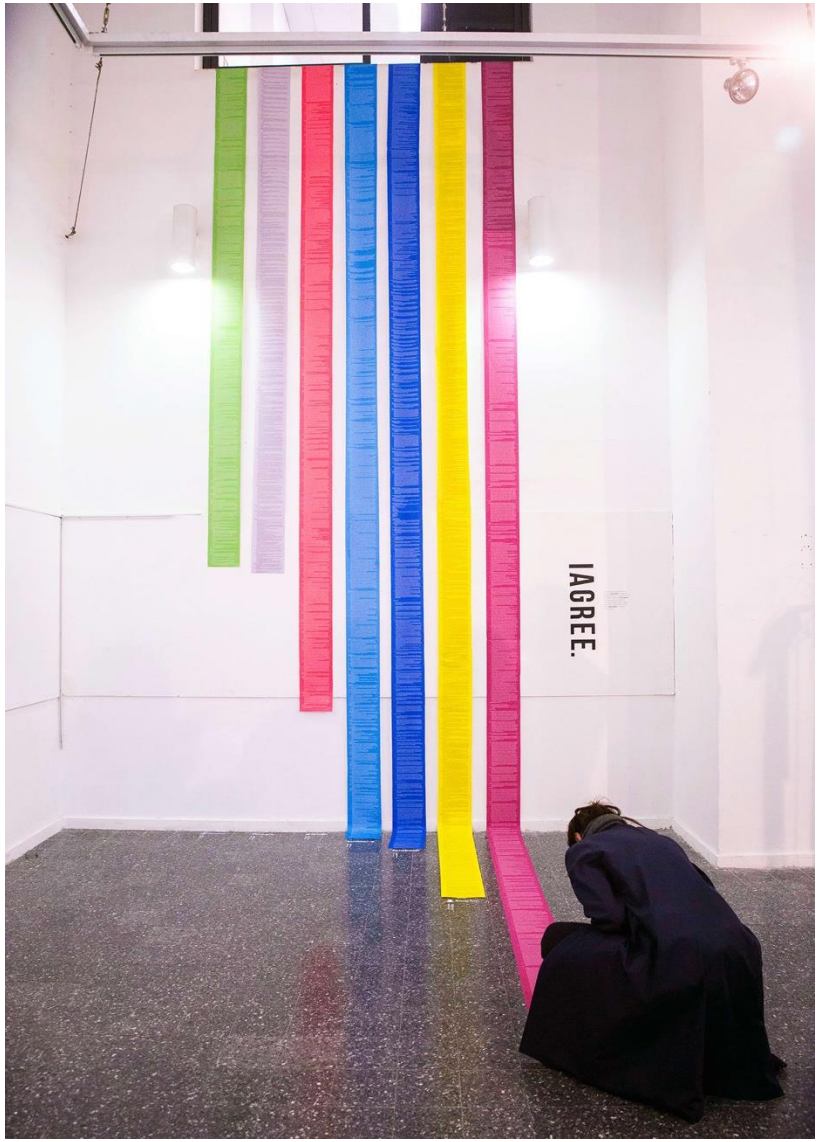
F Exploring the DGA

G Conclusion

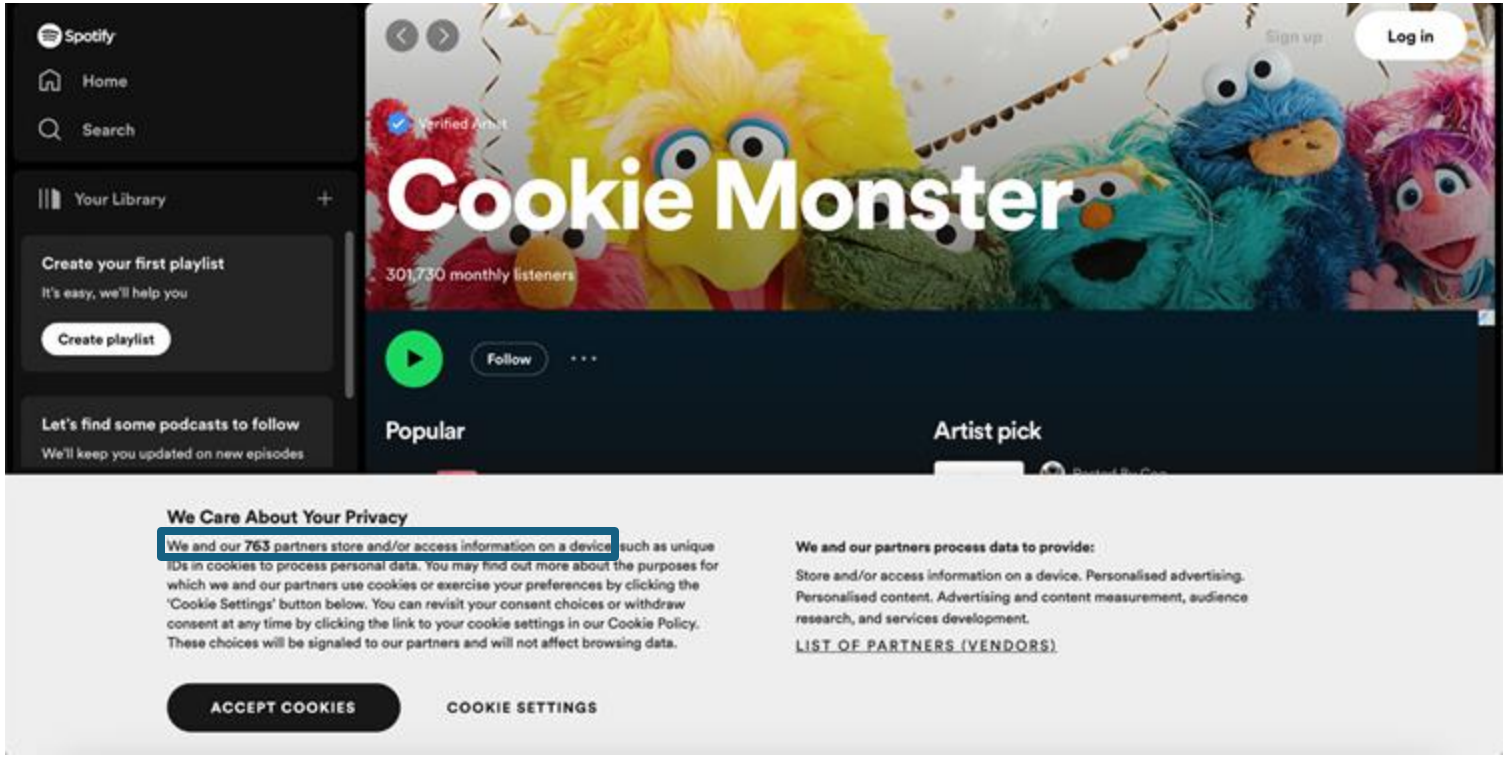

1948
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence
Universal Declaration of Human Rights
1950
Everyone has the right to respect for his private and family life, his home and his correspondence
European Convention on Human Rights
1978
Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen
Spanish Constitution
1981
Convention for the protection of individuals with regard to the processing of personal data
Convention 108 of the Council of Europe
1995
protection of individuals with regard to the processing of personal data and on the free movement of such data
Data Protection Directive
2000
Everyone has the right to the protection of personal data concerning him or her
Charter of Fundamental Rights of the EU
2018
protection of natural persons with regard to the processing of personal data and on the free movement of such data
General Data Protection Regulation / Police Directive

MOTIVATION

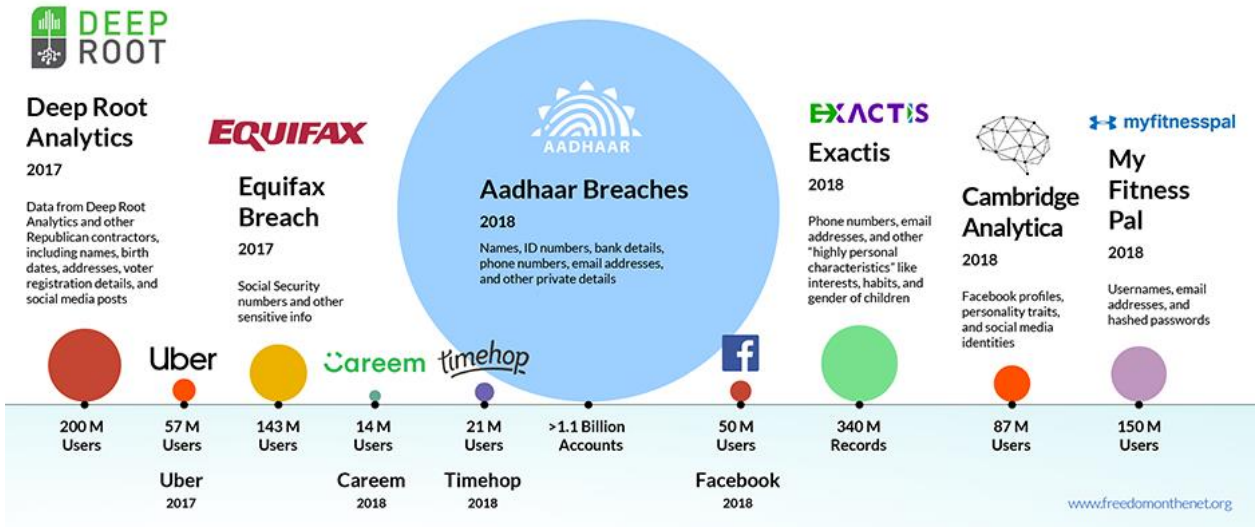
A1 A2 A3



[Photo : Dima Yarovinsky]
https://www.fastcompany.com/90171107/printing-out-the-privacy-policies-of-facebook-snap-and-others

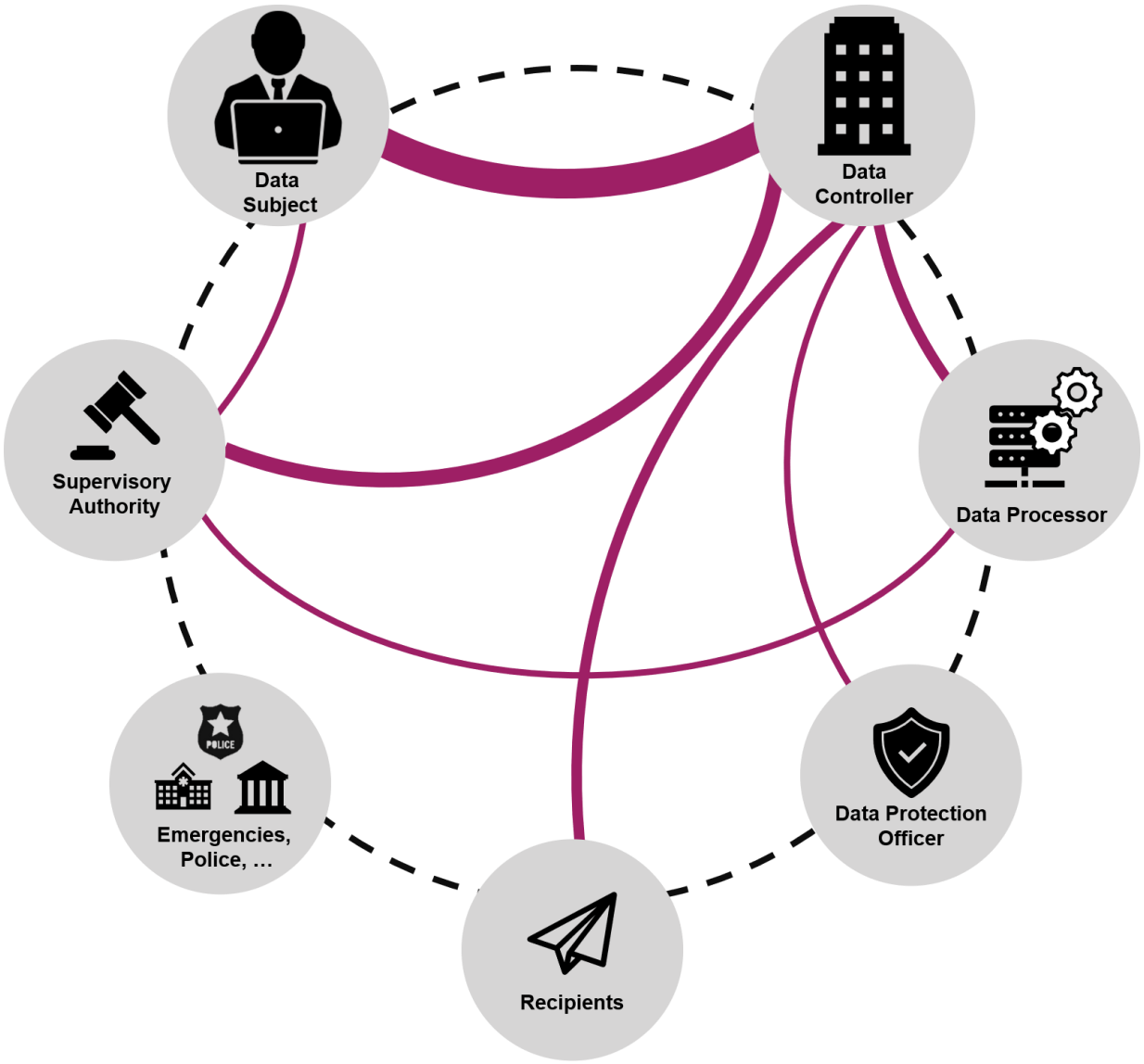


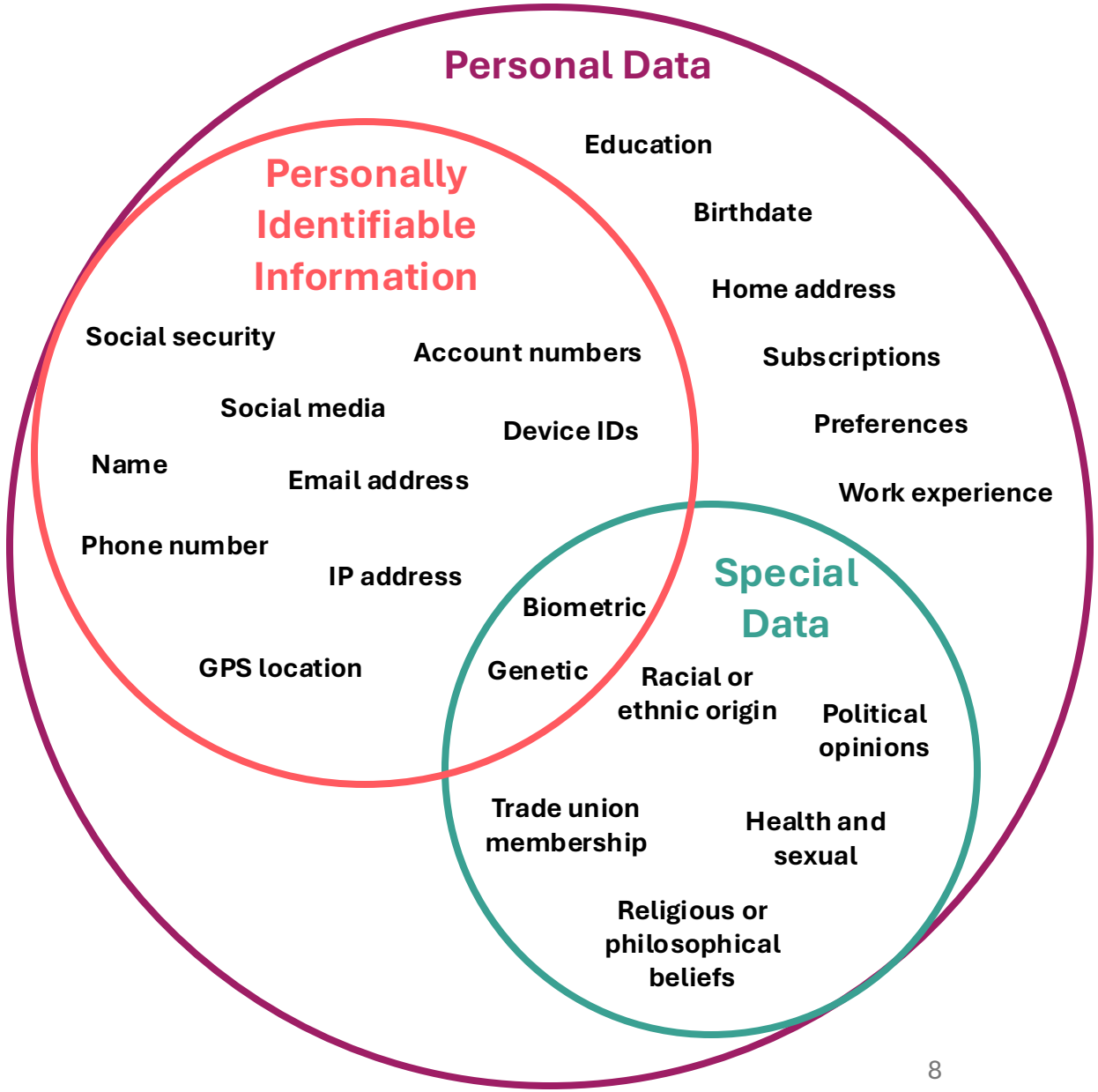
MOTIVATION



THE BATTLE OF THE INTERNET: OPEN VS CLOSED – FURTHER EXPLORATION, Christopher Langley

DEFINITIONS – GDPR





DEFINITIONS – POLICIES & ACCESS CONTROL

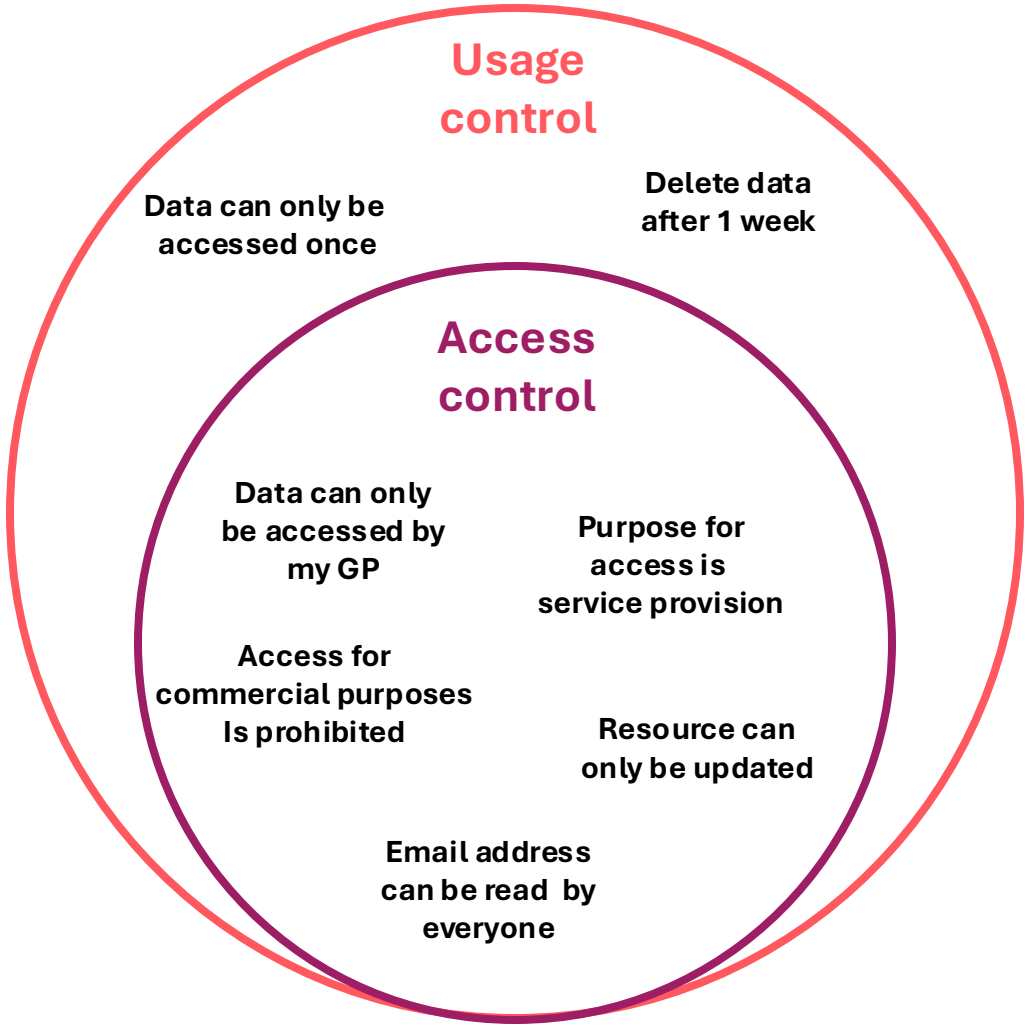
Documents that describe conditions for access and usage of content

- user preferences
- apps privacy policies
- data requests
- data access agreements

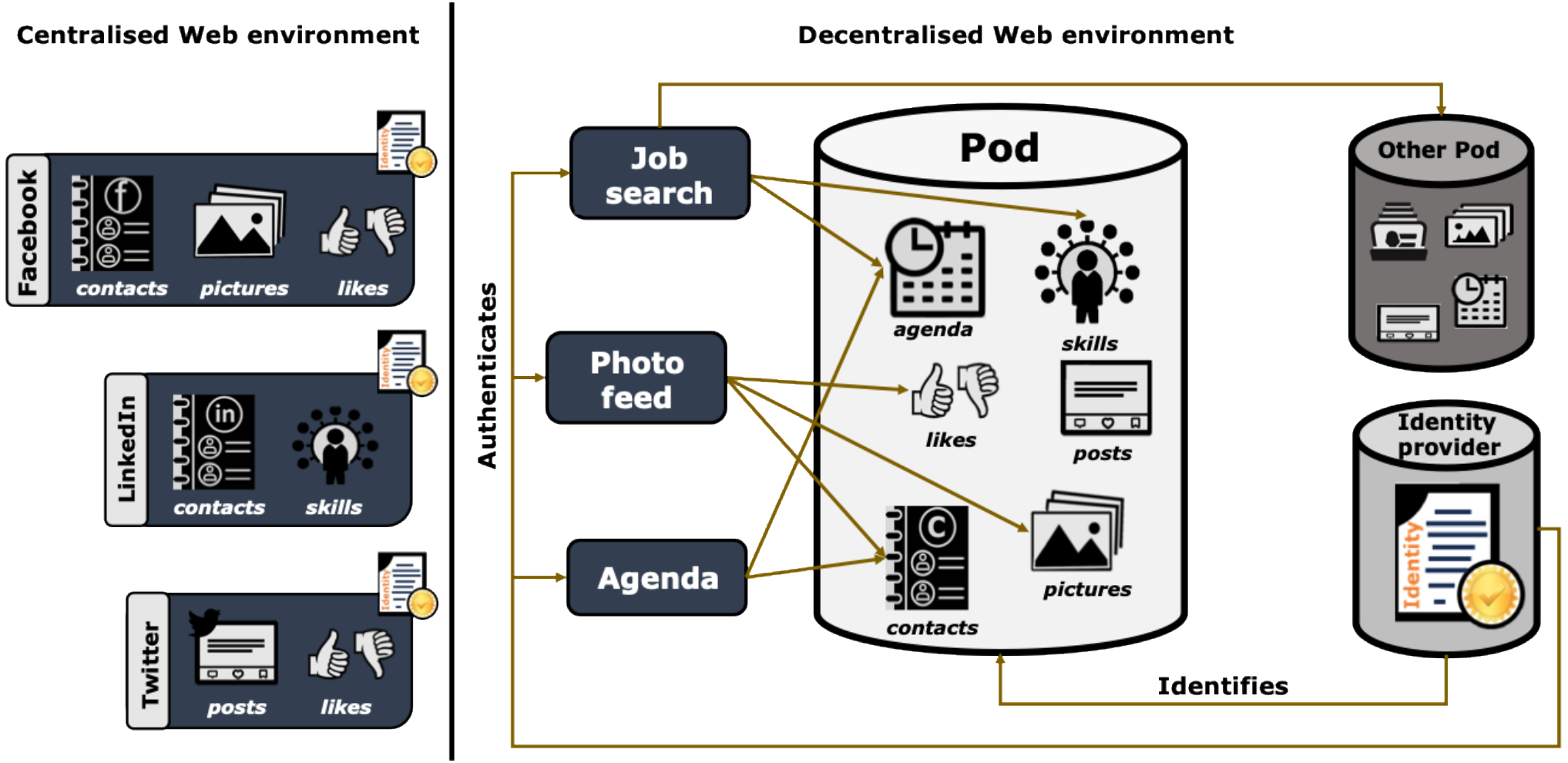
Entity requesting/ being requested access

Requested resource(s)

Rules
Permissions
Prohibitions
Constraints



DEFINITIONS – DECENTRALISATION



OBJECTIVES AND RESEARCH QUESTIONS

To what extent are Semantic Web vocabularies and decentralised technologies able to support the exercising of data subject rights and determine the access conditions to personal data?

RQ1. Are Semantic Web standards and specifications able to represent information related to **privacy preferences**, **data access policies**, and other metadata, aligned with personal **data protection** requirements?

RQ2. Can Semantic Web vocabularies be used to determine **access control conditions** to personal data stored in **decentralised data systems**?

RQ3. Is it possible, using decentralised Web technologies, to facilitate the **exercising of data subject rights** in light of the GDPR?

OBJECTIVES AND RESEARCH QUESTIONS

Research methodologies and design vocabularies and services to aid EU data subjects in taking control of the movement of their personal data.

O1. Design methods and systems to **assist data subjects** (in representing their privacy preferences and consent) and data controllers (with GDPR requirements) in order to support **automated data transactions, accountability and transparency**.

O2. Design a **policy matching algorithm** that utilises the developed vocabularies to express data-sharing **preferences**, **requests** and **agreements** in decentralised personal datastores.

O3. Design a service, using state of the art vocabularies, to assist with **representing information** connected with GDPR's **data subject rights**.

