AI & Data

Regulating ~~Data~~

Harshvardhan J. Pandit | email: harshvardhan.pandit@adaptcentre.ie

CS7IS1 | 14 October 2024 | Trinity College Dublin

Slides available at: https://harshp.com/research/presentations

Harsh(vardhan J. Pandit)

An Introduction

https://harshp.com/research

- Assistant Professor - School of Computing, DCU (2023+)
- Postdoctoral Researcher at Trinity College Dublin (2020-2022)
- PhD in Computer Science (2020) - Representation of activities involving **personal data and consent for GDPR compliance**
- Chair of W3C Community Groups: **Data Privacy Vocabularies** and Controls Community Group (DPVCG) and Consent (ConsentCG)
- Member, ISO and EU standardisations groups on **Privacy & AI**

GDPR[1]

World-Changing EU law that regulates Processing of Personal Data

1. What is meant by Personal Data ?
2. What is meant by Processing ?
3. How is data is being processed? (what/how/where...)
4. Who is involved? (whose data, processed by whom)
5. How to check processing is following the rules of GDPR?

[1] https://eur-lex.europa.eu/eli/reg/2016/679/oj

Personal Data

Some "definitions" from across the globe

'personal data' means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

GDPR Art.4(1)

any information that (a) **can be used to identify the PII principal to whom such information relates, or (b) is or might be directly or indirectly linked to a PII principal**

ISO 29100:2011

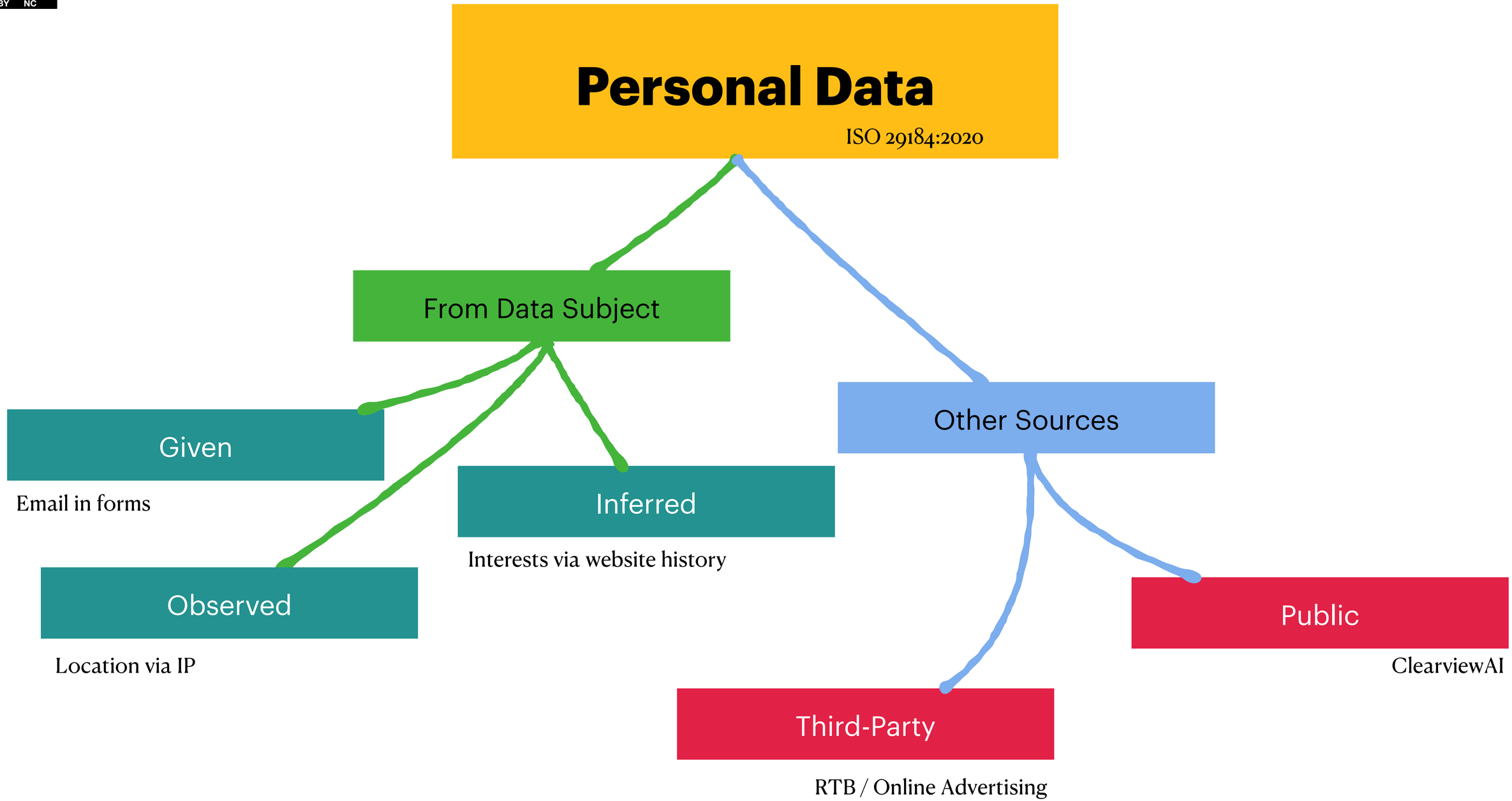
"Personal information" means information that **identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly**, with a particular consumer or household.

CCPA 1798.140 (o)(1)

Personal Data

Identifiers, and Identifiability

1. Identifiers: Harsh (name), pandith@tcd.ie (email)
2. Non-identifiers: Black (hair), Brown (eyes), 1.66m (height), etc.
3. For a room full of people, combine non-identifier to uniquely identify a person (me) — thus creating an identifier !!!
4. Useful technique for **fingerprinting**, **profiling**, **tracking**


Personal Data
ISO 29184:2020
From Data Subject
Other Sources
Given
Email in forms
Inferred
Interests via website history
Observed
Location via IP
Public
ClearviewAI
Third-Party
RTB / Online Advertising

F: Findable
A: Accessible
I: Interoperable
R: Reusable

Harmonising FAIR data sharing with Legal Compliance

Harmonising FAIR data sharing with Legal Compliance

F: Findable
A: Accessible
I: Interoperable
R: Reusable

Harmonising FAIR data sharing with Legal Compliance

- Copyright Law
- Privacy Regulation
- Data Protection Regulation
  - GDPR
- AI Act
- Digital Markets Act
- Data Act
- Digital Services Act

Legally Compliant FAIR =
Legally Compliant Data Sharing
= Legally Compliant Value

F: Findable
A: Accessible
I: Interoperable
R: Reusable

Harmonising FAIR data sharing with Legal Compliance

- Copyright Law
- Privacy Regulation
- Data Protection Regulation
  - GDPR
- AI Act
- Digital Markets Act
- Data Act
- Digital Services Act

Legally Compliant FAIR =
Legally Compliant Data Sharing
= Legally Compliant Value

F: Findable
A: Accessible
I: Interoperable
R: Reusable

Harmonising FAIR data sharing with Machine-Readable Metadata for Legal Compliance

