Protect

Enhancing Solid with Legally-aware Policies

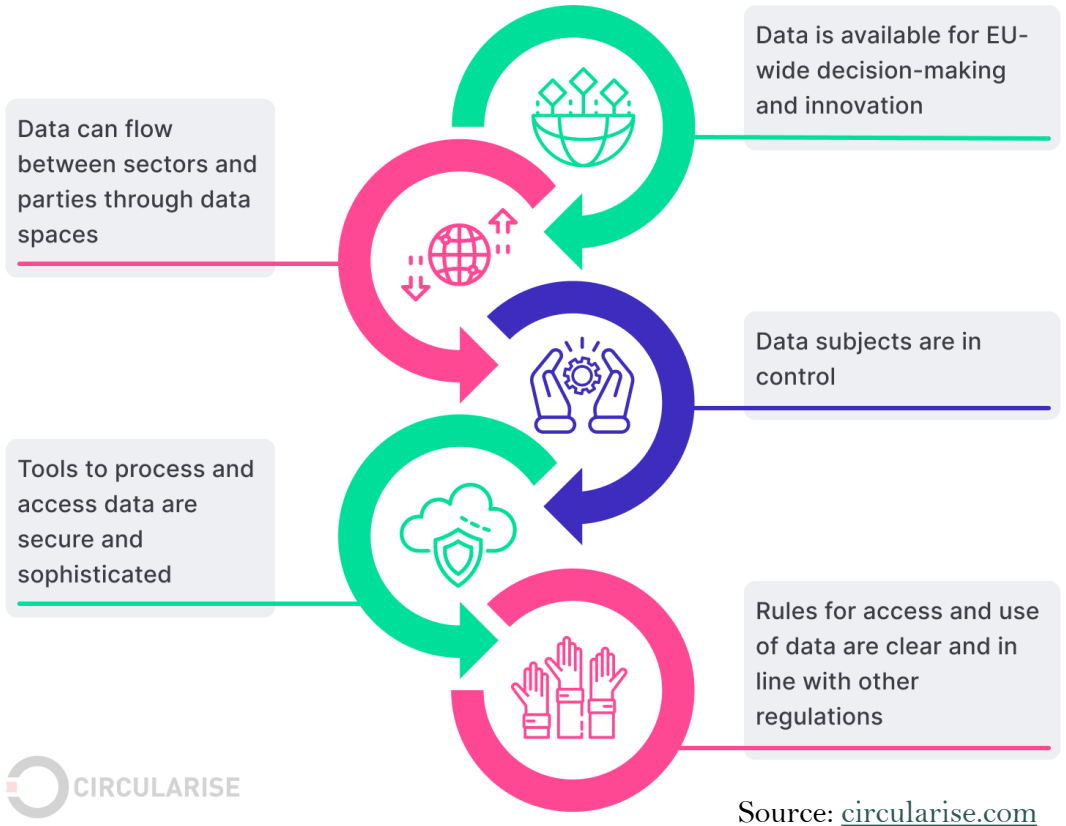
Beatriz Esteves, Ontology Engineering Group, Universidad Politécnica de Madrid
beatriz.gesteves@upm.es | besteves4@eupolicy.social

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 813497.