OBJECTIVES AND RESEARCH QUESTIONS

A1 A2 A3

Methodology

- Analyse knowledge sources (GDPR, EDPB/EDPS guidelines, ...)
- Review state-of-the-art languages & ontologies

- Identify key elements of decentralised data systems, including entities involved
- Develop policy matching algorithm using the developed vocabularies

- Identify terms and relations based on this analysis to create the ontology
- Create shapes for consistent modelling of policies and other metadata
- Develop user interfaces and APIs to generate policies and other metadata

Evaluation

- Ontology quality evaluation (Detection of common pitfalls & Alignment with FAIR principles)

- Representation of competency questions as SPARQL queries
- Evaluation of applicability to real-world cases (DUODRL and DGA)

- Alignment with ISO/IEC 27560
- Evaluation of conformance with GDPR (Legal experts validation)

THESIS OVERVIEW

SEMANTIC WEB

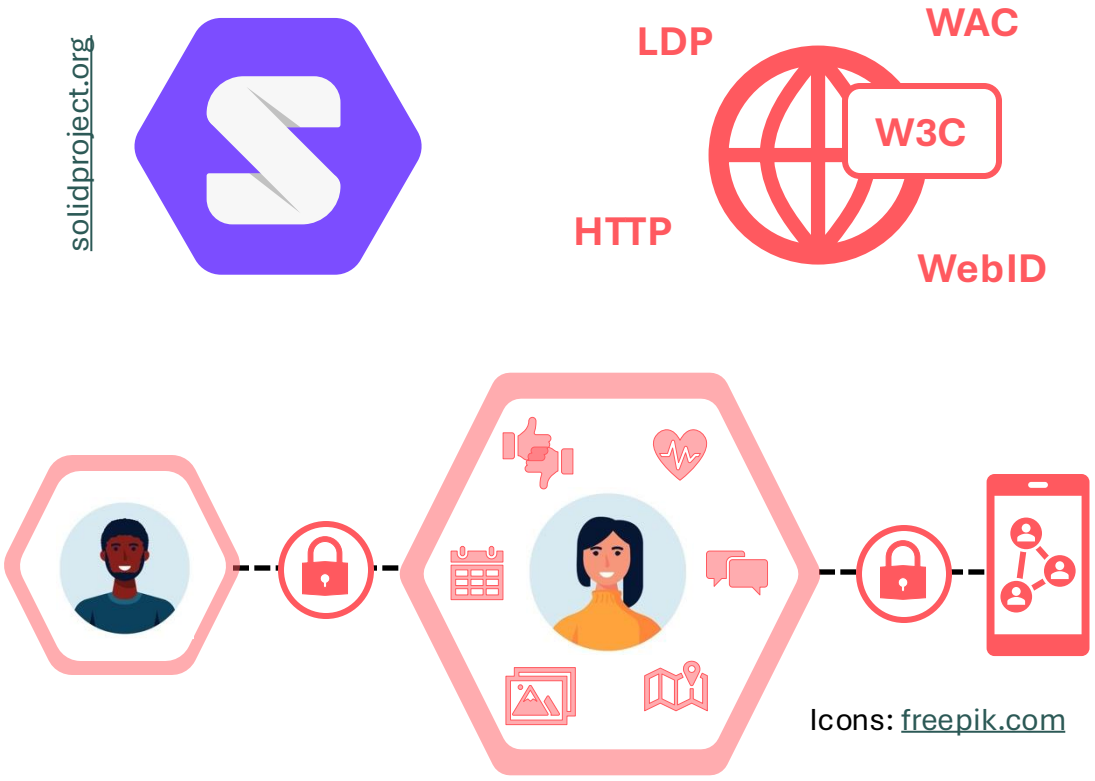
- A Introduction A1 A2 A3
- B State of the art
- C Vocabularies for personal data stores
- D Legal challenges
- E Policy-based algorithms
- F Exploring the DGA
- G Conclusion

THESIS OVERVIEW

SEMANTIC WEB

- **A** Introduction — A1 A2 A3
- **B** State of the art
  - B1 – Decentralised Web
  - B2 – Data protection vocabularies
  - B3 – Policy languages
- **C** Vocabularies for personal data stores
- **D** Legal challenges
- **E** Policy-based algorithms
- **F** Exploring the DGA
- **G** Conclusion

solidproject.org



Icons: freepik.com

Solid is a specification for decentralised data stores based on interoperable data formats and protocols

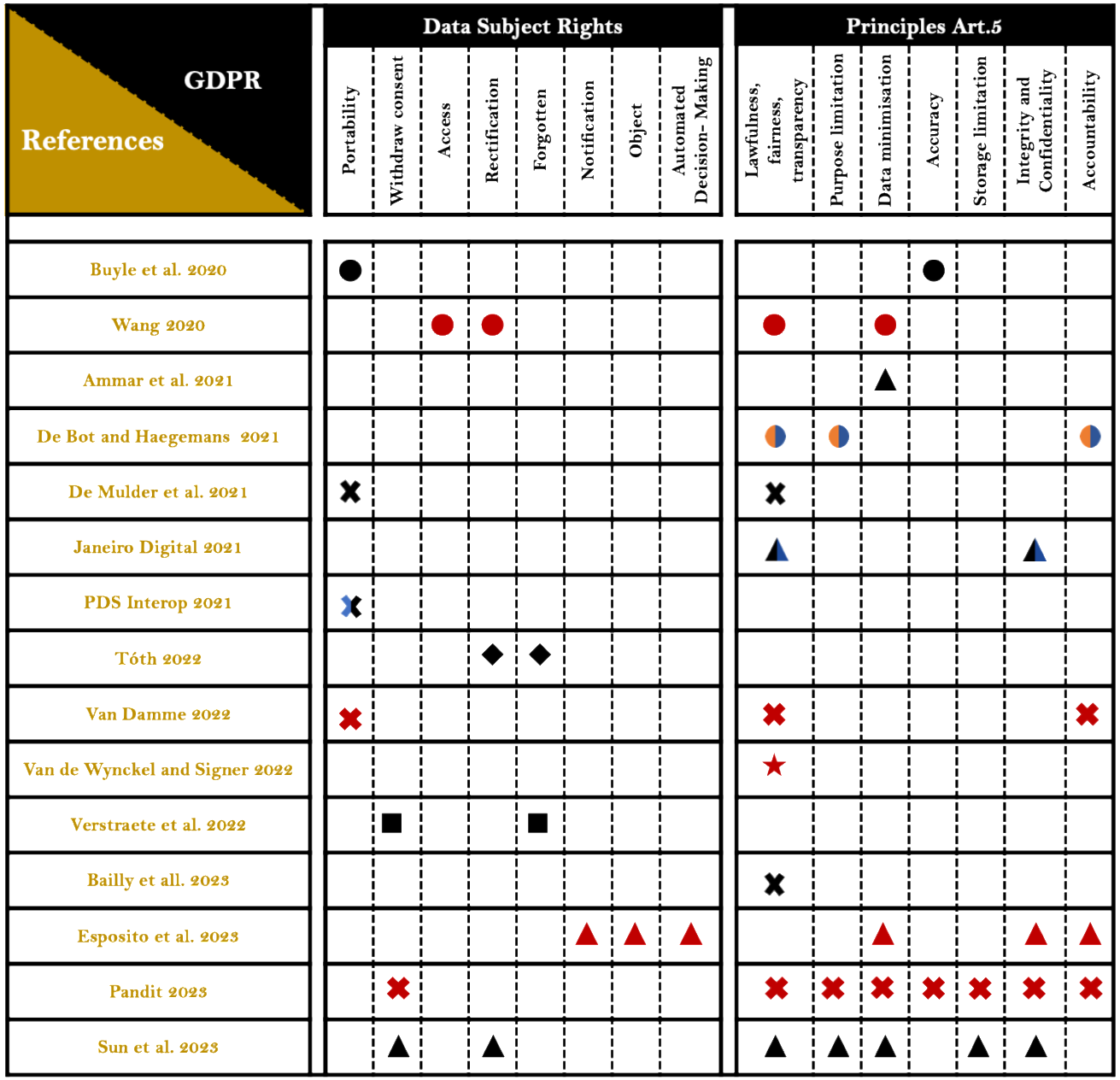
Solid's authorisation mechanism currently relies on two access control languages – WAC and ACP

WAC – Web Access Control

```
<#authorization1> a acl:Authorization ;
    acl:agent <https://beatriz.providerZ.com/profile/card#me> ;
    acl:accessTo <https://victor.providerY.com/docs/file1.ttl> ;
    acl:mode acl:Read, acl:Write .
```

ACP – Access Control Policy

```
<#grant1> a acp:AccessGrant ;
    acp:grant acl:Read, acl:Write ;
    acp:context [
        acp:agent <https://beatriz.providerZ.com/profile/card#me> ;
        acp:issuer <https://identityProviderZ.com> ;
        acp:target <https://victor.providerY.com/docs/file1.ttl> ;
        acp:client <https://clientApplicationA.com> ] .
```

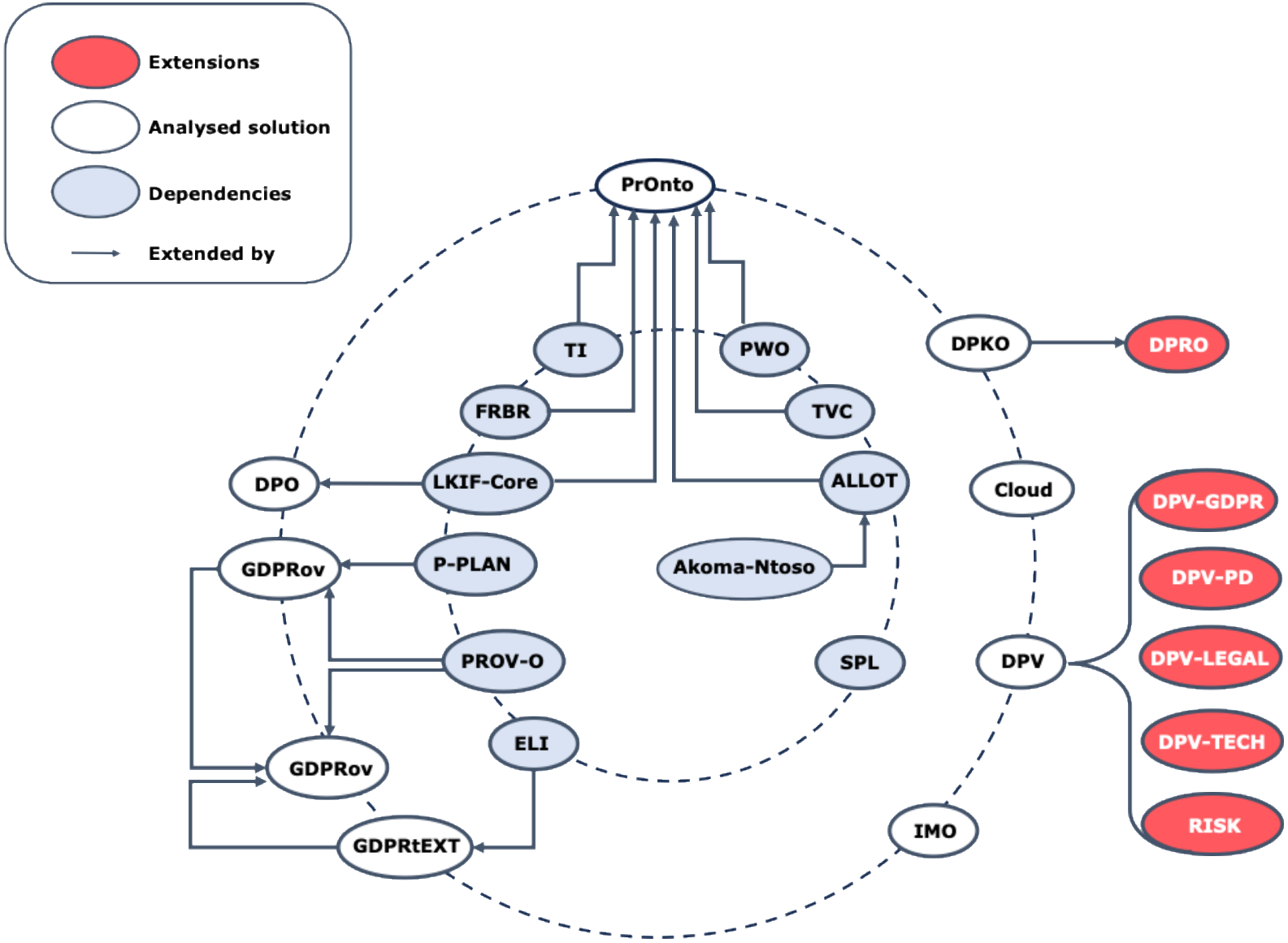


Red – theory
Black – apps
Orange – identity provider
Blue – Pod provider

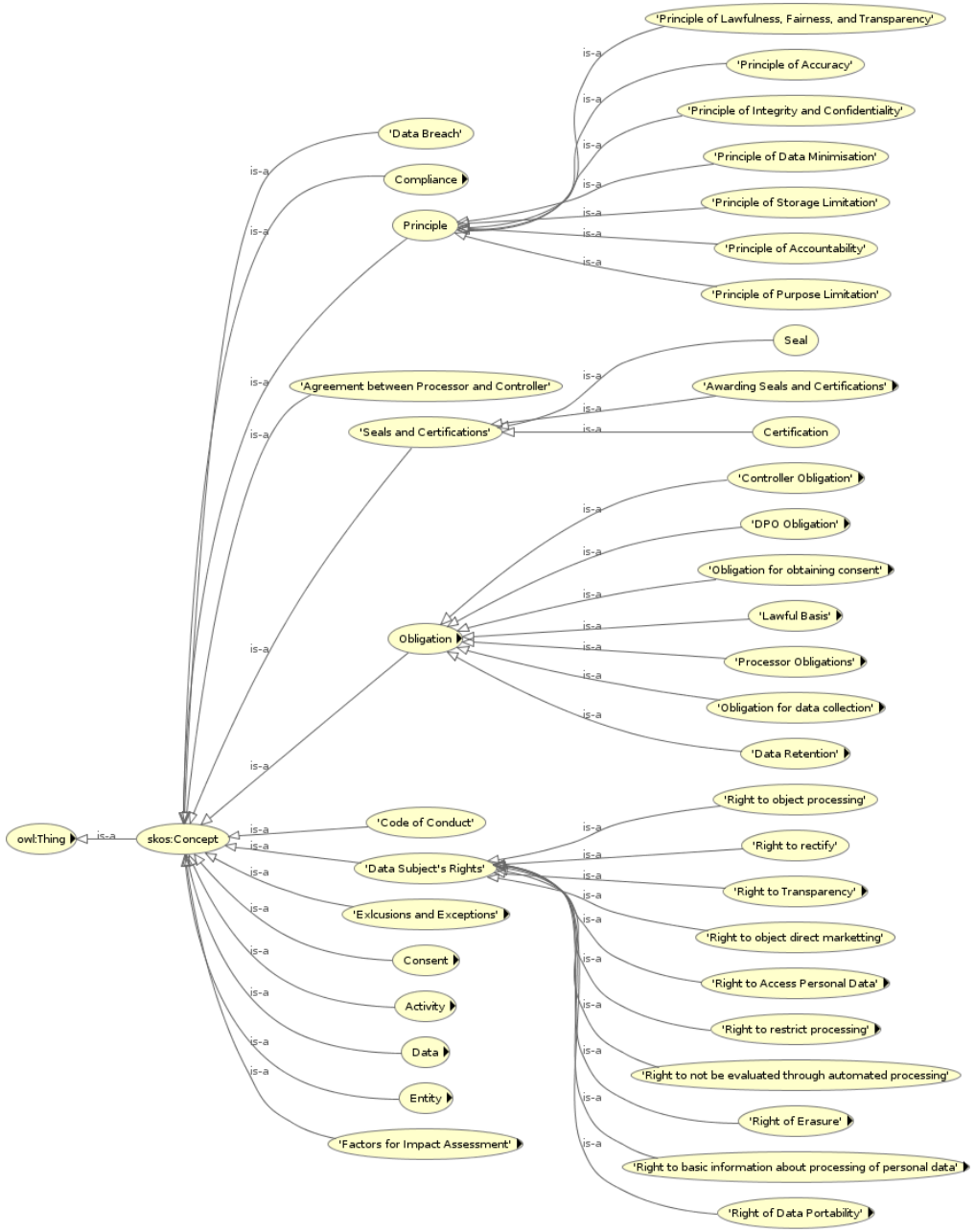
○ – Government
△ – Health
☆ – Location
☐ – Human resources
◇ – Hospitality
✕ – No domain

- Strong focus on the **'lawfulness, fairness and transparency'** principle
- Distinct works were also found to tackle the right to **data portability**, **withdrawal of consent**, and **rectification**
- No work was found on the right to **restrict the processing** of personal data

DATA PROTECTION VOCABULARIES



- **DPV** and **GDPRtEXT** include the most concepts to represent, at least partially, privacy terms from the 'right to be informed' (Arts. 13 and 14) and other data subject rights (Arts. 15 to 22)
- Only DPV has be updated in the past two years
- DPKO, IMO, and PrOnto lack open and accessible resources



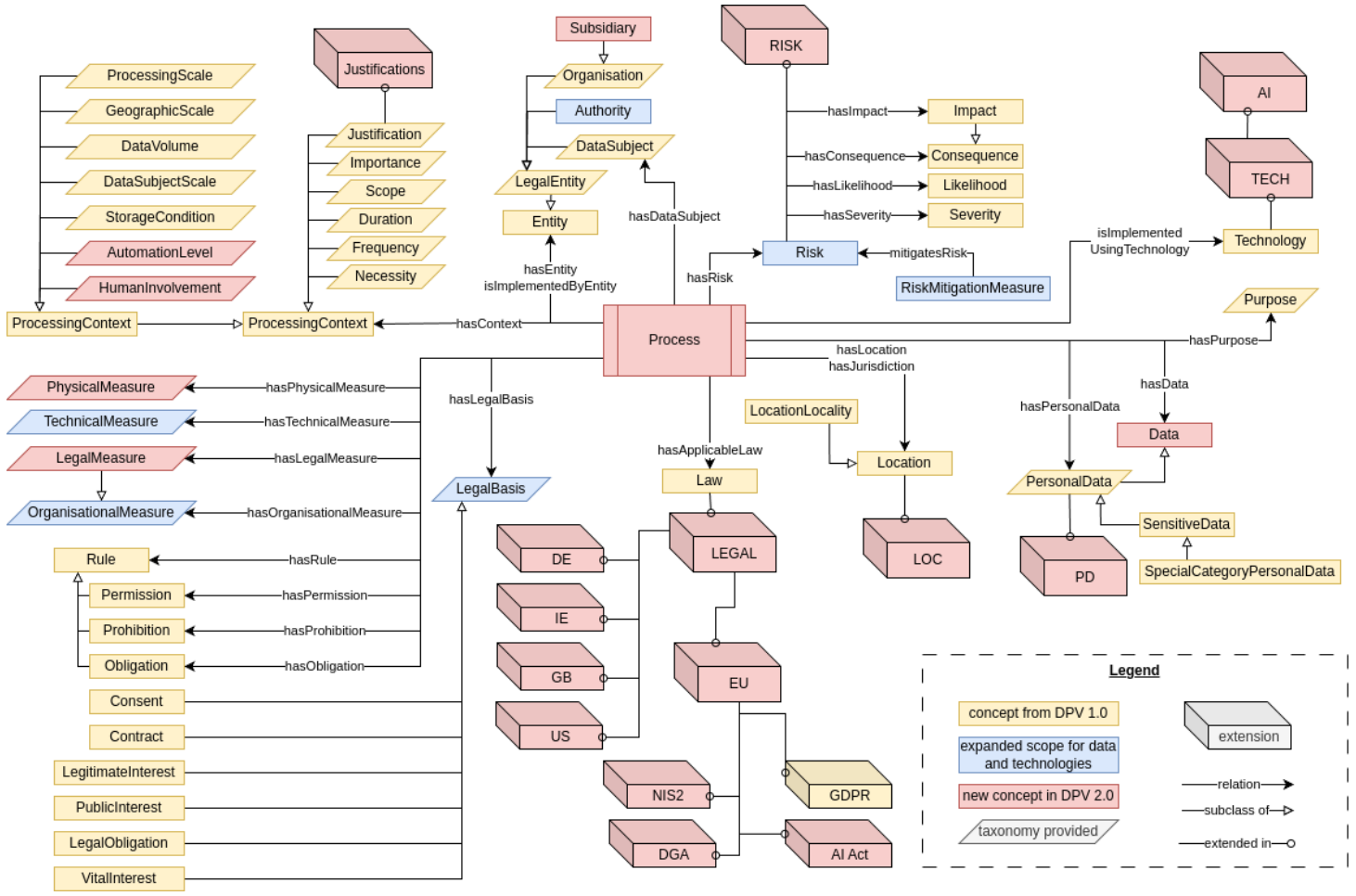
GDPRtEXT

- **GDPR as a linked data resource**
- Extends the European Legislation Identifier (ELI) ontology to connect GDPR concepts with the specific chapters, articles or points of the regulatory text
- Main concepts: **legal entities**, **rights** and **obligations**, **principles** and **activities** which specify processes and actions defined in the GDPR
- Terms are linked to the relevant GDPR provisions using *rdfs:isDefinedBy*.

https://w3id.org/GDPRtEXT

Harshvardhan J. Pandit, Kaniz Fatema, Declan O'Sullivan, and Dave Lewis. **GDPRtEXT – GDPR as a Linked Data Resource**. *The Semantic Web*, volume 10843 of Lecture Notes in Computer Science, pages 481–495. Springer International Publishing, 2018. doi: 10.1007/978-3-319-93417-4_31.

DATA PROTECTION VOCABULARIES



Data Privacy Vocabulary (DPV)

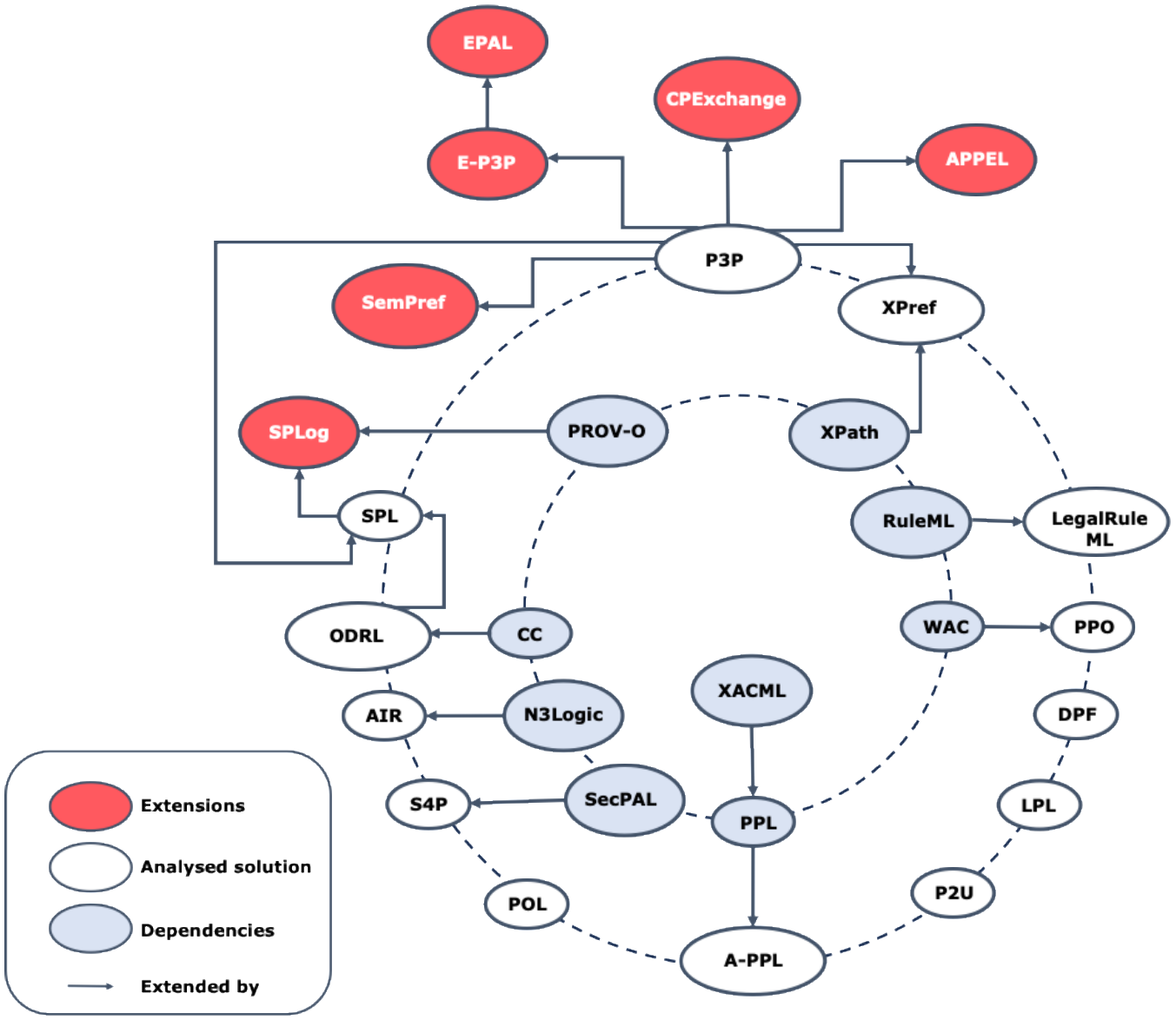
https://w3id.org/dpv

- Developed by the **W3C** Data Privacy Vocabularies and Controls Community Group (**DPVCG**)
- Defines a **jurisdiction-agnostic** ontology for expressing metadata about the processing of personal data
- Provides **hierarchical taxonomies**, from abstract to more specific concepts, to instantiate specific concepts in practical use-cases
- Has law-specific extensions

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. **Creating a Vocabulary for Data Privacy: The First-Year Report of Data Privacy Vocabularies and Controls Community Group (DPVCG)**. *On the Move to Meaningful Internet Systems: OTM 2019 Conferences*, volume 11877 of Lecture Notes in Computer Science, pages 714–730. Springer International Publishing, 2019. doi: 10.1007/978-3-030-33246-4_44.

Harshvardhan J. Pandit, Beatriz Esteves, Georg P. Krog, Paul Ryan, Delaram Golpayegani, and Julian Flake. **Data Privacy Vocabulary (DPV) – Version 2.0**. In *The Semantic Web – ISWC 2024*, pages 171–93. Cham: Springer Nature Switzerland, 2024. doi: 10.1007/978-3-031-77847-6_10.

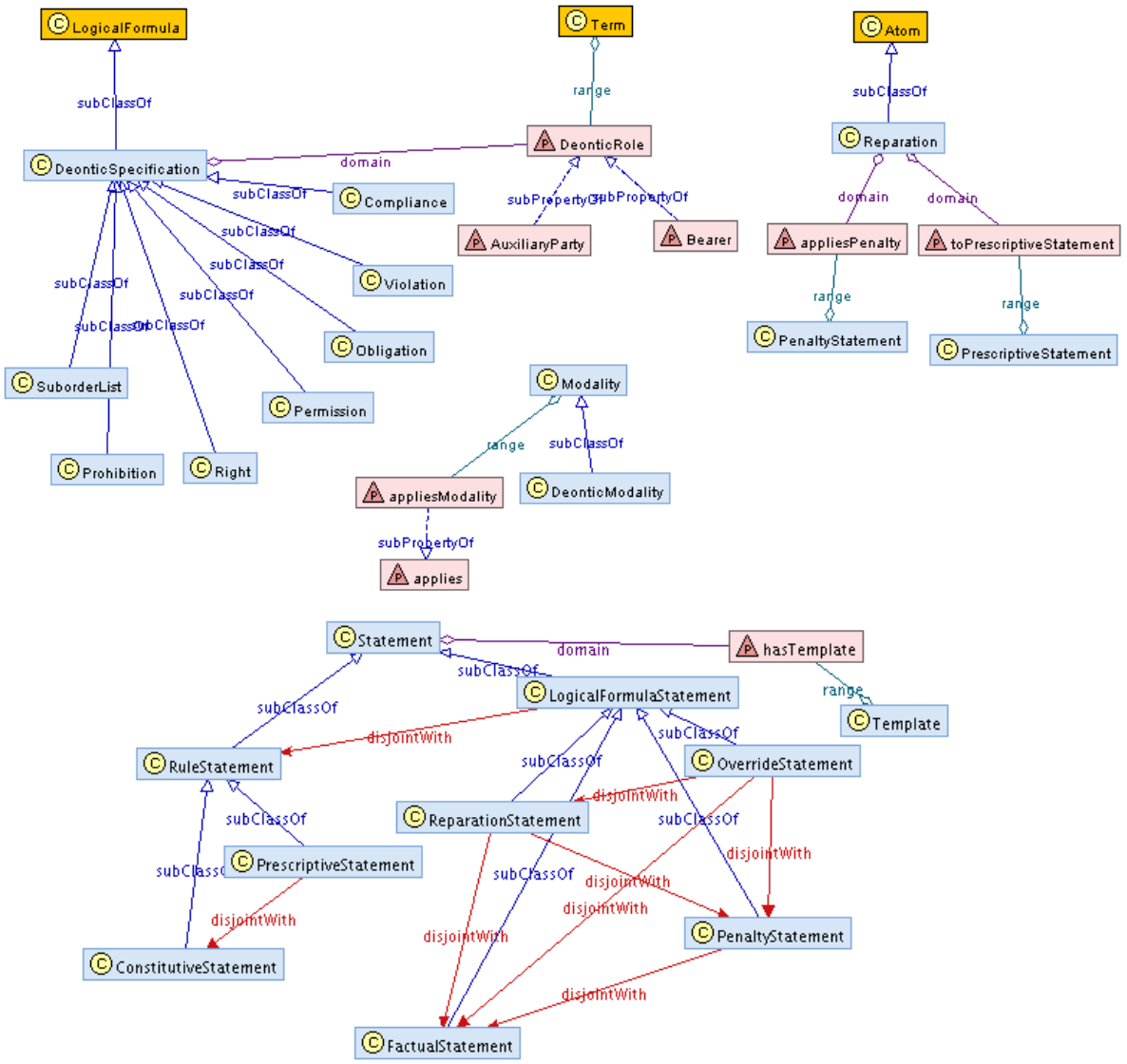
POLICY LANGUAGES



(C1) Ability to model deontic concepts, e.g., permissions, prohibitions, obligations.
(C2) Ability to model GDPR concepts.
(C3) Existence of taxonomies of terms to populate policy conditions.
(C4) Existence of mechanisms to assist with compliance.
(C5) Resource is maintained/continues to be actively developed.
(C6) Existence of an open and accessible specification.