ODRL

Data Privacy Vocabulary

Copyright Law

Privacy Regulation

Data Protection Regulation

GDPR

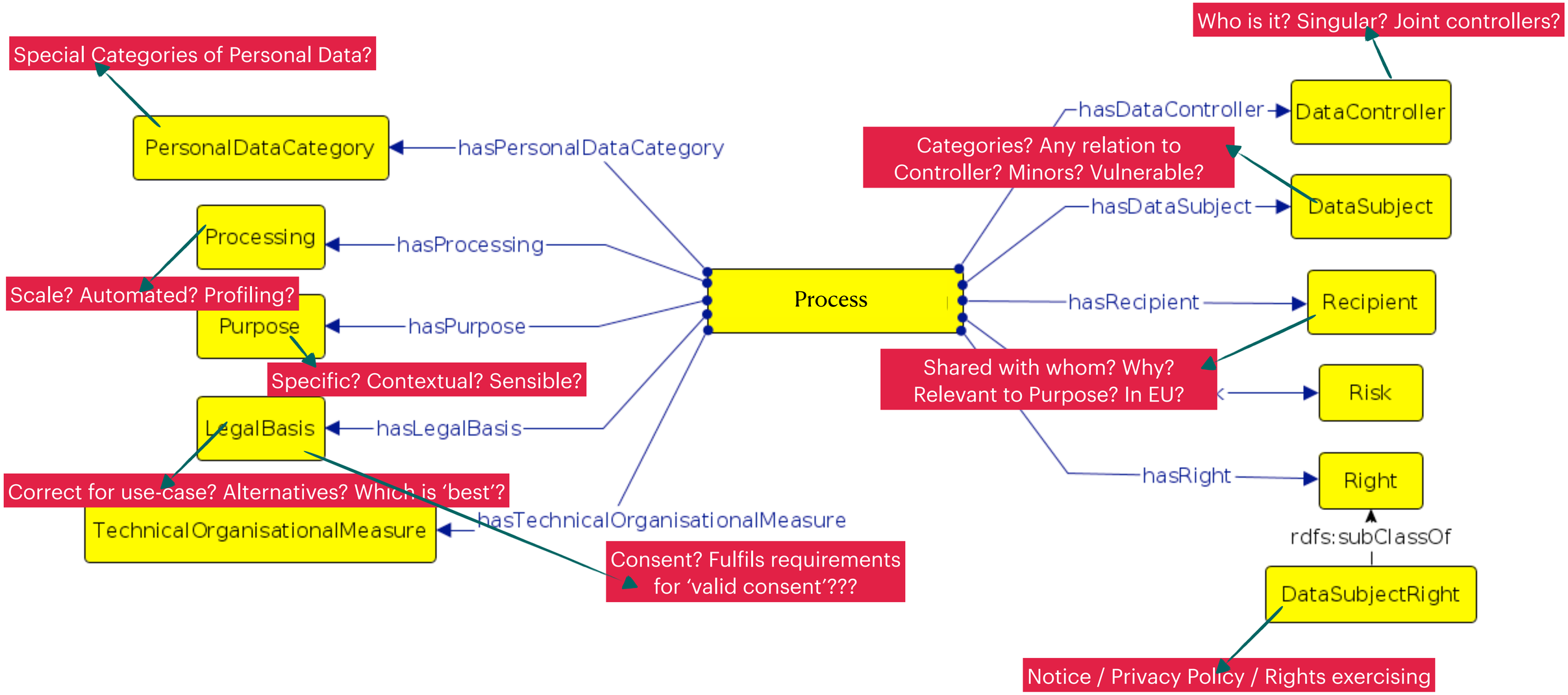
Digital Services Act

Data Act

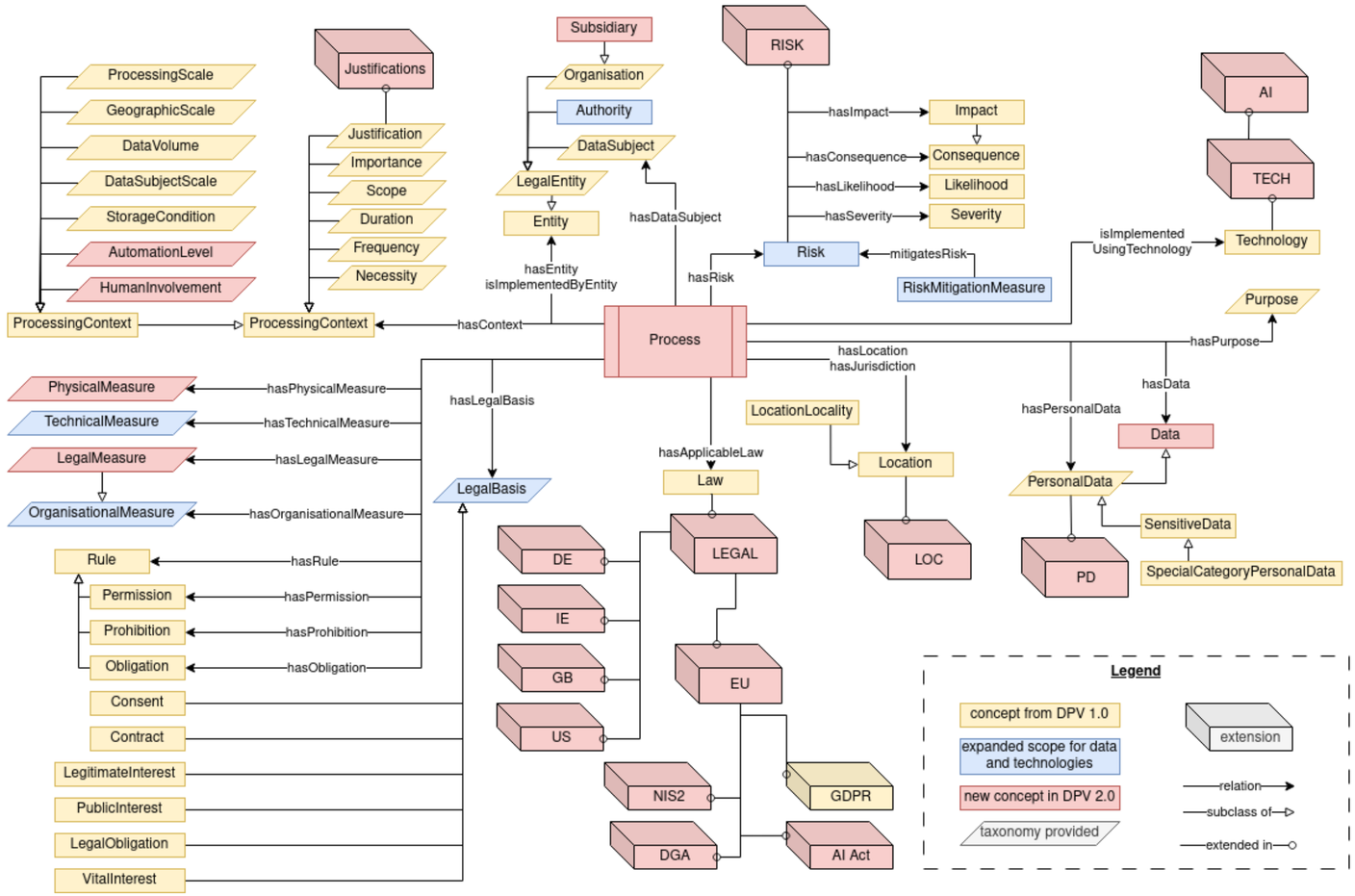
AI Act

Digital Markets Act

Labelling FAIR data for ‘sharing’ in legally compliant manner



DPV Version 2.0 was published 01 August 2024, and has been *accepted for presentation at International Semantic Web Conference* https://doi.org/10.48550/arXiv.2404.13426



Purpose
Personal Data
Processing
Legal Basis
Legal Role
Tech/Org Measures
Risk
Rights

Serialisations
RDF (canonical)
CSV
JSON

Semantics
RDFS+SKOS
OWL2

W3C Data Privacy Vocabularies and Controls Community Group (DPVCG)
The DPVCG was established as part of the EU H2020 SPECIAL Project in 2018. The project completed in 2020.

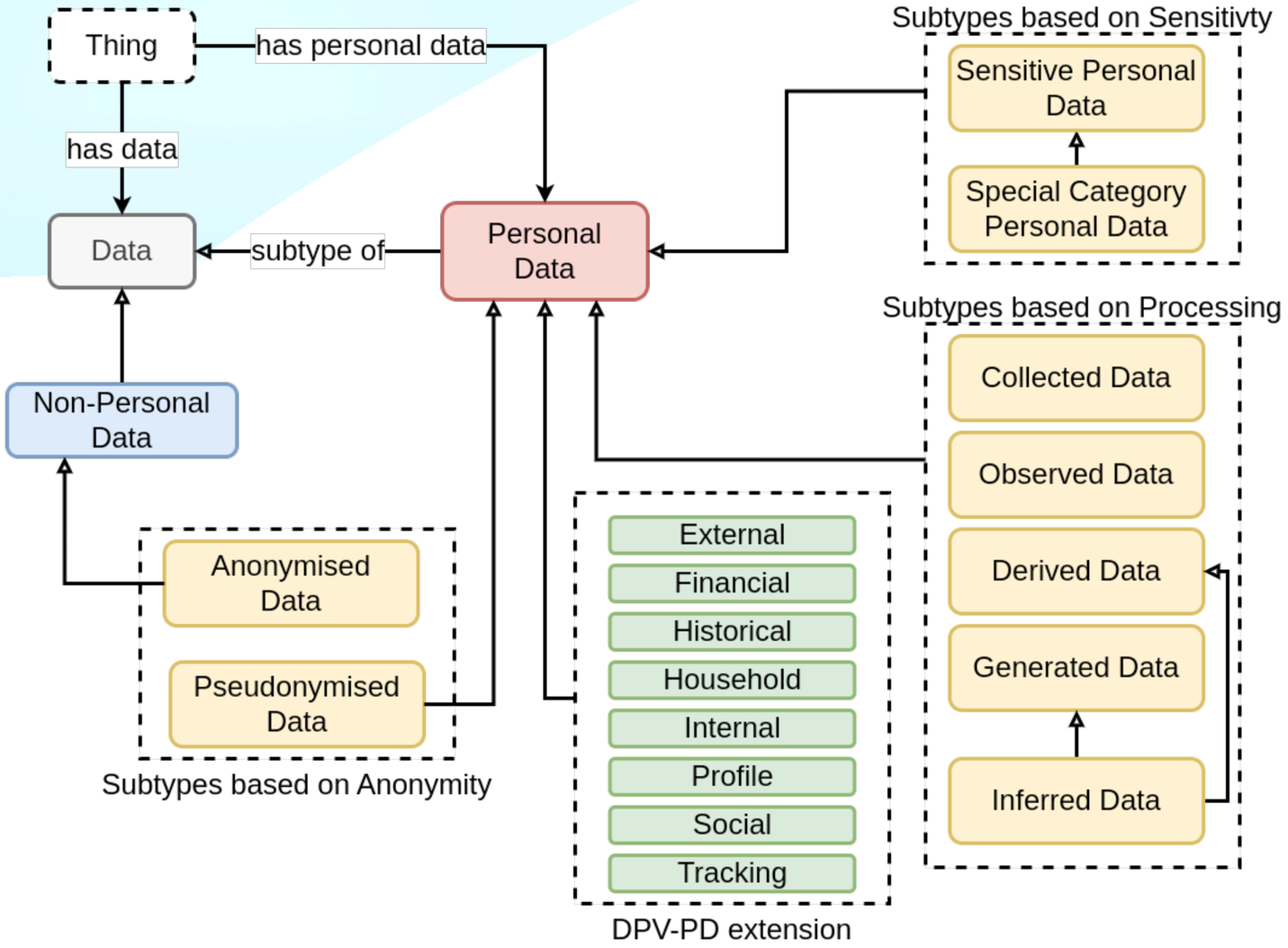
Data Privacy Vocabulary (DPV)