Ontology Engineering Group

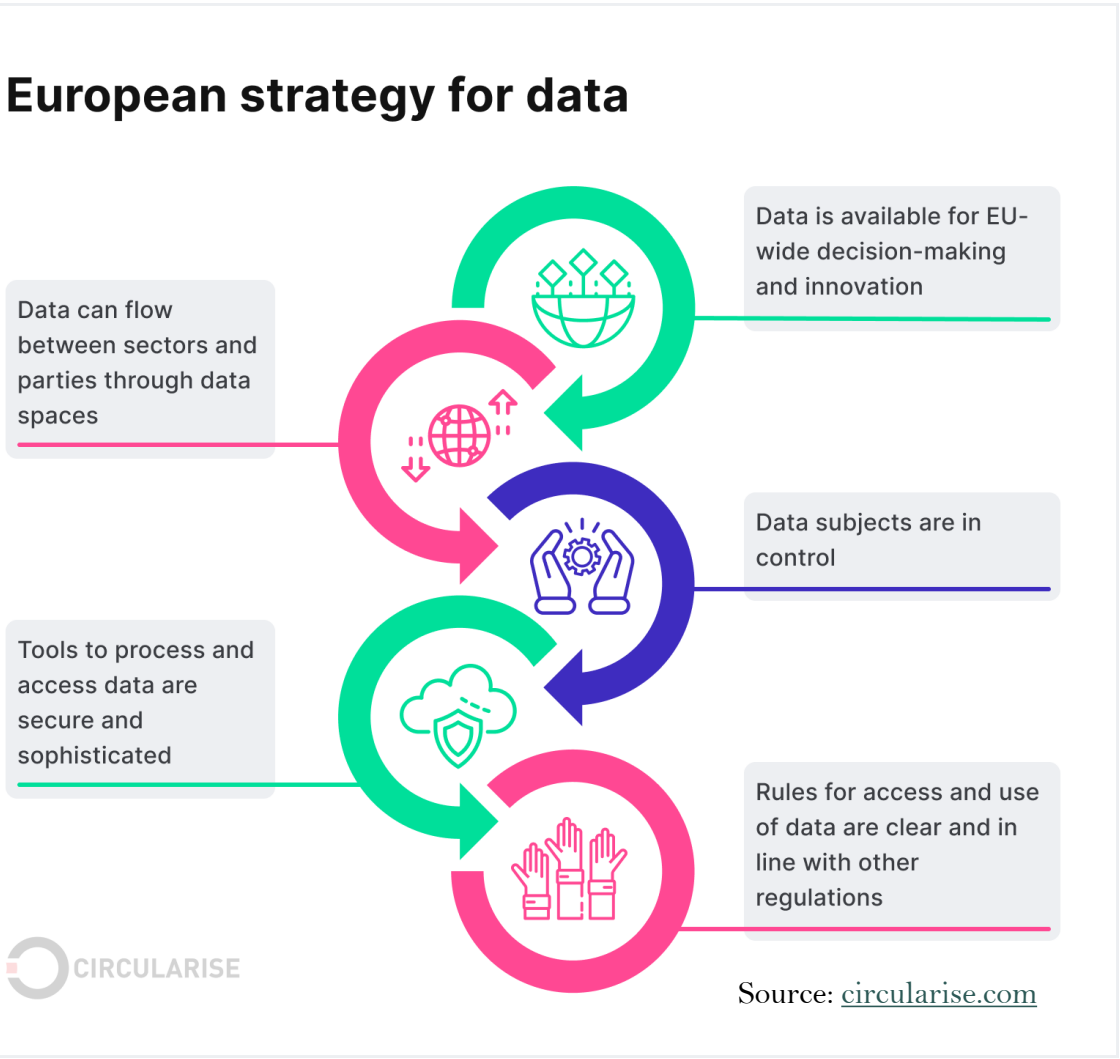
POLITÉCNICA

Motivation

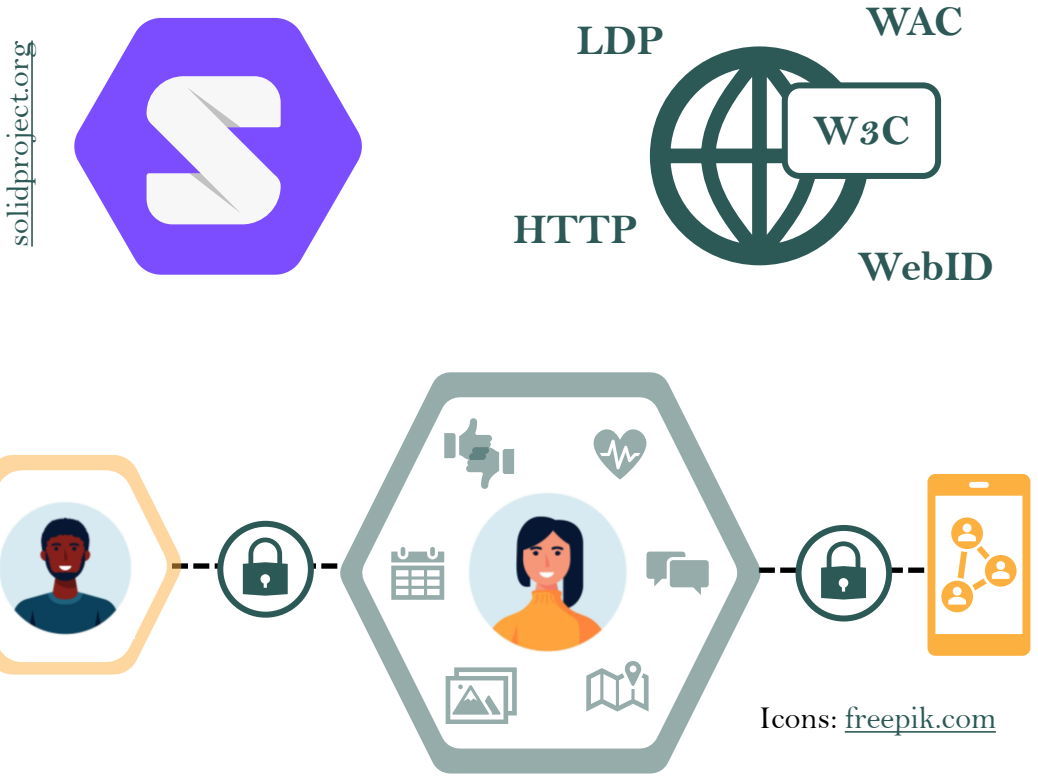


Source: circularise.com

Motivation



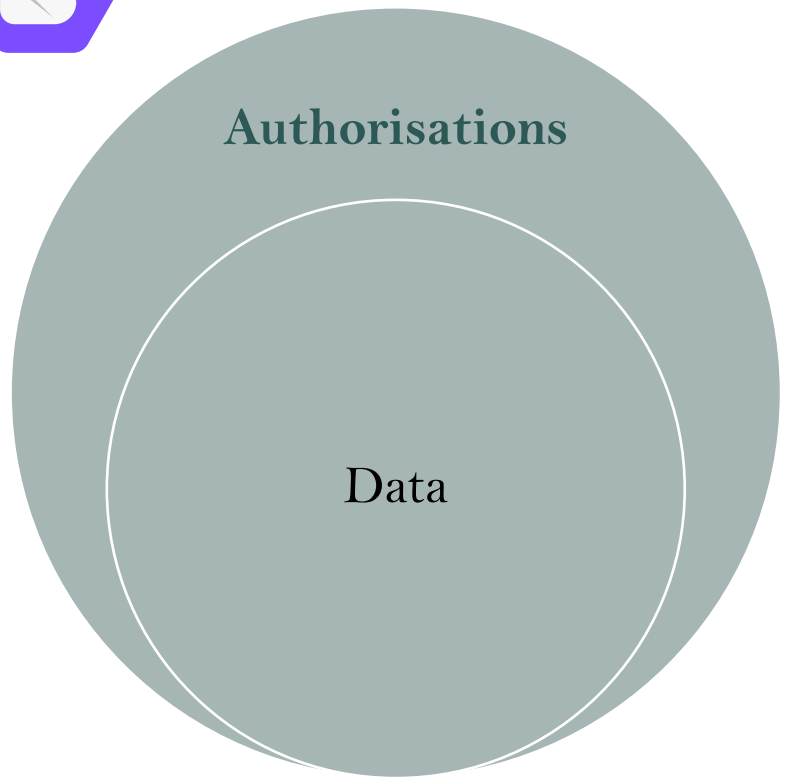
Source: circularise.com



Icons: freepik.com

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

Problems – Giving Access to Data in Solid



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

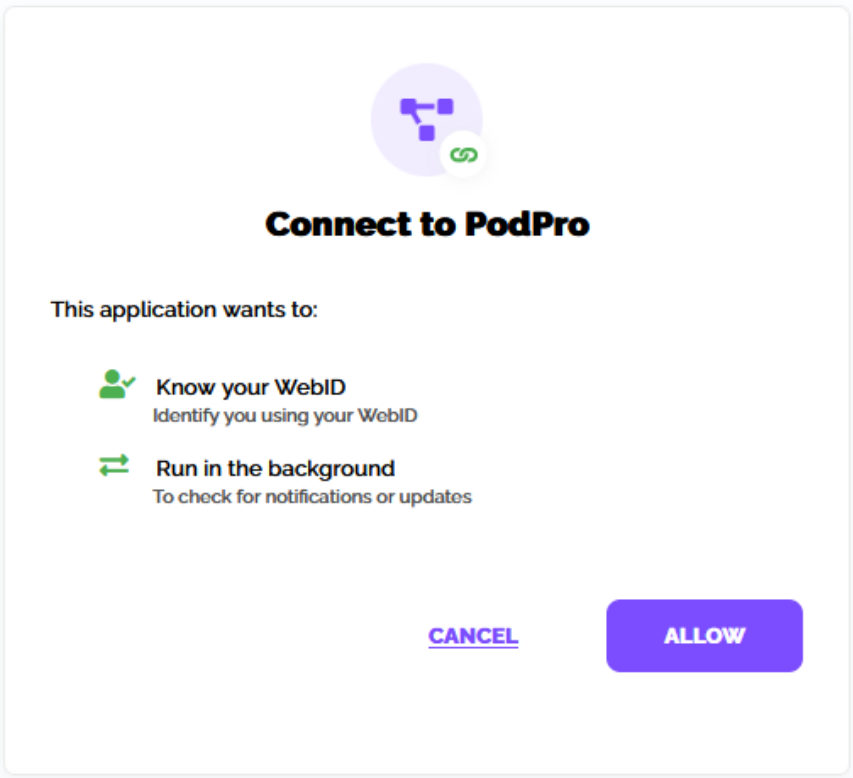
WAC – Web Access Control

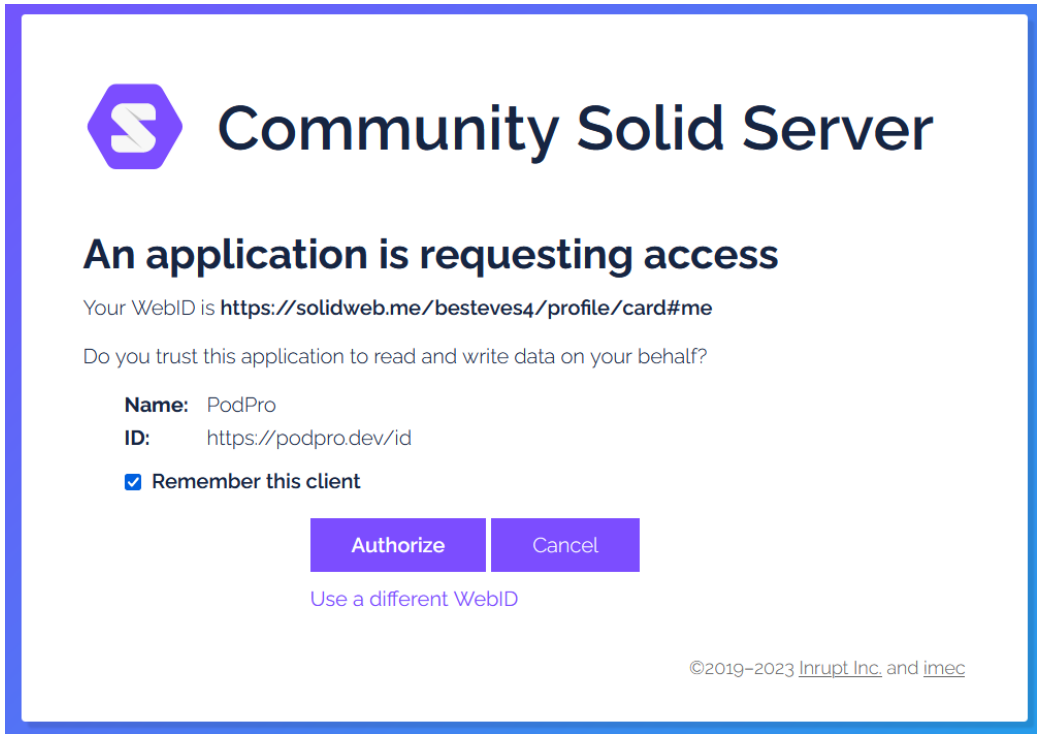
```
<#authorization1>
    a acl:Authorization ;
    acl:agent <https://beatriz.providerZ.com/profile/card#me> ;
    acl:accessTo <https://victor.providerY.com/docs/file1.ttl> ;
    acl:mode acl:Read, acl:Write .
```