	C1	C2	C3	C4	C5	C6
LegalRuleML	Yes	Partially	No	Yes	Yes	Yes
ODRL	Yes	Partially	Yes	No	Yes	Yes
SPL	No	Partially	Yes	Yes	No	Yes
A-PPL	Yes	Partially	No	Yes	No	No
DPF	Yes	Partially	No	Yes	Unknown	No
P3P	No	Partially	Yes	No	No	Yes
AIR	No	No	No	Yes	No	Yes
LPL	No	Partially	No	Yes	Unknown	No
S4P	No	Partially	No	Yes	No	No
P2U	No	Partially	No	No	No	No
POL	No	Partially	No	No	No	No
PPO	No	No	No	No	No	No
XPref	No	No	No	No	No	No

POLICY LANGUAGES

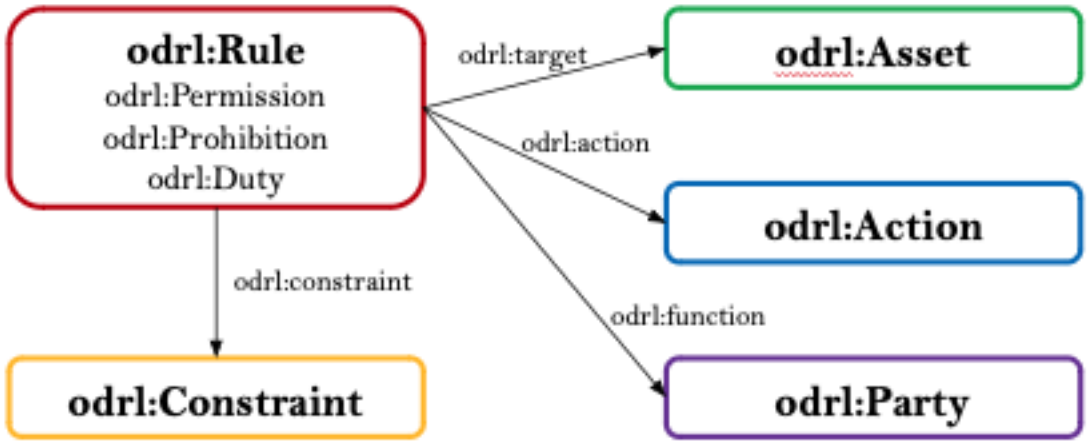


LegalRuleML

- **XML-based** rule interchange language for the legal domain
- Key attributes include the utilisation of multiple semantic annotations for various **legal interpretations**, **deontic operators**, **temporal rule management**, and **statements** segment involves the formalisation of norms
- Used PrOnto ontology to model rules and verify compliance with GDPR's requirements

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

Open Digital Rights Language (ODRL)



Who [can | cannot | must] act what
in which resource how

- W3C Recommendation
- Maintained by the W3C ODRL Community Group
- Composed by several specifications
  - ODRL Information Model – W3C Recommendation
  - ODRL Core Vocabulary – W3C Recommendation
  - ODRL Implementation Best Practices
  - ODRL Profile Best Practices
  - ODRL Formal Semantics [Under development]
- Easily extendable through the use of ODRL profiles

Renato Iannella, Serena Villata. **ODRL Information Model 2.2 – W3C Recommendation 15 February 2018**, 2018. URL: https://www.w3.org/TR/odrl-model/.

Renato Iannella, Michael Steidl, Stuart Myles, Víctor Rodríguez-Doncel. **ODRL Vocabulary & Expression 2.2 – W3C Recommendation** 15 February 2018, 2018. URL: https://www.w3.org/TR/odrl-vocab/.

THESIS OVERVIEW

SEMANTIC WEB

B

A Introduction A1 A2 A3

B State of the art B1 B2 B3

C Vocabularies for personal data stores

D Legal challenges

E Policy-based algorithms

F Exploring the DGA

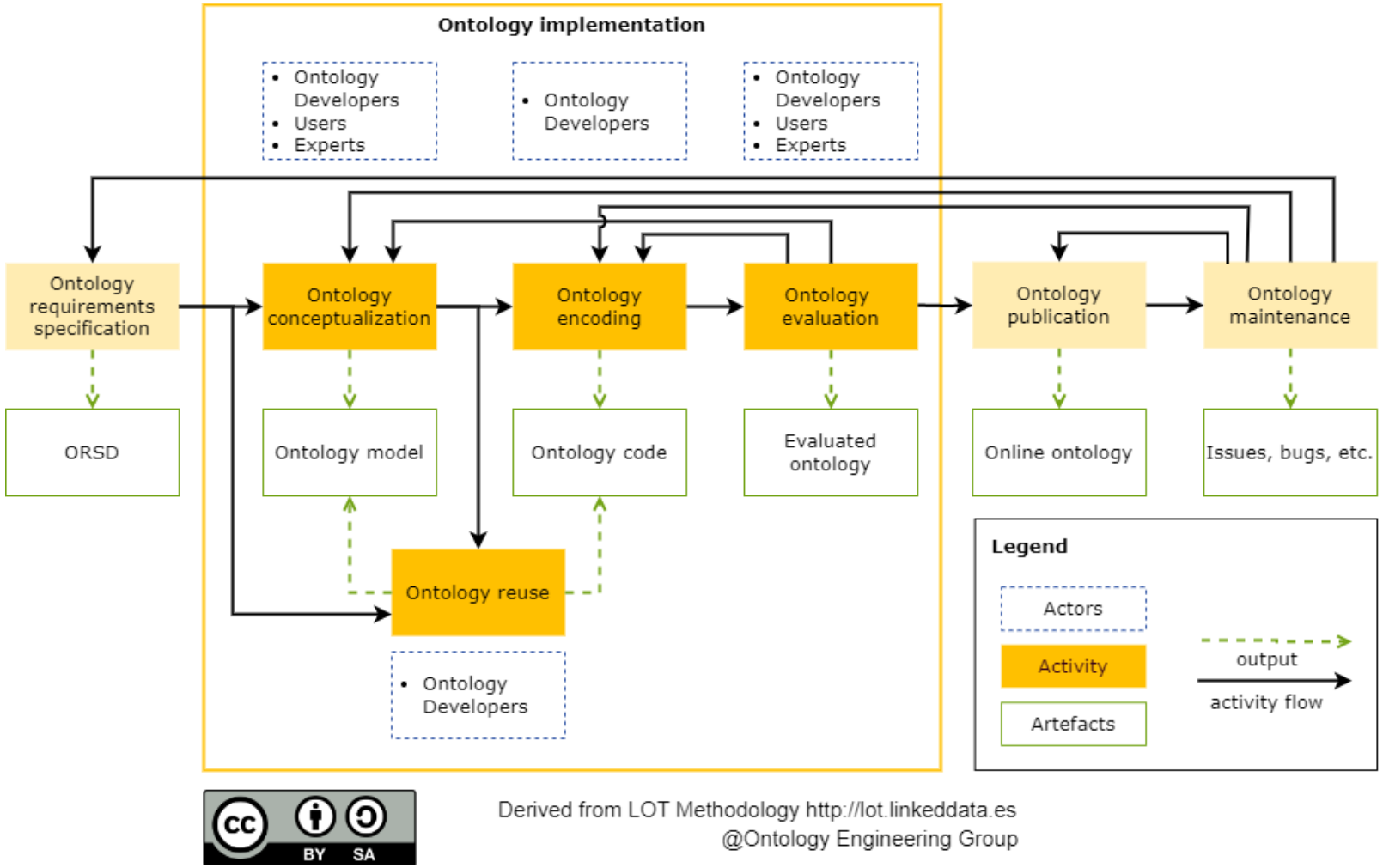
G Conclusion

THESIS OVERVIEW

SEMANTIC WEB

B

- **A** Introduction A1 A2 A3
- **B** State of the art B1 B2 B3
- **C** Vocabularies for personal data stores
  - C1 – Decentralised WEB
  - C2 – Data protection vocabularies
  - C3 – Policy Languages
- **D** Legal challenges
- **E** Policy-based algorithms
- **F** Exploring the DGA
- **G** Conclusion



Conceptualisation: Chowlk

Encoding: VSCode

Evaluation:
- CQs as SPARQL queries
- OOPS!
- FOOPS!
- Legal experts

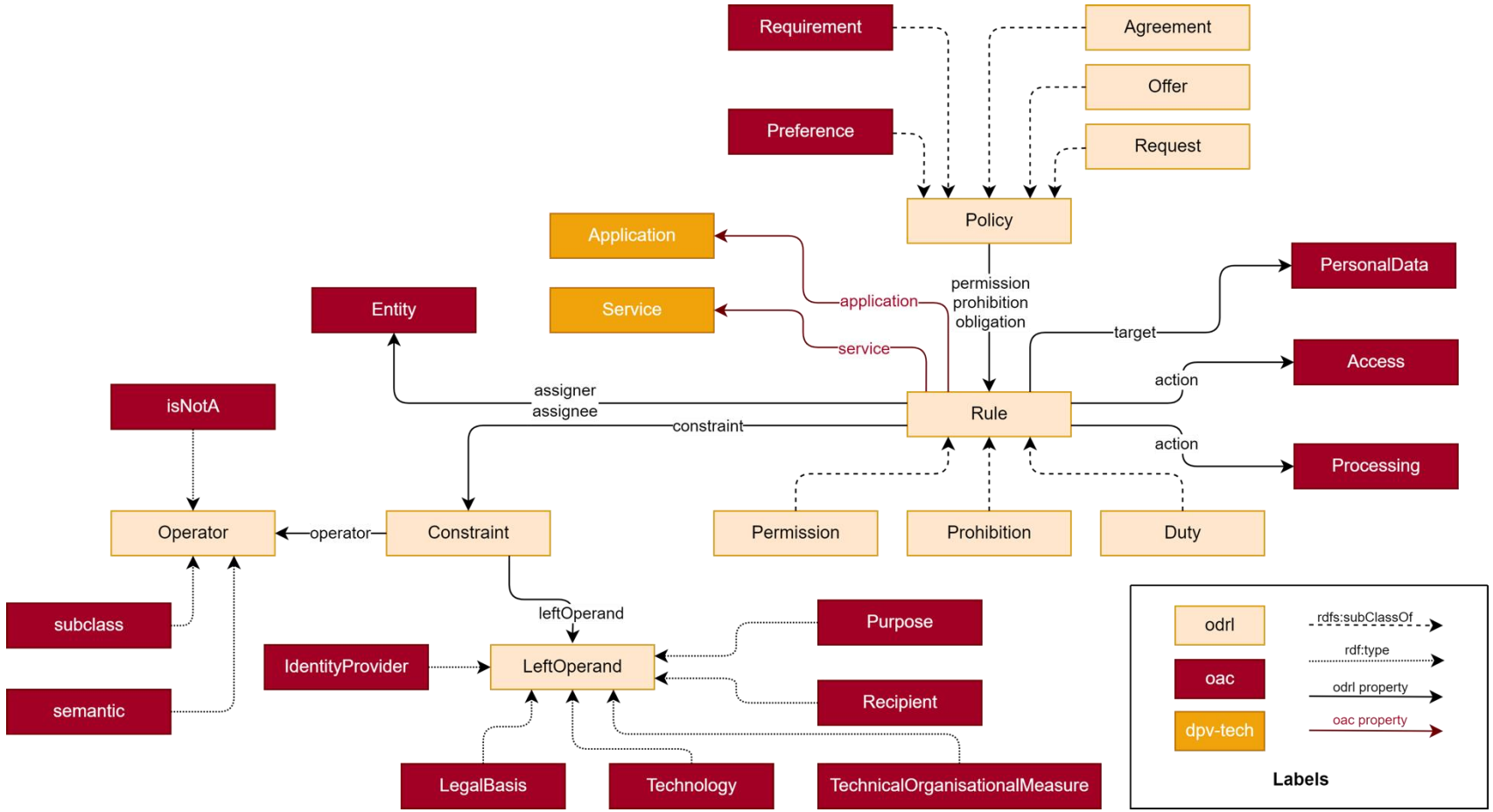
Publication: w3id.org

Maintenance: GitHub

- Accessible policies
- Provenance information
- Fulfil rights and obligations
- Security measures by default and by design

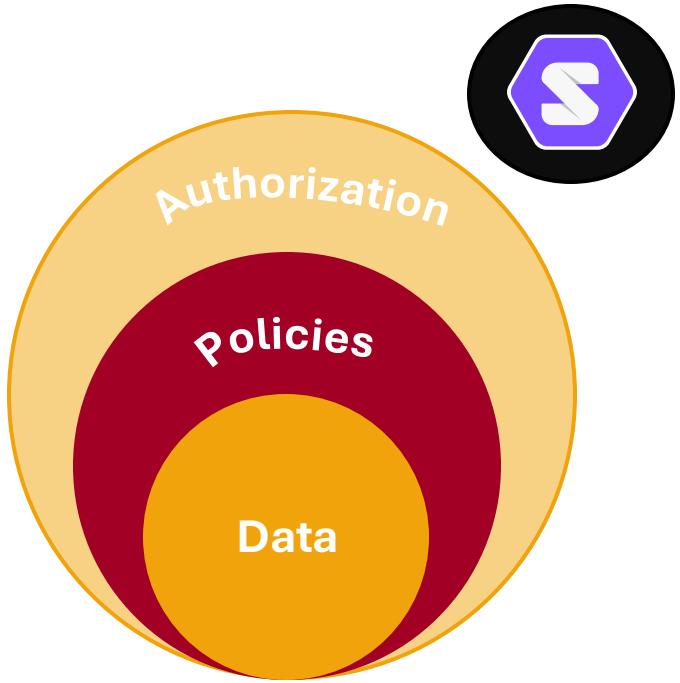
- Human-centric preferences
- Broad and narrow permissions
- Handle conflicts
- Understandability

R1. Support specifying **user preferences as policies**.
R2. Incorporate vocabulary specifying or **aligned to legal concepts**.
R3. Support specifying permissions and prohibitions at **arbitrary granularity**.
R4. Support **identifying and resolving conflicts** based on scope.
R5. **Record policies** used to authorise access.
R6. Support querying policies and authorisations for **introspection of data use**.

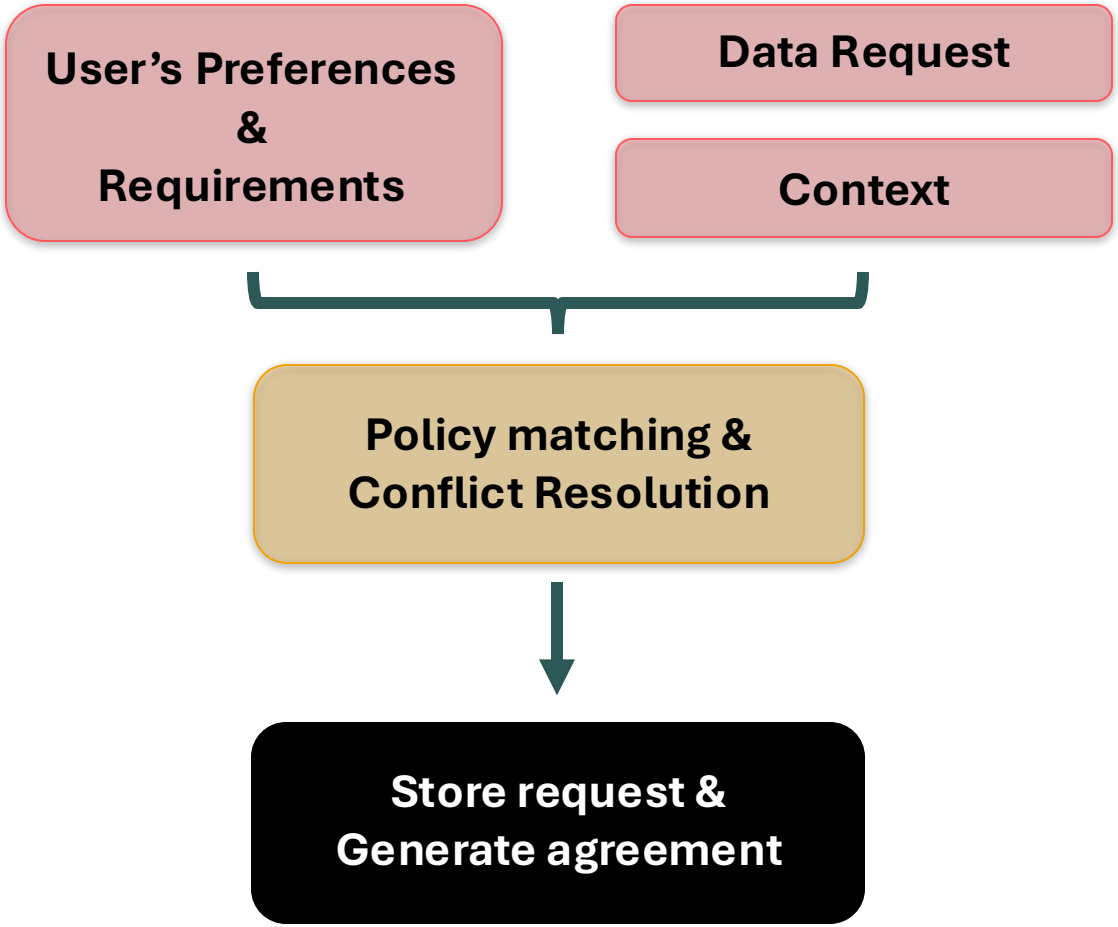


ODRL profile for Access Control (OAC)

https://w3id.org/oac



Beatriz Esteves, Harshvardhan J. Pandit, and Víctor Rodríguez-Doncel. **ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid**. In *2021 IEEE European Symposium on Security and Privacy Workshops*, pages 298–306, 2021. doi: 10.1109/EuroSPW54576.2021.00038.




```
<https://example.com/agreement1> a odrl:Agreement ;
  odrl:profile oac: ;
  dct:description "Agreement to read physical trait data in a R&D
  ↪  project" ;
  dct:creator ex:userA ;
  dct:issued "2022-11-08T18:13:37"^^xsd:dateTime ;
  odrl:uid ex:agreement1 ;
  dct:references ex:offer1, ex:request1 ;
  dpv:hasDataSubject ex:userA ;
  dpv:hasDataController ex:userB ;
  dpv:hasLegalBasis dpv:Consent ;
  odrl:permission [
    odrl:assigner ex:userA ;
    odrl:assignee ex:userB ;
    odrl:action oac:Read ;
    odrl:target oac:PhysicalTrait ;
    odrl:constraint [
      dct:title "Purpose for processing is to conduct research in the R&D
      ↪  project X." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:eq ;
      odrl:rightOperand ex:RDProjectX ] ] .
```

ODRL Profile for Access Control

Draft release 09 October 2023

Version: 0.2
Latest editor's draft:
https://w3id.org/oac

Editors:
Beatriz Esteves (Ontology Engineering Group, Universidad Politécnica de Madrid)
Harshvardhan J. Pandit (ADAPT Centre, Trinity College Dublin)
Víctor Rodríguez-Doncel (Ontology Engineering Group, Universidad Politécnica de Madrid)

Previous versions:
v0.1

Participate:
GitHub profile
File a bug
Commit history
Pull requests

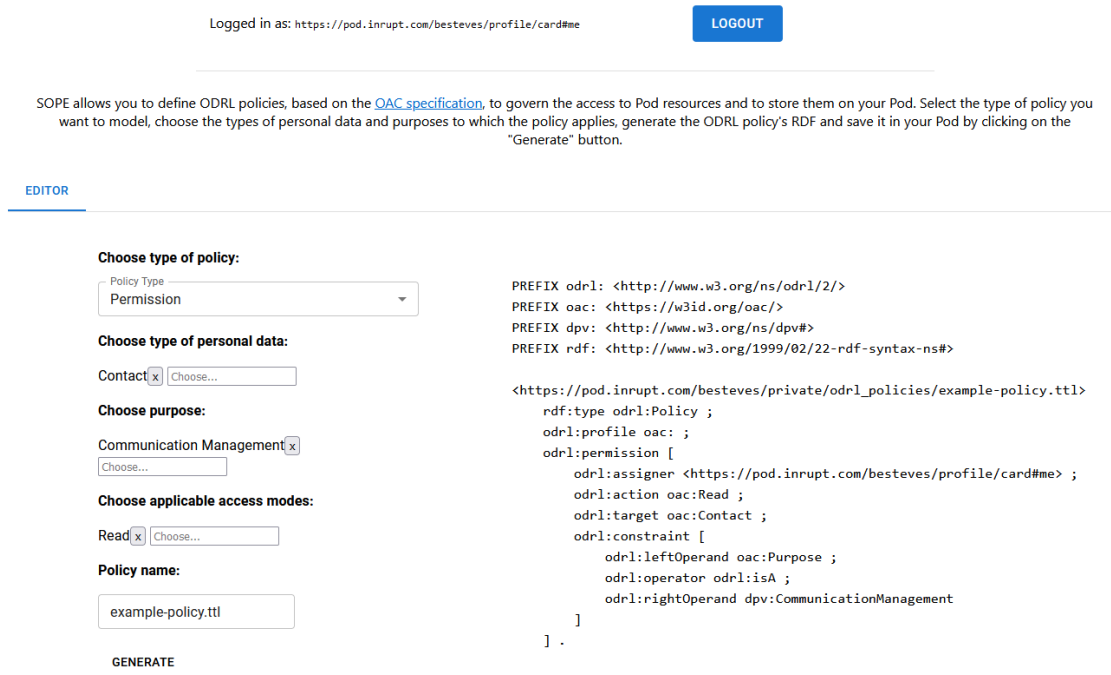
Download serialization:
Format TTL

License:
License CC-BY 4.0

Abstract

This document presents a new profile, the ODRL Profile for Access Control (OAC), that extends the WAC access control list mechanism by using the Open Digital Rights Language (ODRL) to define access control policies that express permissions and / or prohibitions associated with data stored in a decentralised storage environment

https://w3id.org/oac/repo



https://w3id.org/people/besteves/sope/repo

Beatriz Esteves, Víctor Rodríguez-Doncel, Harshvardhan J. Pandit, Nicolas Mondada, and Pat McBennett. **Using the ODRL Profile for Access Control for Solid Pod Resource Governance**. In *The Semantic Web: ESWC 2022 Satellite Events*, pages 16–20. Springer International Publishing, 2022. ISBN 978-3-031-11609-4. doi: 10.1007/978-3-031-11609-4_3.

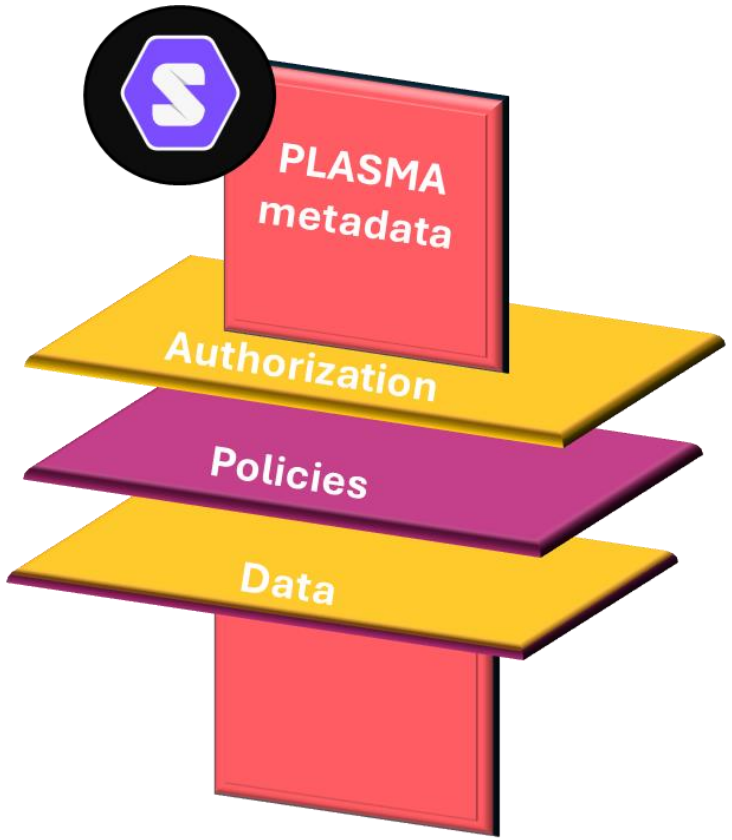
Requisites for a GDPR-aligned Solid

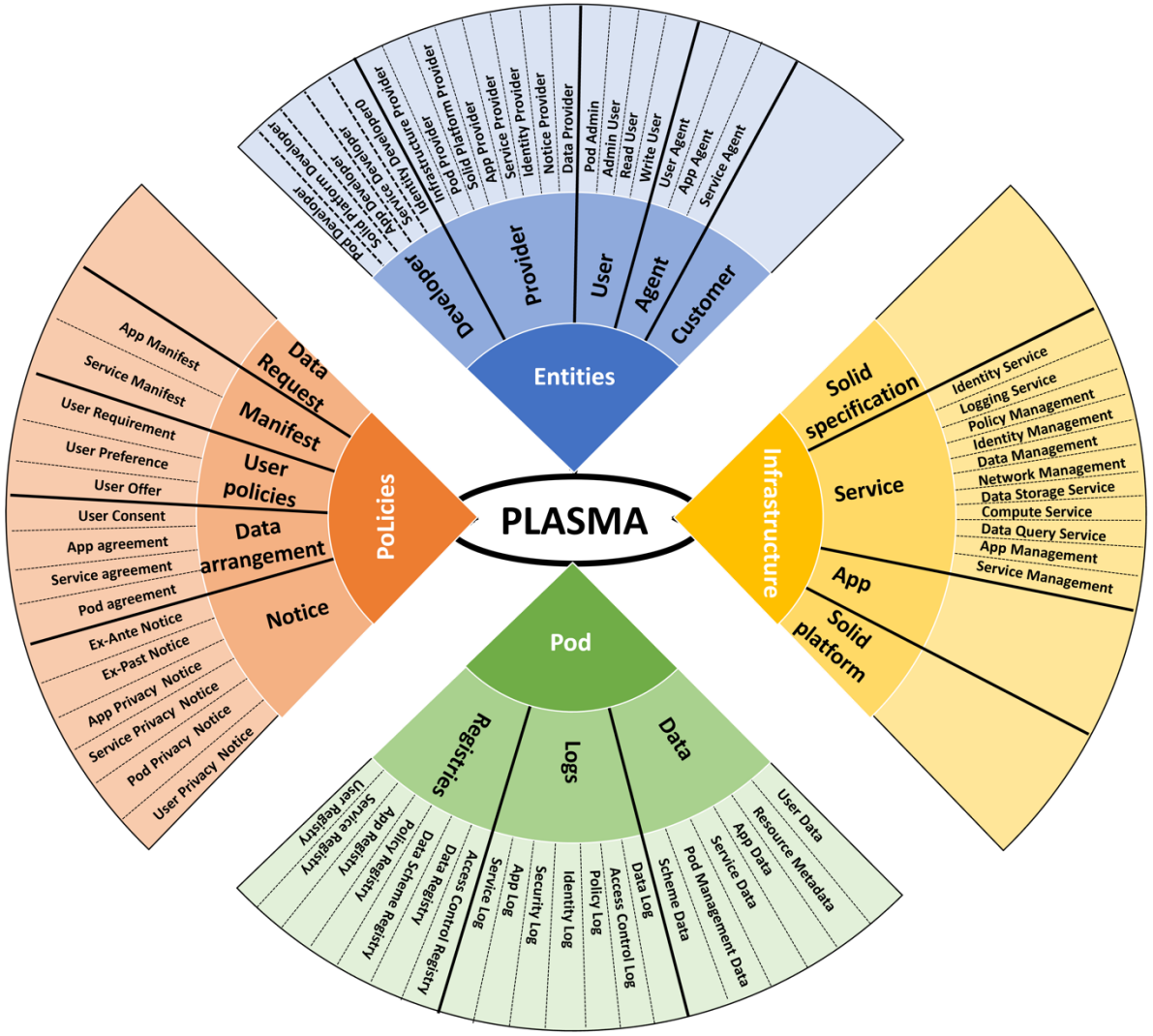
R1. Support specifying **user preferences as policies**.
R2. Incorporate vocabulary specifying or **aligned to legal concepts**.
R3. Support specifying permissions and prohibitions at **arbitrary granularity**.
R4. Support **identifying and resolving conflicts** based on scope.
R5. **Record policies** used to authorise access.
R6. Support querying policies and authorisations for **introspection of data use**.

