# Balancing Access and Privacy of Personal Health Data

Beatriz Esteves, UGent – imec

# Balancing Access and Privacy of Personal Health Data

Data is not flowing properly

From raw data to Digital Trust

Health data sharing with ODRL and DPV

# Balancing Access and Privacy of Personal Health Data

Data is not flowing properly

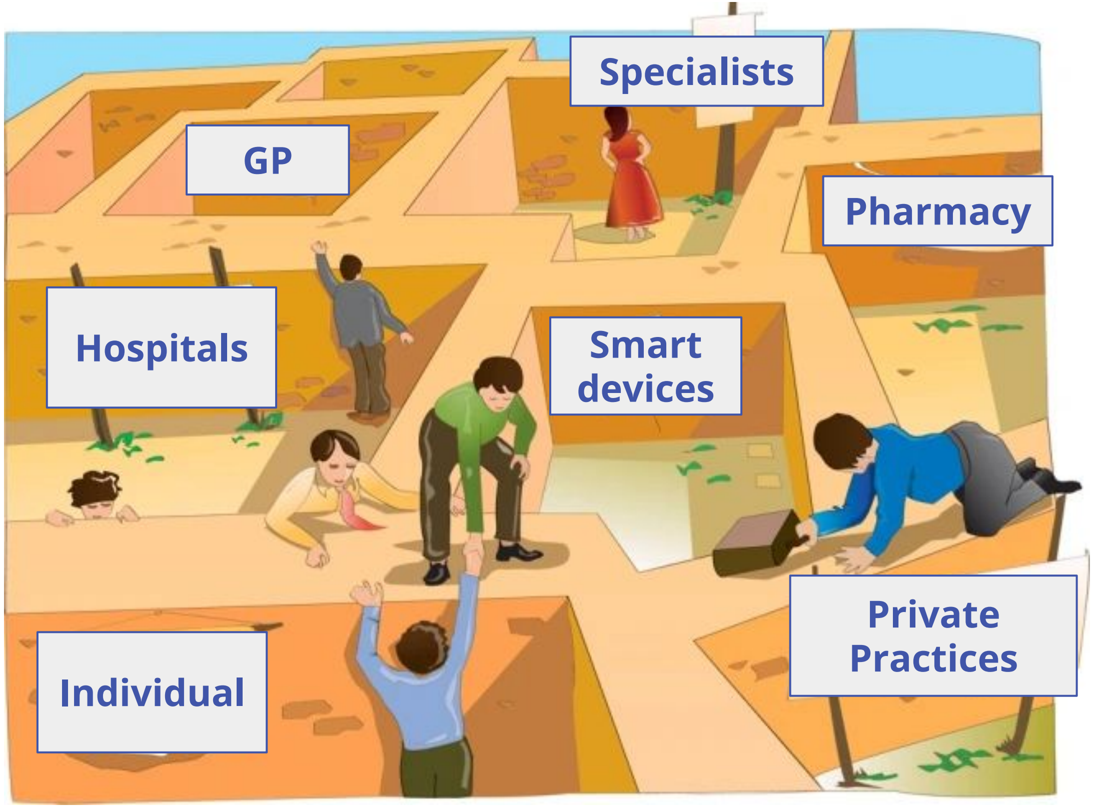
From raw data to Digital Trust

Health data sharing with ODRL and DPV

# Data doesn't flow well enough…

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

# Data doesn’t flow well enough…

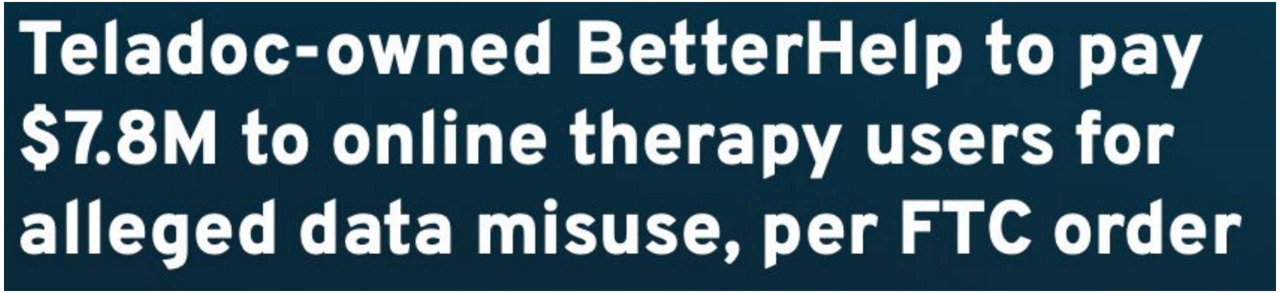


THE BATTLE OF THE INTERNET: OPEN VS CLOSED – FURTHER EXPLORATION, Christopher Langley

# … or its flowing in the wrong way

*“**2023 was the worst-ever year for breached healthcare records** with breached records i**ncreasing by 156% from 2022** to 133,068,542 breached records, beating the previous record of 113 million records set in 2015. In 2023, an **average of 373,788 healthcare records were breached every day**.” [In the US only]*

Security Breaches in Healthcare in 2023, The HIPPA Journal



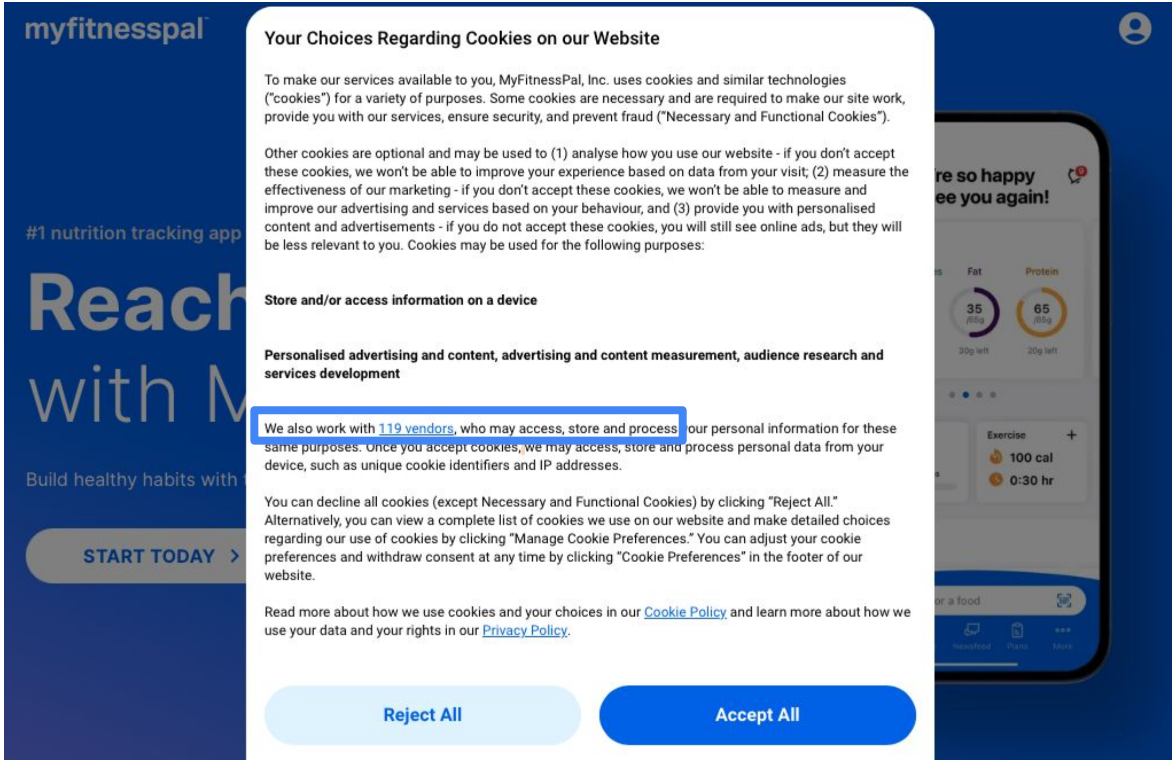
Teladoc-owned BetterHelp to pay $7.8M to online therapy users for alleged data misuse, per FTC order

FIERCE Healthcare

# Transparency as an obligation

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

# And if that wasn’t enough…



Your Choices Regarding Cookies on our Website

To make our services available to you, MyFitnessPal, Inc. uses cookies and similar technologies ("cookies") for a variety of purposes. Some cookies are necessary and are required to make our site work, provide you with our services, ensure security, and prevent fraud ("Necessary and Functional Cookies").