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>
 ] .
```

Problems – Giving Access to Data in Solid



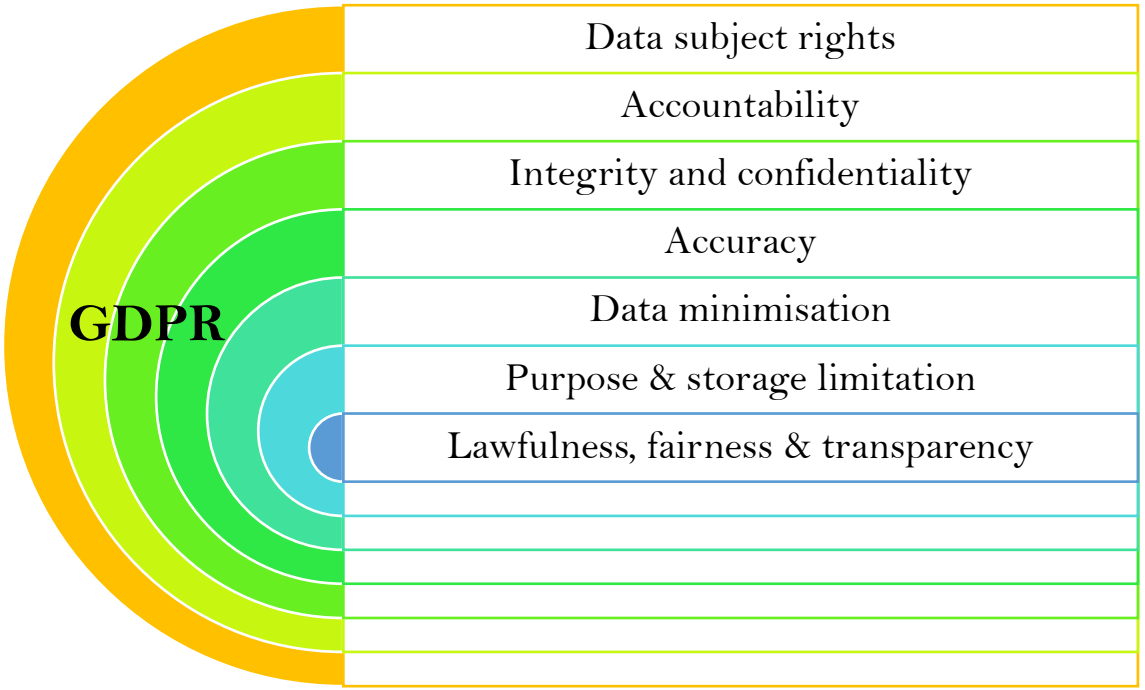


Is this enough for Solid users to know what is happening to their data? Is it enough to comply with GDPR's requirements?

Problems – Alignment with legal requirements

"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]



What is missing from Solid?

No records of agreements for the provision of services

Lack of tools to give / withdraw consent

Lack of tools to exercise data subject rights

No information on the identity and contact details of providers

Accountability documentation is missing (ROPAs, DPIAs, …)

Record keeping and log maintenance are nonexistent

Lack of tools to rectify data inaccuracies

Difficulty for users to set (granular) access to resources

Access grants valid in perpetuity

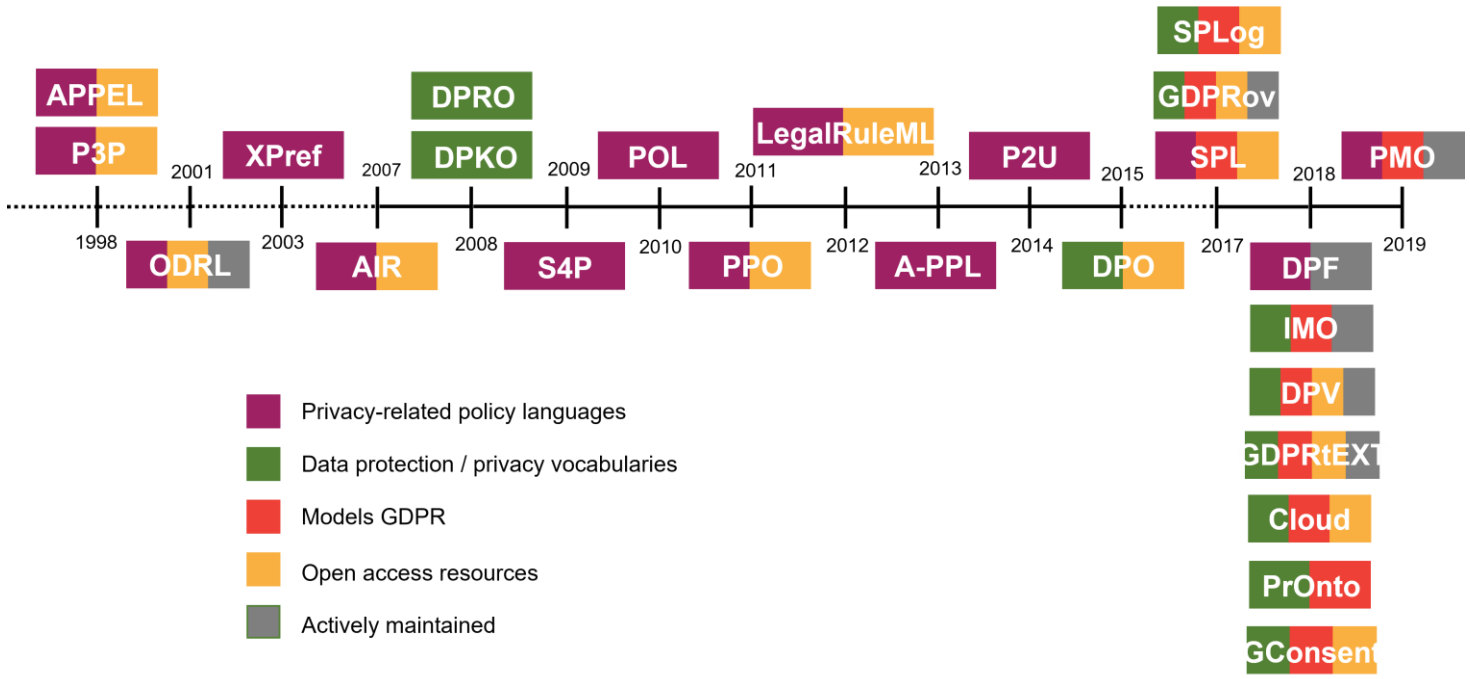
Data requests miss a purpose

Compatibility of purposes cannot be checked

Consent dialogue not enough for informed decision