R7. Record information about **Pod, apps, services, data**, and their **providers/developers**.
R8. Support specifying of different **agreements** and **notices**.
R9. Record **provenance information** for future introspection and convenient access to data.
R10. Provide **conformance conditions** to assist with legal compliance.

PLASMA

https://w3id.org/plasma





Policy LAnguage for Solid's Metadata-based Access control

https://w3id.org/plasma

```
<https://example.com/PodManagementData> a plasma:PodManagementData ;
    dcterms:description "Metadata of User A's Pod"@en ;
    odrl:hasPolicy  <https://example.com/PodAgreement> ;
    plasma:hasProvider <https://example.com/PodProvider_EntityA> ;
    plasma:hasDeveloper <https://example.com/PodDeveloper_EntityB> ;
    plasma:hasProvider <https://example.com/SolidPlatformProvider_EntityC> ;
    plasma:hasProvider <https://example.com/InfrastructureProvider_EntityD> ;
    plasma:implementedSolidPlatform <https://example.com/SolidPlatform_E> ;
    plasma:implementedSolidSpecification <https://example.com/SolidSpecification_v0_10_0> .

<https://example.com/PodAgreement> a plasma:PodAgreement .

<https://example.com/PodProvider_EntityA> a plasma:PodProvider ;
    dpv:hasName "Entity A" ;
    dpv:hasAddress "Address of Entity A" ;
    dpv:hasContact "mailto:entity_a@mail.com" .

<https://example.com/SolidPlatform_E> a plasma:SolidPlatform ;
    plasma:hasProvider <https://example.com/SolidPlatformProvider_EntityC> ;
    dcterms:source <https://example.com/products/solid-server> ;
    dpv:hasPolicy <https://example.com/products/solid-server/privacy-policy> ;
    schema:codeRepository <https://example.com/code-repository/solid-server> ;
    pav:version "0.1.0" ;
    dcterms:license <https://dalicc.net/licenselibrary/CC-BY_v4> .

<https://example.com/SolidSpecification_v0_10_0> a plasma:SolidSpecification ;
    dcterms:conformsTo <https://solidproject.org/TR/2022/protocol-20221231> ;
    dcterms:creator "Sarven Capadisli", "Tim Berners-Lee", "Ruben Verborgh", "Kjetil Kjernsmo" ;
    dcterms:license <https://dalicc.net/licenselibrary/MIT> ;
    pav:version "0.10.0" ;
    dcterms:created "2022-12-31"^^xsd:date ;
    schema:codeRepository <https://github.com/solid/specification> .
```

Beatriz Esteves, and Harshvardhan J Pandit. **Using Patterns to Manage Governance of Solid Apps**. In *14th Workshop on Ontology Design and Patterns (WOP 2023@ISWC 2023)*, 2023. https://ceur-ws.org/Vol-3636/paper5.pdf.

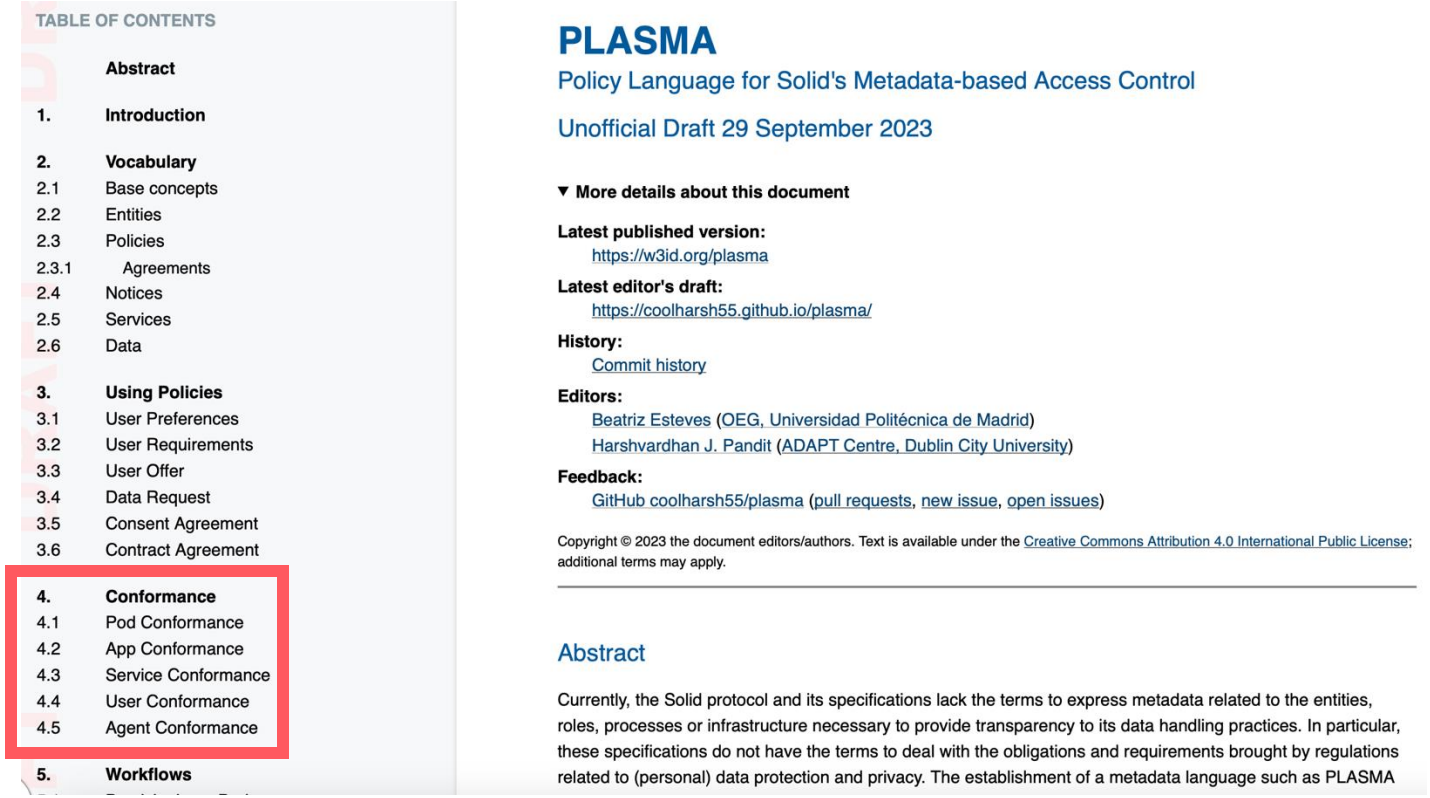


TABLE OF CONTENTS

PLASMA

Policy Language for Solid's Metadata-based Access Control

Unofficial Draft 29 September 2023

▼ More details about this document

Latest published version:
https://w3id.org/plasma

Latest editor's draft:
https://coolharsh55.github.io/plasma/

History:
Commit history

Editors:
Beatriz Esteves (OEG, Universidad Politécnica de Madrid)
Harshvardhan J. Pandit (ADAPT Centre, Dublin City University)

Feedback:
GitHub coolharsh55/plasma (pull requests, new issue, open issues)

Abstract

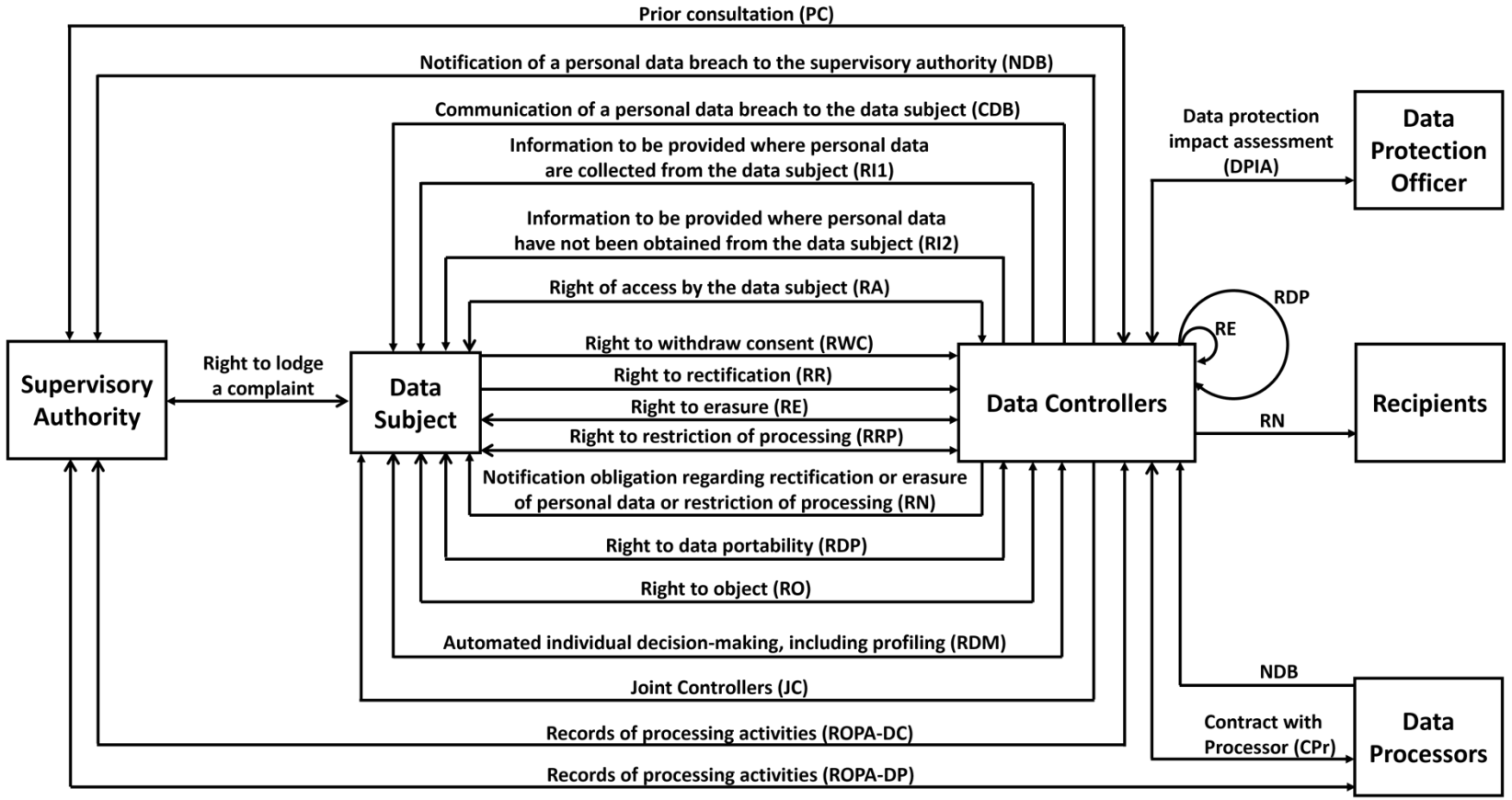
Currently, the Solid protocol and its specifications lack the terms to express metadata related to the entities, roles, processes or infrastructure necessary to provide transparency to its data handling practices. In particular, these specifications do not have the terms to deal with the obligations and requirements brought by regulations related to (personal) data protection and privacy. The establishment of a metadata language such as PLASMA

```
shapes:PodManagementData
        rdf:type sh:NodeShape ;
        rdfs:label "Pod Management Data"@en ;
        sh:property shapes:PodManagementData_description ,
            shapes:PodManagementData_hasPolicy ,
            shapes:PodManagementData_hasDeveloper ,
            shapes:PodManagementData_hasProvider ,
            shapes:PodManagementData_implementedSolidPlatform ,
            shapes:PodManagementData_implementedSolidSpecification ;
        sh:targetClass  <https://w3id.org/plasma#PodManagementData> .

shapes:PodManagementData_description
        sh:datatype         rdf:langString ;
        sh:maxCount         1 ;
        sh:minCount         1 ;
        sh:name             "description"@en ;
        sh:nodeKind         sh:Literal ;
        sh:path             <http://purl.org/dc/terms/description> .
```

https://w3id.org/plasma/repo

These rights, combined with the **transparency** and **accountability** measures imposed on organisations, aim to strike a balance between the **interests of data subjects** and the **legitimate needs of businesses and institutions** in the digital age.



Technological gap between regulation & tools for rights exercising

Organisations:

Unintuitive/inaccessible tools
Manual processes

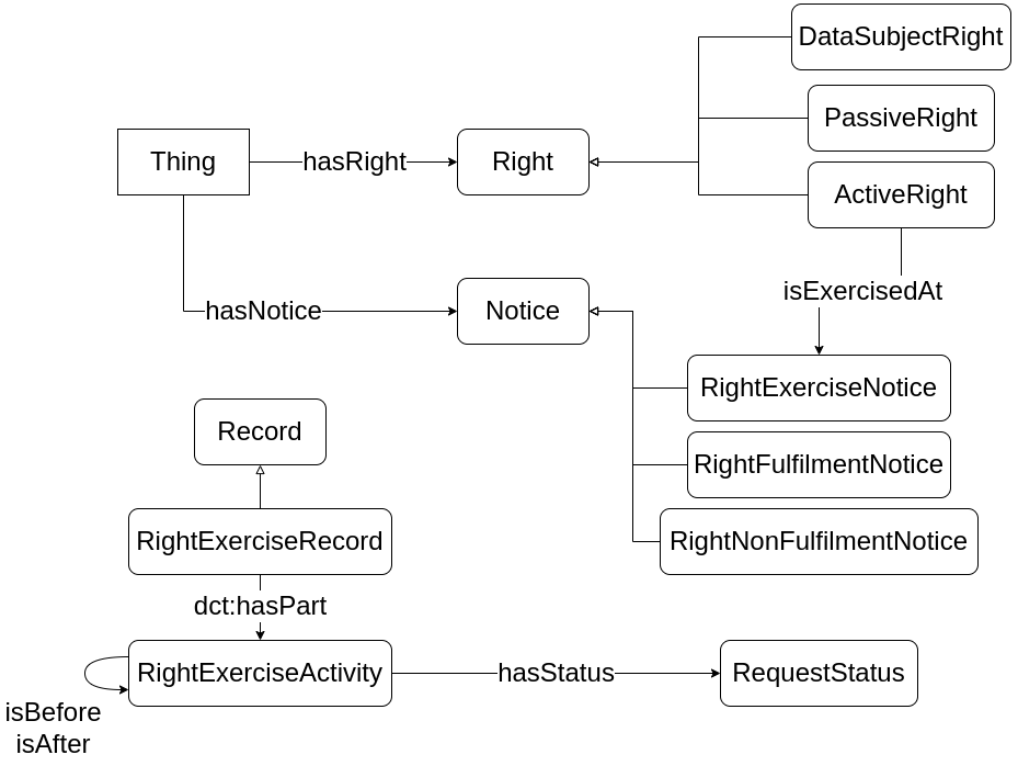
Users:

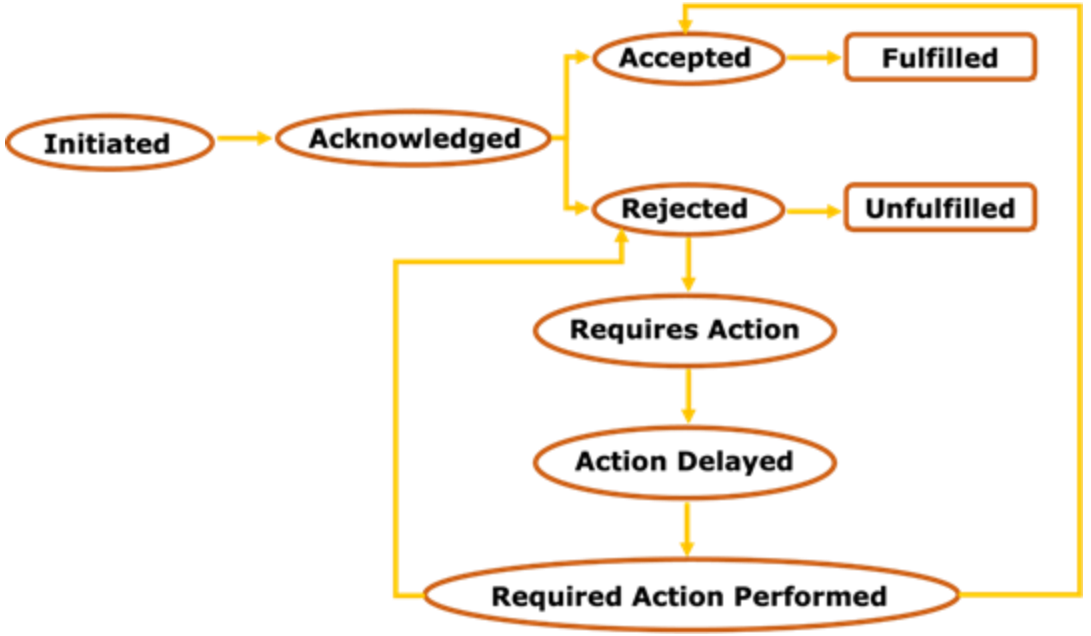
Time consuming
Inconsistent across platforms

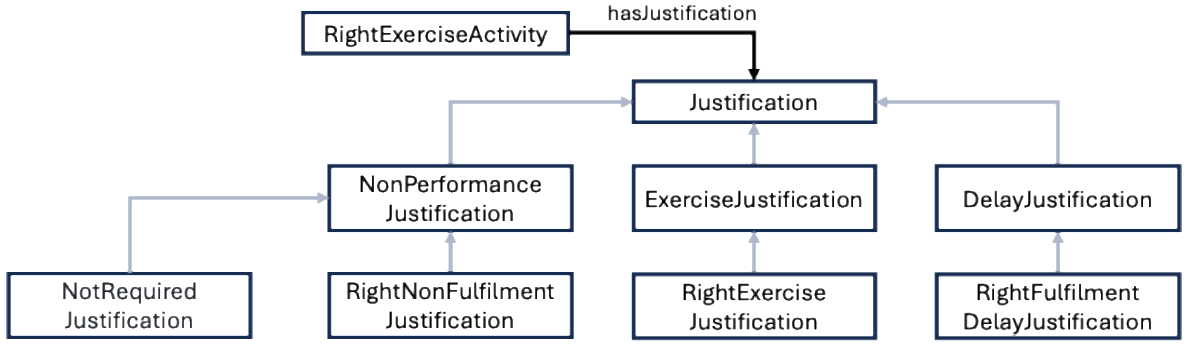
EXERCISING RIGHTS

M C1 C2 C3

R1. Linking personal data **processing activities** to **applicable rights**
R2. Providing **notices** related to said rights
R3. Documenting **activities** related to the **exercise of rights**
R4. GDPR rights as **executable requests**







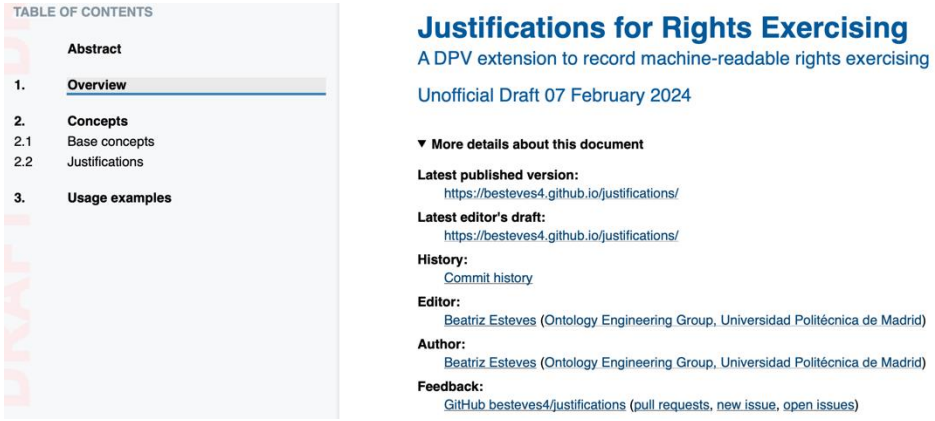


TABLE OF CONTENTS

Justifications for Rights Exercising

A DPV extension to record machine-readable rights exercising

Unofficial Draft 07 February 2024

▼ More details about this document

Latest published version:
https://besteves4.github.io/justifications/

Latest editor's draft:
https://besteves4.github.io/justifications/

History:
Commit history

Editor:
Beatriz Esteves (Ontology Engineering Group, Universidad Politécnica de Madrid)

Author:
Beatriz Esteves (Ontology Engineering Group, Universidad Politécnica de Madrid)

Feedback:
GitHub besteves4/justifications (pull requests, new issue, open issues)

http://w3id.org/people/besteves/justifications

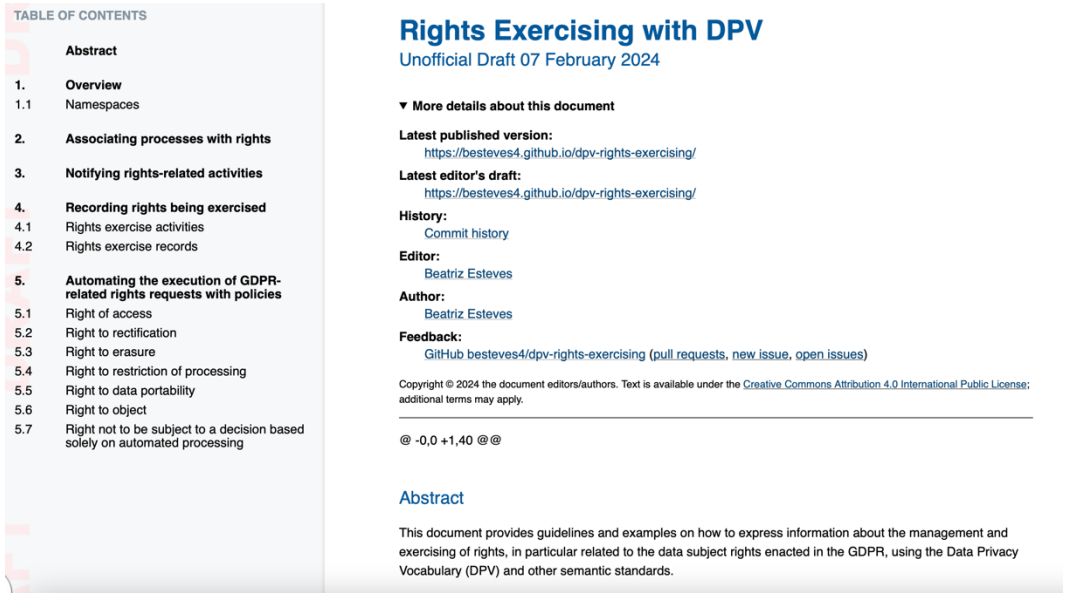


TABLE OF CONTENTS

Rights Exercising with DPV

Unofficial Draft 07 February 2024

▼ More details about this document

Latest published version:
https://besteves4.github.io/dpv-rights-exercising/

Latest editor's draft:
https://besteves4.github.io/dpv-rights-exercising/

History:
Commit history

Editor:
Beatriz Esteves

Author:
Beatriz Esteves

Feedback:
GitHub besteves4/dpv-rights-exercising (pull requests, new issue, open issues)

@ -0,0 +1,40 @@@

Abstract

This document provides guidelines and examples on how to express information about the management and exercising of rights, in particular related to the data subject rights enacted in the GDPR, using the Data Privacy Vocabulary (DPV) and other semantic standards.

http://w3id.org/people/besteves/rights

State of the art 'Justifications' taxonomy with 62 terms (already integrated into DPV)

```
ex:RejectRightToErasure a dpv:RightNonFulfilmentNotice ;
    dcterms:issued "2024-09-06"^^xsd:date ;
    dcterms:description "Notice of non-fulfillment related to an exercised right to erasure" ;
    dcterms:identifier "x4ghyun-658393" ;
    dcterms:language "EN" ;
    dcterms:publisher ex:DataController ;
    dpv:hasRight eu-gdpr:A17 ;
    dpv:hasDataController ex:DataController ;
    dpv:isImplementedByEntity ex:DataController ;
    foaf:page <https://example.org/DataController/RejectRightToErasure> ;
    dpv:hasRecipient ex:DataSubject ;
    dpv:hasStatus dpv:RequestUnfulfilled ;
    dpv:hasJustification justifications:FreedomOfExpressionImpaired .

ex:DataSubject a dpv:DataSubject .
```

Beatriz Esteves, Victor Rodriguez-Doncel, and Ricardo Longares. **Automating the Response to GDPR's Right of Access**. In *Legal Knowledge and Information Systems*, pages 170–175. IOS Press, 2022. doi: 10.3233/FAIA220462.