Other cookies are optional and may be used to (1) analyse how you use our website - if you don't accept these cookies, we won't be able to improve your experience based on data from your visit; (2) measure the effectiveness of our marketing - if you don't accept these cookies, we won't be able to measure and improve our advertising and services based on your behaviour, and (3) provide you with personalised content and advertisements - if you do not accept these cookies, you will still see online ads, but they will be less relevant to you. Cookies may be used for the following purposes:

**Store and/or access information on a device**

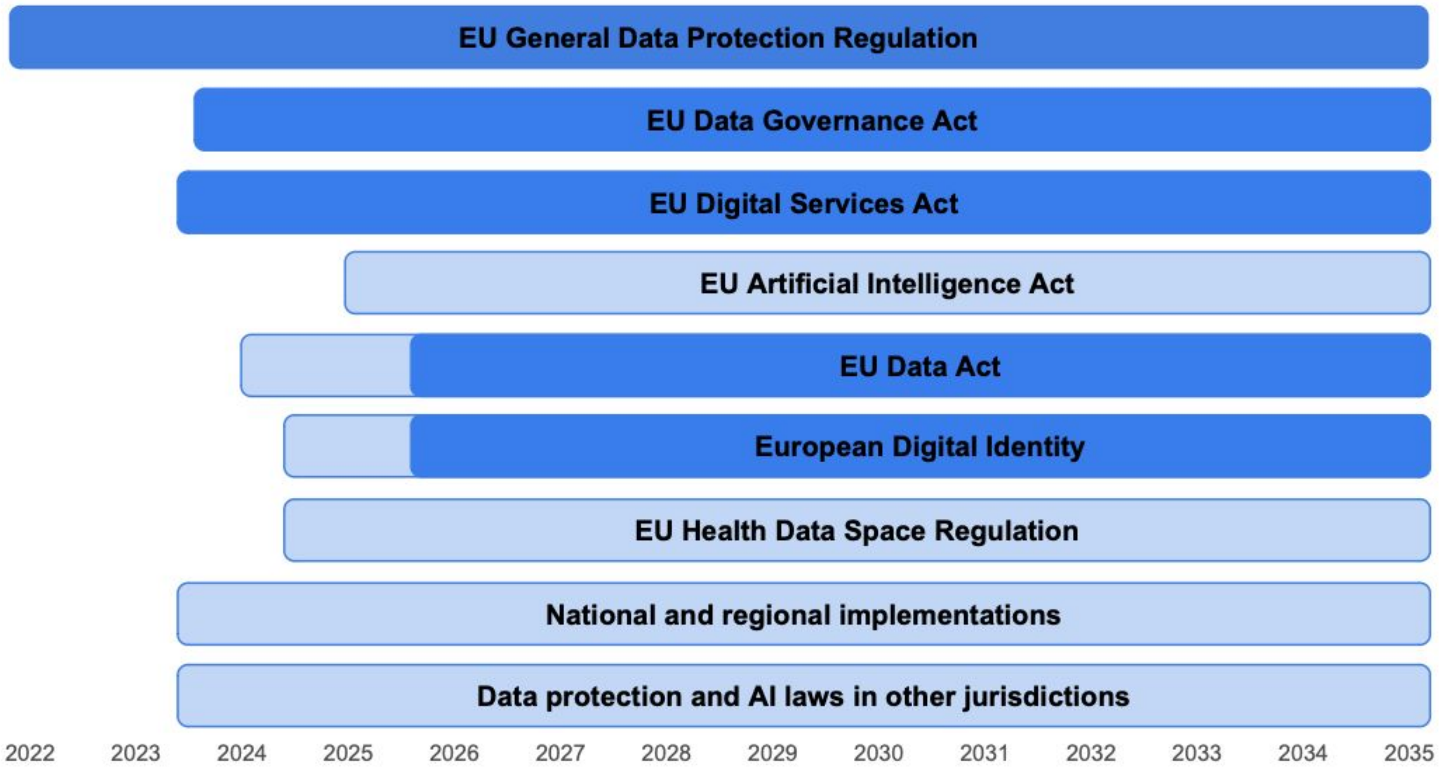
**Personalised advertising and content, advertising and content measurement, audience research and services development**

We also work with 119 vendors, who may access, store and process your personal information for these same purposes. Once you accept cookies, we may access, store and process personal data from your device, such as unique cookie identifiers and IP addresses.

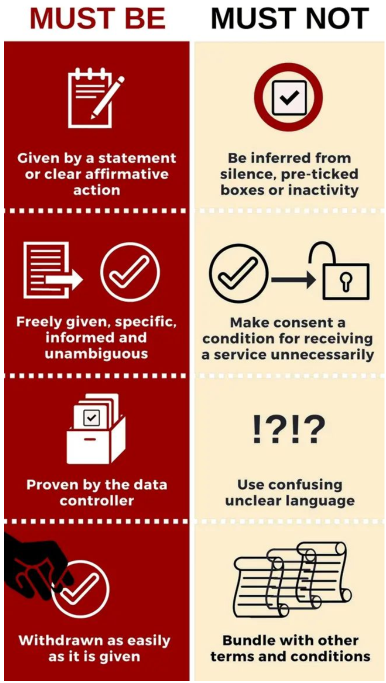
You can decline all cookies (except Necessary and Functional Cookies) by clicking "Reject All." Alternatively, you can view a complete list of cookies we use on our website and make detailed choices regarding our use of cookies by clicking "Manage Cookie Preferences." You can adjust your cookie preferences and withdraw consent at any time by clicking "Cookie Preferences" in the footer of our website.

Read more about how we use cookies and your choices in our Cookie Policy and learn more about how we use your data and your rights in our Privacy Policy.

# And if that wasn’t enough v2…



# Consent will never scale



| MUST BE | MUST NOT |
|---|---|
| Given by a statement or clear affirmative action | Be inferred from silence, pre-ticked boxes or inactivity |
| Freely given, specific, informed and unambiguous | Make consent a condition for receiving a service unnecessarily |
| Proven by the data controller | !?!?<br>Use confusing unclear language |
| Withdrawn as easily as it is given | Bundle with other terms and conditions |

foiman.com

# Consent will never scale

PAY
CONSENT
?
SHOW ME THE MONEY!

Dall-E rendering of how the EDPB views choices
https://www.linkedin.com/pulse/op-ed-critical-analysis-edpbs-pay-consent-opinion-peter-craddock-obl3e/