https://dpvcg.org/

- ~2200 concepts and 200 relations
- Jurisdiction Agnostic
- Extensions for GDPR, DGA specific concepts
- Available for any use under the W3C Permissive License

Data

Personal Data



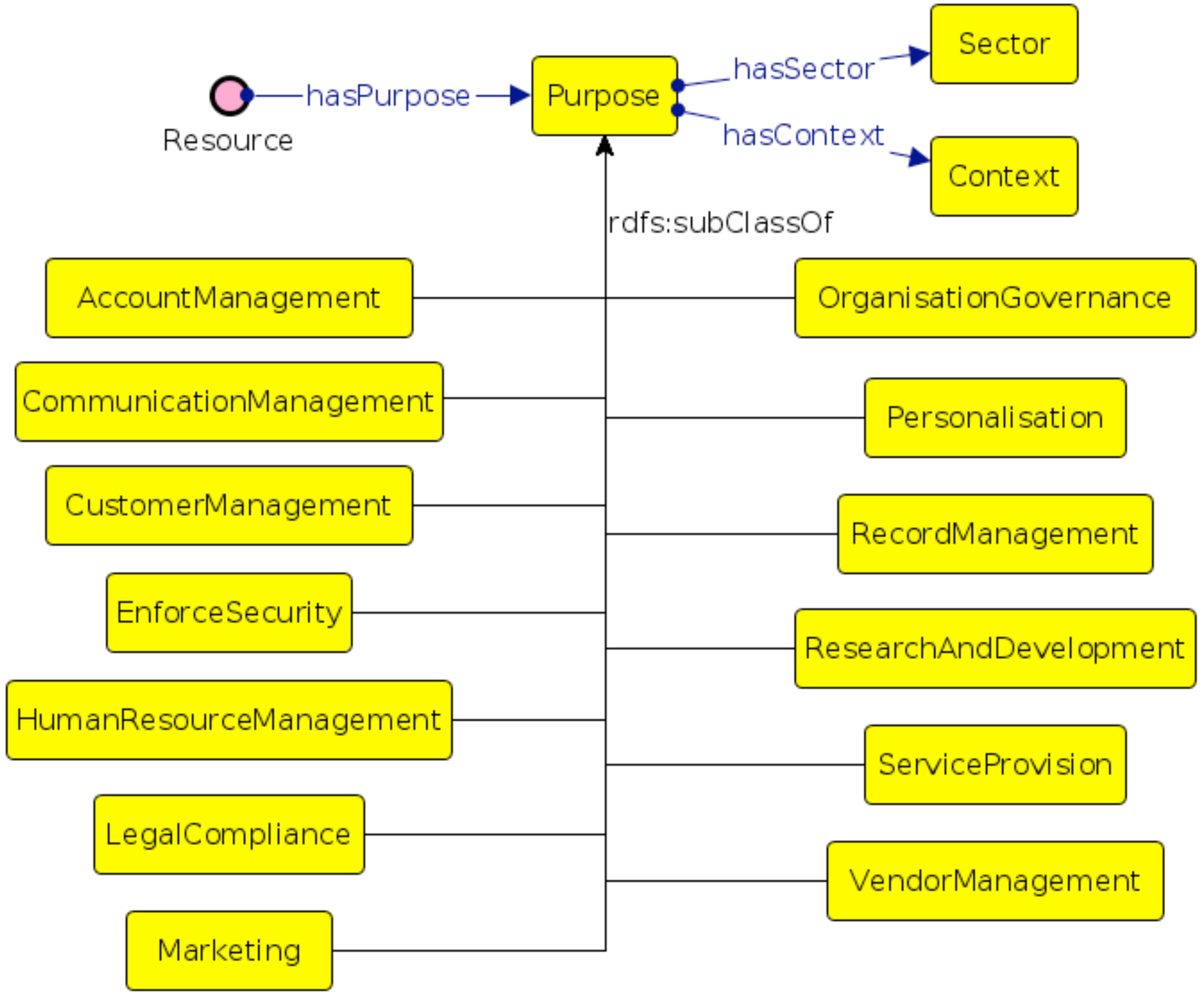
Purposes are intended to be human-readable and human-comprehensible

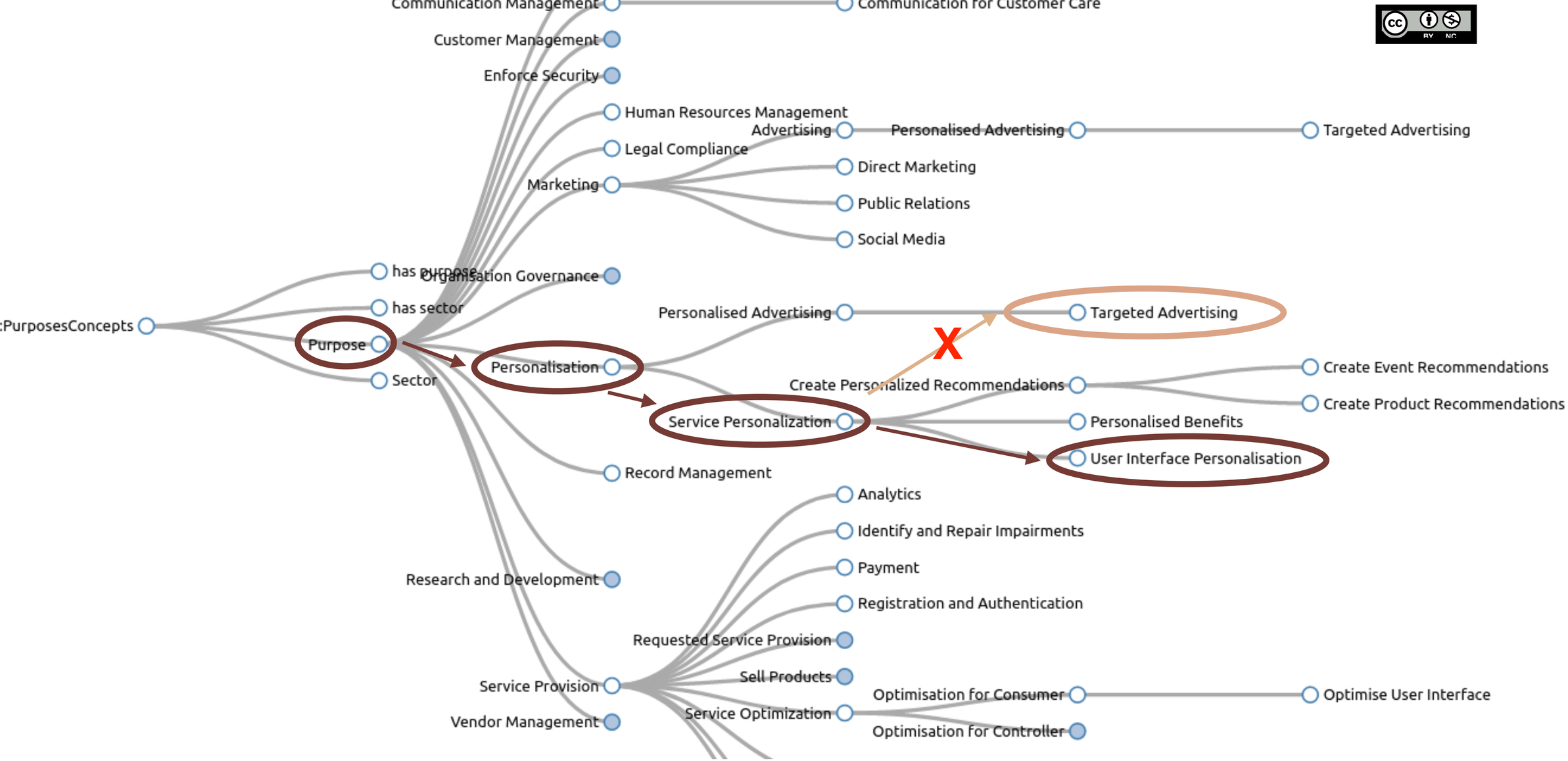
Purposes should not be broad and abstract