Beatriz Esteves, Harshvardhan J. Pandit, Georg P. Krog, and Paul Ryan. **How to Manage My Data? With Machine–Interpretable GDPR Rights!** In *Legal Knowledge and Information Systems*, 269–74. IOS Press, 2024. doi: 10.3233/FAIA241254.

ONTOLOGY EVALUATION

Ontology	FOOPS! score	Findable	Accessible	Interoperable	Reusable
OAC	91%	8/9	2/3	3/3	8.83/9
PLASMA	91%	8/9	2/3	3/3	8.83/9
DPV	64%	5.33/9	2/3	3/3	4.92/9
ODRL	64%	4.5/9	3/3	3/3	4.75/9
DCAT	64%	4.33/9	3/3	3/3	5.14/9
ACP	52%	5.33/9	2/3	2/3	3.12/9
ActivityStreams	19%	2/9	1.5/3	0/3	1/9
ACL	2%	0/9	0.5/3	0/3	0/9
DCMI	2%	0/9	0.5/3	0/3	0/9

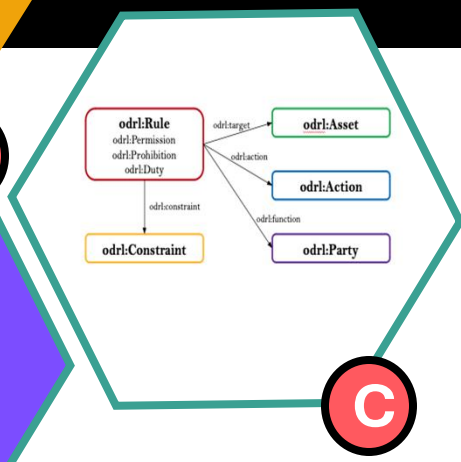
Legal terms validated by legal scholars and Data Protection Officers and integrated into the outcomes of the W3C DPVCG

Validation of OAC's competency questions with SPARQL queries.

CQO*	SPARQL query
CQO1	SELECT ?policy WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . }
CQO2	SELECT ?action WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:permission|odrl:prohibition ?rule . ?rule odrl:action ?action . }
CQO3	SELECT ?data WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:permission|odrl:prohibition ?rule . ?rule odrl:target ?data . }
CQO4	SELECT ?constraint WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:permission ?rule . ?rule odrl:constraint ?constraint . }
CQO5	SELECT ?assigner ?assignee WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:permission|odrl:prohibition ?rule . OPTIONAL { ?rule odrl:assigner ?assigner } . OPTIONAL { ?rule odrl:assignee ?assignee } . }
CQO6	SELECT ?conflict_term WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:conflict ?conflict_term . }
CQO7	SELECT ?context WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:permission|odrl:prohibition ?rule . ?rule dpv:hasContext ?context . }
CQO8	SELECT ?legal_basis WHERE { ?policy_uri a ?policy . ?policy_uri odrl:uid ?policy_id . ?policy_uri odrl:permission|odrl:prohibition ?rule . ?rule odrl:constraint ?constraint . ?constraint odrl:leftOperand oac:LegalBasis . ?constraint odrl:rightOperand ?legal_basis . }
CQO9	SELECT ?entity ?address ?contact ?name WHERE { ?entity a oac:Entity . ?entity dpv:hasAddress ?address . ?entity dpv:hasContact ?contact . ?entity dpv:hasName ?name . }

THESIS OVERVIEW

SEMANTIC WEB



A **Introduction** A1 A2 A3

B **State of the art** B1 B2 B3

C **Vocabularies for personal data stores** C1 C2 C3

D **Legal challenges**

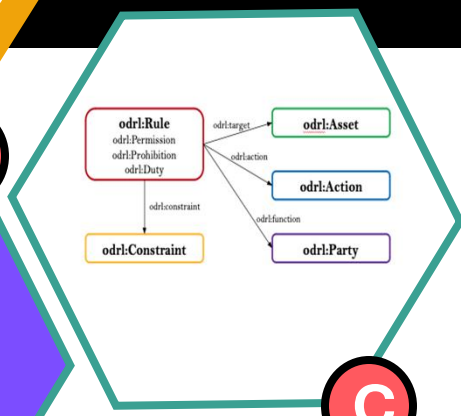
E **Policy-based algorithms**

F **Exploring the DGA**

G **Conclusion**

THESIS OVERVIEW

SEMANTIC WEB



A Introduction A1 A2 A3

B State of the art B1 B2 B3

C Vocabularies for personal data stores C1 C2 C3

D Legal challenges

- D1 – PIMS as a Legal-Tech tool
- D2 – Policies as a precursor of consent
- D3 – Automation of consent
- D4 – Exceptions

E Policy-based algorithms

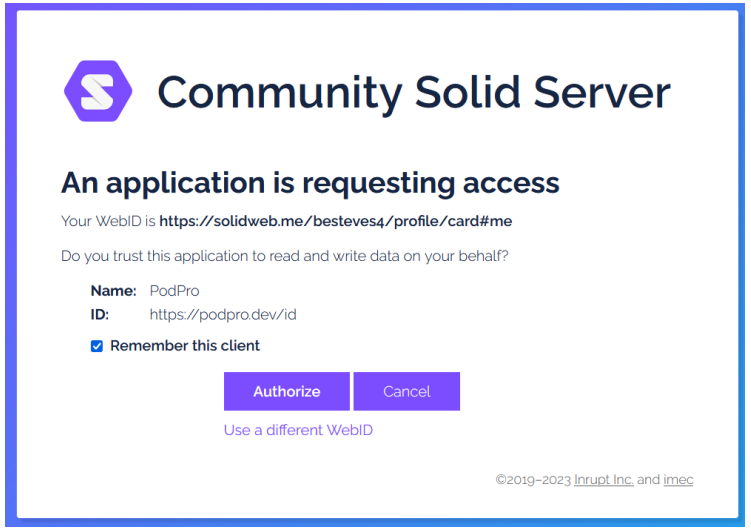
F Exploring the DGA

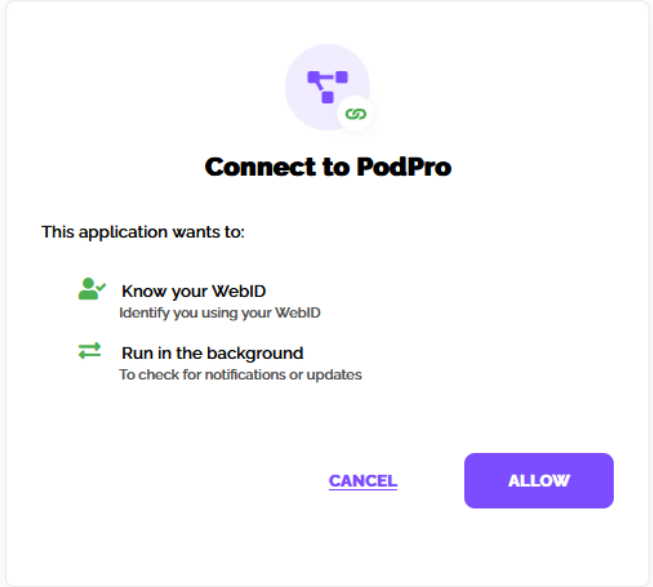
G Conclusion

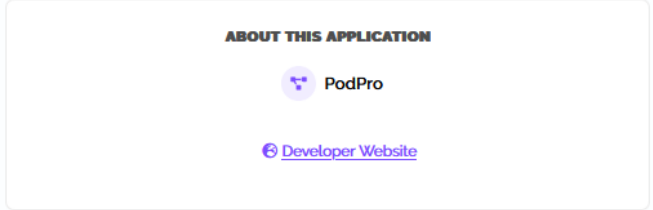
PIMS AS A LEGAL-TECH TOOL

"PIMS provide features for individuals to be able to access their personal data, as well as to rectify or erase them, as provided for by the GDPR, either because the data are in repositories under their direct control or because all shared data are linked to a source, which is again in the control of the individual."

EDPS TechDispatch #3/2020 – PIMS [Source]







Beatriz Esteves, Haleh Asgarinia, Andres Chomczyk Penedo, Blessing Mutiro, and Dave Lewis. **Fostering trust with transparency in the data economy era: an integrated ethical, legal, and knowledge engineering approach**. In *1st International Workshop on Data Economy*, pages 57–63. ACM, 2022. doi: 10.1145/3565011.3569061.

Haleh Asgarinia, Andres Chomczyk Penedo, Beatriz Esteves, and Dave Lewis. **"Who Should I Trust with My Data?" Ethical and Legal Challenges for Innovation in New Decentralized Data Management Technologies**. *Information 14(7)*, 2023. doi: 10.3390/info14070351.

Marcu Florea and Beatriz Esteves. **Is Automated Consent in Solid GDPR-Compliant? An Approach for Obtaining Valid Consent with the Solid Protocol**. *Information 14(12)*, 2023. doi: 10.3390/info14120631.

Is this enough for Solid users to know what is happening to their data? Is it enough to comply with GDPR's requirements?

POLICIES AS A PRECURSOR OF CONSENT


```
<https://example.com/agreement1> a odrl:Agreement ;
  odrl:profile oac: ;
  dct:description "Agreement to read physical trait data in a R&D
  ↪  project" ;
  dct:creator ex:userA ;
  dct:issued "2022-11-08T18:13:37"^^xsd:dateTime ;
  odrl:uid ex:agreement1 ;
  dct:references ex:offer1, ex:request1 ;
  dpv:hasDataSubject ex:userA ;
  dpv:hasDataController ex:userB ;
  dpv:hasLegalBasis dpv:Consent ;
  odrl:permission [
    odrl:assigner ex:userA ;
    odrl:assignee ex:userB ;
    odrl:action oac:Read ;
    odrl:target oac:PhysicalTrait ;
    odrl:constraint [
      dct:title "Purpose for processing is to conduct research in the R&D
      ↪  project X." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:eq ;
      odrl:rightOperand ex:RDProjectX ] ] .
```

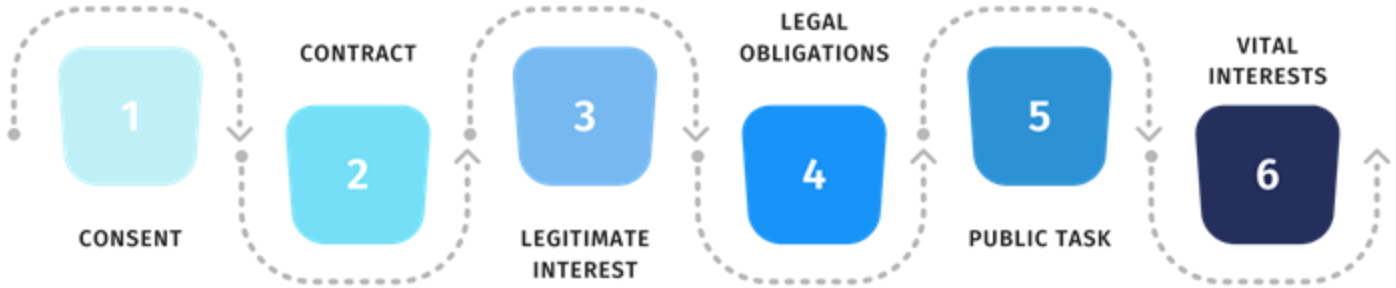
"the data subject has, by active behaviour, given his or her consent to the processing of his or her personal data and that he or she has obtained, beforehand, information relating to all the circumstances surrounding that processing, in an intelligible and easily accessible form, using clear and plain language, allowing that person easily to understand the consequences of that consent, so that it is given with full knowledge of the facts"

Case C-61/19 held in 2020 at the European Court of Justice [Source]

foiman.com

Can consent be automated?

No, but that's ok!



dataprivacymanager.net

```
<https://example.com/agreement2> a odrl:Agreement, plasma:DataAgreement ;
  odrl:profile oac: ;
  dct:description "Agreement to read age data for academic research based on a contract." ;
  dct:creator ex:userA ;
  dct:issued "2022-11-14T01:11:29"^^xsd:dateTime ;
  odrl:uid ex:agreement2 ;
  dct:references ex:offer2, ex:request2 ;
  dpv:hasDataSubject ex:userA ;
  dpv:hasDataController ex:userB ;
  dpv:hasLegalBasis dpv:Contract ;
  odrl:permission [
    odrl:assigner ex:userA ;
    odrl:assignee ex:userB ;
    odrl:action oac:Read ;
    odrl:target oac:Contact ;
    odrl:constraint [
      dct:title "Purpose for access is to conduct research in the academic project X, conducted in University Y." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:eq ;
      odrl:rightOperand ex:AcademicResearchProjectX ] ] .
```

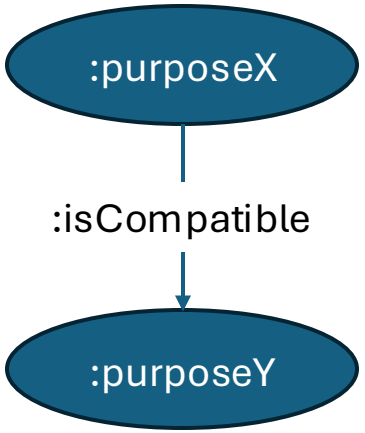
AUTOMATION OF CONSENT

Compatibility of purposes

Processing of personal data for purposes that are incompatible with the purpose specified at the time of data collection are prohibited

↓

If the purposes are found to be compatible but there is no legal basis for processing, either renewed consent must be obtained or an alternative legal basis must be identified.



Delegation

Consenting to the use of personal data

↓

Consenting to the use of privacy agent

"a dedicated software that would work as a surrogate and automatically manage consent on behalf of the data subject".

Le Métayer and Monteleone, 2009

Agent's actions MUST reflect user preferences

↓

Data controller MUST demonstrate compliance

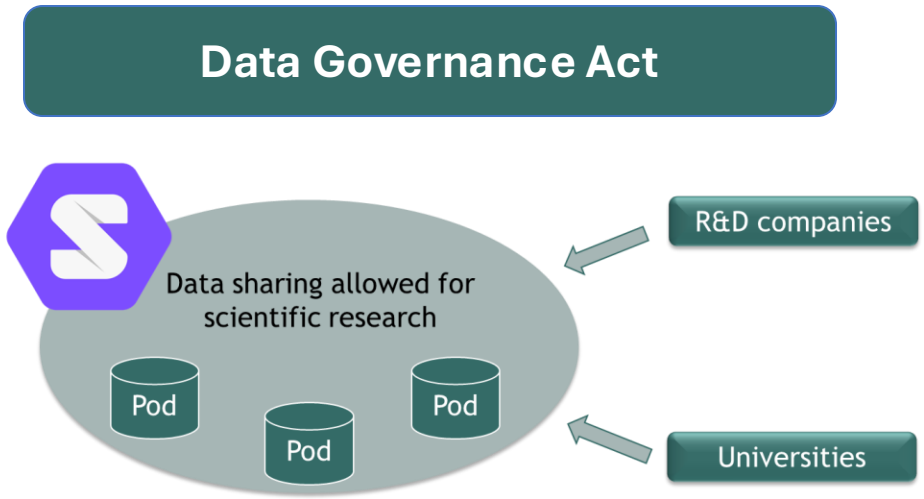
↓

Documenting matching process and its outcomes MAY infringe user's privacy

EXCEPTIONS

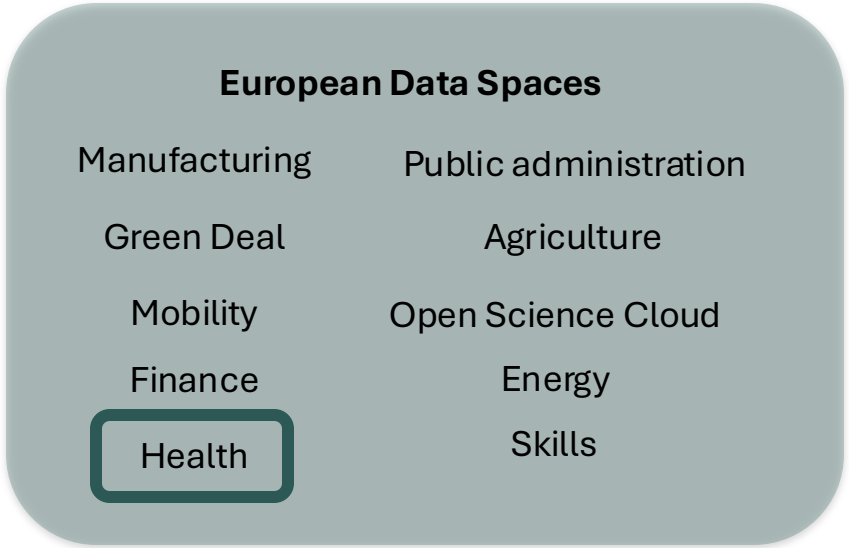
"further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')"

GDPR Article 5(1)(b)



Policies for the (re)use of data

- Permissions and duties for the processing of public-sector data
- Conditions for data sharing by intermediation services
- Policies to share data for altruistic purposes



Article 34

Purposes for which electronic health data can be processed for secondary use

1. Health data access bodies shall only provide access to electronic health data referred to in Article 33 where the intended purpose of processing pursued by the applicant complies with:

(a) activities for reasons of public interest in the area of public and occupational health, such as protection against serious cross-border threats to health, public health surveillance or ensuring high levels of quality and safety of healthcare and of medicinal products or medical devices;

(b) to support public sector bodies or Union institutions, agencies and bodies including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandates;

(c) to produce national, multi-national and Union level official statistics related to health or care sectors;

(d) education or teaching activities in health or care sectors;

(e) scientific research related to health or care sectors;

(f) development and innovation activities for products or services contributing to public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;

(g) training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices;

(h) providing personalised healthcare consisting in assessing, maintaining or restoring the state of health of natural persons, based on the health data of other natural persons.

THESIS OVERVIEW

A Introduction

B State of the art

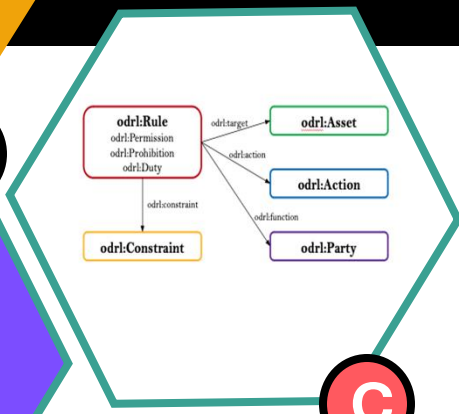
C Vocabularies for personal data stores

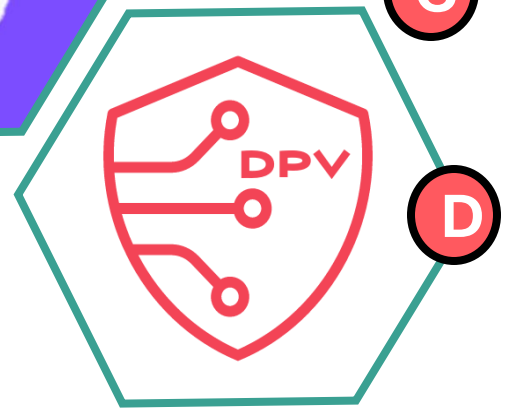
D Legal challenges

E Policy-based algorithms

F Exploring the DGA

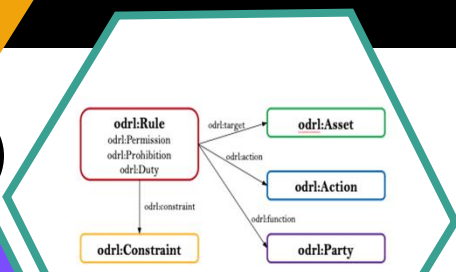
G Conclusion

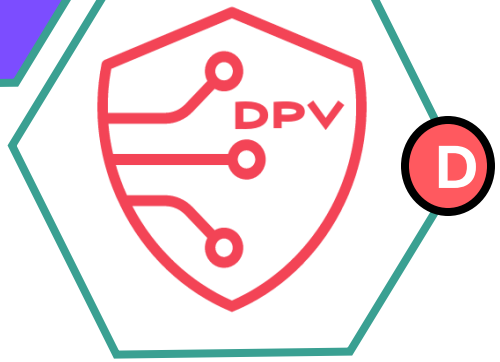




THESIS OVERVIEW

SEMANTIC WEB





A Introduction A1 A2 A3

B State of the art B1 B2 B3

C Vocabularies for personal data stores C1 C2 C3

D Legal challenges D1 D2 D3 D4

E Policy-based algorithms

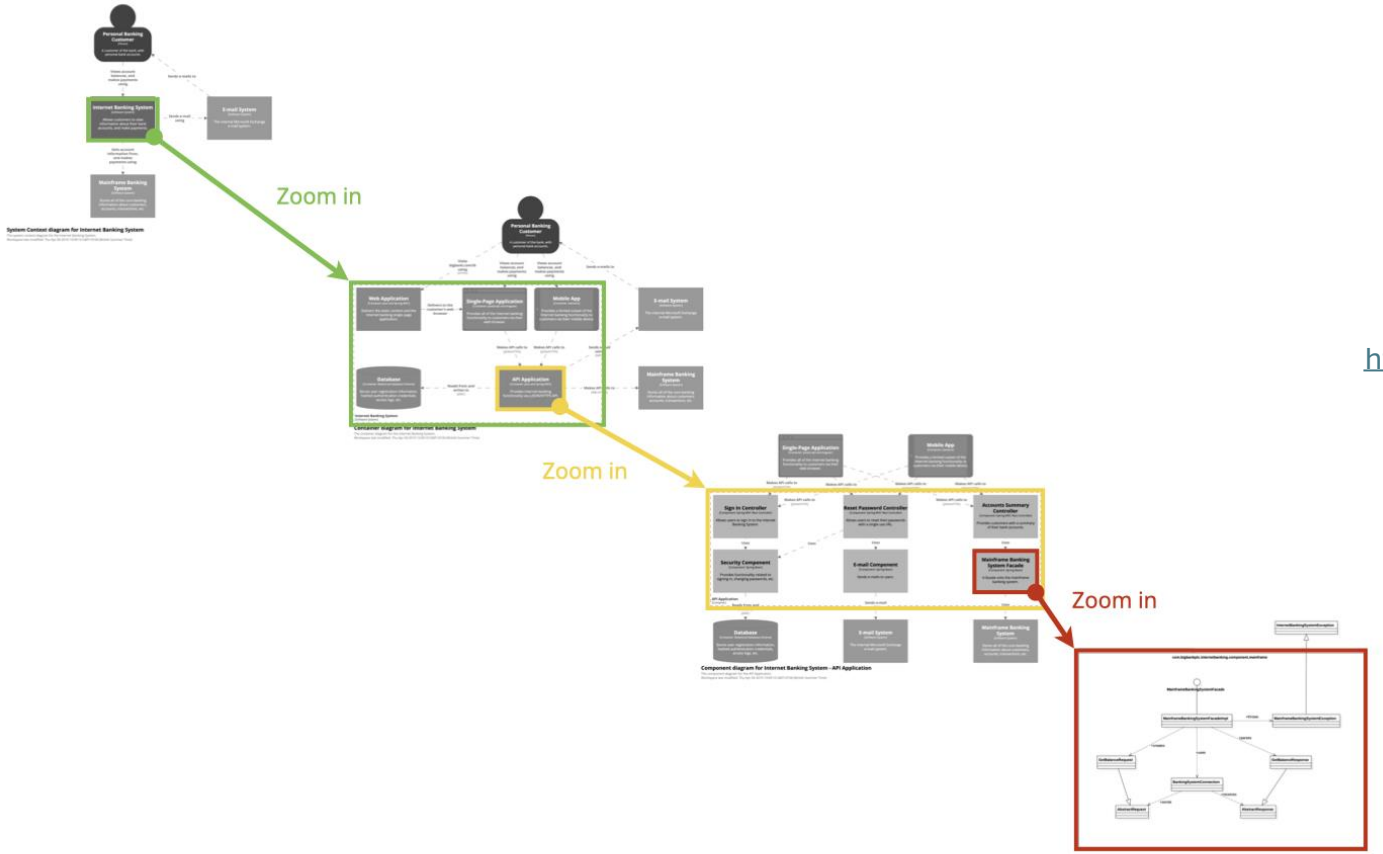
- E1 – Policy-based architecture
- E2 – Policy matching algorithm
- E3 – PoC for health data sharing

F Exploring the DGA

G Conclusion

C4 graphical notation model

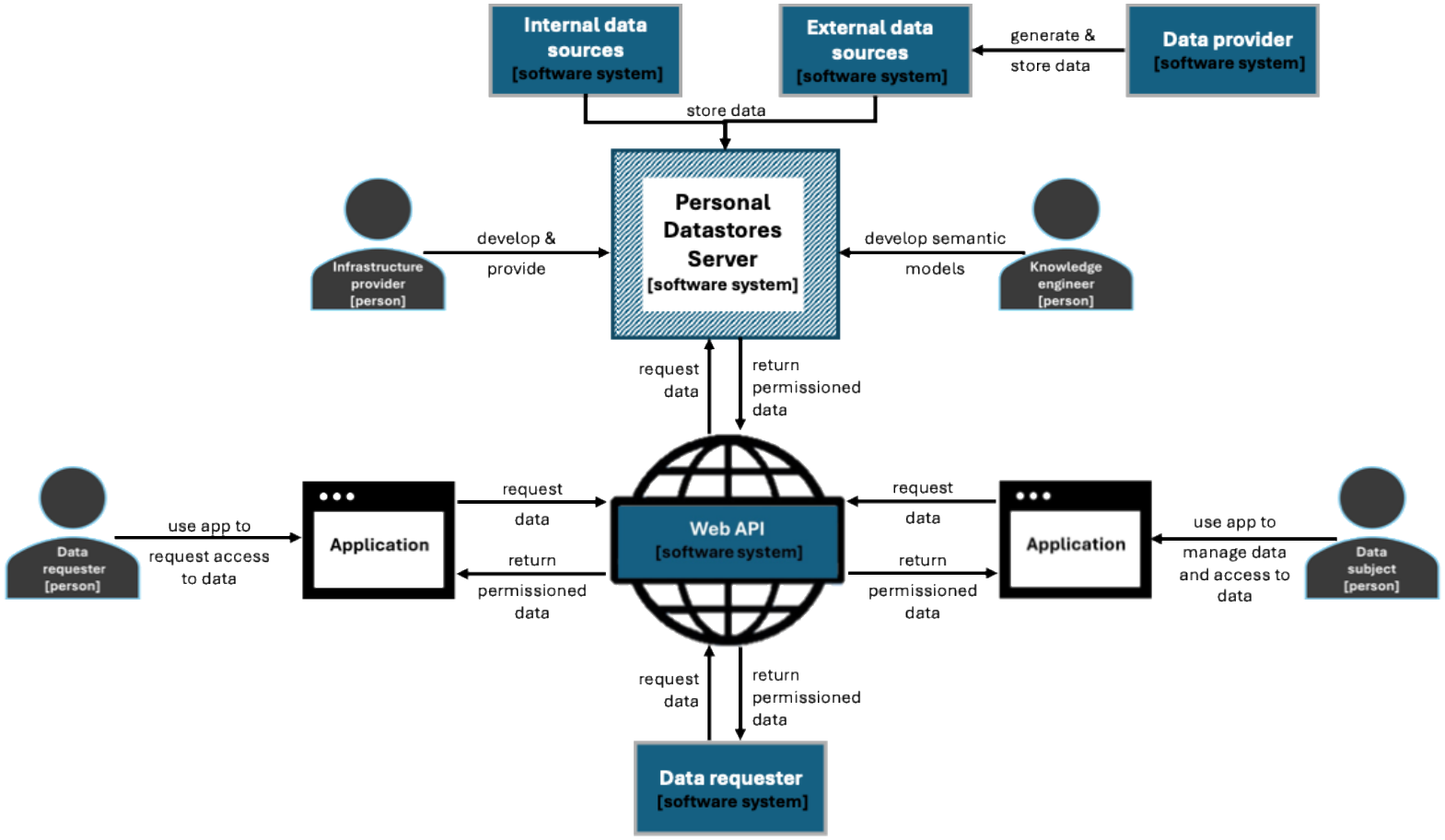
Simon Brown. **The C4 model for visualising software architecture**. *Leanpub*, 2015. URL: https://leanpub.next/visualising-software-architecture.