# Balancing Access and Privacy of Personal Health Data

Data is not flowing properly

From raw data to Digital Trust

Health data sharing with ODRL and DPV

# Technical contracts ≠ legal contracts

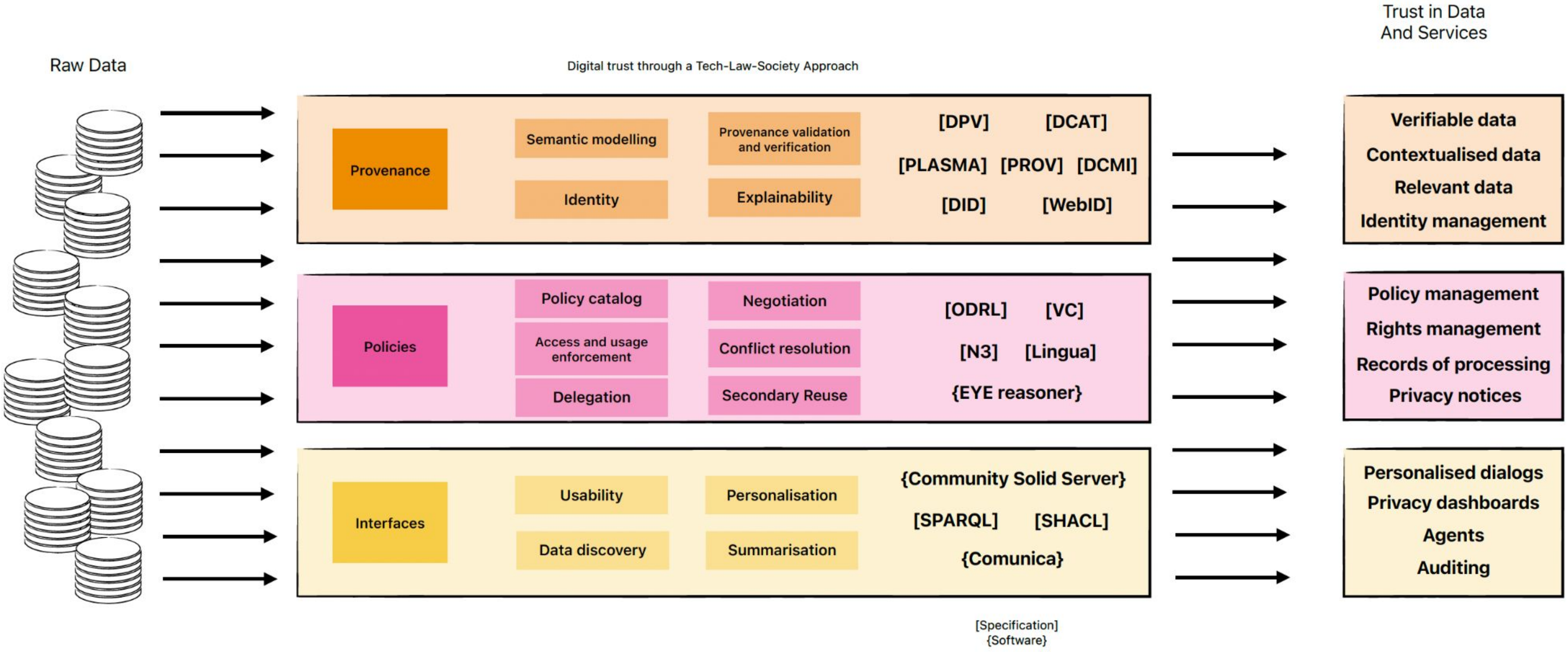
- Technical contracts focus on usage and pricing of data and services
- Legal contracts focus on the rights and obligations of the involved parties

- We want to bridge this gap by having services that allow the *negotiation* of which legal ground to use and move away from the overuse and misuse of consent

# From raw data to digital trust

- **Trust is a shared human understanding...**
  - It grows and evolves over time
- **Make data flow better...**
  - People want to know that their data is being used according to their wishes
    - Rights exercising made easy
  - Businesses need to have data available at the right time
    - Data is relevant / correct / complete
    - Legal compliance made easy

# How are we making it happen?



Raw Data

Digital trust through a Tech-Law-Society Approach

Trust in Data
And Services

Provenance

Semantic modelling

Provenance validation and verification

Identity

Explainability

[DPV] [DCAT]

[PLASMA] [PROV] [DCMI]

[DID] [WebID]

Verifiable data

Contextualised data

Relevant data

Identity management

Policies

Policy catalog

Negotiation

Access and usage enforcement

Conflict resolution

Delegation

Secondary Reuse

[ODRL] [VC]

[N3] [Lingua]

{EYE reasoner}

Policy management

Rights management

Records of processing

Privacy notices

Interfaces

Usability

Personalisation

Data discovery

Summarisation

{Community Solid Server}

[SPARQL] [SHACL]

{Comunica}

Personalised dialogs

Privacy dashboards

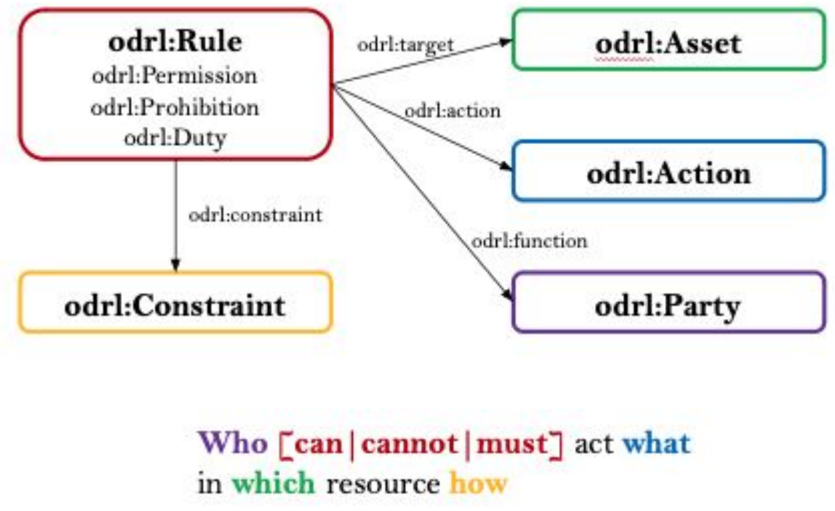
Agents

Auditing

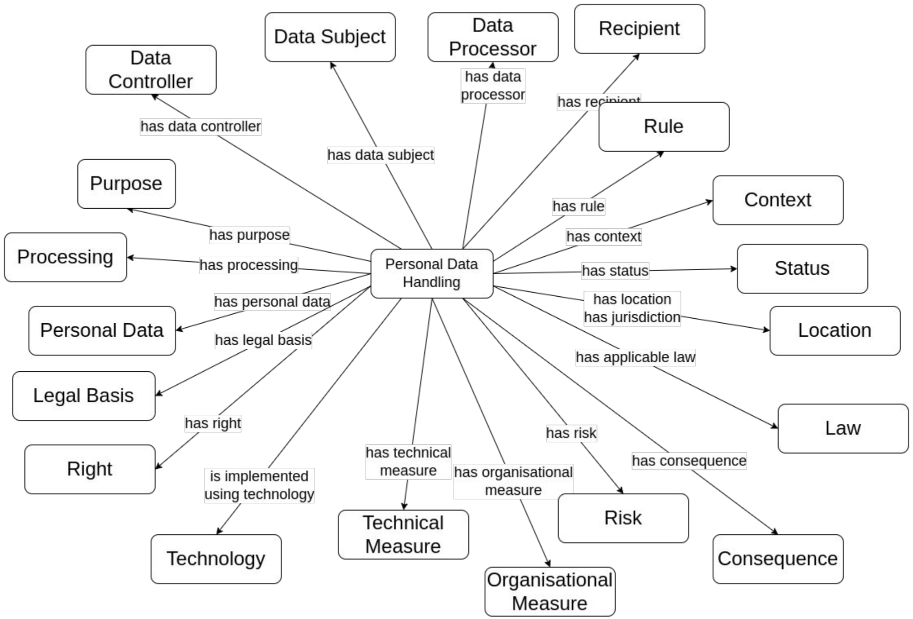
[Specification]
{Software}

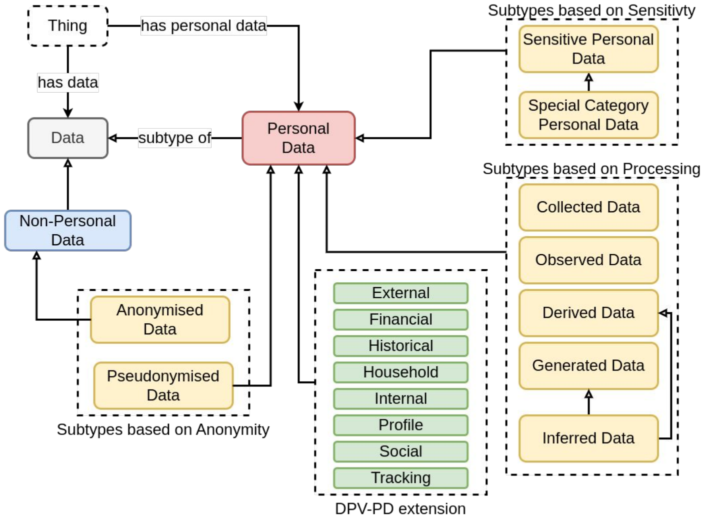
# Open Digital Rights Language (ODRL)