Purposes should be specific and contextual to their use-case

Purposes can be grouped or categorised, but not replaced, e.g. with Marketing for ‘Sending new product emails’

Purposes don’t have to necessarily benefit the data subject e.g. service optimisation





Rich Taxonomies providing controlled hierarchical vocabularies for explicit and exact representation of information

```
Purpose
 -> Personalisation
 --> Service Personalisation
 ---> UI/UX Personalisation
```

Processing Overview

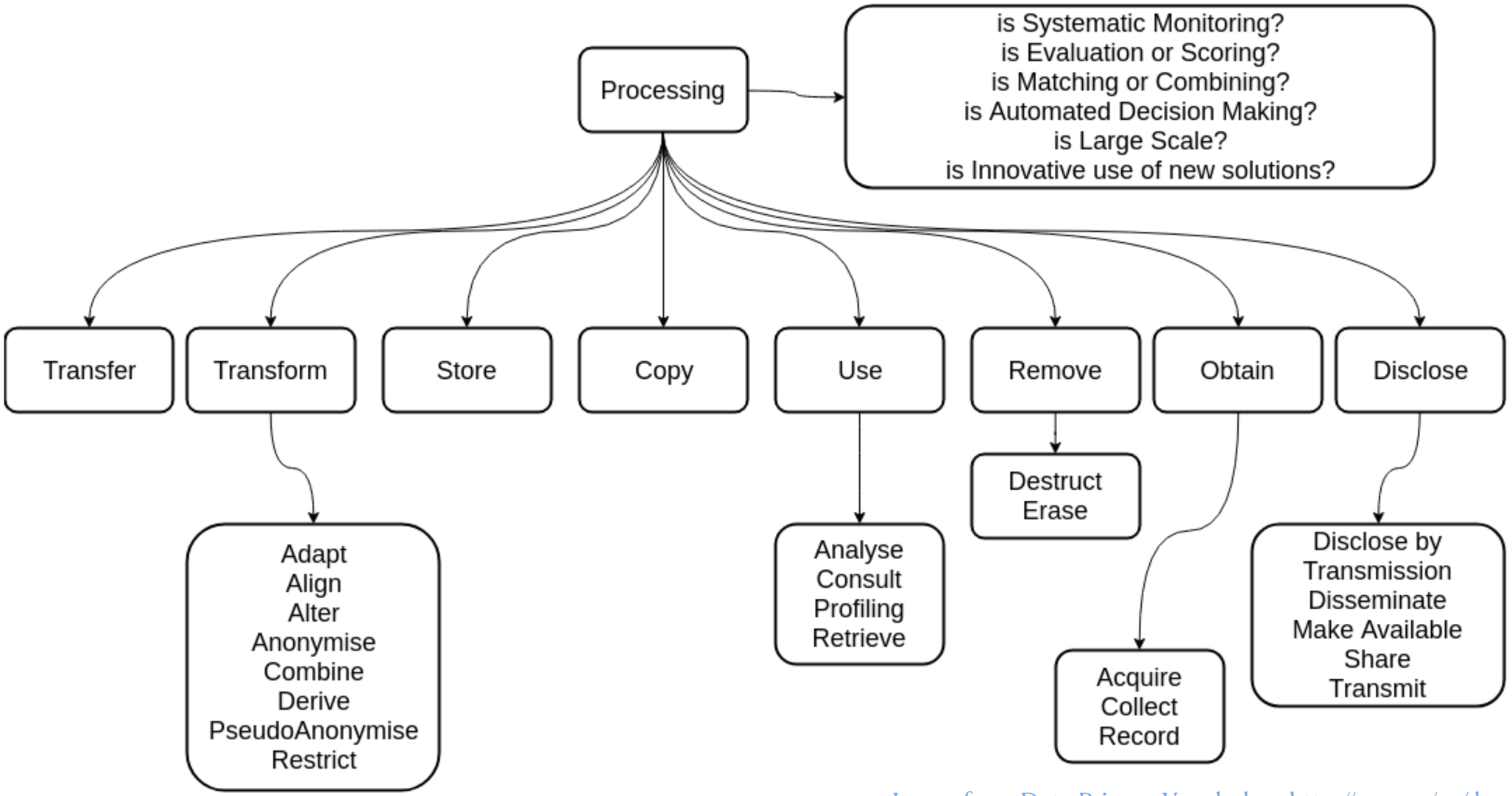
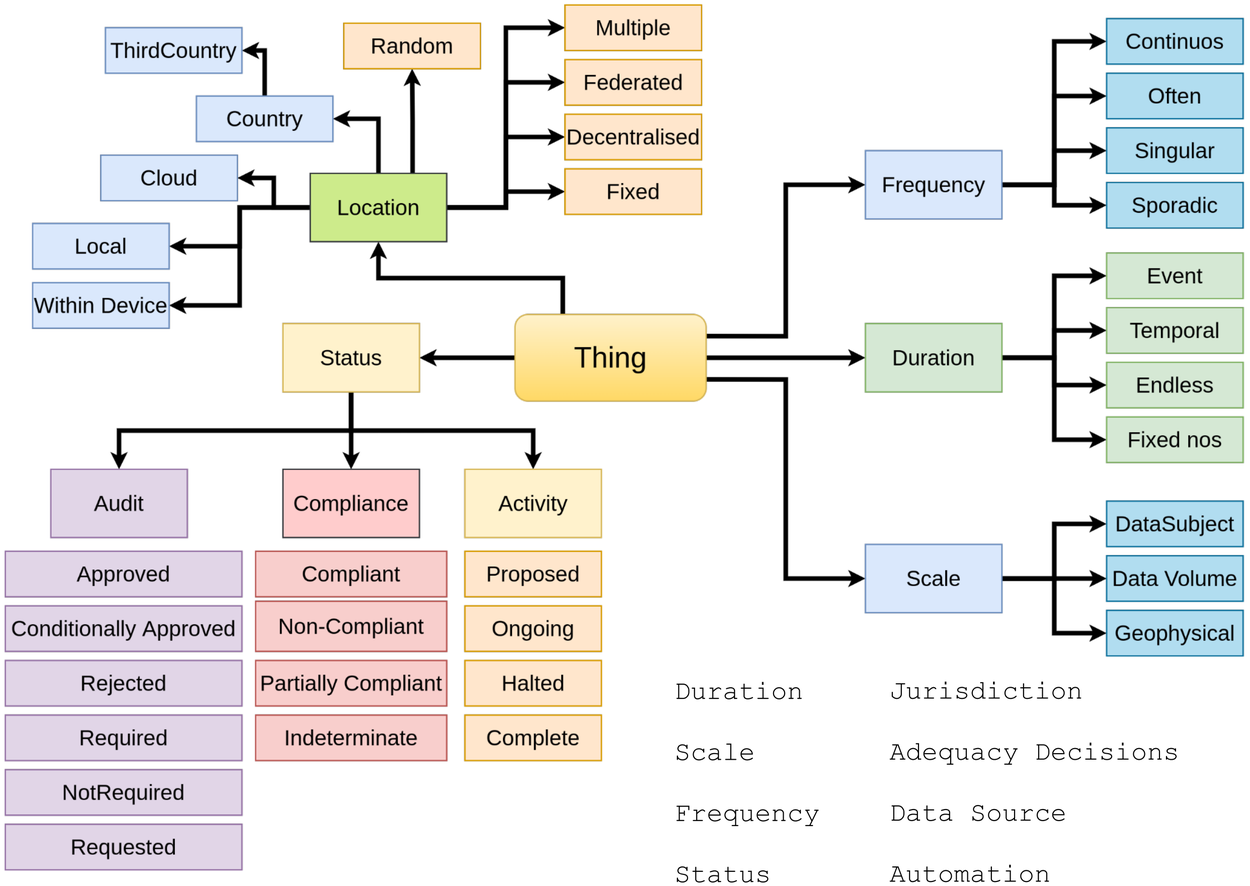