https://c4model.com

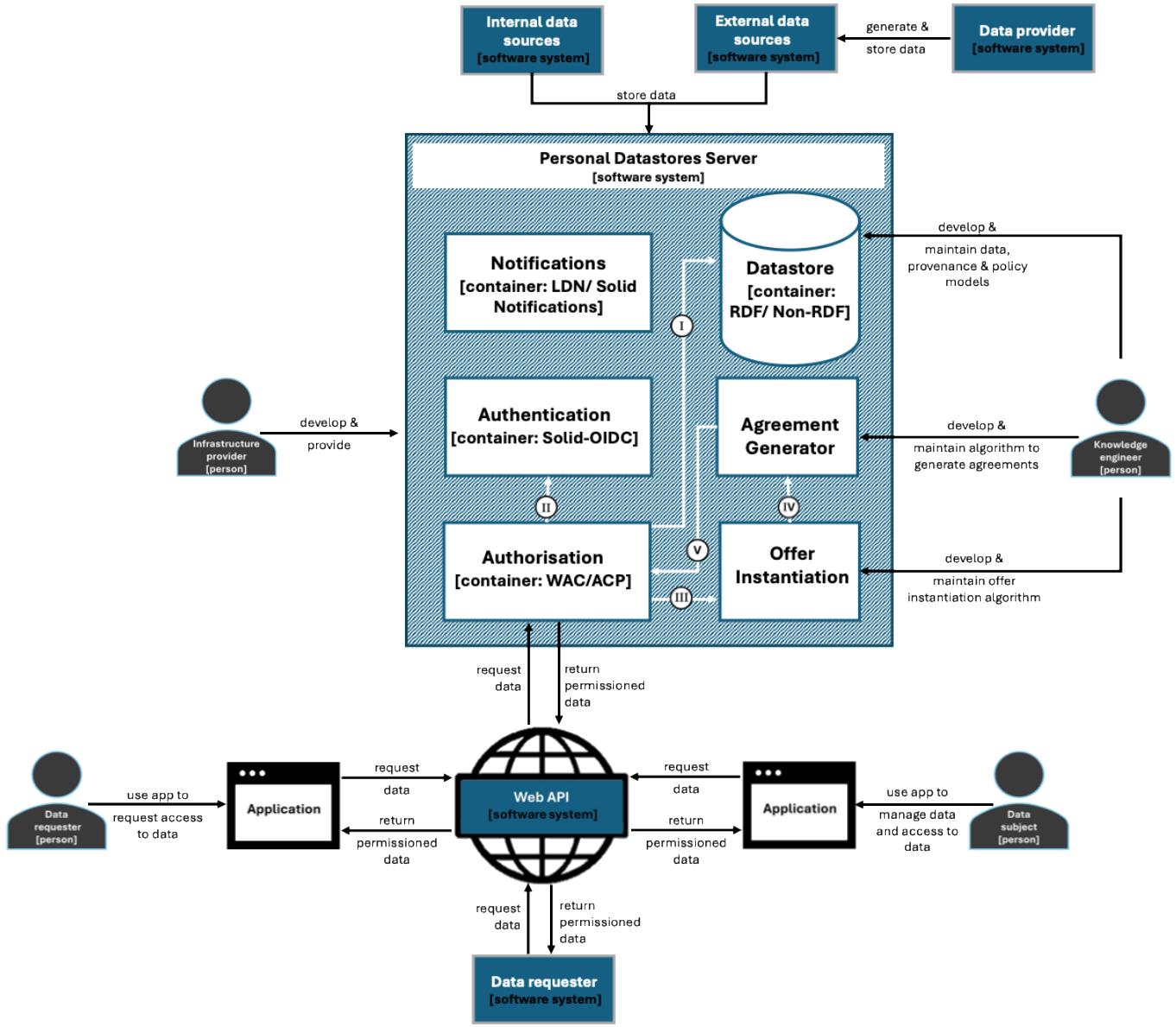
POLICY-BASED ARCHITECTURE - CONTEXT

E1 E2 E3

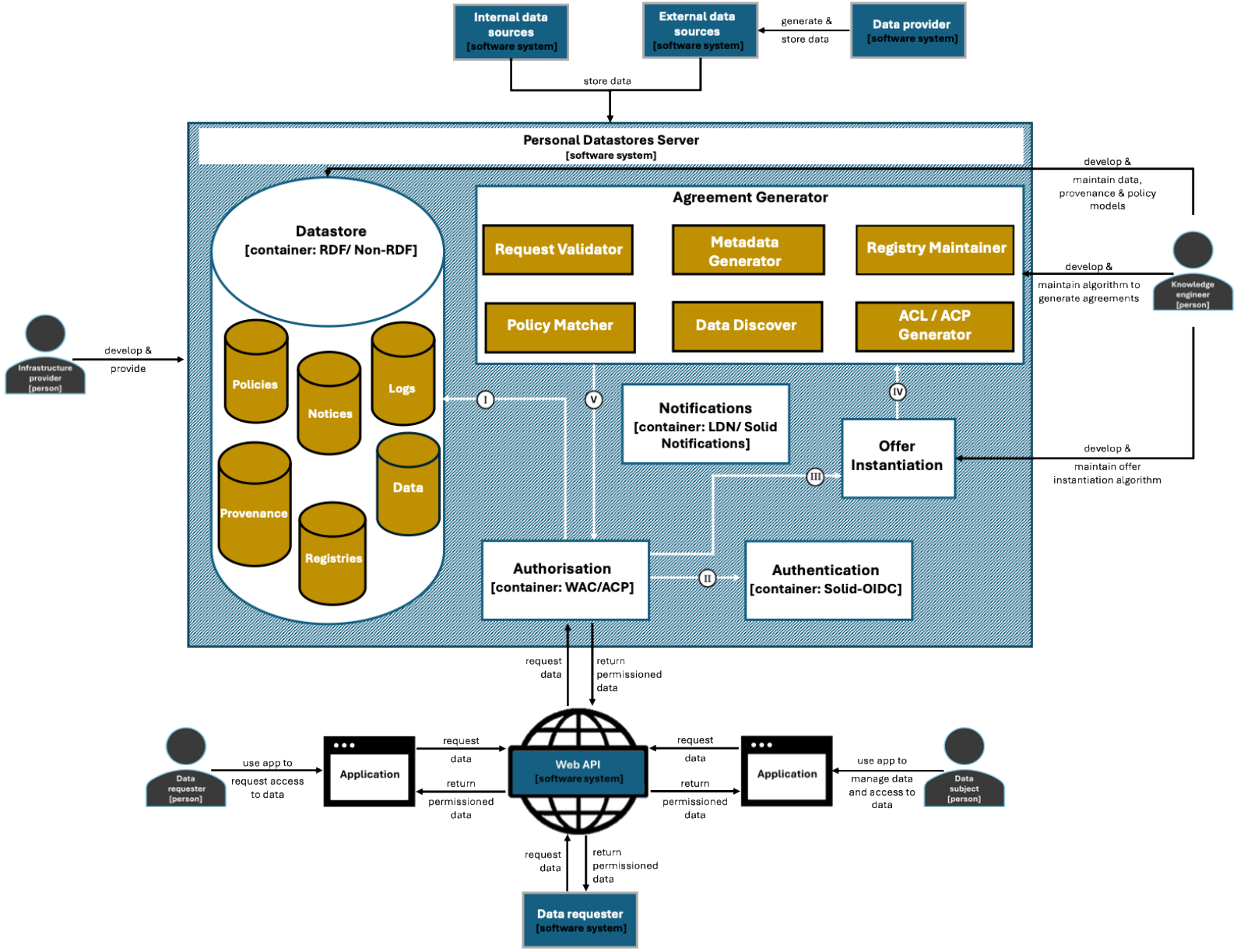


POLICY-BASED ARCHITECTURE - CONTAINER

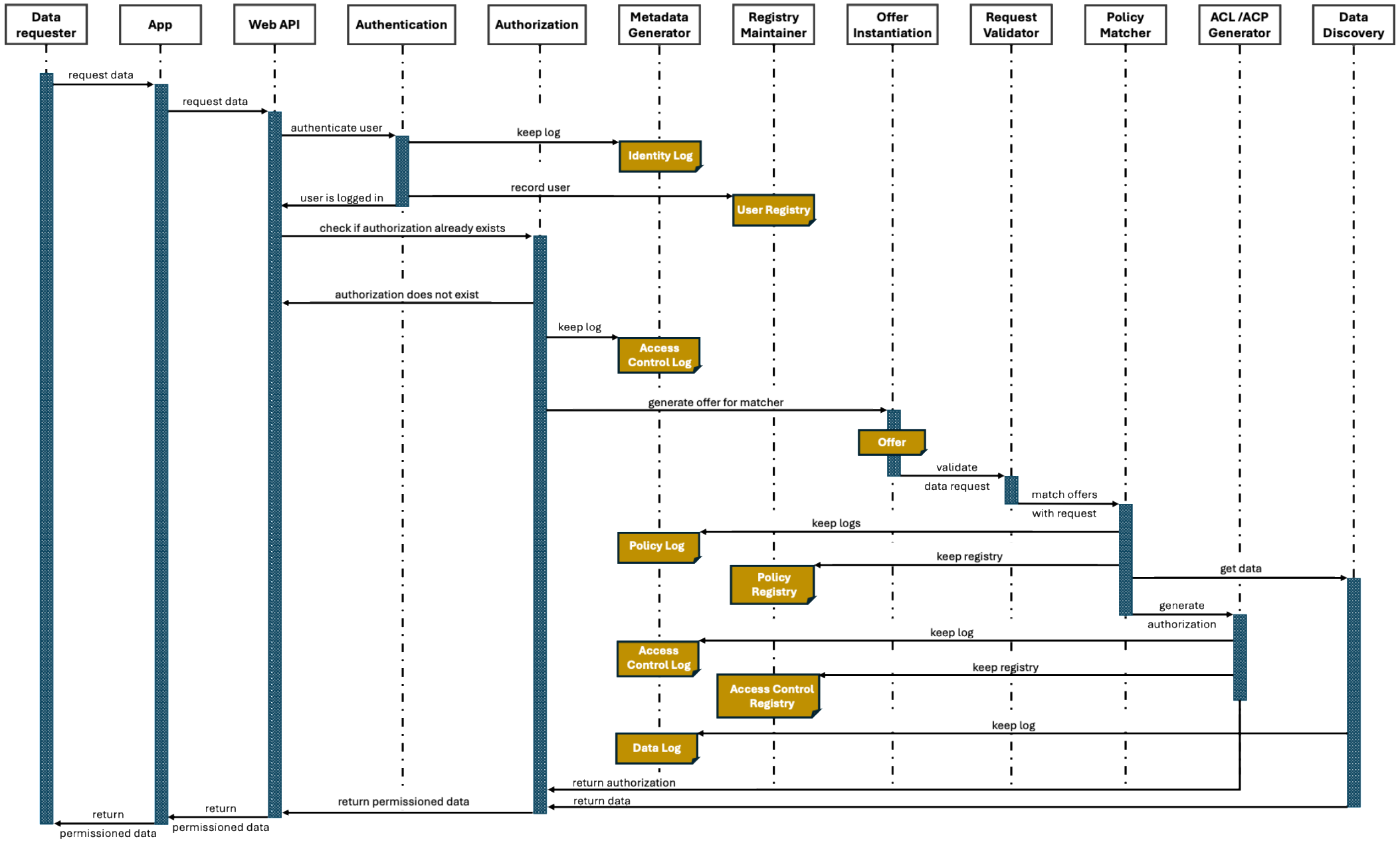
E1 E2 E3



POLICY-BASED ARCHITECTURE - COMPONENT



POLICY-BASED ARCHITECTURE - CODE



POLICY MATCHING ALGORITHM

1. Retrieve the data requester's odrl:Request and the user policy's odrl:Offer.
2. Match the odrl:Offer with the odrl:Request.
3. Record the outcome of the matching algorithm as an odrl:Agreement.
4. If the matching result is positive, i.e., the request and the offer are compatible, then access is permitted; if negative then access is denied.
5. Associate the agreement with the odrl:Offer and odrl:Request that were used to generate it.
6. Include provenance and other relevant information to document the creation and acceptance of the agreement among the parties.

Offer			Request		Outcome	
Rule	Purpose	Data	Purpose	Data	Decision	Reason
Prohibition	Academic research	Contact	Research and development	Age	DENY	request purpose ∩ offer purpose ≠ ∅
Prohibition	Academic research	Age range	Payment	Age	DENY	request data ∩ offer data ≠ ∅
Prohibition	Academic research	Contact	Payment	Age	GRANT	request purpose ∩ offer purpose = ∅ request data ∩ offer data = ∅
Permission	Academic research	Age	Commercial research	Age	DENY	request purpose ∉ offer purpose
Permission	Research and development	Age	Academic research	Age range	GRANT	request purpose ⊆ offer purpose request data ∩ offer data ≠ ∅

for *prohibition* ← *odrl:Offer* **do**
  if *offer:target* ∩ *request:target* ≠ ∅ **then** *decision* ← *DENY*
  if *odrl:assignee* ∈ *offer:prohibition* **then**
    if *offer:assignee* ≡ *request:assignee* **then** *decision* ← *DENY*
  if *odrl:action* ∈ *offer:prohibition* **then**
    if *offer:action* ∩ *request:action* ≠ ∅ **then** *decision* ← *DENY*
  for *constraint* ← *prohibition* **do**
    if *oac:Purpose* ← *constraint* **then**
      if *offer:Purpose* ∩ *request:Purpose* ≠ ∅ **then** *decision* ← *DENY*
    else if *oac:Recipient* ← *constraint* **then**
      if *offer:Recipient* ∩ *request:Recipient* ≠ ∅ **then** *decision* ← *DENY*
    else if *oac:LegalBasis* ← *constraint* **then**
      if *offer:LegalBasis* ∩ *request:LegalBasis* ≠ ∅ **then** *decision* ← *DENY*
    else if *oac:TOM* ← *constraint* **then**
      if *offer:TOM* ∩ *request:TOM* ≠ ∅ **then** *decision* ← *DENY*
    else if *oac:Technology* ← *constraint* **then**
      if *offer:Technology* ∩ *request:Technology* ≠ ∅ **then** *decision* ← *DENY*
    else if *oac:IdP* ← *constraint* **then**
      if *offer:IdP* ∩ *request:IdP* ≠ ∅ **then** *decision* ← *DENY*
for *permission* ← *odrl:Offer* **do**
  if *offer:target* ∩ *request:target* = ∅ **then** *decision* ← *DENY*
  if *odrl:assignee* ∈ *offer:permission* **then**
    if *offer:assignee* ∉ *request:assignee* **then** *decision* ← *DENY*
  if *odrl:action* ∈ *offer:permission* **then**
    if *offer:action* ∩ *request:action* = ∅ **then** *decision* ← *DENY*
  for *constraint* ← *permission* **do**
    if *oac:Purpose* ← *constraint* **then**
      if *request:Purpose* ∉ *offer:Purpose* **then** *decision* ← *DENY*
    else if *oac:Recipient* ← *constraint* **then**
      if *request:Recipient* ∉ *offer:Recipient* **then** *decision* ← *DENY*
    else if *oac:LegalBasis* ← *constraint* **then**
      if *request:LegalBasis* ∉ *offer:LegalBasis* **then** *decision* ← *DENY*
    else if *oac:TOM* ← *constraint* **then**
      if *request:TOM* ∉ *offer:TOM* **then** *decision* ← *DENY*
    else if *oac:Technology* ← *constraint* **then**
      if *request:Technology* ∉ *offer:Technology* **then** *decision* ← *DENY*
    else if *oac:IdP* ← *constraint* **then**
      if *request:IdP* ∉ *offer:IdP* **then** *decision* ← *DENY*
if ∄*DENY* **then** *decision* ← *GRANT*

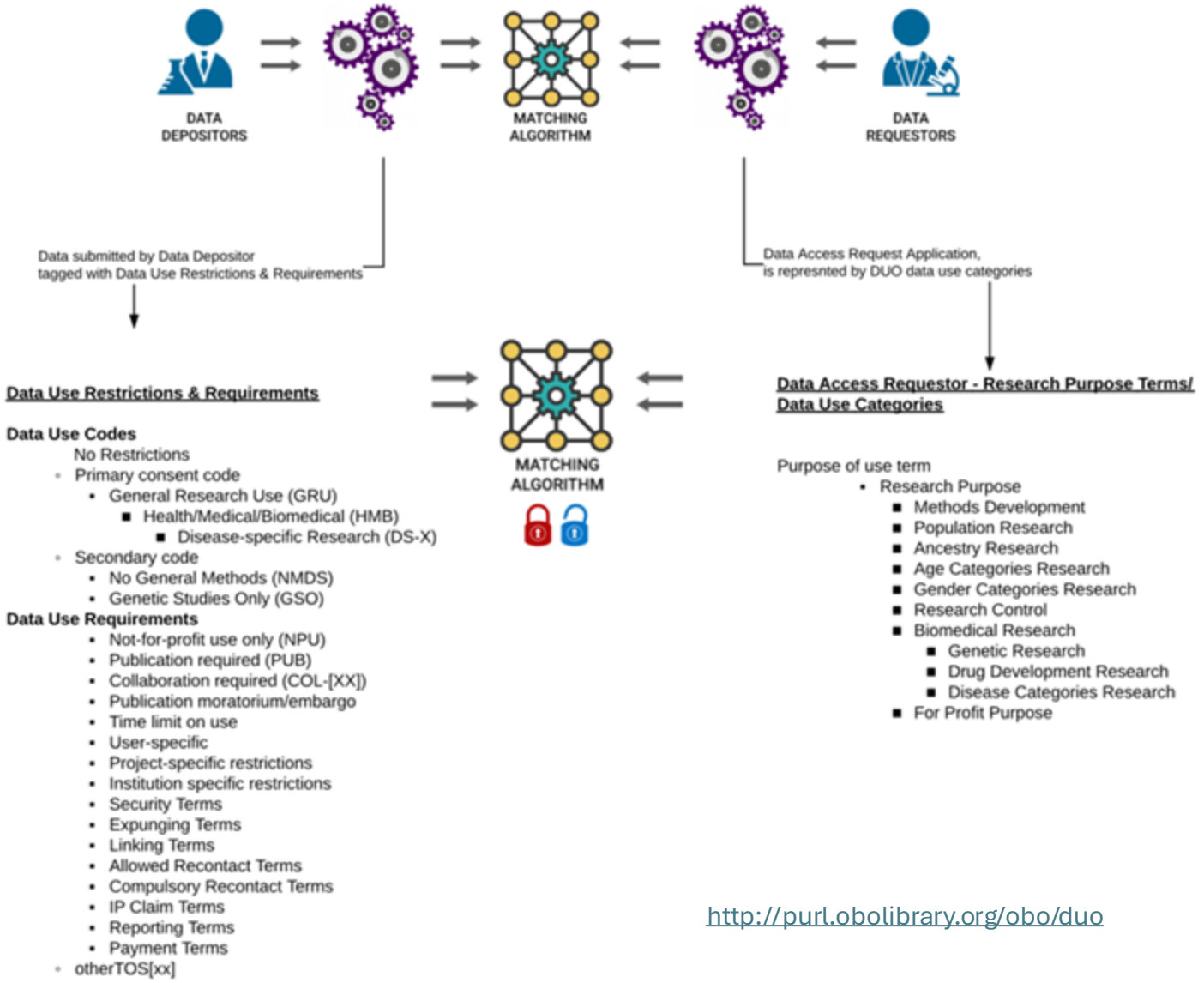
POC FOR HEALTH DATA SHARING

The (GA4GH) Data Use Ontology (DUO) includes terms describing data use conditions, particularly for research data in the health/clinical/biomedical domain.

Datasets are annotated with semantic information using DUO, and then this is used to 'match' available data with requests using a matching algorithm.

DUO uses OWL (so it is semantic-aware), however, it defines usage conditions as human-readable labels.

```
<http://purl.obolibrary.org/obo/DUO_00000044>
   a owl:Class ;
   rdfs:label "population origins or ancestry
      research prohibited" .
```



http://purl.obolibrary.org/obo/duo

Re-modelling DUO concepts with ODRL

Harshvardhan J. Pandit and Beatriz 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.

Concept	Code	Rule Type	Constraint	Placeholder
DUO0000001	**Data Use Permission**			
DUO0000042	GRU	Permission	Purpose is :GRU	
DUO0000006	HMB	Permission	Purpose is :HMB and not :POA	
DUO0000007	DS	Permission	Purpose is :DS and mondo:0000001	:TemplateDisease
DUO0000004	NRES	Permission	Purpose is odrl:Purpose	
DUO0000011	POA	Permission	Purpose is :POA	
DUO0000011	POA	Prohibition	Purpose is not :POA	
DUO0000017	**Data Use Modifier**			
DUO0000043	CC	Permission	Purpose is :CC	
DUO0000020	COL	Duty	Action is :CollaborateWithStudyPI	
DUO0000021	IRB	Duty	Action is :ProvideEthicalApproval	
DUO0000016	GSO	Permission	Purpose is :GS or :GSG	
DUO0000016	GSO	Prohibition	Purpose is :GS and not :GSG	
DUO0000022	GS	Permission	Spatial is equal to specified :Location	:TemplateLocation
DUO0000022	GS	Prohibition	Spatial is not equal to specified :Location	:TemplateLocation
DUO0000028	IS	Permission	Assignee is :ApprovedInstitution	:TemplateInstitution
DUO0000028	IS	Prohibition	Assignee is not :ApprovedInstitution	:TemplateInstitution
DUO0000015	NMDS	Prohibition	Purpose is :MDS	
DUO0000018	NPUNCU	Permission	Assignee is :NonProfitOrganisation and Purpose is :NCU	
DUO0000018	NPUNCU	Prohibition	Assignee is :ForProfitOrganisation and Purpose is :NCU	
DUO0000018	NPUNCU	Prohibition	Assignee is :NonProfitOrganisation and Purpose is not :NCU	
DUO0000046	NCU	Permission	Purpose is :NCU	
DUO0000046	NCU	Prohibition	Purpose is not :NCU	
DUO0000045	NPU	Permission	Assignee is :NonProfitOrganisation	
DUO0000045	NPU	Prohibition	Assignee is :ForProfitOrganisation	
DUO0000044	NPOA	Prohibition	Purpose is :POA	
DUO0000027	PS	Permission	Project is :ApprovedProject	:TemplateProject
DUO0000027	PS	Prohibition	Project is not :ApprovedProject	:TemplateProject
DUO0000024	MOR	Duty	Action is odrl:distribute :ResultsOfStudies with odrl:dateTime	:TemplateDateTime
DUO0000019	PUB	Duty	Action is odrl:distribute :ResultsOfStudies	
DUO0000012	RS	Permission	Purpose is specified :Research	:TemplateResearch
DUO0000012	RS	Prohibition	Purpose is not specified :Research	:TemplateResearch
DUO0000029	RTN	Duty	Action is :ReturnDerivedOrEnrichedData	
DUO0000025	TS	Permission	Time is less than specified :TemplateDateTime	:TemplateDateTime
DUO0000026	US	Permission	Assignee is :ApprovedUser	:TemplateUser
DUO0000026	US	Prohibition	Assignee is not :ApprovedUser	:TemplateUser
OBI0000066	**Investigation**			
DUO0000034		Permission	Purpose is :AgeCategoryResearch	
DUO0000034		Permission	Age is specified :Age	:TemplateAgeCategory
DUO0000033		Permission	Purpose is :POA	
DUO0000037		Permission	Purpose is :HMB	
DUO0000040		Permission	Purpose is :DS and mondo:0000001	:TemplateDisease
DUO0000039		Permission	Purpose is :DrugDevelopment	
DUO0000038		Permission	Purpose is :GS	
DUO0000035		Permission	Purpose is :GenderCategoryResearch	
DUO0000035		Permission	Gender is specified :Gender	:TemplateGender
DUO0000031		Permission	Purpose is :MDS	
DUO0000032		Permission	Purpose is :PopulationGroupResearch	
DUO0000032		Permission	Population is specified :Population	:TemplatePopulation
DUO0000036		Permission	Purpose is :ResearchControl	

```
:DUO_0000011 a odrl:Set ;
    odrl:uid :DUO_0000011 ;
    rdfs:label "DUO_0000011" ;
    rdfs:comment "POA - population origins or ancestry research only" ;
    skos:exactMatch obo:DUO_0000042 ;
    odrl:permission [
        odrl:action odrl:use ;
        odrl:target :TemplateDataset ;
        odrl:constraint [
            odrl:leftOperand odrl:purpose ;
            odrl:operator odrl:isA ;
            odrl:rightOperand :POA ] ] ;
    odrl:prohibition [
        odrl:action odrl:use ;
        odrl:target :TemplateDataset ;
        odrl:constraint [
            odrl:leftOperand odrl:purpose ;
            odrl:operator :isNotA ;
            odrl:rightOperand :POA ] ] .
```

https://w3id.org/duodrl/repo

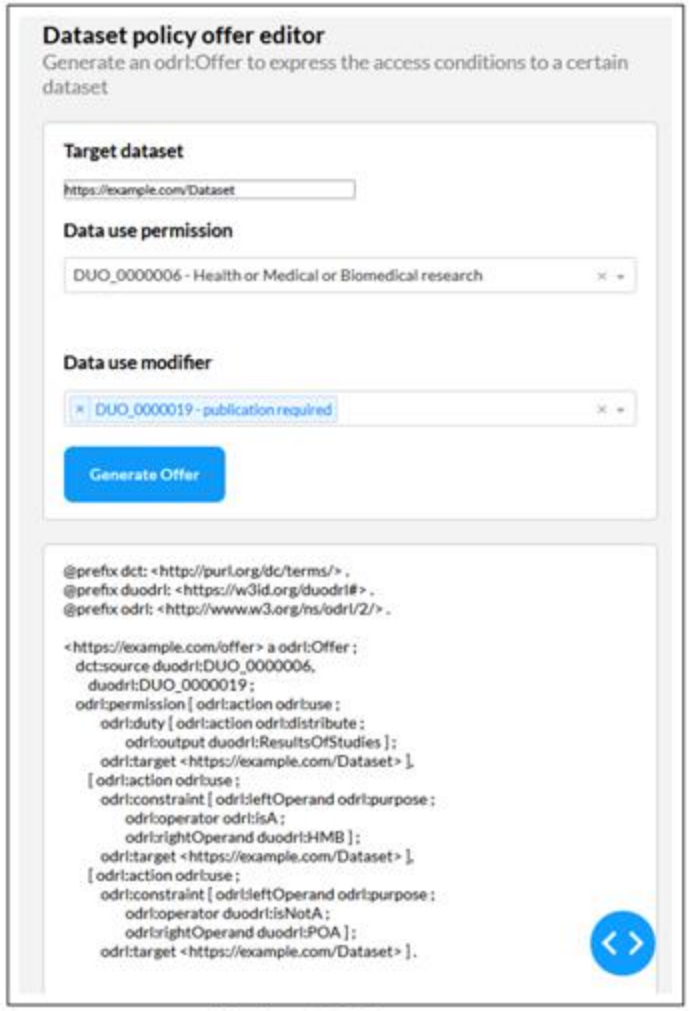
for *prohibition* ← *odrl:Offer* **do**
  if *odrl:assignee* ∈ *offer:prohibition* **then**
    if *offer:assignee* ≡ *request:assignee* **then** *decision* ← *DENY*
  for *constraint* ← *prohibition* **do**
    if *odr:spatial* ← *constraint* **then**
      if *offer:spatial* ∩ *request:spatial* ≠ ∅ **then** *decision* ← *DENY*
    else if *duodrl:Project* ← *constraint* **then**
      if *request:project* ∩ *offer:project* ≠ ∅ **then** *decision* ← *DENY*
    else if *odrl:dateTime* ← *constraint* **then**
      if *timeNow* < *moratoriumDate* **then** *decision* ← *DENY*
    else if *offer:purpose* ∩ *request:purpose* ≠ ∅ **then** *decision* ← *DENY*
for *permission* ← *odrl: Offer* **do**
  if *odrl:assignee* ∈ *offer:permission* **then**
    if *offer:assignee* ∉ *request: assignee* **then** *decision* ← *DENY*
  for *constraint* ← *permission* **do**
    if *odrl:dateTime* ← *constraint* **then**
      if *timeNow* > *timeLimit* **then** *decision* ← *DENY*
    else if *request:purpose* ∈ *groupResearchPurposes* **then**
      if *request:purpose* ∉ *offer:purpose* ⋁ *request:group* ∉ *offer:group* **then** *decision* ← *DENY*
    else if *request:purpose* ∉ *offer:purpose* **then** *decision* ← *DENY*
if ∄*DENY* **then** *decision* ← *GRANT*