- 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



# Data Privacy Vocabulary (DPV)





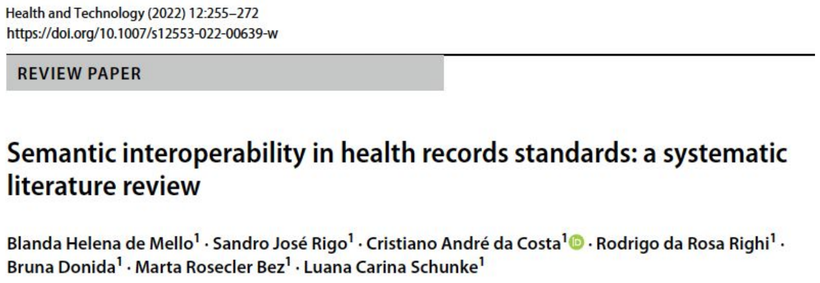
## Balancing Access and Privacy of Personal Health Data

Data is not flowing properly

From raw data to Digital Trust

Health data sharing with ODRL and DPV

# Initiatives to achieve interoperability in healthcare

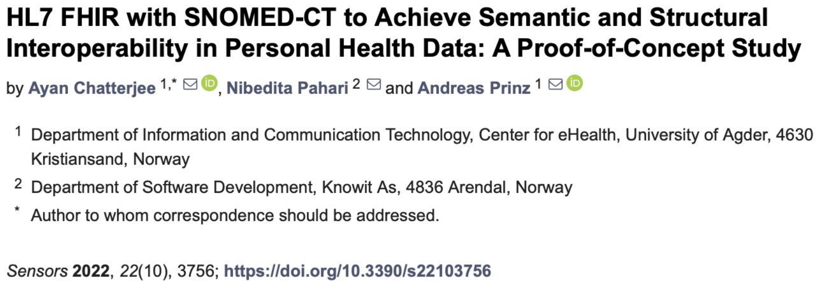


Health and Technology (2022) 12:255–272
https://doi.org/10.1007/s12553-022-00639-w

REVIEW PAPER

**Semantic interoperability in health records standards: a systematic literature review**

Blanda Helena de Mello[1] · Sandro José Rigo[1] · Cristiano André da Costa[1] · Rodrigo da Rosa Righi[1] · Bruna Donida[1] · Marta Rosecler Bez[1] · Luana Carina Schunke[1]



**HL7 FHIR with SNOMED-CT to Achieve Semantic and Structural Interoperability in Personal Health Data: A Proof-of-Concept Study**

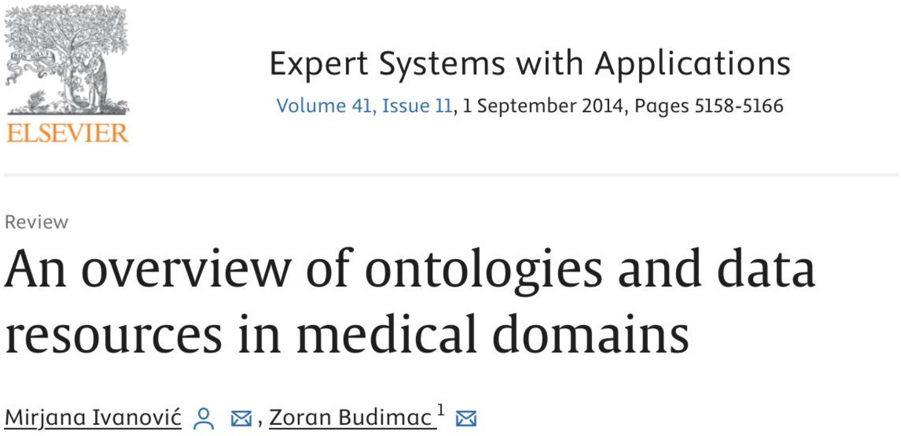
by Ayan Chatterjee [1,*], Nibedita Pahari [2] and Andreas Prinz [1]

[1] Department of Information and Communication Technology, Center for eHealth, University of Agder, 4630 Kristiansand, Norway

[2] Department of Software Development, Knowit As, 4836 Arendal, Norway

[*] Author to whom correspondence should be addressed.

*Sensors* **2022**, *22*(10), 3756; https://doi.org/10.3390/s22103756



ELSEVIER

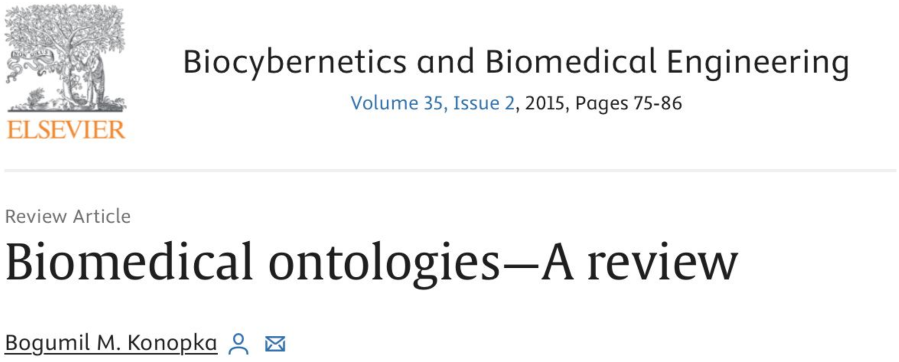
Expert Systems with Applications

Volume 41, Issue 11, 1 September 2014, Pages 5158-5166

Review

An overview of ontologies and data resources in medical domains

Mirjana Ivanović, Zoran Budimac [1]



ELSEVIER

Biocybernetics and Biomedical Engineering

Volume 35, Issue 2, 2015, Pages 75-86

Review Article

Biomedical ontologies—A review

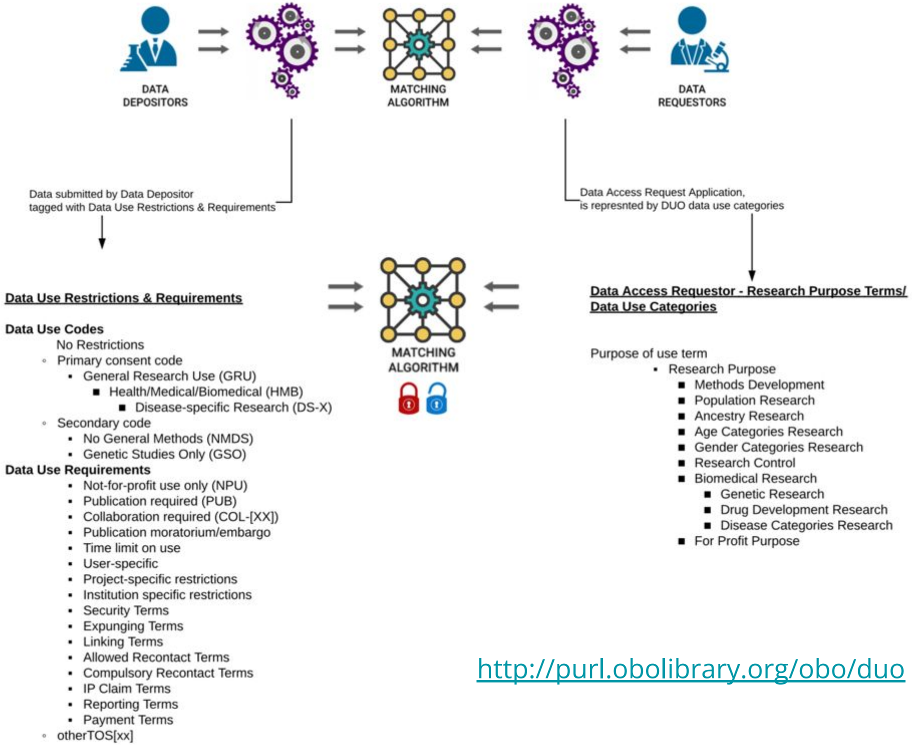
Bogumil M. Konopka

# Global Alliance for Genomics and Health (GA4GH)

*The not-for-profit Global Alliance for Genomics and Health (GA4GH) sets standards and frames policies to expand genomic data use within a human rights framework.*

https://www.ga4gh.org/

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



Data submitted by Data Depositor tagged with Data Use Restrictions & Requirements