Image from Data Privacy Vocabulary http://w3.org/ns/dpv



Duration
Scale
Frequency
Status
Audits
Compliance
Location

Jurisdiction
Adequacy Decisions
Data Source
Automation
Storage conditions
Decision Making
Human Involvement
Consequences & Impacts

Where DPV is being used:

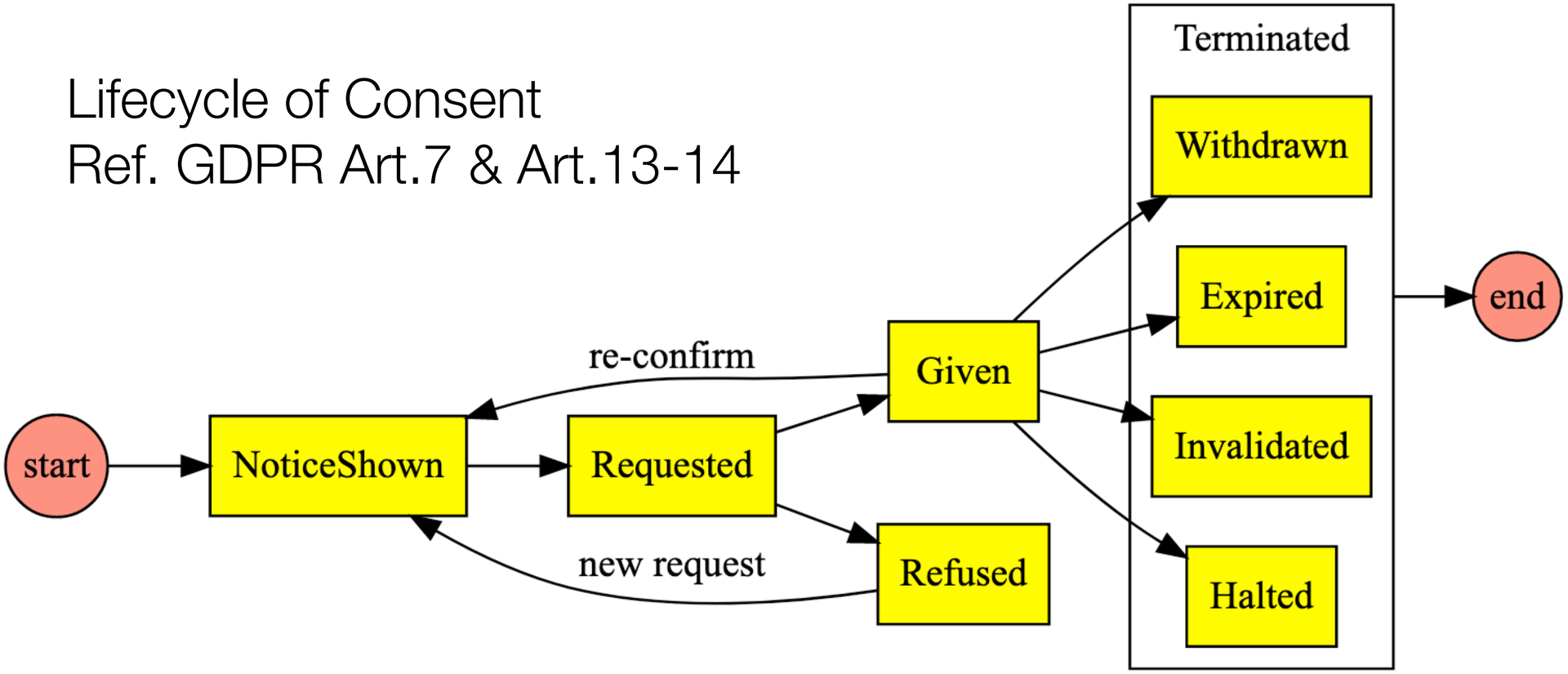
1. Record of Processing Activities
2. Compliance Checking
3. Impact Assessments (DPIA)
4. Risk Management
5. Data Breach Management
6. Subject Access Request
7. Data Portability
8. Data Transfers
9. Privacy Policies

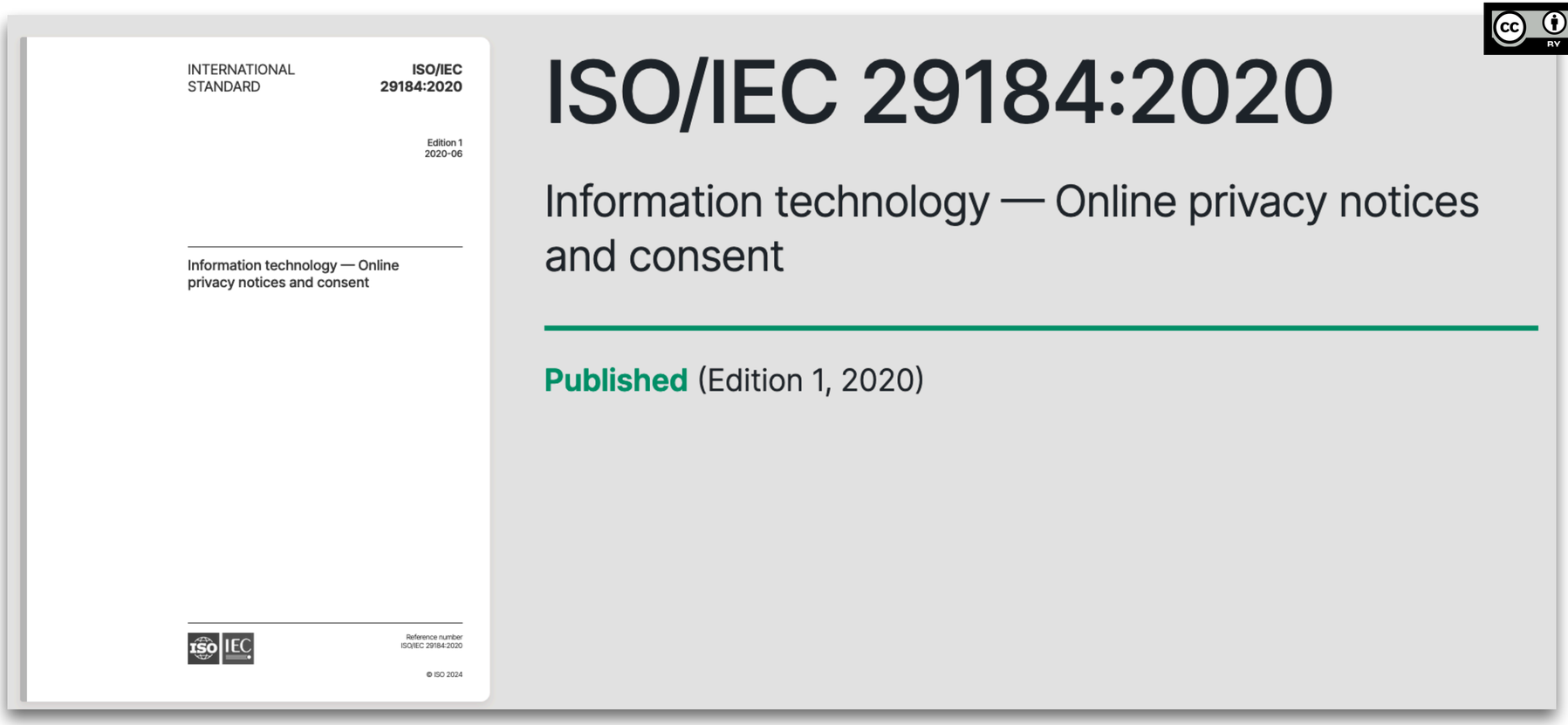
What's new in DPV 2.1 (due DEC'24)

- **!!! AI Act !!!**
- NIS2
- Rights Impact Assessments
- Rights Exercise Specification
- Multi-lingual (DE/FR/IT/ES)
- Machine-readable notices
- More Legal Basis e.g. Contracts. and Legitimate Interests
- Automating DPIA checking