Offer			Request		Outcome	
Rule	Purpose	Location	Purpose	Location	Decision	Reason
Permission	GS	Spain	GS	Europe	DENY	Europe ∉ Spain
Permission	GS	Europe	GS	Spain	GRANT	Spain ⊆ Europe
Prohibition	GS	Spain	GS	Europe	DENY	Europe ∩ Spain ≠ ∅
Prohibition	GS	Europe	GS	Spain	DENY	Spain ∩ Europe ≠ ∅
Prohibition	GS	UK	GS	Spain	GRANT	Spain ∩ UK = ∅
Permission	HMB		DS-Cancer		GRANT	DS-Cancer ⊆ HMB
Prohibition	DS-Cancer		HMB		DENY	HMB ∩ DS-Cancer ≠ ∅

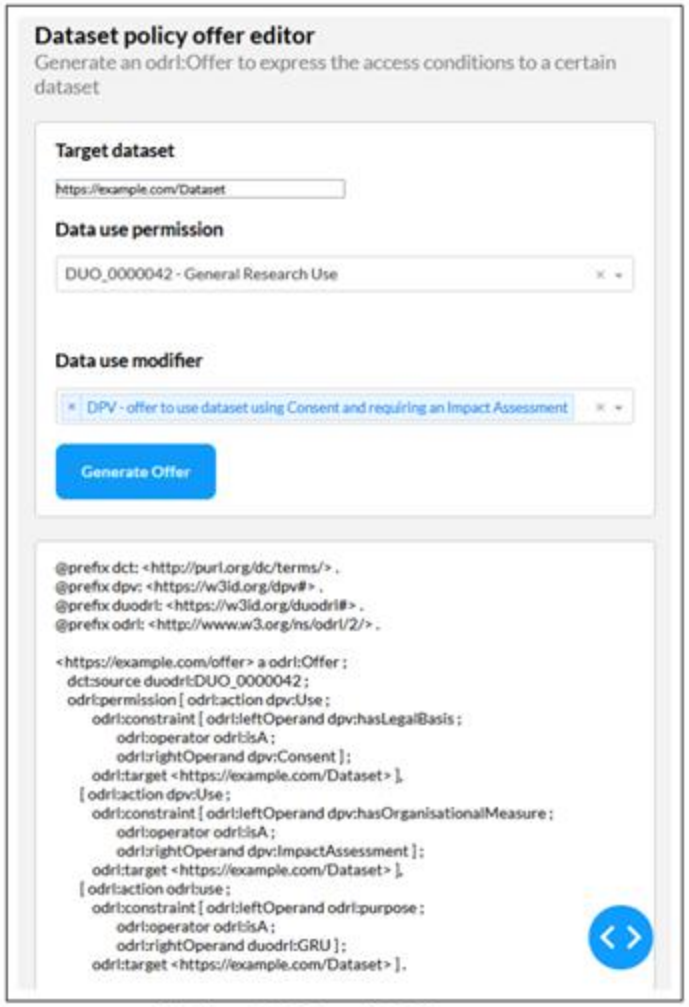
Legal compliance with OAC & DPV

```
ex:offer_agnostic a odrl:Offer ;
    odrl:uid ex:offer_agnostic ;
    odrl:profile oac: ;
    rdfs:label "Offer to use dataset for GRU using consent, and requiring
     ↪ an impact assessment" ;
    dcterms:source duodrl:DUO_0000042 ;
    dcterms:issued "2024-04-26"^^xsd:date ;
    odrl:target ex:EHR ;
    odrl:action oac:Use ;
    odrl:assigner ex:provider ;
    odrl:assignee ex:requester ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand oac:LegalBasis ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:Consent ] ] ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand oac:TechnicalOrganisationalMeasure ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:ImpactAssessment ] ] .
ex:offer_gdpr a odrl:Offer ;
    odrl:uid ex:offer_gdpr ;
    odrl:profile oac: ;
    rdfs:label "Offer to use dataset for GRU using GDPR's explicit
     ↪ consent, and requiring a DPIA" ;
    dcterms:source duodrl:DUO_0000042 ;
    dcterms:issued "2024-04-30"^^xsd:date ;
    odrl:target ex:EHR ;
    odrl:action oac:Use ;
    odrl:assigner ex:provider ;
    odrl:assignee ex:requester ;
    dpv:hasDataSubject ex:provider ;
    dpv:hasDataController ex:requester ;
    dpv:hasApplicableLaw legal-eu:law-GDPR ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand oac:LegalBasis ;
            odrl:operator odrl:isA ;
            odrl:rightOperand eu-gdpr:A6-1-a-explicit-consent ] ] ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand oac:TechnicalOrganisationalMeasure ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:DPIA ] ] .
```

POC FOR HEALTH DATA SHARING



(a) from DUO concepts



(b) from DUO and DPV concepts

	Algorithm approaches			
Feature	**Thesis**	**DUO**	**ACP**	**WAC**
Requirement	OAC	Data Use Permission, Data Use Modifier		
Preference	OAC			
Offer	ODRL		ACR	Authorisation
Request	ODRL	Investigation	Context	
Agreement	ODRL		Access grant	Authorisation
Permissions	ODRL	Data Use Permission	allow	✓
Prohibitions	ODRL	Data Use Modifier	deny	
Duties	ODRL	Data Use Modifier		
Data	OAC/DPV	*	*	*
Processing	OAC/DPV		Read, Write, Append, Control	Read, Write, Append, Control
Assigner	ODRL			
Assignee	ODRL	✓	agent	agent, agent group
Application	OAC		client	origin
Service	OAC			
Legal roles	OAC/DPV			
Purpose	OAC/DPV	✓		
Legal basis	OAC/DPV			
TOM	OAC/DPV	✓		
Technology	OAC/DPV			
Identity provider	OAC		issuer	
Spatial	ODRL	✓		
Project	DUODRL	✓		
Temporal	ODRL	✓		
Disease	DUODRL	✓		
Gender	DUODRL	✓		
Age	DUODRL	✓		
Population	DUODRL	✓		

https://w3id.org/duodrl/app

THESIS OVERVIEW

A Introduction

B State of the art

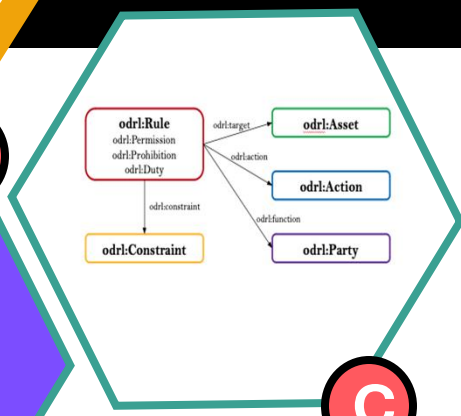
C Vocabularies for personal data stores

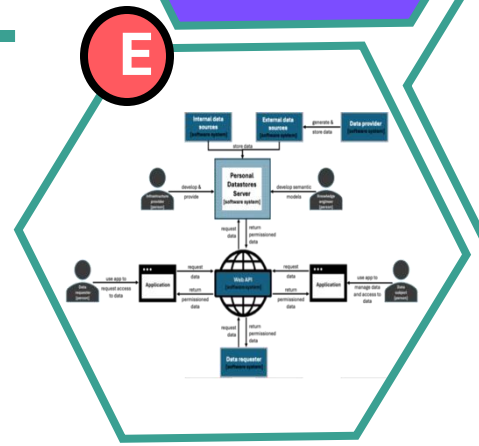
D Legal challenges

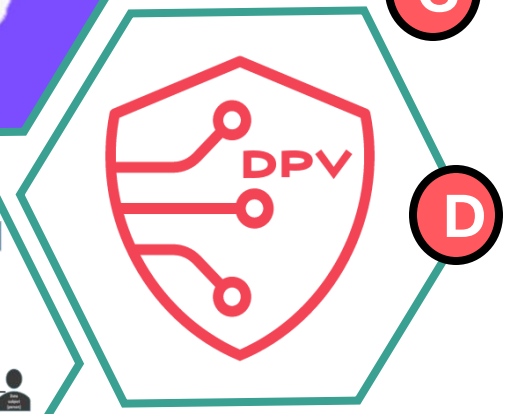
E Policy-based algorithms

F Exploring the DGA

G Conclusion



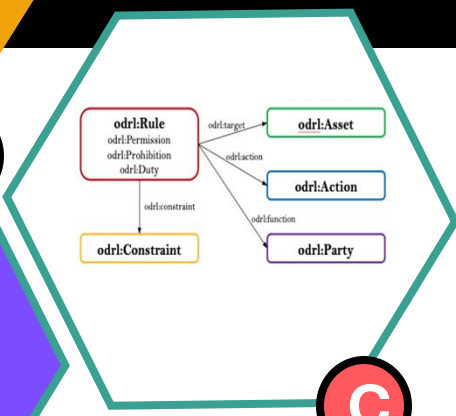


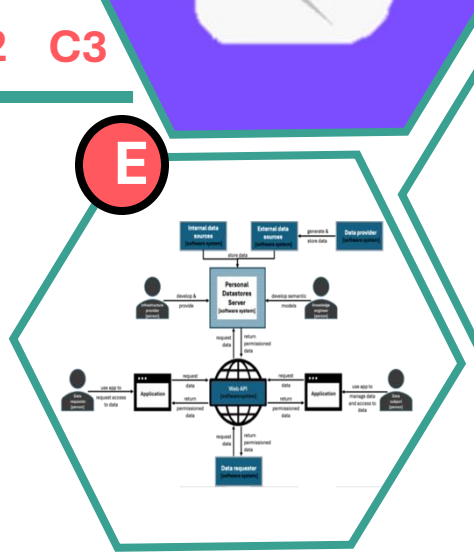


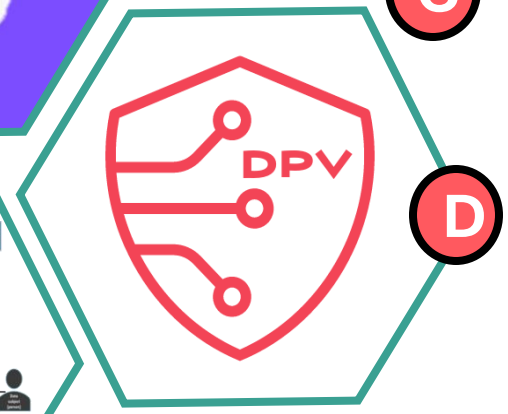
THESIS OVERVIEW

SEMANTIC WEB

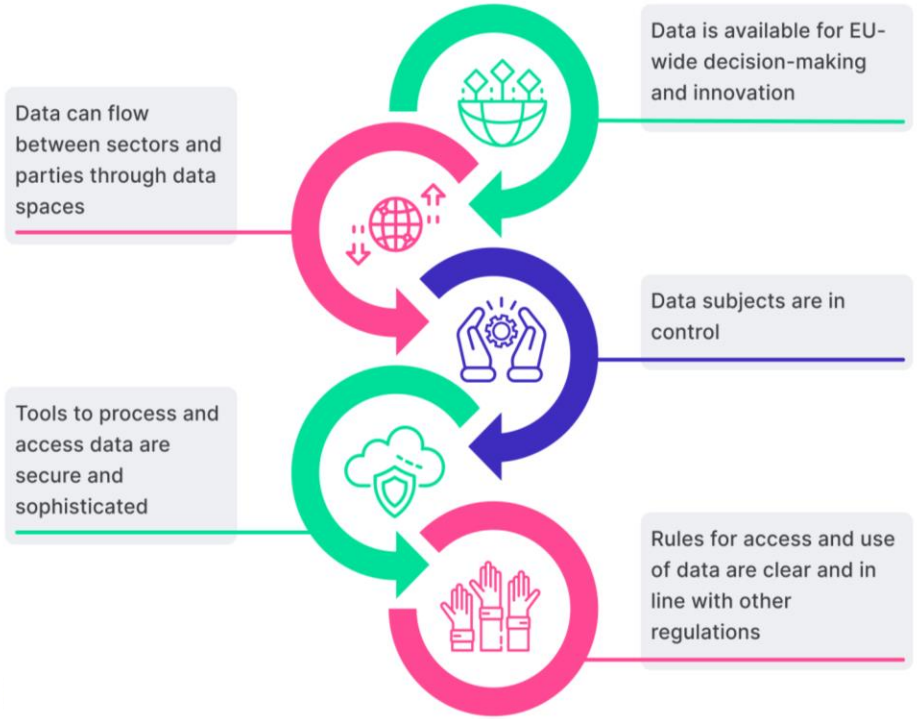
- **A** Introduction A1 A2 A3
- **B** State of the art B1 B2 B3
- **C** Vocabularies for personal data stores C1 C2 C3
- **D** Legal challenges D1 D2 D3 D4
- **E** Policy-based algorithms E1 E2 E3
- **F** Exploring the DGA
  - F1 – Decentralised WEB
  - F2 – Data protection vocabularies
  - F3 – Policy Languages
- **G** Conclusion

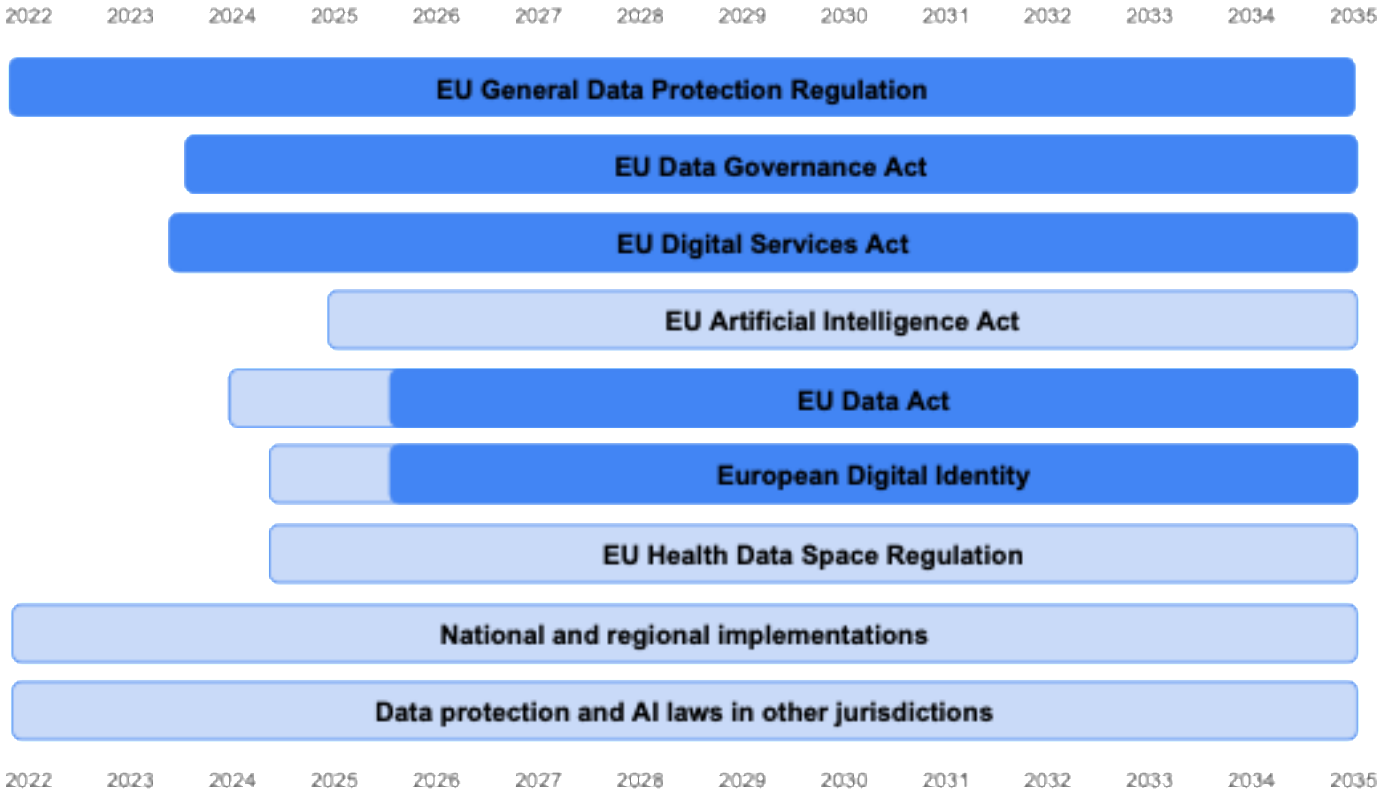






INFORMATION FLOWS IN THE DGA



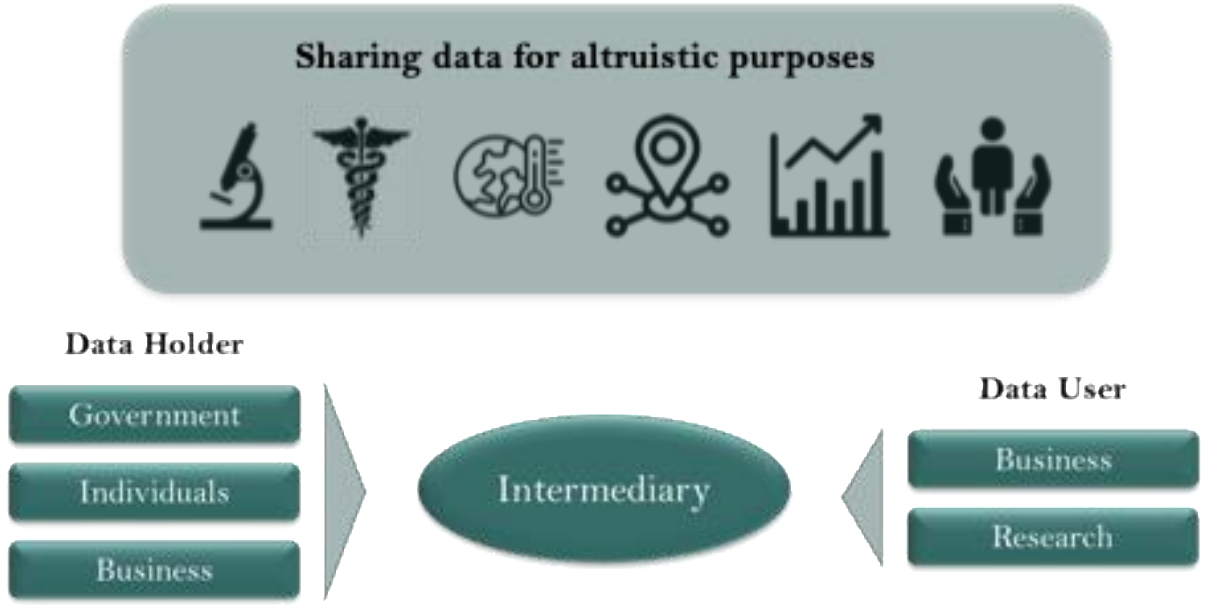


Source: circularise.com

INFORMATION FLOWS IN THE DGA

"This Regulation lays down: (a) conditions for the re-use [...] of certain categories of data [...]; (b) a [...] framework for the provision of data intermediation services; (c) a framework for voluntary registration of entities which collect and process data made available for altruistic purposes"

REGULATION (EU) 2022/868 (Data Governance Act) [Source]



Challenges

Availability / Discovery of datasets

Establishment of conditions for usage and access to data

Production of Documentation

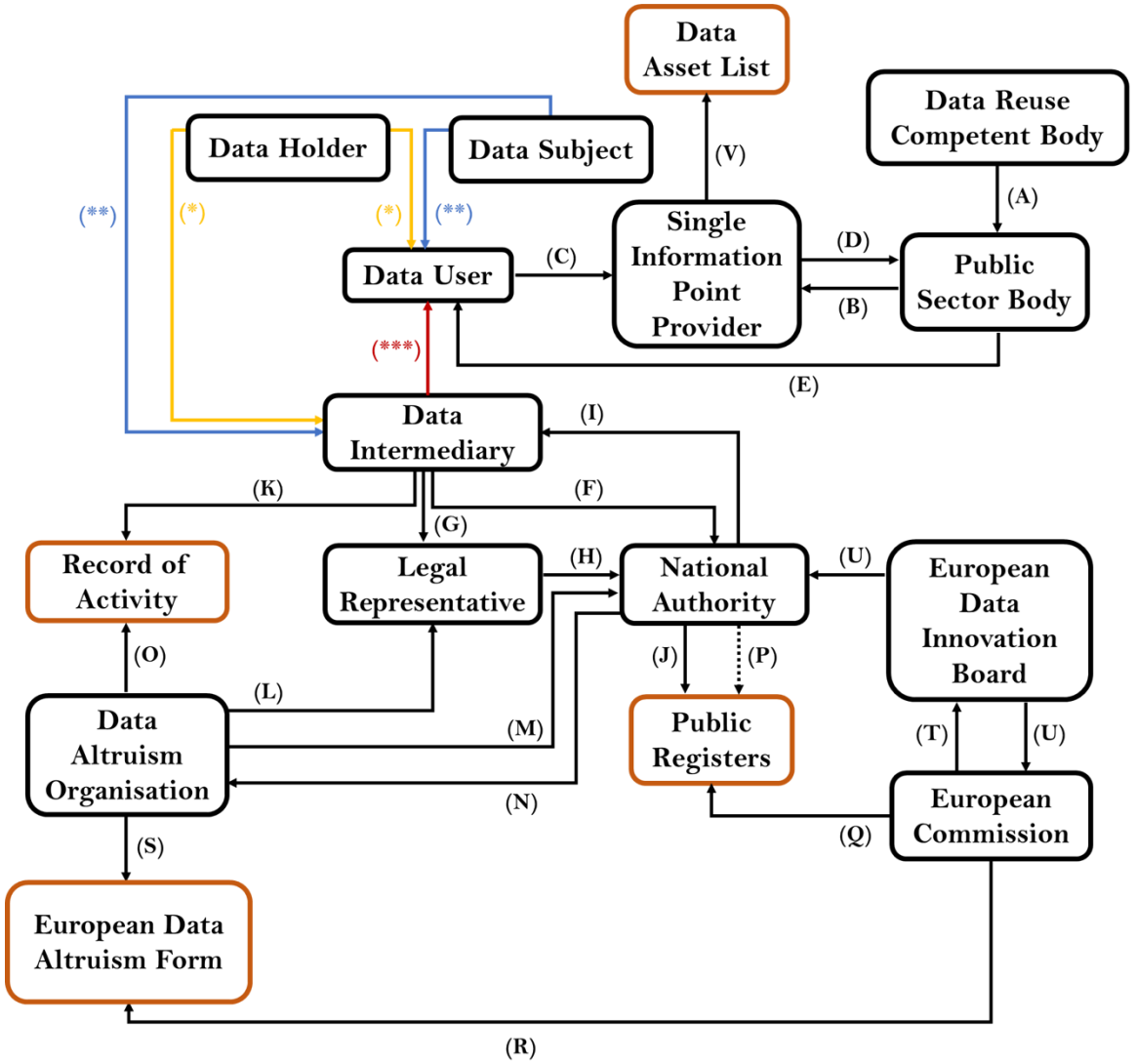
Gaps

Identify stakeholders & information flows between them

Model data-sharing policies and consent terms

Generate registers of altruistic and data intermediary activities

INFORMATION FLOWS IN THE DGA



(A) Assist/ act on behalf
(B) Conditions for reuse
(C) Search datasets & Request for reuse
(D) Transmit request for reuse
(E) Decision on the request
(F) Notify
(G) Designate if not established in the EU
(H) Cooperate
(I) Issue confirmation of Compliance with notification obligation & Verify compliance with conditions for providing intermediary services
(J) Publish & update database of data intermediaries
(K) Keep
(L) Designate if not established in the EU
(M) Submit application, Notify changes & Send annual activity report
(N) Verify compliance with requirements for providing data altruism activities
(O) Keep
(P) Publish & update database of data altruism organisations
(Q) Maintain
(R) Develop
(S) Adopt
(T) Establish
(U) Supervise / provide advice
(V) Maintain & make available
(*) Data sharing based on permission for non-personal data or for personal data (where they are not a data subject)
(**) Data sharing based on consent for personal data
(***) Data sharing under open or commercial licence

DGAterms

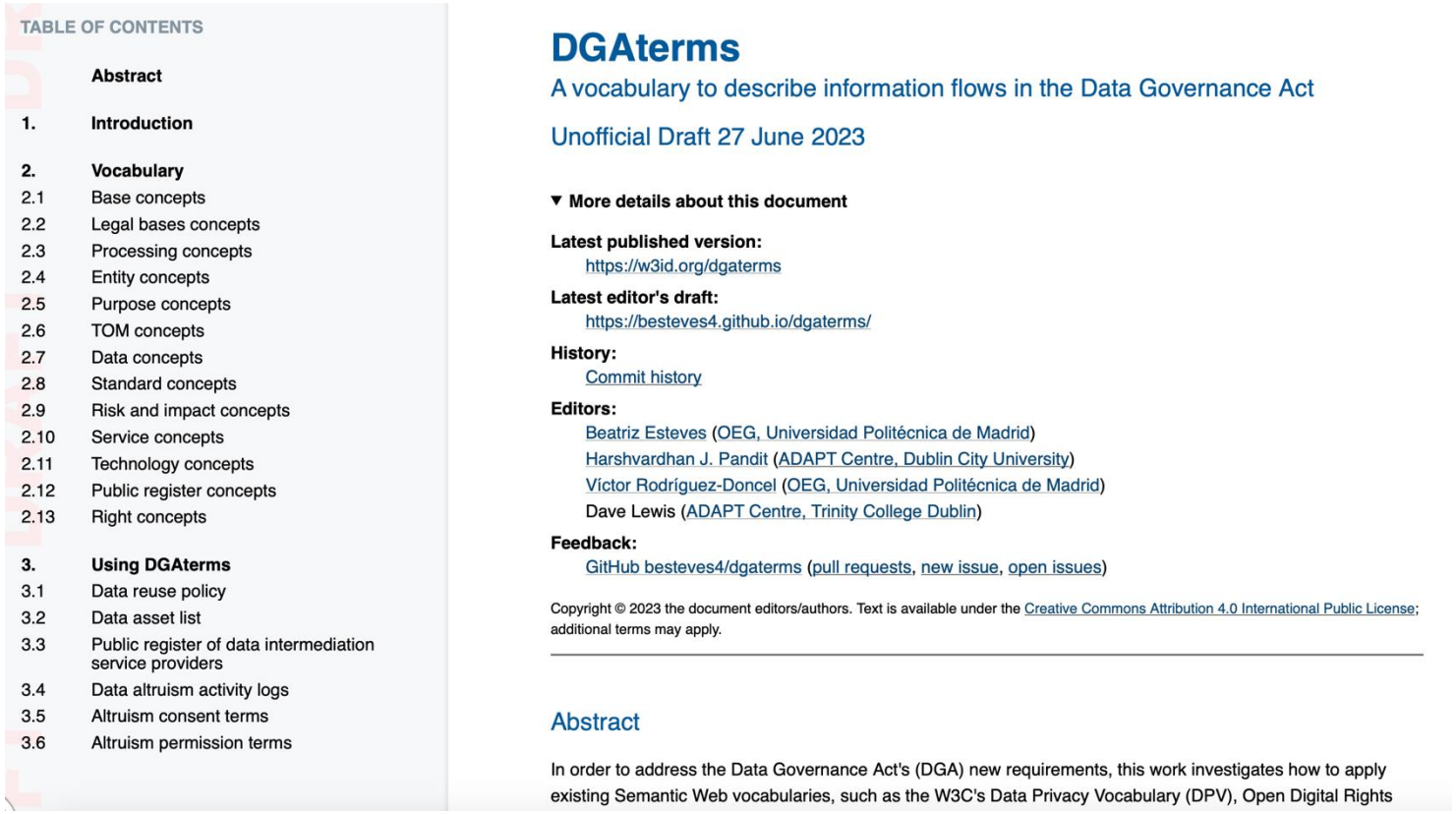


TABLE OF CONTENTS

DGAterms

A vocabulary to describe information flows in the Data Governance Act

Unofficial Draft 27 June 2023

▼ More details about this document

Latest published version:
https://w3id.org/dgaterms

Latest editor's draft:
https://besteves4.github.io/dgaterms/

History:
Commit history

Editors:
Beatriz Esteves (OEG, Universidad Politécnica de Madrid)
Harshvardhan J. Pandit (ADAPT Centre, Dublin City University)
Víctor Rodríguez-Doncel (OEG, Universidad Politécnica de Madrid)
Dave Lewis (ADAPT Centre, Trinity College Dublin)

Feedback:
GitHub besteves4/dgaterms (pull requests, new issue, open issues)

Abstract

In order to address the Data Governance Act's (DGA) new requirements, this work investigates how to apply existing Semantic Web vocabularies, such as the W3C's Data Privacy Vocabulary (DPV), Open Digital Rights

https://w3id.org/dgaterms

Legal terms validated by legal scholars and Data Protection Officers and integrated into the outcomes of the W3C DPVCG

Use Cases

UC1. Conditions for the Reuse of Public Data

UC2. Policies for Data Altruism

UC3. Records of Altruistic and Intermediation Activities

UC4. Registers of Entities

Data Catalog Vocabulary (DCAT) - Version 3
W3C Recommendation 22 August 2024

DublinCore

DCMI Metadata Terms

Beatriz Esteves and Víctor Rodríguez-Doncel. **Semantifying the Governance of Data in Europe**. In *18th International Conference on Semantic Systems – CEUR Workshop Proceedings*, volume 3235, 2022. URL: https://ceur-ws.org/Vol-3235/paper17.pdf.