Data Access Request Application, is represnted by DUO data use categories

**Data Use Restrictions & Requirements**

**Data Use Codes**
- No Restrictions
- Primary consent code
  - General Research Use (GRU)
    - Health/Medical/Biomedical (HMB)
      - Disease-specific Research (DS-X)
- Secondary code
  - No General Methods (NMDS)
  - Genetic Studies Only (GSO)

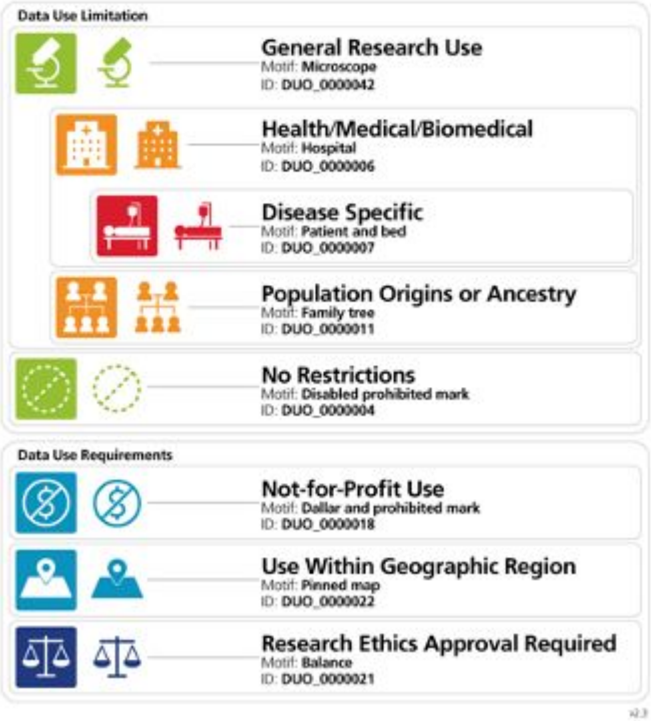
**Data Use Requirements**
- Not-for-profit use only (NPU)
- Publication required (PUB)
- Collaboration required (COL-[XX])
- Publication moratorium/embargo
- Time limit on use
- User-specific
- Project-specific restrictions
- Institution specific restrictions
- Security Terms
- Expunging Terms
- Linking Terms
- Allowed Recontact Terms
- Compulsory Recontact Terms
- IP Claim Terms
- Reporting Terms
- Payment Terms
- otherTOS[xx]

**Data Access Requestor - Research Purpose Terms/ Data Use Categories**

Purpose of use term
- Research Purpose
  - Methods Development
  - Population Research
  - Ancestry Research
  - Age Categories Research
  - Gender Categories Research
  - Research Control
  - Biomedical Research
    - Genetic Research
    - Drug Development Research
    - Disease Categories Research
  - For Profit Purpose

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

# Data Use Ontology (DUO)



Data Use Limitation

General Research Use
Motif: Microscope
ID: DUO_0000042

Health/Medical/Biomedical
Motif: Hospital
ID: DUO_0000006

Disease Specific
Motif: Patient and bed
ID: DUO_0000007

Population Origins or Ancestry
Motif: Family tree
ID: DUO_0000011

No Restrictions
Motif: Disabled prohibited mark
ID: DUO_0000004

Data Use Requirements

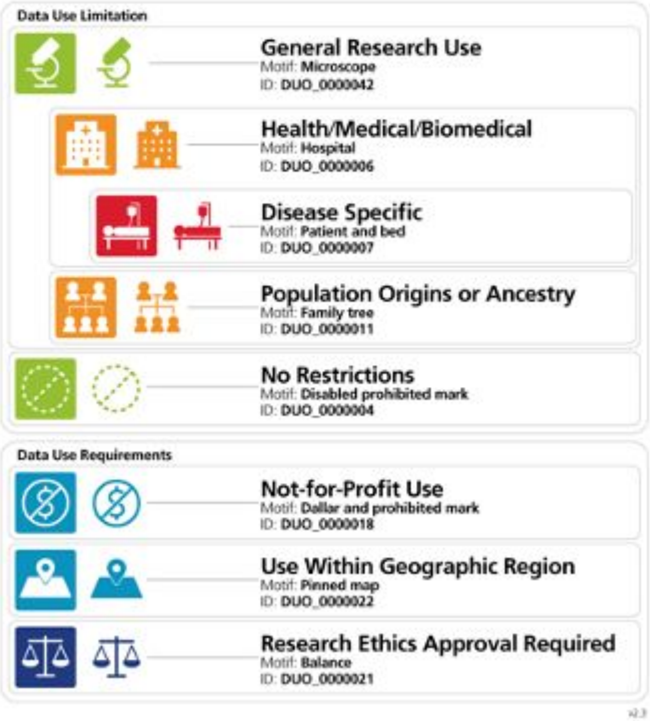
Not-for-Profit Use
Motif: Dallar and prohibited mark
ID: DUO_0000018

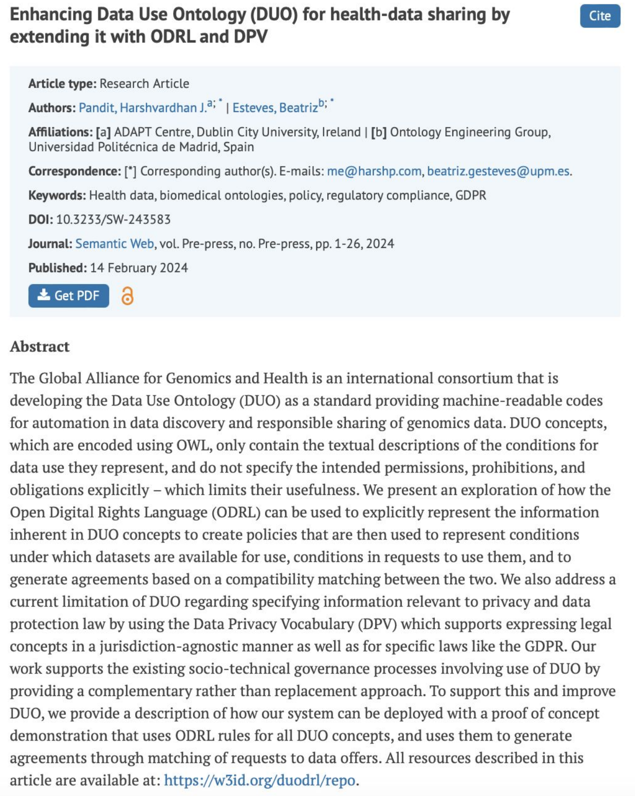
Use Within Geographic Region
Motif: Pinned map
ID: DUO_0000022

Research Ethics Approval Required
Motif: Balance
ID: DUO_0000021

v2.3

# Data Use Ontology (DUO)





## Enhancing Data Use Ontology (DUO) for health-data sharing by extending it with ODRL and DPV

Cite

**Article type:** Research Article

**Authors:** Pandit, Harshvardhan J.[a; *] | Esteves, Beatriz[b; *]

**Affiliations:** [a] ADAPT Centre, Dublin City University, Ireland | [b] Ontology Engineering Group, Universidad Politécnica de Madrid, Spain