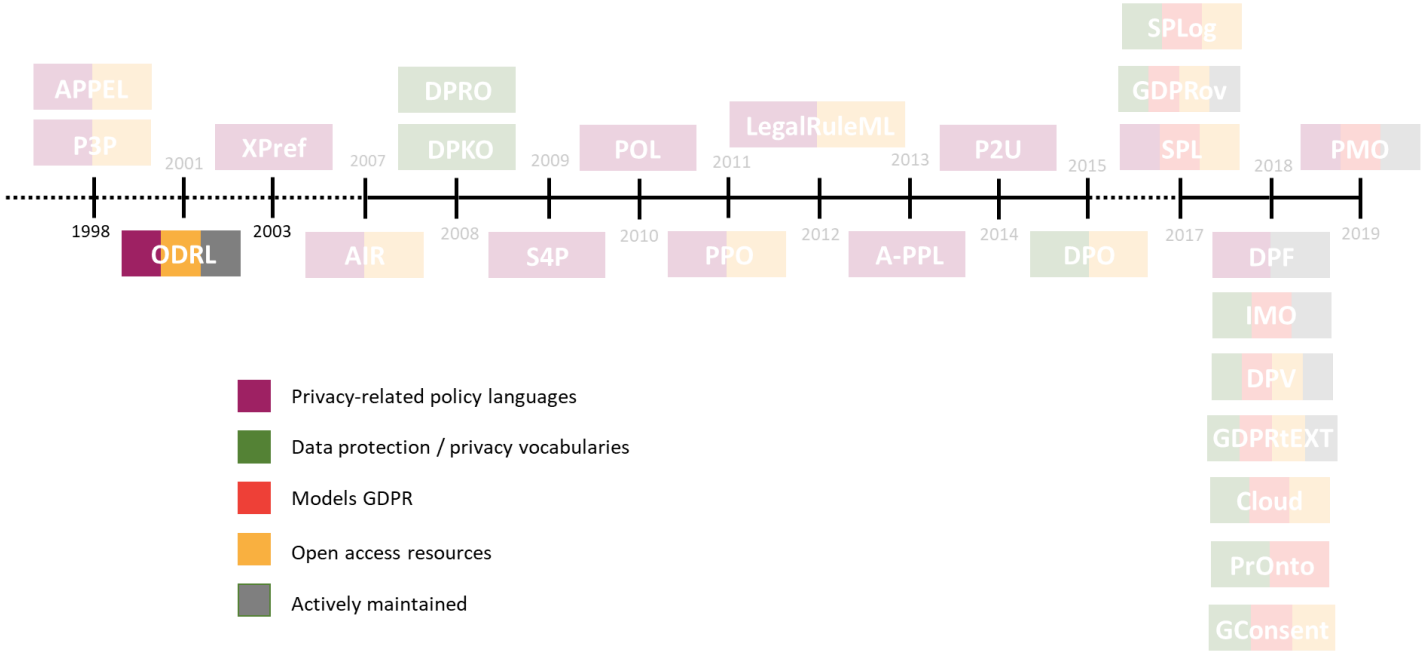
Access grants not sufficient to be a valid record of consent

Introducing a *policy layer* in Solid



Esteves, B. and Rodríguez-Doncel, V., "Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR". *Semantic Web Journal*, *vol.* 2022. https://content.iospress.com/articles/semantic-web/sw223009

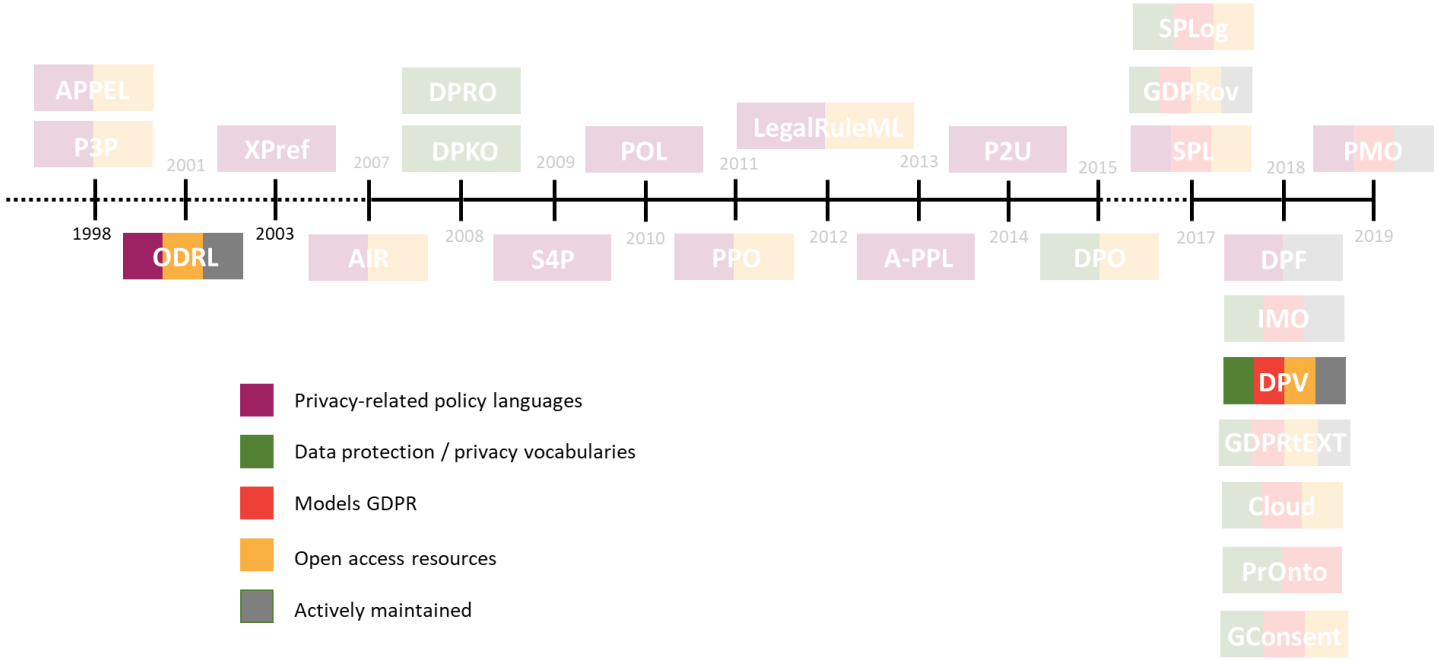
Introducing a *policy layer* in Solid



W3C Recommendation to represent "Policies that express Permissions, Prohibitions and Duties related to the usage of Asset resources"
https://www.w3.org/TR/odrl-model/

Esteves, B. and Rodríguez-Doncel, V., "Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR". *Semantic Web Journal, vol.* 2022.
https://content.iospress.com/articles/semantic-web/sw223009

Introducing a *policy layer* in Solid

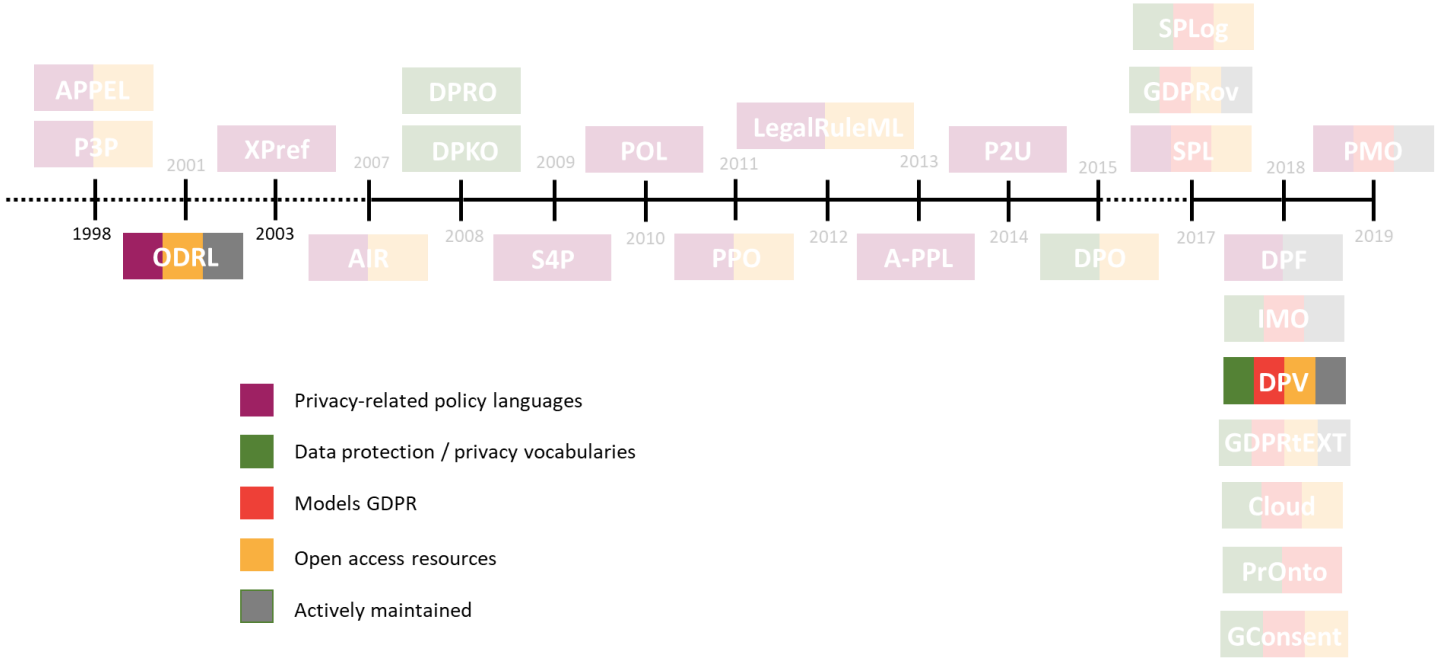


W3C Recommendation to represent "Policies that express Permissions, Prohibitions and Duties related to the usage of Asset resources"
https://www.w3.org/TR/odrl-model/