Beatriz Esteves, Víctor Rodríguez-Doncel, Harshvardhan J. Pandit, and Dave Lewis. **Semantics for Implementing Data Reuse and Altruism Under EU's Data Governance Act**. In *Knowledge Graphs: Semantics, Machine Learning, and Languages*, pages 210–226. IOS Press, 2023. doi: 10.3233/SSW230015.

```
ex:SIPPA_assets a :DataAssetList, dcat:Catalog ;
    dct:description "Asset list maintained by SIPPA" ;
    dct:created "2022-12-10"^^xsd:date ;
    dct:publisher ex:SIPPA ; dcat:dataset ex:dataset_001 .
ex:SIPPA a :SingleInformationPointProvider .
ex:dataset_001 a dcat:Dataset ; dct:publisher ex:publicsectorbodyX ;
    dpv:hasData :StatisticallyConfidentialData ;
    dct:description "Dataset with statistically confidential data" ;
    dct:created "2022-12-04"^^xsd:date ;
    odrl:hasPolicy ex:policy_001 ; :hasFee "0€"^^xsd:string ;
    dcat:mediaType <iana.org/assignments/media-types/text/csv> ;
    dct:extent "5.6MB"^^xsd:string .
```

```
ex:policy_001 a odrl:Offer, :DataReusePolicy ;
    odrl:permission [
        odrl:target ex:dataset_001 ; odrl:action :Reuse ;
        odrl:assigner ex:publicsectorbodyX ;
        odrl:constraint [
            odrl:and [
                odrl:leftOperand odrl:dateTime ;
                odrl:operator odrl:lteq ;
                odrl:rightOperand "2023-12-31"^^xsd:date ], [
                odrl:leftOperand odrl:purpose ;
                odrl:operator odrl:isA ;
                odrl:rightOperand :ScientificResearch ] ] ] .
ex:publicsectorbodyX a :PublicSectorBody ;
    dpv:hasName "Public Sector Body X" ;
    dpv:hasContact "mailto:publicsectorbodyX@email.com" ;
    :hasCompetentBody [
        a :DataReuseCompetentBody ; dpv:hasName "Competent Body X" ;
        dpv:hasContact "mailto:competentbodyX@email.com" ] .
```

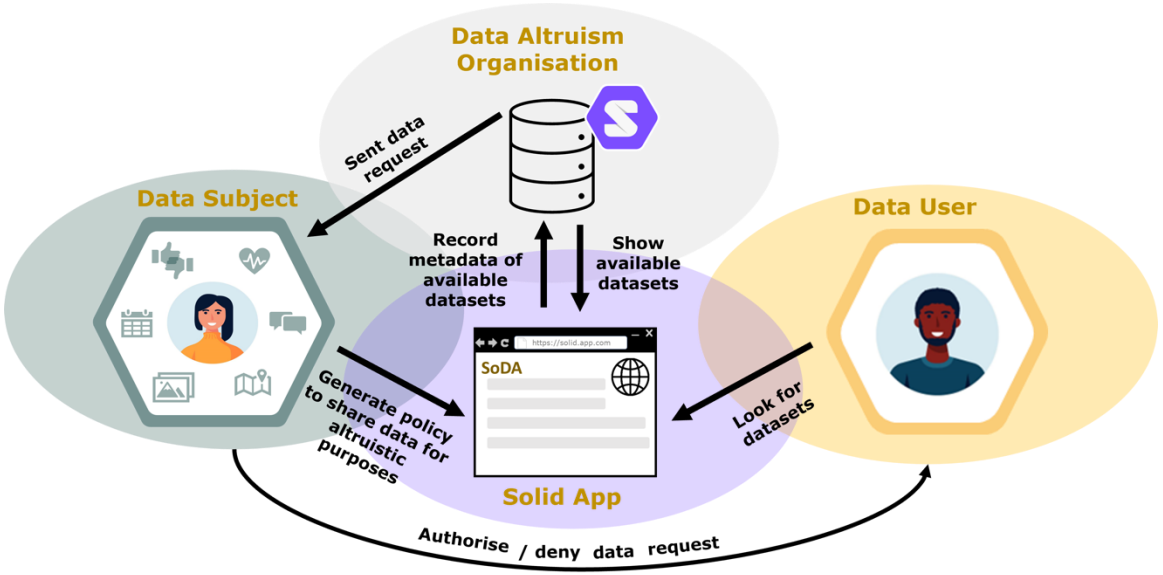
```
ex:publicregistry_DI_PT a :RegisterOfDataIntermediationServiceProviders ;
    dct:description "Public register of intermediaries working in PT" ;
    dct:created "2023-12-15"^^xsd:date ;
    dct:modified "2023-12-23"^^xsd:date ;
    dct:publisher ex:nationalauthority_PT ;
    :hasDataIntermediationServiceProvider ex:DISP_Y .
ex:nationalauthority_PT a :DataIntermediationAuthority ;
    dpv:hasName "Data Intermediation Authority of Portugal" ;
    dpv:hasContact "mailto:nationalauthority_PT@email.com" ;
    dpv:hasJurisdiction "PT" .
ex:DISP_Y a :DataCooperative ;
    dpv:hasName "Data Cooperative Y" ; dpv:hasAddress "Lisboa, Portugal" ;
    dct:description "Provider of anonymised geolocation data" ;
    dcat:landingPage <http://cooperativeA.com/> ;
    dct:date "2023-12-23"^^xsd:date .
```

```
ex:altruism_logs a :RegisterOfDataIAltruismActivity ;
    dct:description "Activity logs of the Data Altruism Organisation A" ;
    dct:created "2023-11-04"^^xsd:date ;
    dct:modified "2023-11-13"^^xsd:date ;
    dct:publisher ex:altruism_A ; dcat:record ex:log_001 .
ex:altruism_A a :DataAltruismOrganisation ;
    dpv:hasName "Data Altruism Organisation A" ;
    dpv:hasAddress "Lisboa, Portugal" ;
    dcat:landingPage <http://example.com/altruism_A> .
ex:log_001 a dcat:CatalogRecord ;
    dct:created "2023-11-13"^^xsd:date ;
    :hasDataUser ex:userZ ; :hasFee "1000€"^^xsd:string ;
    dpv:hasPersonalDataHandling [
        dct:description "Download and reuse anonymised health records to
        ↪ improve healthcare" ;
        dpv:hasProcessing :Download, :Reuse ; dpv:hasDuration 6226453 ;
        dpv:hasPurpose :DataAltruism, :ImproveHealthcare ;
        dpv:hasPersonalData dpv-pd:HealthRecord ;
        dpv:hasTechnicalMeasure dpv:Anonymisation ] .
ex:userZ a :DataUser ; dpv:hasName "Data User Z" ;
    dpv:hasContact "mailto:user_z@email.com" .
```

SOLID FOR DATA ALTRUISM

F1 F2 F3

Beatriz Esteves. **Towards an Architecture for Data Altruism in Solid**. In *ISWC 2023 Posters and Demos: 22nd International Semantic Web Conference*, 2023. URL: https://ceur-ws.org/Vol-3632/ISWC2023_paper_491.pdf.



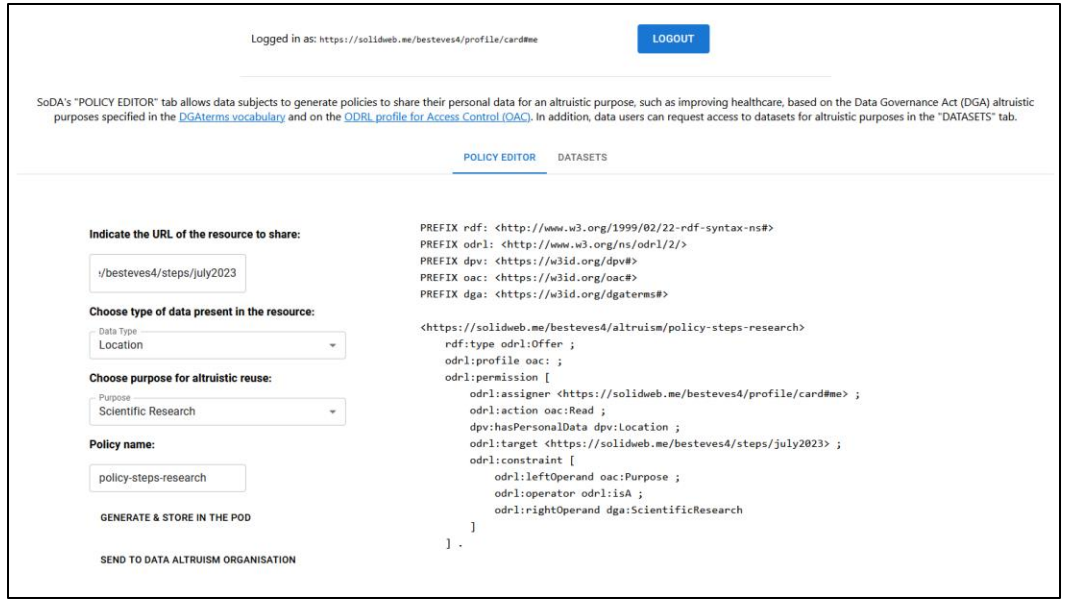
https://w3id.org/people/besteves/soda/repo

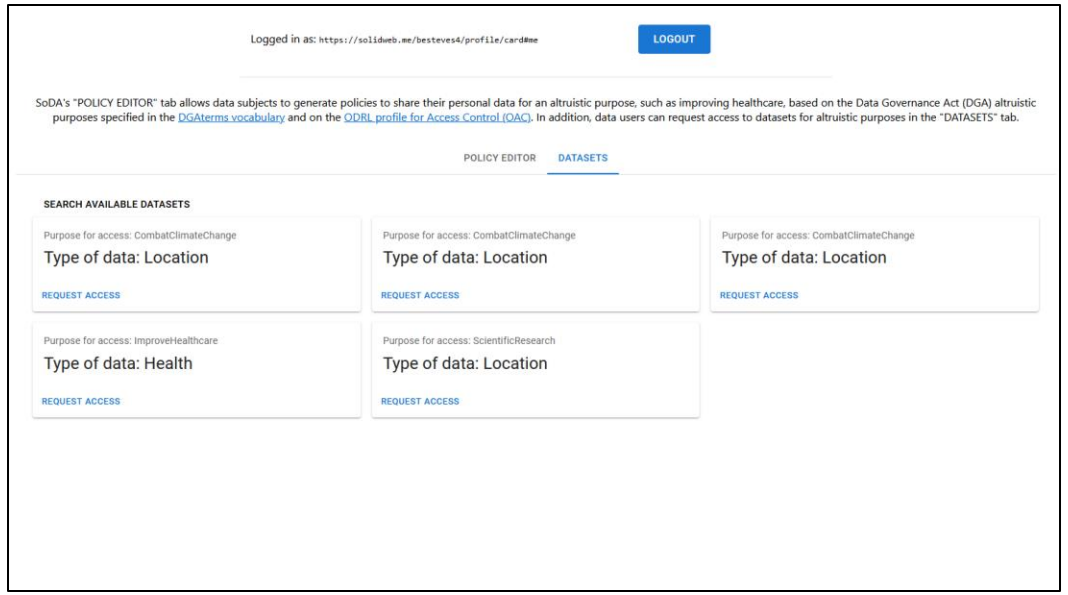
Data spaces

Enhanced interoperability

Data management & discovery

Legal compliance with OAC & DPV

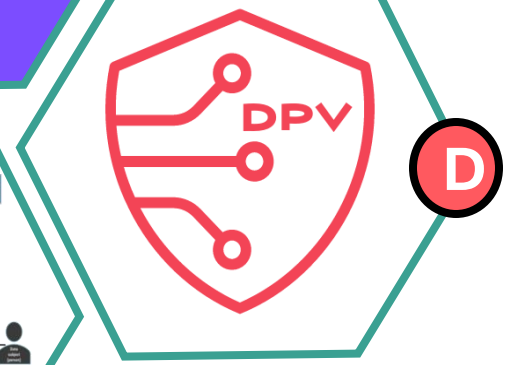


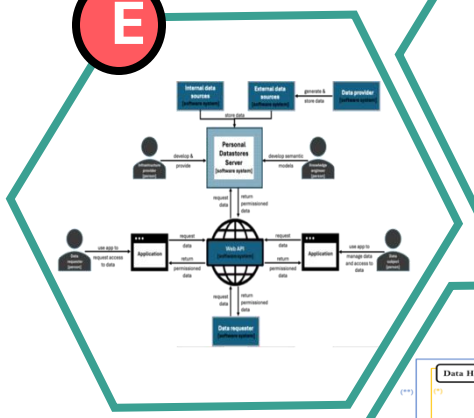


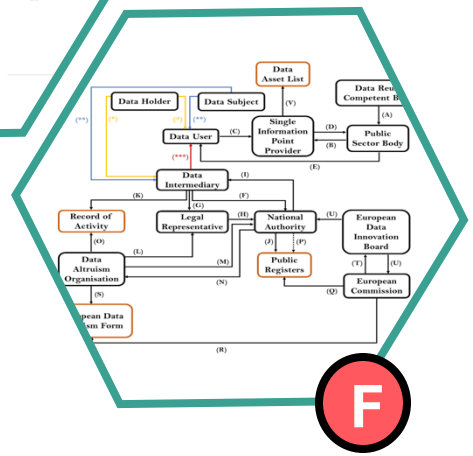
THESIS OVERVIEW

SEMANTIC WEB

- A Introduction A1 A2 A3
- B State of the art B1 B2 B3
- C Vocabularies for personal data stores C1 C2 C3
- D Legal challenges D1 D2 D3 D4
- E Policy-based algorithms E1 E2 E3
- F Exploring the DGA F1 F2 F3
- G Conclusion







This thesis presents **legally-aligned vocabularies and services** were produced to support **policy-based access** to data in **decentralised settings**, providing **accountability** and enhanced **transparency** to people looking at **regaining trust in Web** services.

O1 – Assist entities in the expression of data protection-related information

- Expression of **GDPR-aligned access policies**
- Expression of **provenance** and other **contextual metadata** associated with data stored in decentralised datastores
- Expression of information related with **DGA-based data reuse**
- Analysis of **legal challenges** of consent in **decentralised settings**

O2 – Use machine-readable policies for accessing decentralised personal data

- Design of a **policy matching algorithm** for generating data access agreements
- **Proof of concept implementation** for health data sharing
- Development of Solid-based **UIs for policy generation**

O3 – Aid the exercising of GDPR's data subject rights

- Expression of information related to the **exercising of data subject rights**
- Design of a **service** to assist in the **exercising** and **recording** of such **rights exercise activities**

Usage control and data spaces

Extend existing work to cover usage control, i.e., what happens once data has been accessed, including data reuse for altruistic purposes and the secondary usage of data promoted by the EHDS proposal

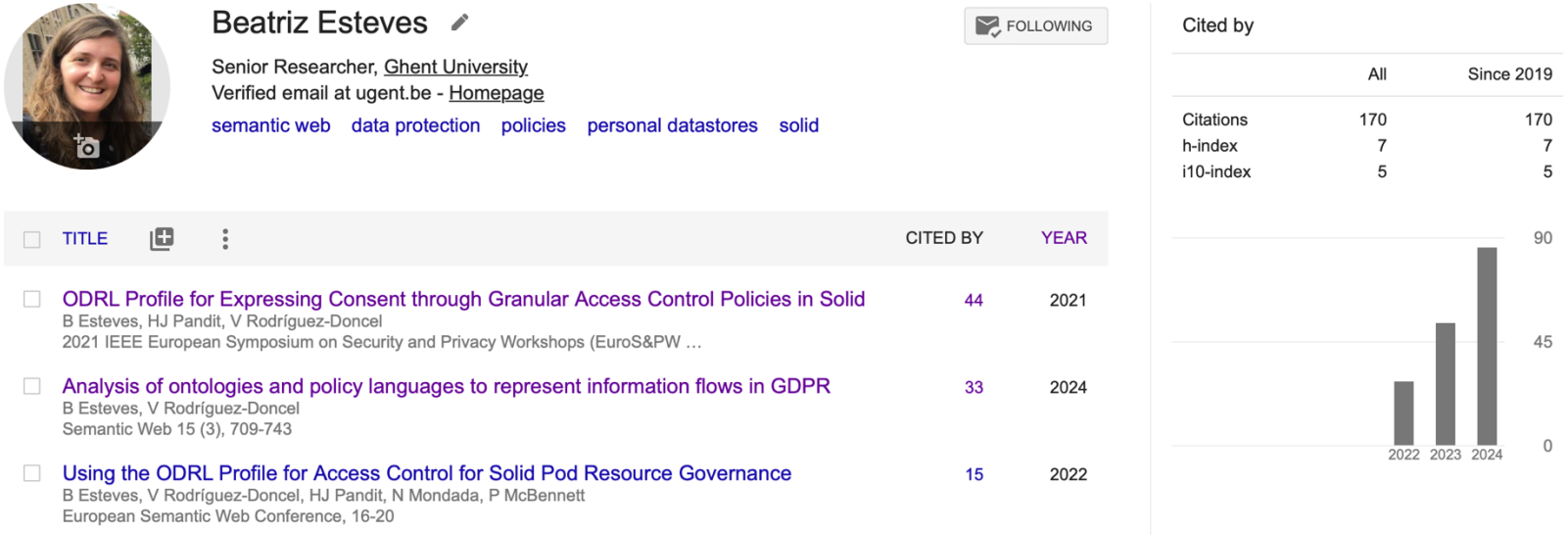
Web agents

Assist data subjects, data controllers, and newly-introduced DGA entities to exercise their rights or fulfil their duties in an automated manner, including assisting data subjects in making decisions, according to their preferences, and aiding data controllers to compile the necessary compliance documentation.

Interaction of data protection and AI laws

Further vocabularies need to be developed and integrated into DPV's existing framework, e.g., related to the DSA, DMA, Data Act, EHDS, and study of how these laws are related and in which data processing scenarios they apply still needs to be performed to be incorporated into the developed decentralised systems.

- Active participation and contribution to W3C specification processes
  - Adoption by industry practitioners
- Peer-reviewed publications in computer science & interdisciplinary venues
  - 4 journal contributions
  - 4 conference contributions
  - 7 workshop/poster/demo contributions
    - Best paper award for "*Beatriz Esteves, and Harshvardhan J Pandit.* ***Using Patterns to Manage Governance of Solid Apps****. In 14th Workshop on Ontology Design and Patterns (WOP 2023@ISWC 2023), 2023. URL: https://ceur-ws.org/Vol-3636/paper5.pdf*"



Beatriz Esteves

FOLLOWING

Senior Researcher, Ghent University
Verified email at ugent.be - Homepage

semantic web data protection policies personal datastores solid

TITLE	CITED BY	YEAR
ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid B Esteves, HJ Pandit, V Rodríguez-Doncel 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW …	44	2021
Analysis of ontologies and policy languages to represent information flows in GDPR B Esteves, V Rodríguez-Doncel Semantic Web 15 (3), 709-743	33	2024
Using the ODRL Profile for Access Control for Solid Pod Resource Governance B Esteves, V Rodríguez-Doncel, HJ Pandit, N Mondada, P McBennett European Semantic Web Conference, 16-20	15	2022

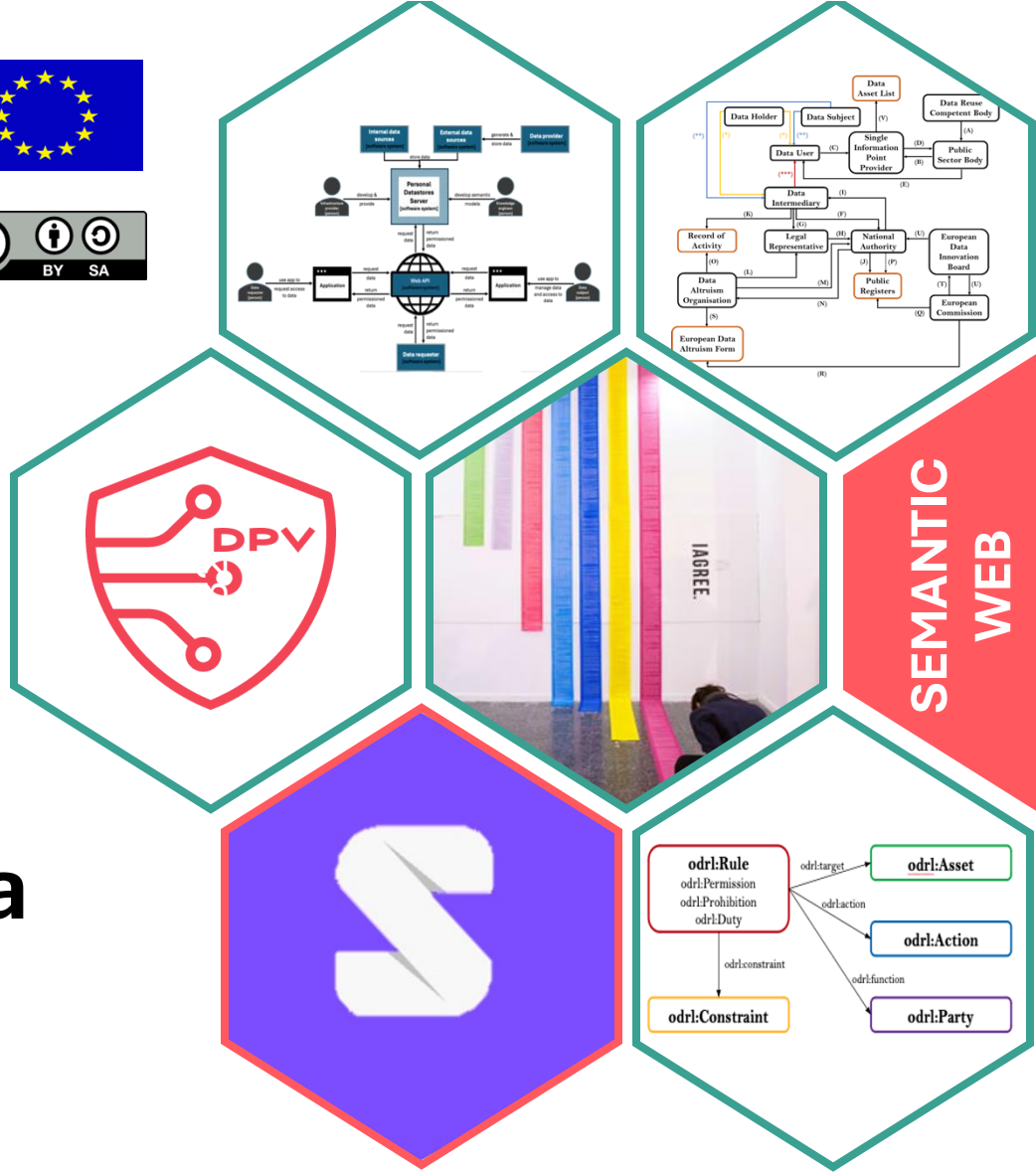
Cited by

	All	Since 2019
Citations	170	170
h-index	7	7
i10-index	5	5

Beatriz Esteves

MSc in Biomedical Engineering

Semantic Representation of Privacy Terms and Policy-based Algorithms for Decentralised Data Environments



Supervisors

Ontology Engineering Group
Universidad Politécnica de Madrid

Dr. Víctor Rodríguez Doncel

ADAPT Centre
Trinity College Dublin

Dr. David Lewis

beatriz.esteves@ugent.be

in/beatriz-esteves-032249156/

besteves4