Actively used by over
30+ Industry and Research projects

Lifecycle of Consent
Ref. GDPR Art.7 & Art.13-14

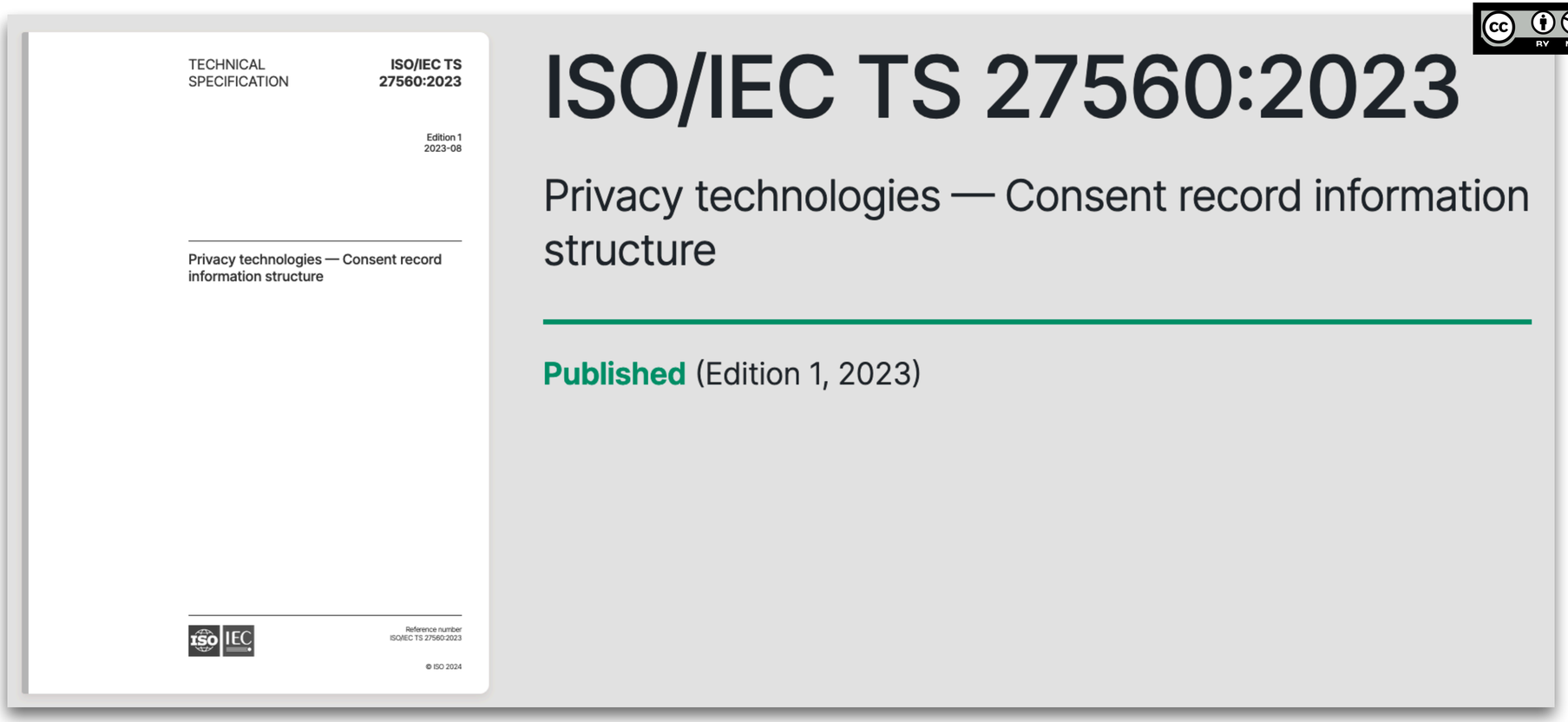




The ISO/IEC 29184:2020 is a Specification that specifies:

1. What information should be in a privacy notice for consent
2. How should privacy notices for consent be structured / presented
3. **How to ask for consent**
4. An example of a 'consent receipt' provided in an Annex

* ISO/IEC 29184:2020 has been accepted as an *EN* or *EuroNorm* i.e. a standard that has been ratified by CEN/CENELEC and approved for use within the EU



The ISO/IEC 27560:2023 is a Technical Specification that enables:

1. Maintaining a **Consent Record**
2. Providing a record of consent to the Data Subject as a **Consent Receipt**
3. Exchange of consent information between information systems
4. Managing the life cycle of recorded consent information

* Jan Lindquist was the co-editor of this standard.
* Harshvardhan J. Pandit was a contributing member to this standard.

3. How to practically create consent records/receipts?

- ISO-27560 DOES NOT prescribe how consent records/ receipts should be **technically represented** in practice.
- Information MUST be represented in a **structured format** e.g. JSON or JSON-LD.
- However, to actually ‘structure’ this information so that it is **interoperable** requires a strict agreement on the structure and interpretation - which requires a standard

3. How to practically create consent records/receipts?

To represent consent information in a consistent and interoperable manner, we require:

- An “ontology” to represent the ‘concept’ e.g. Purpose
- A “taxonomy” reflecting the vocabulary used in practice e.g. “Marketing” or “Service Provision”
- A way to combine different concepts into ‘logical groups’ for how use-cases ‘process personal data’

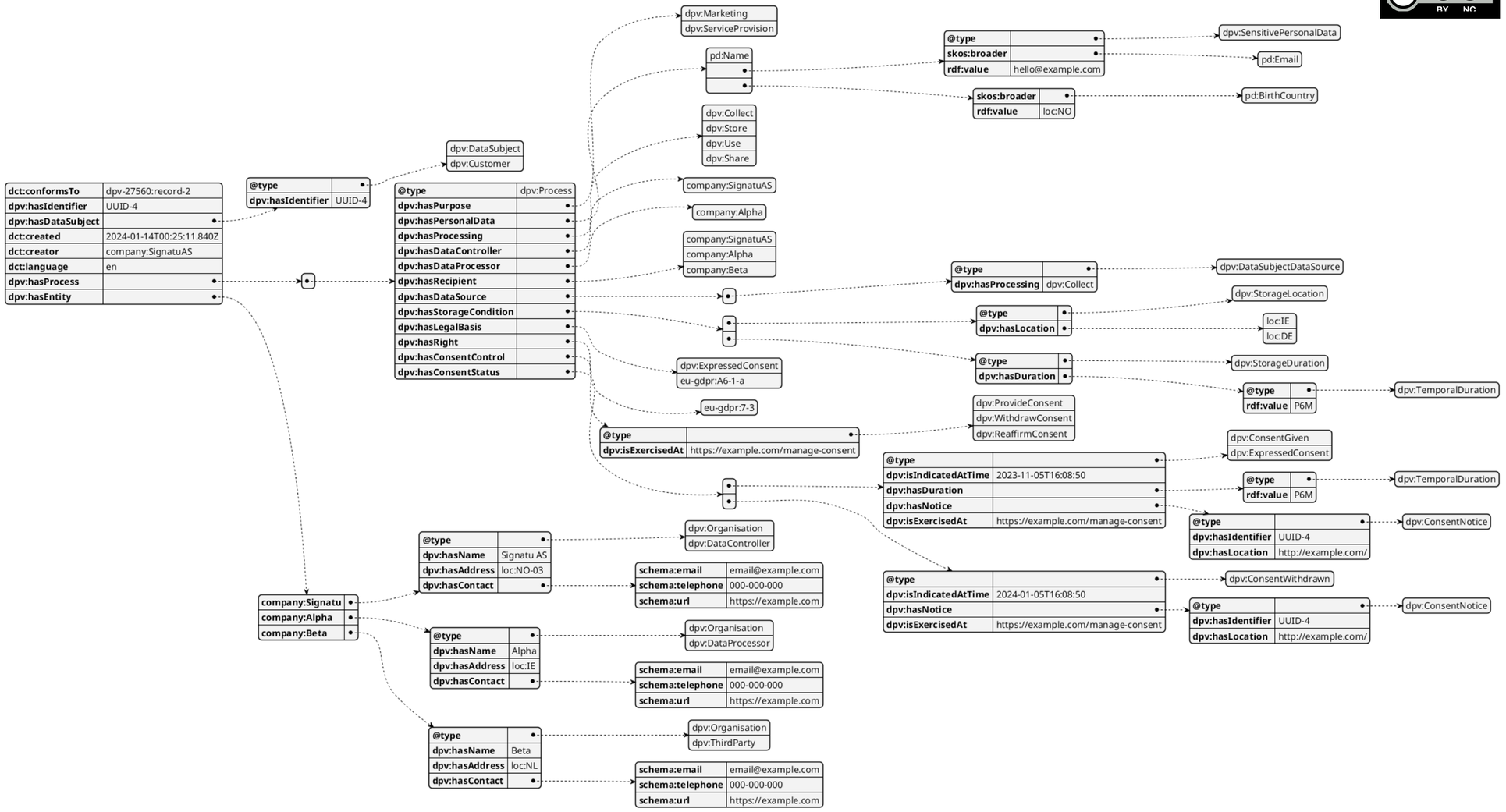
Table 4. DPV concepts for ISO/IEC 27560:2023 Processing fields