W3C Community Group Report to express "machine-readable metadata about the use and processing of personal data based on legislative requirements such as the GDPR"
https://w3id.org/dpv

Esteves, B. and Rodríguez-Doncel, V., "Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR". *Semantic Web Journal, vol.* 2022.
https://content.iospress.com/articles/semantic-web/sw223009

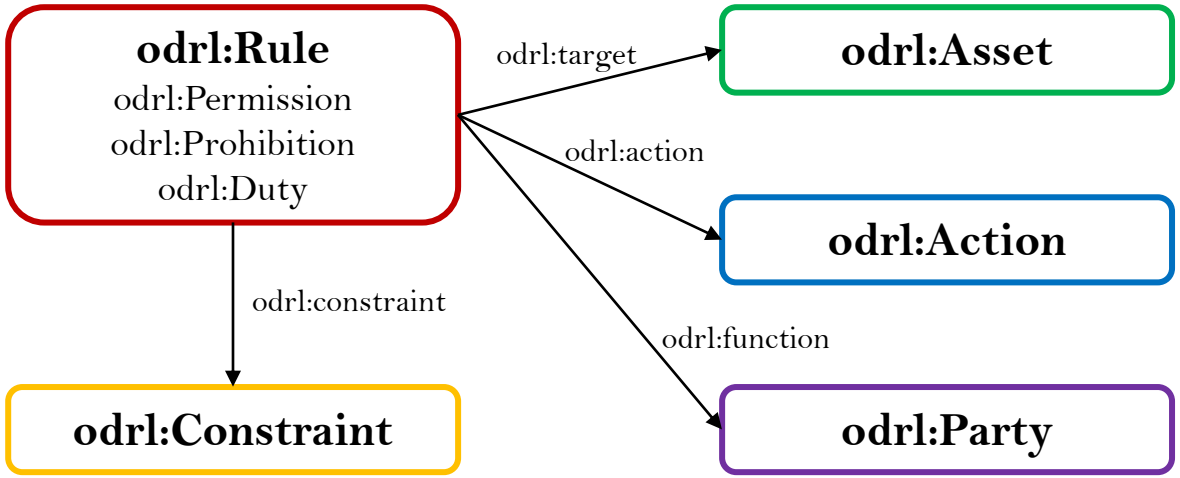
Introducing a *policy layer* in Solid



Esteves, B. and Rodríguez-Doncel, V., "Analysis of Ontologies and Policy Languages to Represent Information Flows in GDPR". *Semantic Web Journal, vol.* 2022. https://content.iospress.com/articles/semantic-web/sw223009

Esteves, B., Pandit, H. J., & Rodríguez-Doncel, V. (2021). *ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid.* In 2021 IEEE European S&P Workshops (pp. 298-306). https://ieeexplore.ieee.org/abstract/document/9583717

Open Digital Rights Language (ODRL)

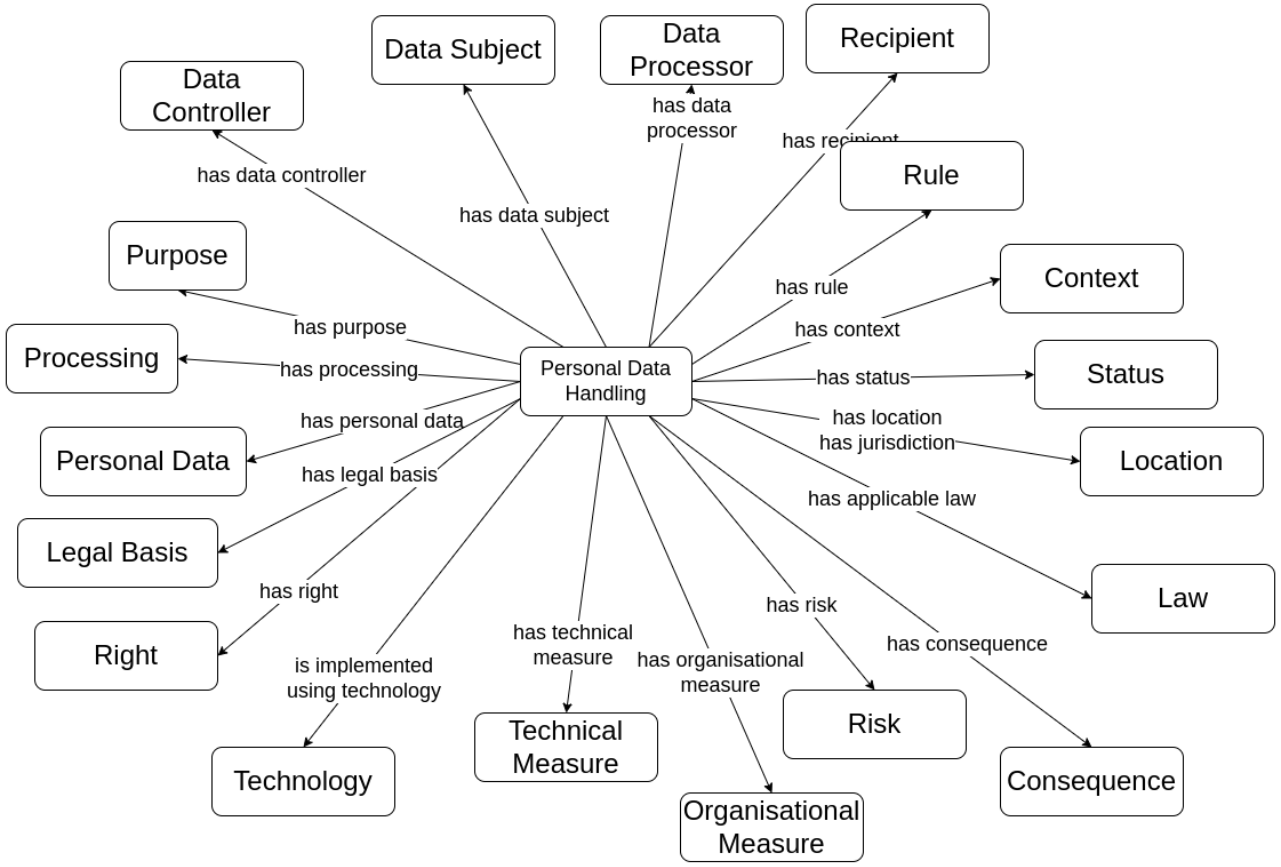


Target asset may be distributed until 2024-01-01