**Correspondence:** [*] Corresponding author(s). E-mails: me@harshp.com, beatriz.gesteves@upm.es.

**Keywords:** Health data, biomedical ontologies, policy, regulatory compliance, GDPR

**DOI:** 10.3233/SW-243583

**Journal:** Semantic Web, vol. Pre-press, no. Pre-press, pp. 1-26, 2024

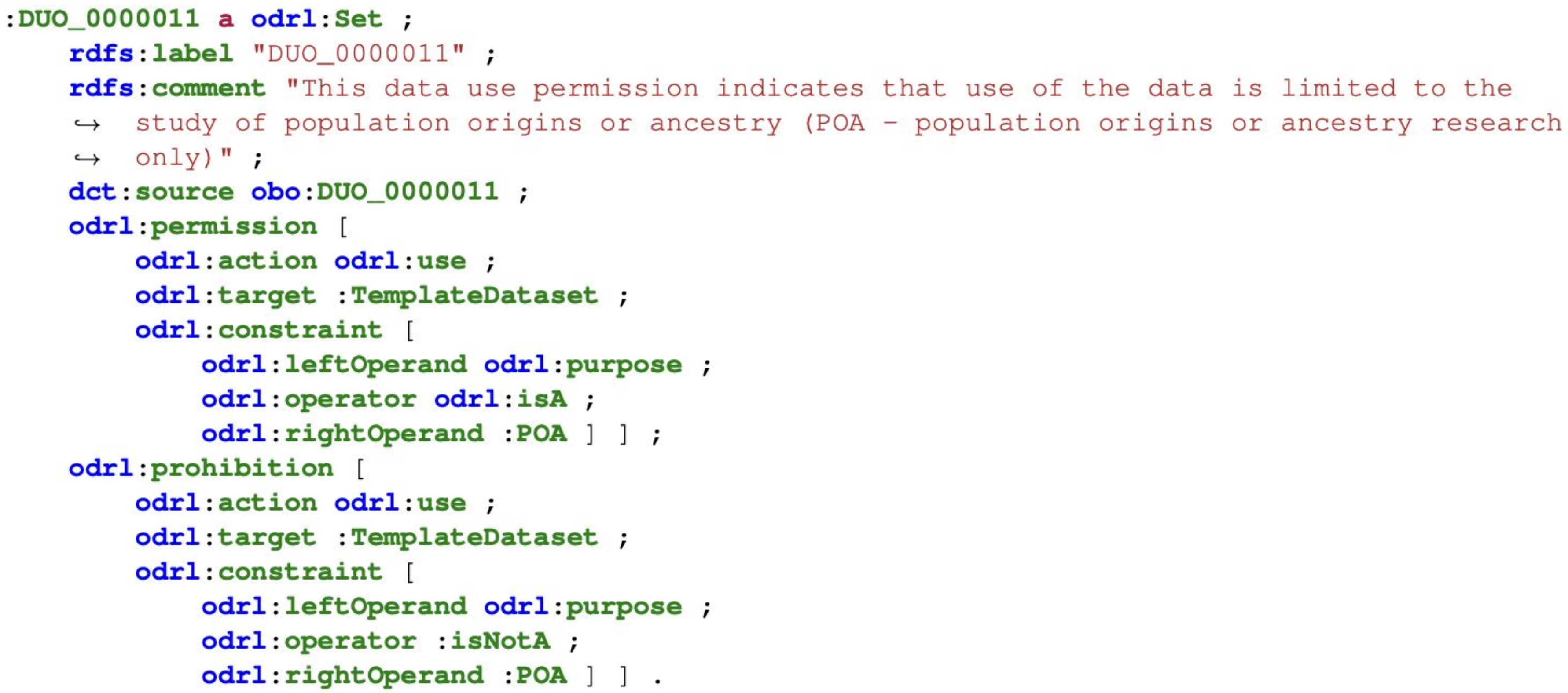
**Published:** 14 February 2024

Get PDF

### Abstract

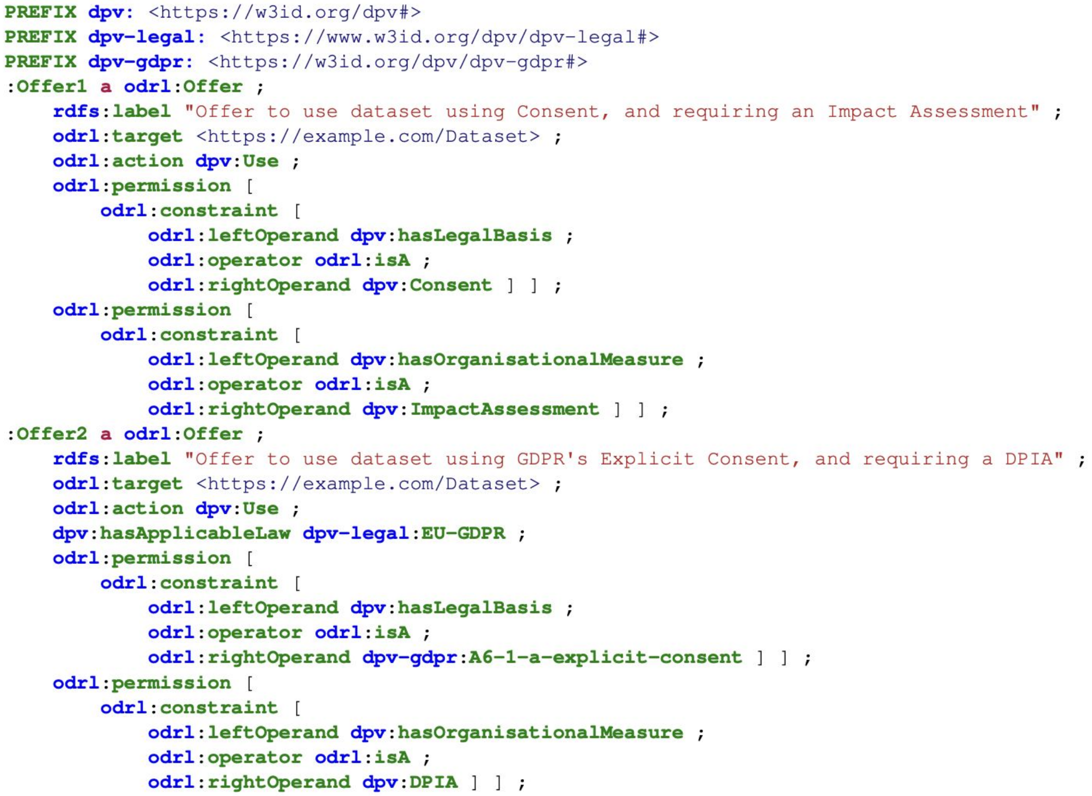
The Global Alliance for Genomics and Health is an international consortium that is developing the Data Use Ontology (DUO) as a standard providing machine-readable codes for automation in data discovery and responsible sharing of genomics data. DUO concepts, which are encoded using OWL, only contain the textual descriptions of the conditions for data use they represent, and do not specify the intended permissions, prohibitions, and obligations explicitly – which limits their usefulness. We present an exploration of how the Open Digital Rights Language (ODRL) can be used to explicitly represent the information inherent in DUO concepts to create policies that are then used to represent conditions under which datasets are available for use, conditions in requests to use them, and to generate agreements based on a compatibility matching between the two. We also address a current limitation of DUO regarding specifying information relevant to privacy and data protection law by using the Data Privacy Vocabulary (DPV) which supports expressing legal concepts in a jurisdiction-agnostic manner as well as for specific laws like the GDPR. Our work supports the existing socio-technical governance processes involving use of DUO by providing a complementary rather than replacement approach. To support this and improve DUO, we provide a description of how our system can be deployed with a proof of concept demonstration that uses ODRL rules for all DUO concepts, and uses them to generate agreements through matching of requests to data offers. All resources described in this article are available at: https://w3id.org/duodrl/repo.