From: Implementing ISO/IEC TS 27560:2023 Consent Records and Receipts for GDPR and DGA

Field	Cardinality	DPV Concept	DPV Property
Process	1..*	dpv:Process	dpv:hasProcess
Purpose	1..*	dpv:Purpose	dpv:hasPurpose
Personal Data	1..*	dpv:	dpv:hasPersonalData
Personal Data Type	1..*	dpv:PersonalData taxonomy	dpv:hasPersonalData or dct:type
Personal Data Identifier	0..*	N/A	dct:identifier
Personal Data Necessity	0..*	dpv:Necessity	dpv:hasNecessity
Sensitive/Special Category	0..*	dpv:SensitivePersonalData, dpv:SpecialCategoryPersonalData	dpv:hasPersonalData or dct:type
Processing Operations	0..*	dpv:Processing	
Data Source	0..*	dpv:DataSource	
Storage Condition	1..*	dpv:StorageCondition, dpv:StorageLocation, dpv: dpv:StorageDeletion	
Processing Condition	0..*	dpv:ProcessingCondition, dpv:ProcessingLocatio dpv:ProcessingDuration	
Geographic Restriction	0..*	dpv:Rule	
Data Controller	1..*	dpv:DataController	
Legal Basis	0..*	dpv:LegalBasis	
Recipients	1..*	dpv:Recipient	
Consent Change & Withdrawal	1..*	dpv:InvolvementControl, dpv:WithdrawingFromAct	

```
{
    "@id": "https://example.com/a6f58318-72e6-46a2-bfd7-f36d795e30cd",
    "@type": "dpv:ConsentRecord",
    "dpv:hasPersonalDataHandling": {
        "@type": "dpv:PersonalDataHandling",
        "dpv:hasPurpose": "dpv:PaymentManagement",
        "dpv:hasPersonalDataHandling": {
            "@type": "dpv:PersonalDataHandling",
            "dpv:hasPersonalData": "dpv-pd:EmailAddress",
            "dpv:hasRecipient": "ex:CompanyA"
        },
        "dpv:hasPersonalDataHandling": {
            "@type": "dpv:PersonalDataHandling",
            "dpv:hasPurpose": "dpv:IdentityVerification",
            "dpv:hasPersonalData": "dpv-pd:OfficialID",
            "dpv:hasRecipient": "ex:CompanyB"
        }
    }
}
```

(example) Consent Record expressed in JSON-LD using DPV



Consent Record implemented using DPV, visualised as a “graph”

The underlying data is defined in RDF, which is a standard for expressing ‘knowledge graphs’

Next Step: Create a technical specification for industry to implement records/receipts in their systems

This will enable consent records to be expressed and interpreted in a consistent and unambiguous manner by dictating EXACTLY what should be present, where, how, and how it should be used to interpret what the consent permits e.g. Purpose -

Purpose

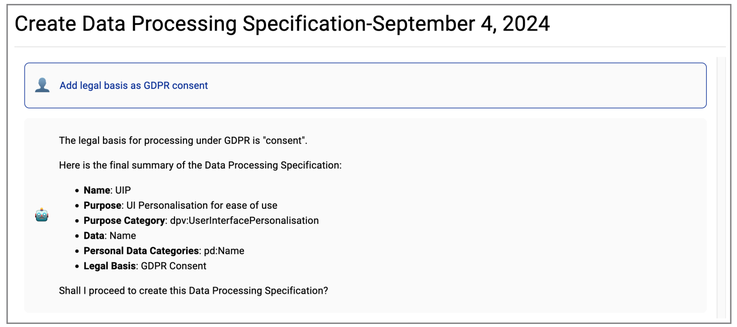
There MUST be a key `dpv:hasPurpose` within the Process object whose value is an **Array**. Each item in the array must either be a **String** or an object that MUST have the key `@type` whose value is a list that MUST contain the item `dpv:Purpose`.

```
{
    "dpv:hasProcess": {
        "dpv:hasPurpose": [
            "dpv:Marketing",
            {
                "@type": ["dpv:Purpose"],
                "skos:broader": "dpv:FraudPreventionDetection",
                "skos:prefLabel": "Preventing Fraud in Emails"
            }
        ]
    }
}
```

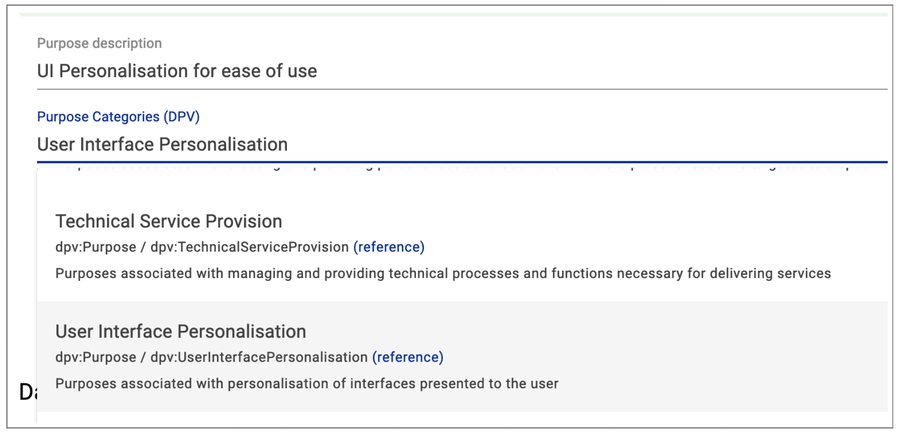
Working with Signatu AS, which provides Legal Compliance and Consent Management Platforms to ensure this is a practical solution

Consent Records/Receipts Implemented by Signatu AS, which is a Consent Management / Data Governance platform for Legal Compliance https://signatu.com/

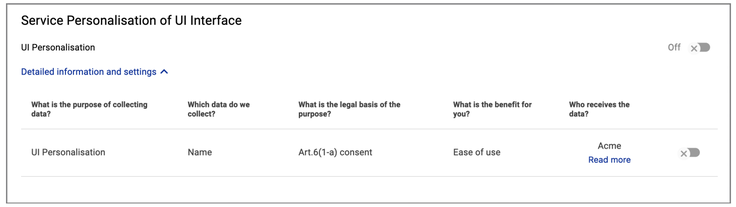
1 Chatbot to enter data



2 Represent with DPV



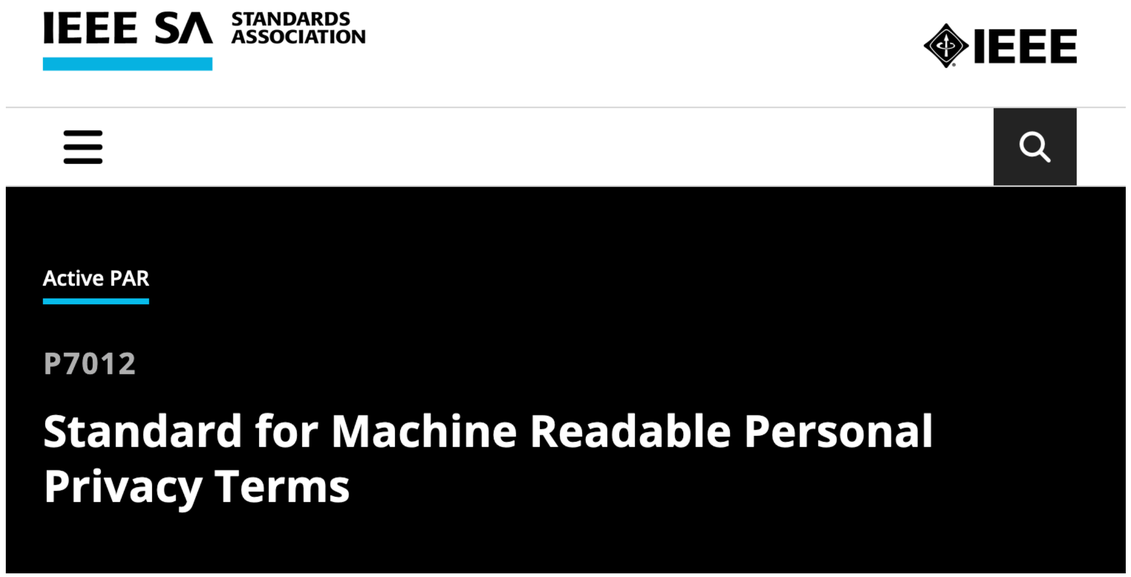
3 Generate Notice



4 Generate Consent Records with Events

However, Consent is HARD (and has 99 other problems)