```
<#policy1> a odrl:Offer ;
 odrl:permission [
  odrl:assigner <http://example.com/org:43>;
  odrl:target <http://example.com/document:44>;
  odrl:action odrl:distribute;
  odrl:constraint [
   odrl:leftOperand odrl:dateTime;
   odrl:operator odrl:lt;
   odrl:rightOperand "2024-01-01"^^xsd:date
  ] ]
].
```

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

Data Privacy Vocabulary (DPV)

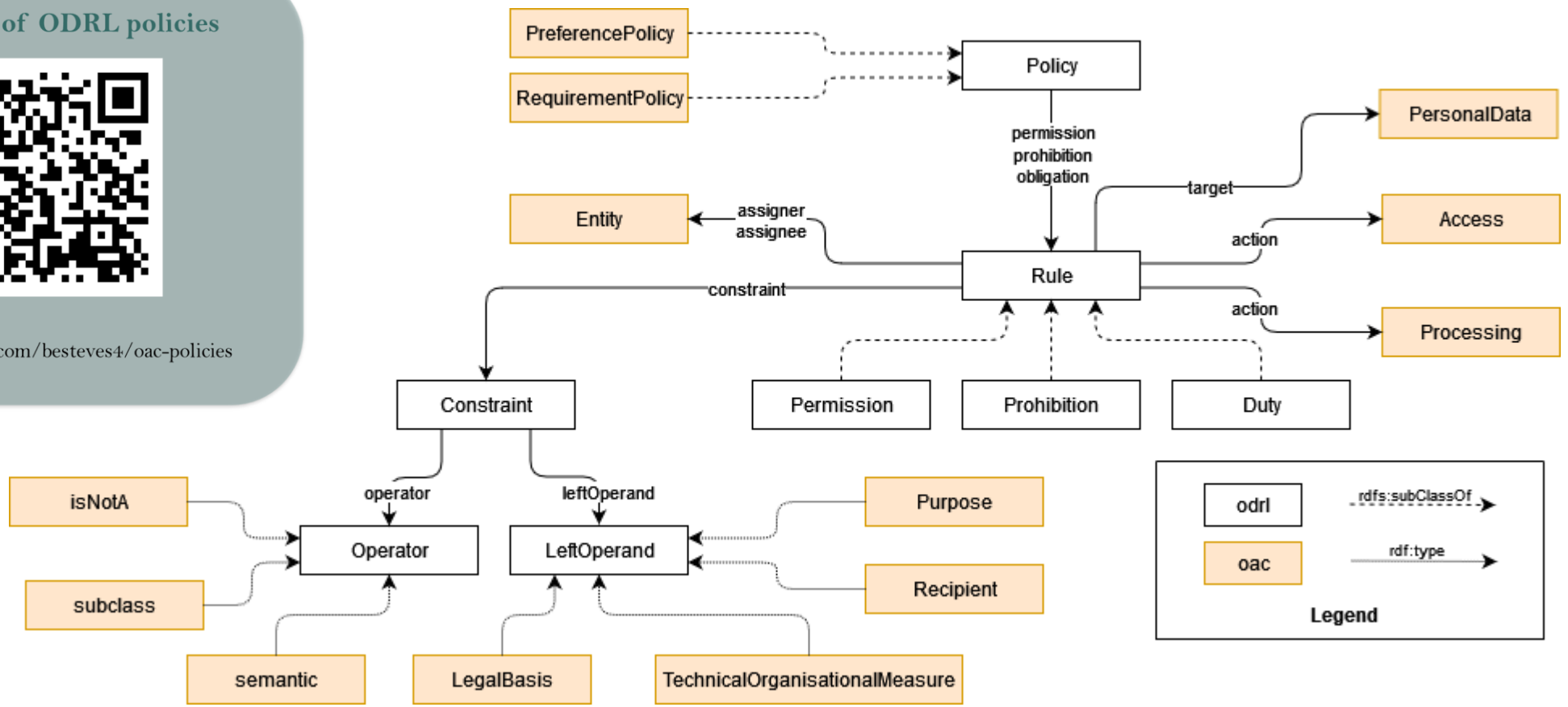


- *Primer for Data Privacy Vocabulary*: An introductory document for DPV's concepts and taxonomies.
- Extensions to Concepts:
  - [DPV-GDPR]: for GDPR concepts; serialisations: [DPV-SKOS-GDPR], [DPV-OWL-GDPR]
  - [DPV-PD] for Personal Data concepts; serialisations: [DPV-SKOS-PD], [DPV-OWL-PD]
  - [DPV-LEGAL] for Jurisdiction-relevant concepts; serialisations: [DPV-SKOS-LEGAL], [DPV-OWL-LEGAL]
  - [DPV-TECH] for Technology concepts; serialisations: [DPV-SKOS-TECH], [DPV-OWL-TECH]
  - [RISK] for Risk Assessment and Management concepts; serialisations: [RISK-SKOS], [RISK-OWL]
- *Guidelines for Adoption and Use of DPV*:
  - *Guide on DPV's serialisations and semantics* (coming soon)
  - *Guide for using DPV with RDFS and SKOS* (coming soon)
  - *Guide for using DPV in OWL2*
  - *Guide for Privacy Notices using DPV* (coming soon)
  - *Guide for Consent Records using DPV* (being updated for v1)
  - *Guide for GDPR DPIA's using DPV* (being updated for v1)
  - *Guide for GDPR ROPA's using DPV* (being updated for v1)
- Other Resources:
  - *DPV Use-Cases and Requirements*
  - *DPV Examples*
  - *NACE Taxonomy serialised in RDFS*
  - *Extension providing EU Rights* serialisations: [RIGHTS-EU-SKOS], [RIGHTS-EU-OWL]

ODRL profile for Access Control (OAC)

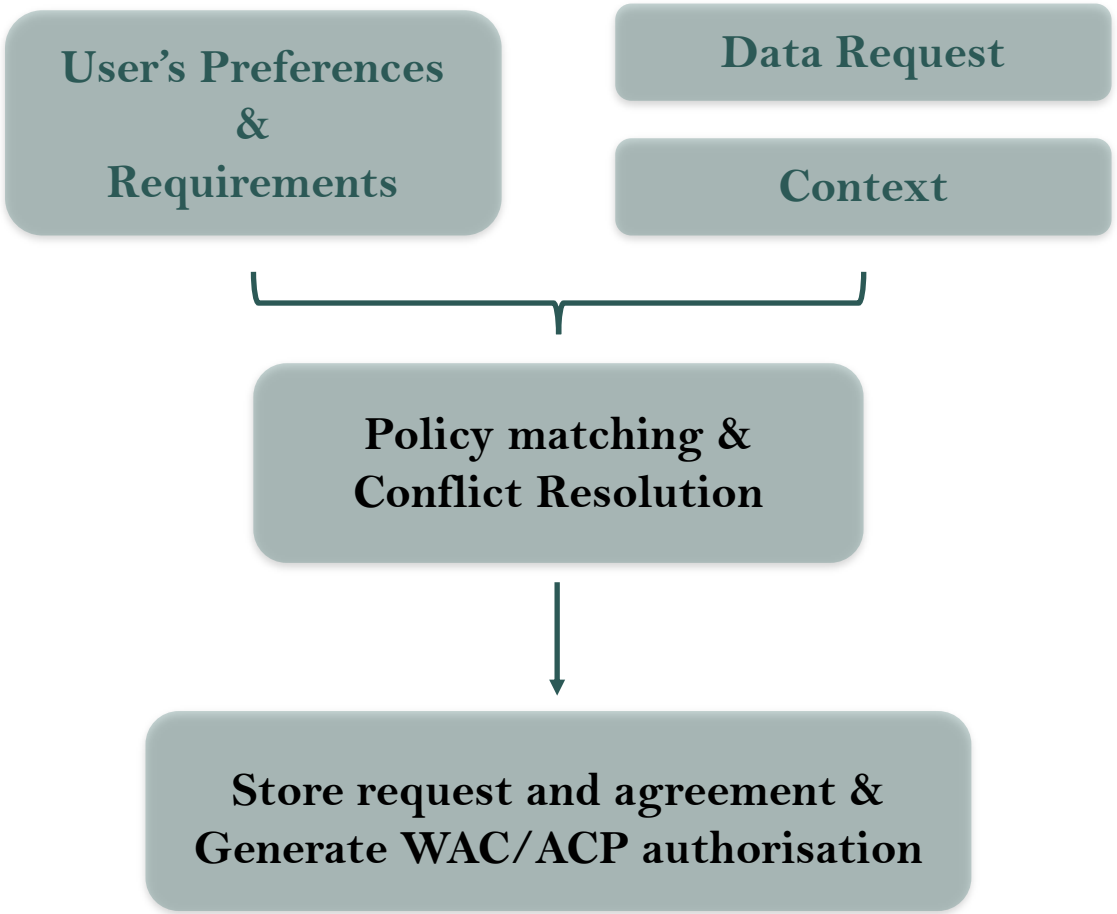
Collection of ODRL policies

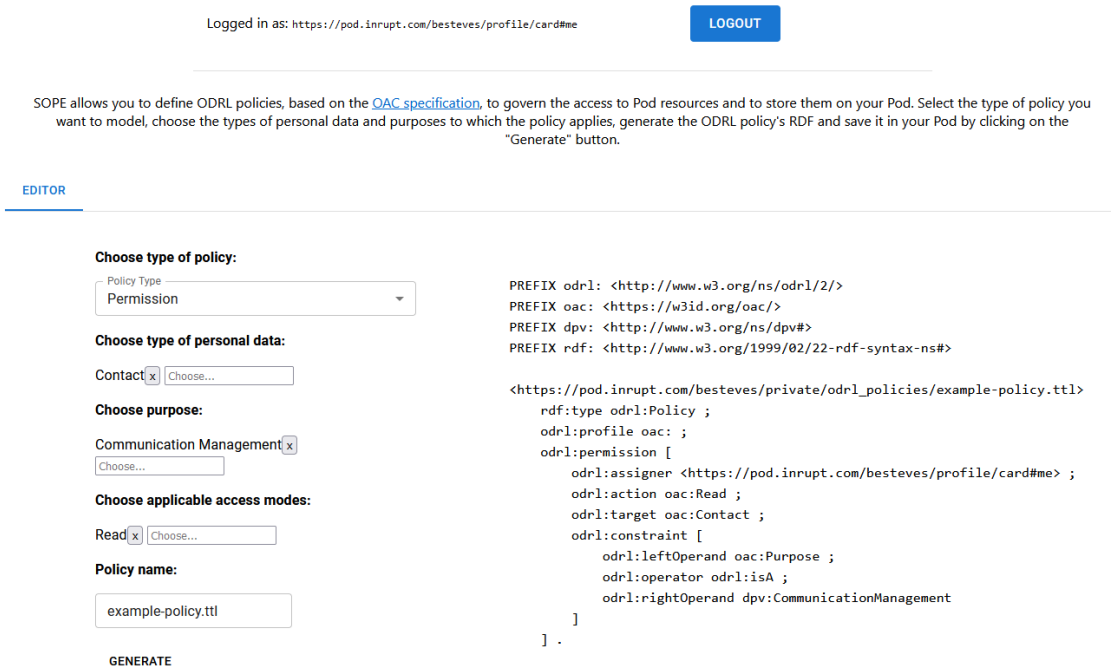
https://github.com/besteves4/oac-policies



https://w3id.org/oac

ODRL profile for Access Control (OAC)





https://github.com/besteves4/solid-sope

Esteves, B., Rodríguez-Doncel, V., Pandit, H.J., Mondada, N., McBennett, P. (2022). "Using the ODRL Profile for Access Control for Solid Pod Resource Governance". In: *The Semantic Web: ESWC 2022 Satellite Events*. ESWC 2022. Lecture Notes in Computer Science, vol 13384. Springer, Cham. https://doi.org/10.1007/978-3-031-11609-4_3

Using Policies – User Offer