# Enhancing DUO with ODRL

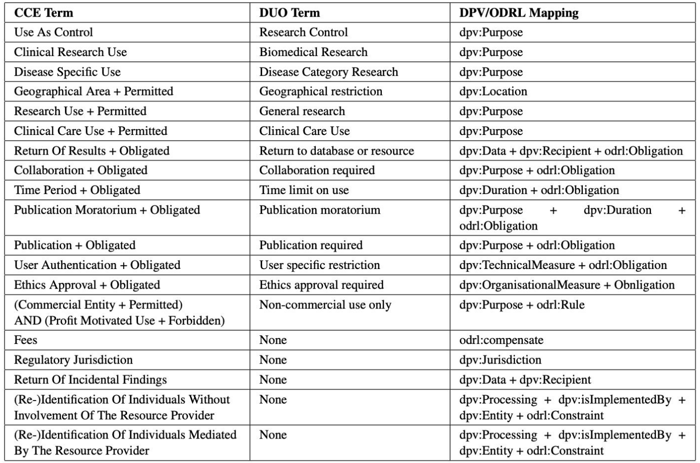


```
:DUO_0000011 a odrl:Set ;
    rdfs:label "DUO_0000011" ;
    rdfs:comment "This data use permission indicates that use of the data is limited to the
    ↪  study of population origins or ancestry (POA - population origins or ancestry research
    ↪  only)" ;
    dct:source obo:DUO_0000011 ;
    odrl:permission [
        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 ] ] .
```

# Enhancing DUO with ODRL and DPV



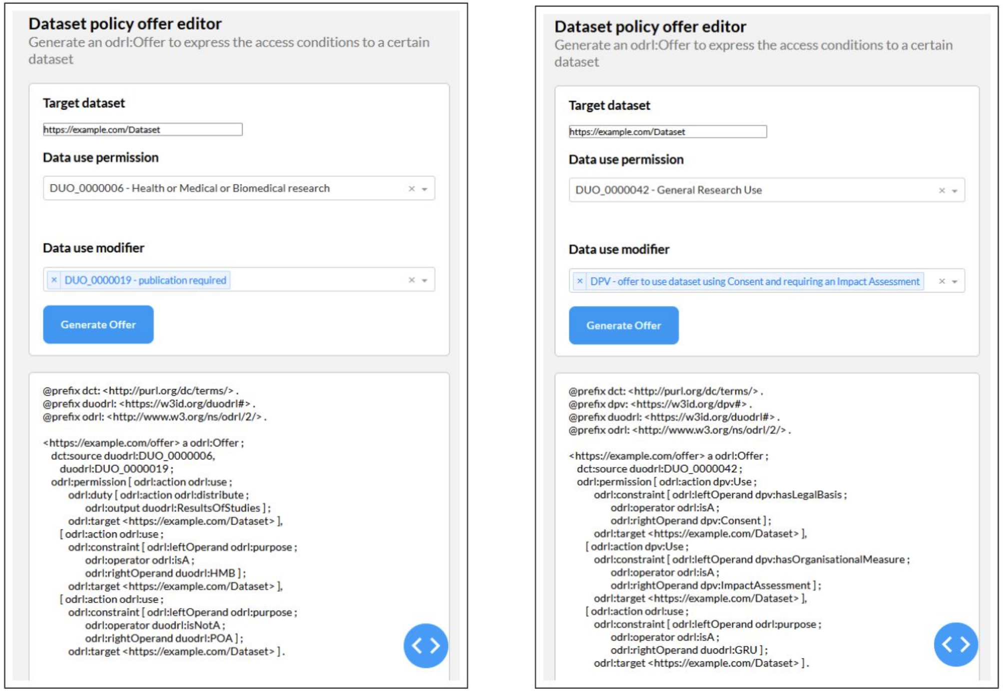
```
PREFIX dpv: <https://w3id.org/dpv#>
PREFIX dpv-legal: <https://www.w3id.org/dpv/dpv-legal#>
PREFIX dpv-gdpr: <https://w3id.org/dpv/dpv-gdpr#>
:Offer1 a odrl:Offer ;
    rdfs:label "Offer to use dataset using Consent, and requiring an Impact Assessment" ;
    odrl:target <https://example.com/Dataset> ;
    odrl:action dpv:Use ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand dpv:hasLegalBasis ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:Consent ] ] ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand dpv:hasOrganisationalMeasure ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:ImpactAssessment ] ] ;
:Offer2 a odrl:Offer ;
    rdfs:label "Offer to use dataset using GDPR's Explicit Consent, and requiring a DPIA" ;
    odrl:target <https://example.com/Dataset> ;
    odrl:action dpv:Use ;
    dpv:hasApplicableLaw dpv-legal:EU-GDPR ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand dpv:hasLegalBasis ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv-gdpr:A6-1-a-explicit-consent ] ] ;
    odrl:permission [
        odrl:constraint [
            odrl:leftOperand dpv:hasOrganisationalMeasure ;
            odrl:operator odrl:isA ;
            odrl:rightOperand dpv:DPIA ] ] ;
```



| **CCE Term** | **DUO Term** | **DPV/ODRL Mapping** |
|---|---|---|
| Use As Control | Research Control | dpv:Purpose |
| Clinical Research Use | Biomedical Research | dpv:Purpose |
| Disease Specific Use | Disease Category Research | dpv:Purpose |
| Geographical Area + Permitted | Geographical restriction | dpv:Location |
| Research Use + Permitted | General research | dpv:Purpose |
| Clinical Care Use + Permitted | Clinical Care Use | dpv:Purpose |
| Return Of Results + Obligated | Return to database or resource | dpv:Data + dpv:Recipient + odrl:Obligation |
| Collaboration + Obligated | Collaboration required | dpv:Purpose + odrl:Obligation |
| Time Period + Obligated | Time limit on use | dpv:Duration + odrl:Obligation |
| Publication Moratorium + Obligated | Publication moratorium | dpv:Purpose + dpv:Duration + odrl:Obligation |
| Publication + Obligated | Publication required | dpv:Purpose + odrl:Obligation |
| User Authentication + Obligated | User specific restriction | dpv:TechnicalMeasure + odrl:Obligation |
| Ethics Approval + Obligated | Ethics approval required | dpv:OrganisationalMeasure + Obnligation |
| (Commercial Entity + Permitted)<br>AND (Profit Motivated Use + Forbidden) | Non-commercial use only | dpv:Purpose + odrl:Rule |
| Fees | None | odrl:compensate |
| Regulatory Jurisdiction | None | dpv:Jurisdiction |
| Return Of Incidental Findings | None | dpv:Data + dpv:Recipient |
| (Re-)Identification Of Individuals Without Involvement Of The Resource Provider | None | dpv:Processing + dpv:isImplementedBy + dpv:Entity + odrl:Constraint |
| (Re-)Identification Of Individuals Mediated By The Resource Provider | None | dpv:Processing + dpv:isImplementedBy + dpv:Entity + odrl:Constraint |

# Enhancing DUO with ODRL and DPV

Fig. 1. Proof-of-concept implementation showing generation of `odrl:Offer` policies



**Dataset policy offer editor**

Generate an odrl:Offer to express the access conditions to a certain dataset

**Target dataset**

https://example.com/Dataset

**Data use permission**

DUO_0000006 - Health or Medical or Biomedical research

**Data use modifier**

DUO_0000019 - publication required

```
@prefix dct: <http://purl.org/dc/terms/> .
@prefix duodrl: <https://w3id.org/duodrl#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .

<https://example.com/offer> a odrl:Offer ;
  dct:source duodrl:DUO_0000006,
    duodrl:DUO_0000019 ;
  odrl:permission [ odrl:action odrl:use ;
      odrl:duty [ odrl:action odrl:distribute ;
          odrl:output duodrl:ResultsOfStudies ] ;
      odrl:target <https://example.com/Dataset> ],
    [ odrl:action odrl:use ;
      odrl:constraint [ odrl:leftOperand odrl:purpose ;
          odrl:operator odrl:isA ;
          odrl:rightOperand duodrl:HMB ] ;
      odrl:target <https://example.com/Dataset> ],
    [ odrl:action odrl:use ;
      odrl:constraint [ odrl:leftOperand odrl:purpose ;
          odrl:operator duodrl:isNotA ;
          odrl:rightOperand duodrl:POA ] ;
      odrl:target <https://example.com/Dataset> ] .
```