```
<https://example.com/offer1> a odrl:Offer ;
  dct:description "Offer to read identifier data for identity
  ↪ verification and demographic data for research and development" ;
  dct:source ex:preference1, ex:requirement1 ;
  dct:creator ex:userA ;
  dct:issued "2022-11-08T17:26:35"^^xsd:dateTime ;
  odrl:uid ex:offer1 ;
  odrl:profile oac: ;
  odrl:assigner ex:userA ;
  odrl:permission [
    dpv:hasContext dpv:Optional ;
    odrl:target oac:Demographic ;
    odrl:action oac:Read ;
    odrl:constraint [
      dct:title "Purpose for access is to conduct research and
      ↪ development." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:ResearchAndDevelopment ] ] ;
  odrl:permission [
    dpv:hasContext dpv:Required ;
    odrl:target oac:Identifier ;
    odrl:action oac:Read ;
    odrl:constraint [
      dct:title "Purpose for access is to verify the identity of the
      ↪ assigner." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:IdentityVerification ] ] .
```

Using Policies – User Offer & Data Request

```
<https://example.com/offer1> a odrl:Offer ;
  dct:description "Offer to read identifier data for identity
  ↪ verification and demographic data for research and development" ;
  dct:source ex:preference1, ex:requirement1 ;
  dct:creator ex:userA ;
  dct:issued "2022-11-08T17:26:35"^^xsd:dateTime ;
  odrl:uid ex:offer1 ;
  odrl:profile oac: ;
  odrl:assigner ex:userA ;
  odrl:permission [
    dpv:hasContext dpv:Optional ;
    odrl:target oac:Demographic ;
    odrl:action oac:Read ;
    odrl:constraint [
      dct:title "Purpose for access is to conduct research and
      ↪ development." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:ResearchAndDevelopment ] ] ;
  odrl:permission [
    dpv:hasContext dpv:Required ;
    odrl:target oac:Identifier ;
    odrl:action oac:Read ;
    odrl:constraint [
      dct:title "Purpose for access is to verify the identity of the
      ↪ assigner." ;
      odrl:leftOperand oac:Purpose ;
      odrl:operator odrl:isA ;
      odrl:rightOperand dpv:IdentityVerification ] ] .
```