(a) from DUO concepts

**Dataset policy offer editor**

Generate an odrl:Offer to express the access conditions to a certain dataset

**Target dataset**

https://example.com/Dataset

**Data use permission**

DUO_0000042 - General Research Use

**Data use modifier**

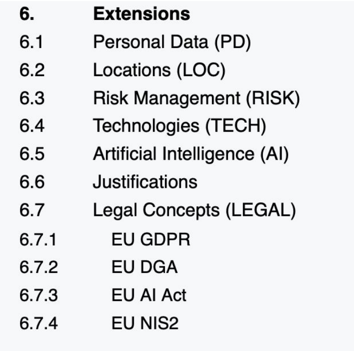
DPV - offer to use dataset using Consent and requiring an Impact Assessment

```
@prefix dct: <http://purl.org/dc/terms/> .
@prefix dpv: <https://w3id.org/dpv#> .
@prefix duodrl: <https://w3id.org/duodrl#> .
@prefix odrl: <http://www.w3.org/ns/odrl/2/> .

<https://example.com/offer> a odrl:Offer ;
  dct:source duodrl:DUO_0000042 ;
  odrl:permission [ odrl:action dpv:Use ;
      odrl:constraint [ odrl:leftOperand dpv:hasLegalBasis ;
          odrl:operator odrl:isA ;
          odrl:rightOperand dpv:Consent ] ;
      odrl:target <https://example.com/Dataset> ],
    [ odrl:action dpv:Use ;
      odrl:constraint [ odrl:leftOperand dpv:hasOrganisationalMeasure ;
          odrl:operator odrl:isA ;
          odrl:rightOperand dpv:ImpactAssessment ] ;
      odrl:target <https://example.com/Dataset> ],
    [ odrl:action odrl:use ;
      odrl:constraint [ odrl:leftOperand odrl:purpose ;
          odrl:operator odrl:isA ;
          odrl:rightOperand duodrl:GRU ] ;
      odrl:target <https://example.com/Dataset> ] .
```

(b) from DUO and DPV concepts

# What about Health Data Spaces?



**6. Extensions**

6.1 Personal Data (PD)

6.2 Locations (LOC)

6.3 Risk Management (RISK)

6.4 Technologies (TECH)

6.5 Artificial Intelligence (AI)

6.6 Justifications

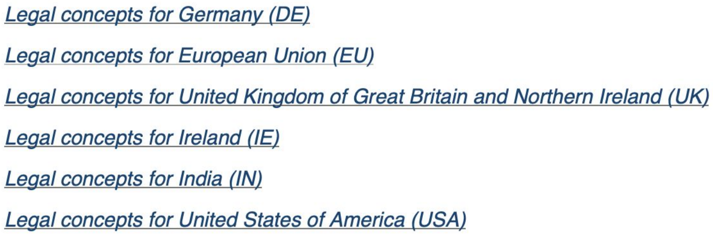
6.7 Legal Concepts (LEGAL)

6.7.1 EU GDPR

6.7.2 EU DGA

6.7.3 EU AI Act

6.7.4 EU NIS2



*Legal concepts for Germany (DE)*

*Legal concepts for European Union (EU)*

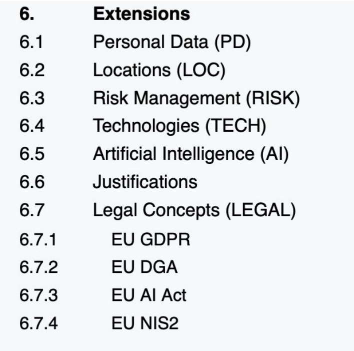
*Legal concepts for United Kingdom of Great Britain and Northern Ireland (UK)*

*Legal concepts for Ireland (IE)*

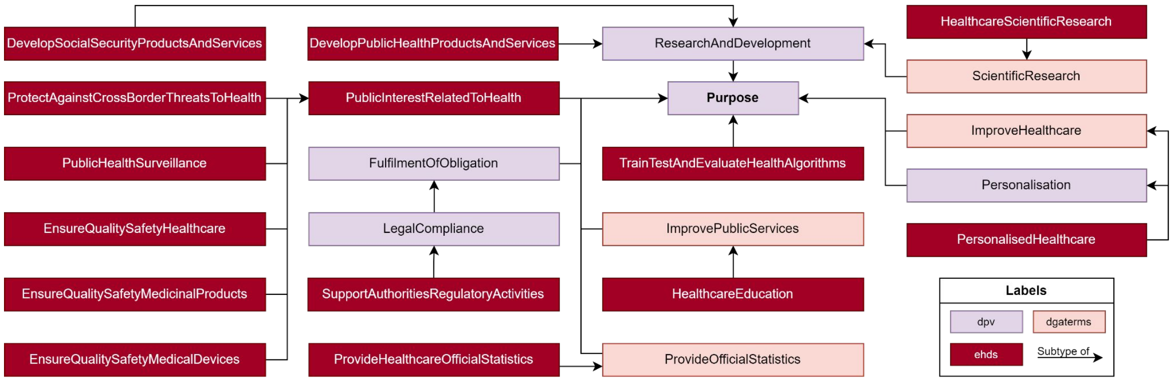
*Legal concepts for India (IN)*

*Legal concepts for United States of America (USA)*

# What about Health Data Spaces?



**6. Extensions**
6.1 Personal Data (PD)
6.2 Locations (LOC)
6.3 Risk Management (RISK)
6.4 Technologies (TECH)
6.5 Artificial Intelligence (AI)
6.6 Justifications
6.7 Legal Concepts (LEGAL)
6.7.1 EU GDPR
6.7.2 EU DGA
6.7.3 EU AI Act
6.7.4 EU NIS2


DevelopSocialSecurityProductsAndServices
DevelopPublicHealthProductsAndServices
ResearchAndDevelopment
HealthcareScientificResearch
ScientificResearch
ProtectAgainstCrossBorderThreatsToHealth
PublicInterestRelatedToHealth
Purpose
ImproveHealthcare
PublicHealthSurveillance
FulfilmentOfObligation
TrainTestAndEvaluateHealthAlgorithms
Personalisation
EnsureQualitySafetyHealthcare
LegalCompliance
ImprovePublicServices
PersonalisedHealthcare
EnsureQualitySafetyMedicinalProducts
SupportAuthoritiesRegulatoryActivities
HealthcareEducation
Labels
dpv
dgaterms
ehds
Subtype of
EnsureQualitySafetyMedicalDevices
ProvideHealthcareOfficialStatistics
ProvideOfficialStatistics

*Legal concepts for Germany (DE)*

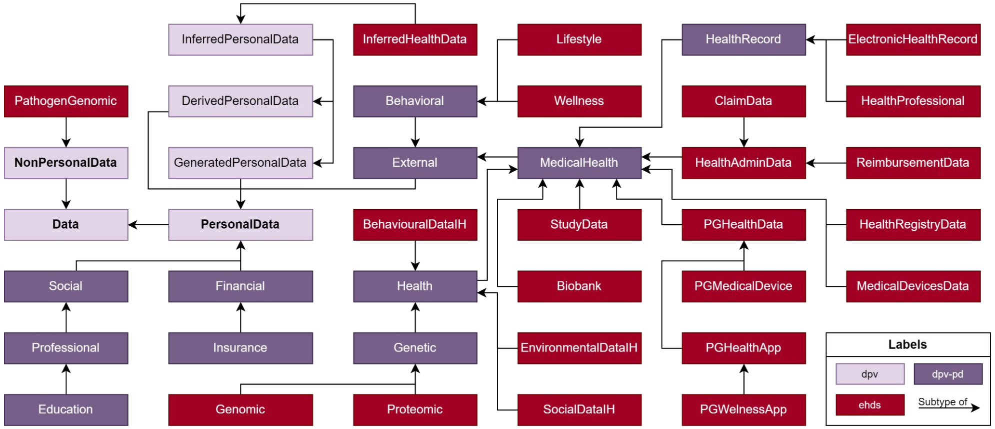
*Legal concepts for European Union (EU)*

*Legal concepts for United Kingdom of Great Britain and Northern Ireland (UK)*

*Legal concepts for Ireland (IE)*

*Legal concepts for India (IN)*

*Legal concepts for United States of America (USA)*



# Balancing Access and Privacy of Personal Health Data

Beatriz Esteves, UGent – imec