```
<https://example.com/request1> a odrl:Request ;
  dct:description "Request to use physical trait data in a R&D project" ;
  dct:creator ex:userB ;
  dct:issued "2022-11-08T17:58:31"^^xsd:dateTime ;
  odrl:uid ex:request1;
  odrl:profile oac: ;
  odrl:permission [
    odrl:assignee ex:userB ;
    odrl:action oac:Use ;
    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 ] ] .

ex:RDProjectX a dpv:ResearchAndDevelopment ;
  rdfs:label "Conduct research in the R&D project X." .
```

Using Policies – Consent Agreement

```
<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 ] ] .
```

Challenges

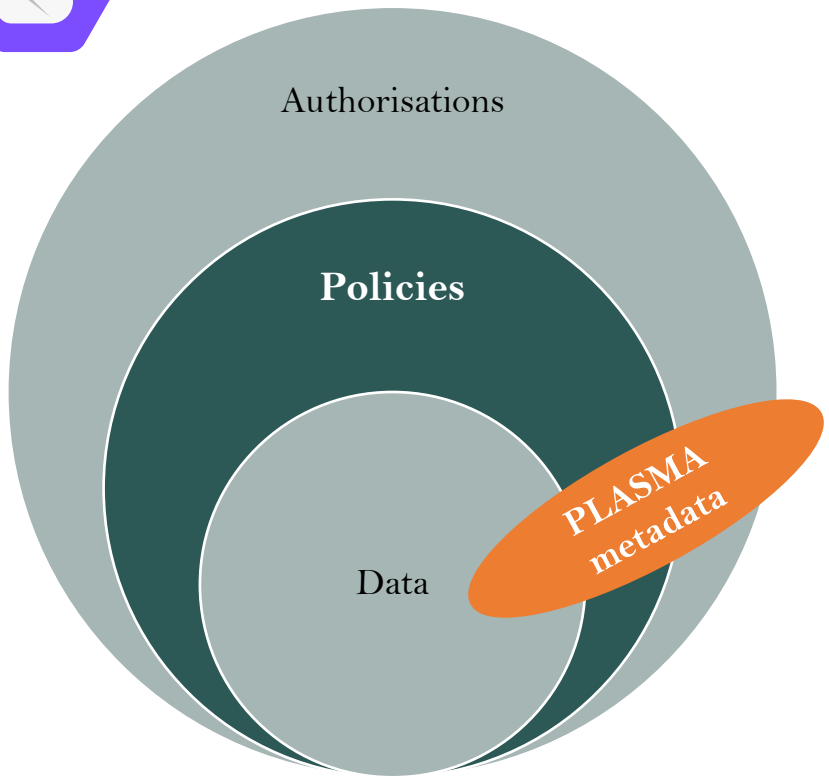
- Associate Pod resources with the data type they contain
- Deal with processing activities beyond access – share, make a copy, …
- Generate WAC / ACP authorisations from the result of the policy matching

Using Policies + Metadata

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. Record (store) policies used to authorize access.
R5. Keep information about the developers and/or providers of Pods, apps, services, data, identity, infrastructure, …
R6. Keep activity logs (what? who? why? where? when? how?) to establish responsibilities and accountability within the Solid ecosystem.
R7. Maintain registries (of policies, users, apps, data, …) for convenient access to data and metadata within a Pod.

OAC + PLASMA



PLASMA - Policy LAnguage for Solid's Metadata-based Access control

TABLE OF CONTENTS

PLASMA

Policy Language for Solid's Metadata-based Access Control

Unofficial Draft 01 November 2022

▾ **More details about this document**

Latest published version:
https://harshp.com/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, Trinity College Dublin)

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

Source: Flaticon

Abstract

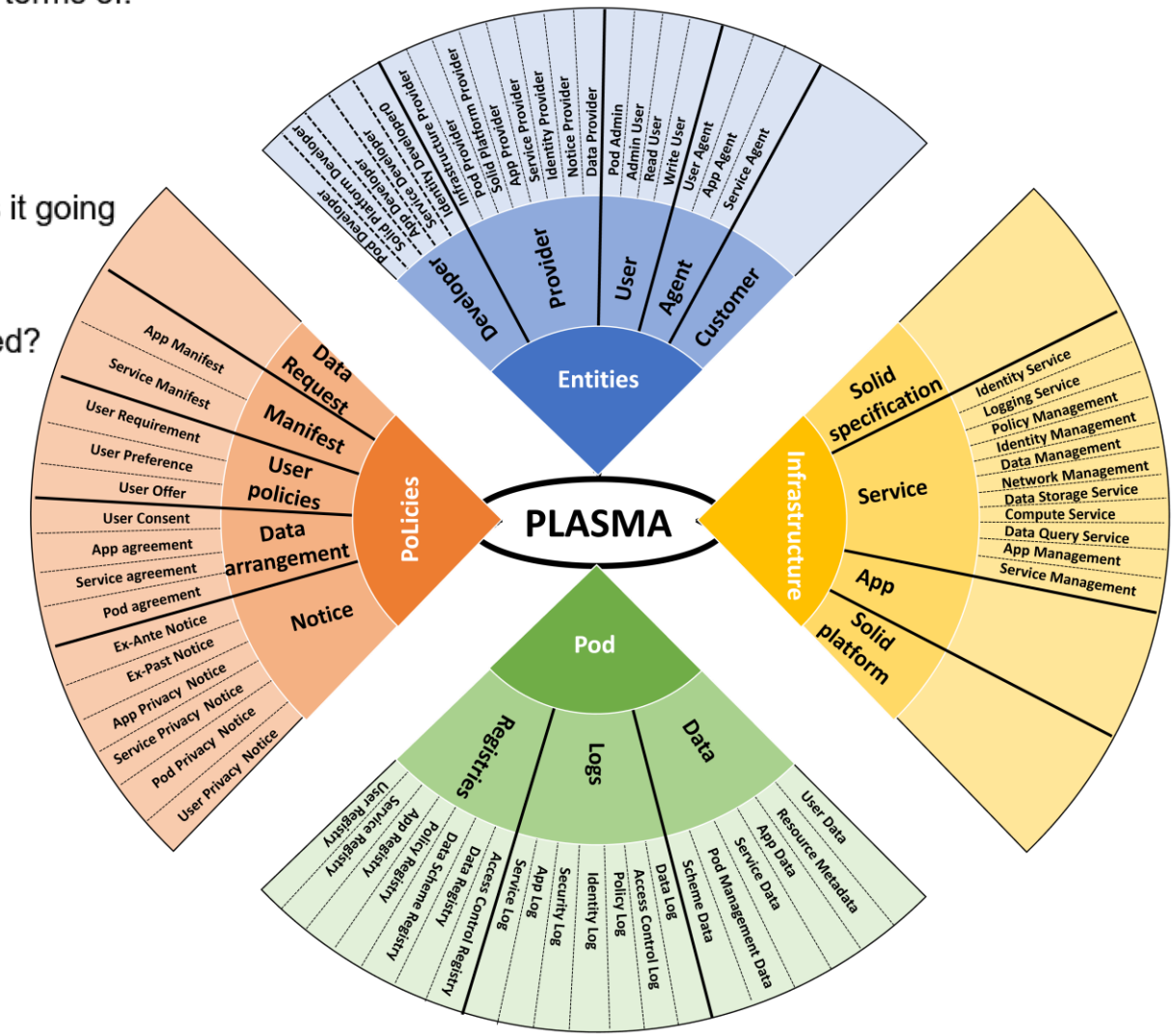
Currently, the Solid protocol and its specifications lack the terms to express metadata related to the entities,

PLASMA - Policy LAnguage for Solid's Metadata-based Access control

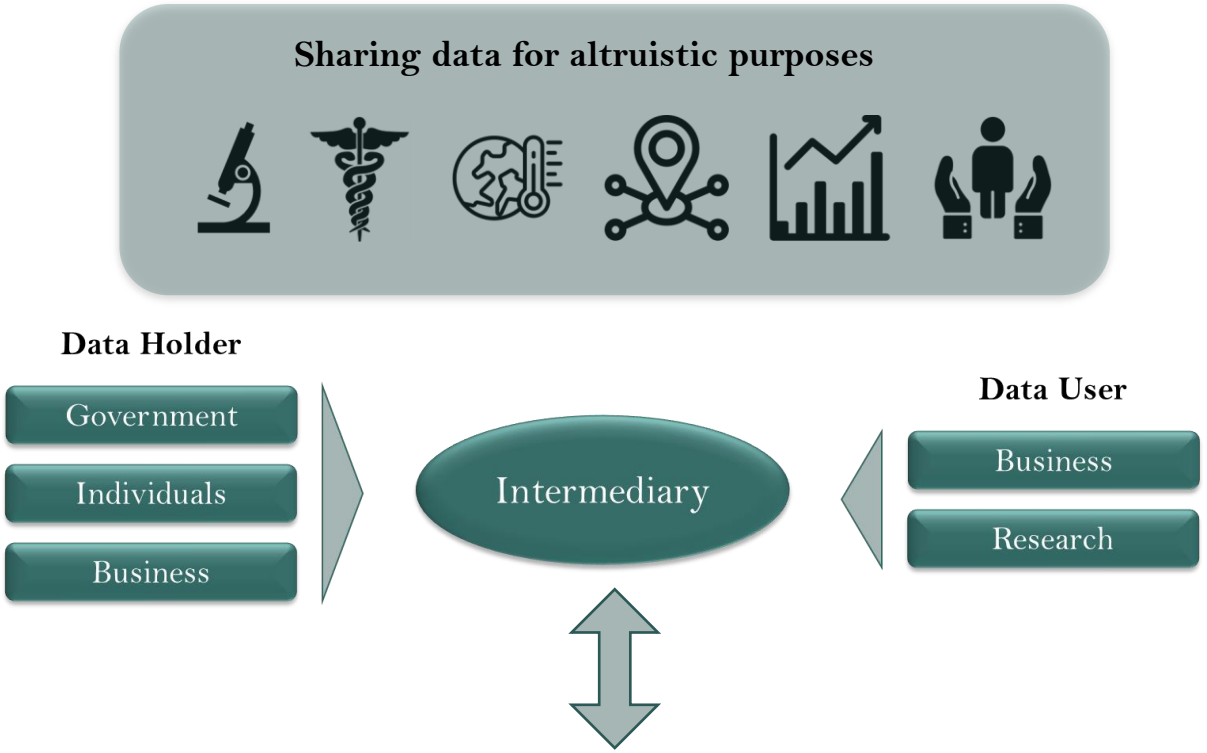
PLASMA aims to provide a set of taxonomies to express Solid-related use-cases in terms of:

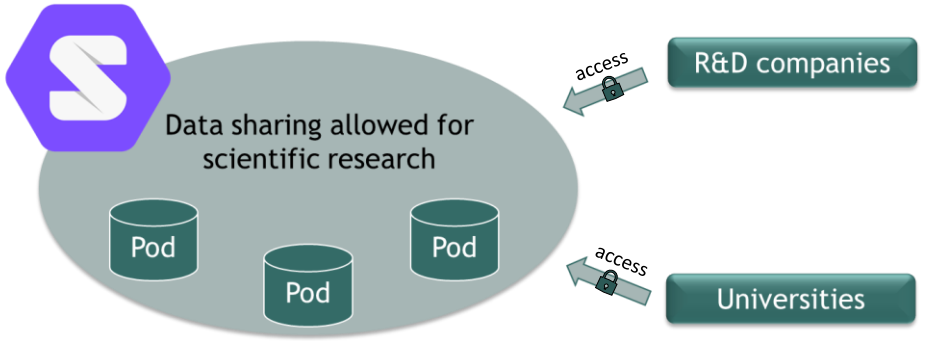
- *What?* i.e. the data in question
- *Who?* i.e. who's data and who is requesting/using/providing it
- *Where?* i.e. where the data is coming from, where it will be stored and where is it going
- *Why?* i.e. for what purpose is the data being requested/used/shared?
- *When?* i.e. over what temporal duration is the data being requested/used/shared?
- *How?* i.e. how is this being done, by what means and technologies

PLASMA



New data regulations – DGA, Data Act, Health Data Spaces, …





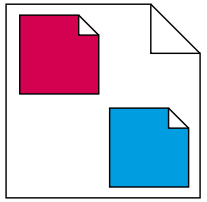
Policies for the (re)use of data

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

```
ex:policy1 a odrl:Offer ;
   odrl:profile oac: ; odrl:uid ex:policy1 ;
   odrl:permission [
      odrl:assigner <https://beatriz.providerZ.com/profile/card#me> ;
      odrl:target oac:Demographic ;
      odrl:action odrl:use ;
      odrl:constraint [
         odrl:leftOperand oac:Purpose ;
         odrl:operator odrl:isA ;
         odrl:rightOperand :CombatClimateChange ] ] .
```

Conclusions & Future Work

- Ensure compatibility of Solid servers, apps and services with the new *policy layer*
- Maintain and update vocabularies according to the requirements mandated by new data-related regulations and guidelines from European supervisory authorities.
- Have different template policies for different use cases – the Pod can be created with a predefined set of policies according to the data that is going to be stored
- Explore RDF surfaces as a new component to validate policies, reason over user preferences and data requests and perform usage control



Protect

Enhancing Solid with Legally-aware Policies

Beatriz Esteves, Ontology Engineering Group, Universidad Politécnica de Madrid
beatriz.gesteves@upm.es | besteves4@eupolicy.social

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 813497.

Ontology Engineering Group

POLITÉCNICA