Working with IEEE P7012 to create Machine-Readable ‘Contracts’ for convenient Service Terms and Data Reuse/Altruism



https://standards.ieee.org/ieee/7012/7192/

No EU representation here! I’m involved, and we must be part of initiatives like this…

Conduct a Data Protection Impact Assessment

automate

machine-readable

interoperable format

queryable

verifiable

reuse standards & guidelines

RQ: How to assist with this?

share information

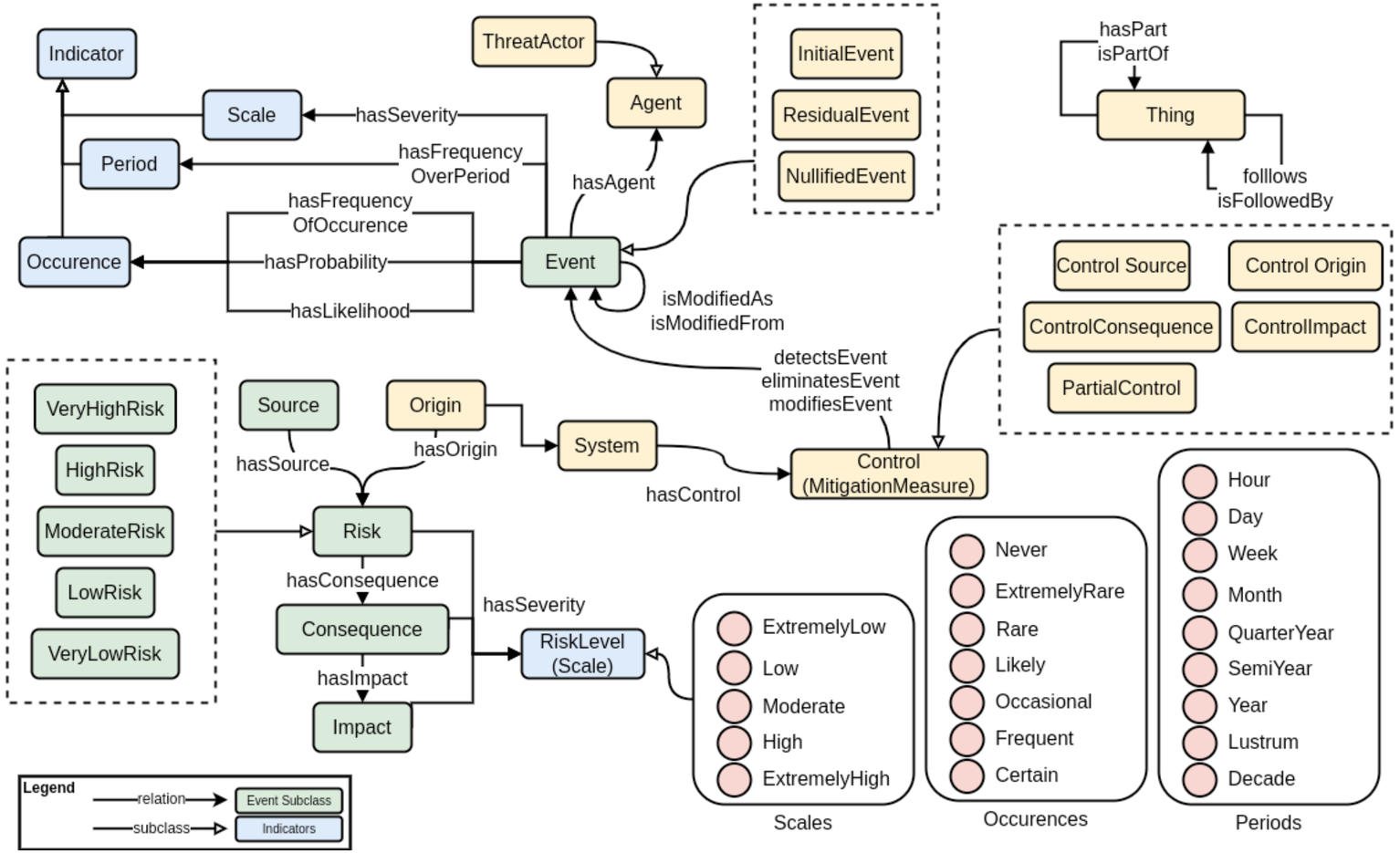
simplify risk assessment

assist with other GDPR compliance

practical application

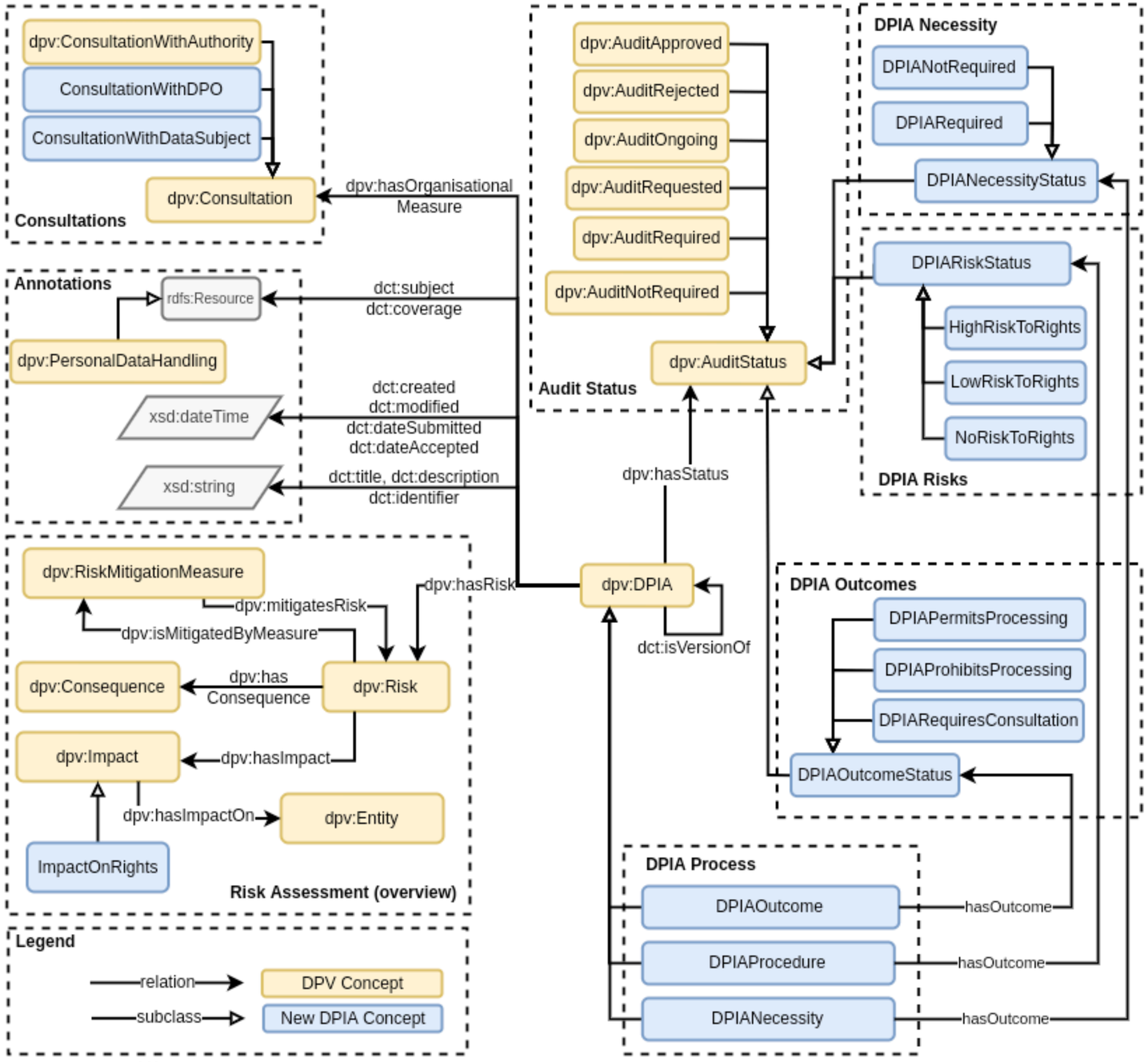
Risk Assessment Ontology

DPV



DPV

Data Protection Impact Assessment (DPIA)



Data Processing Catalog (DPCat) https://w3id.org/dpcat

extends DCAT v2 standard

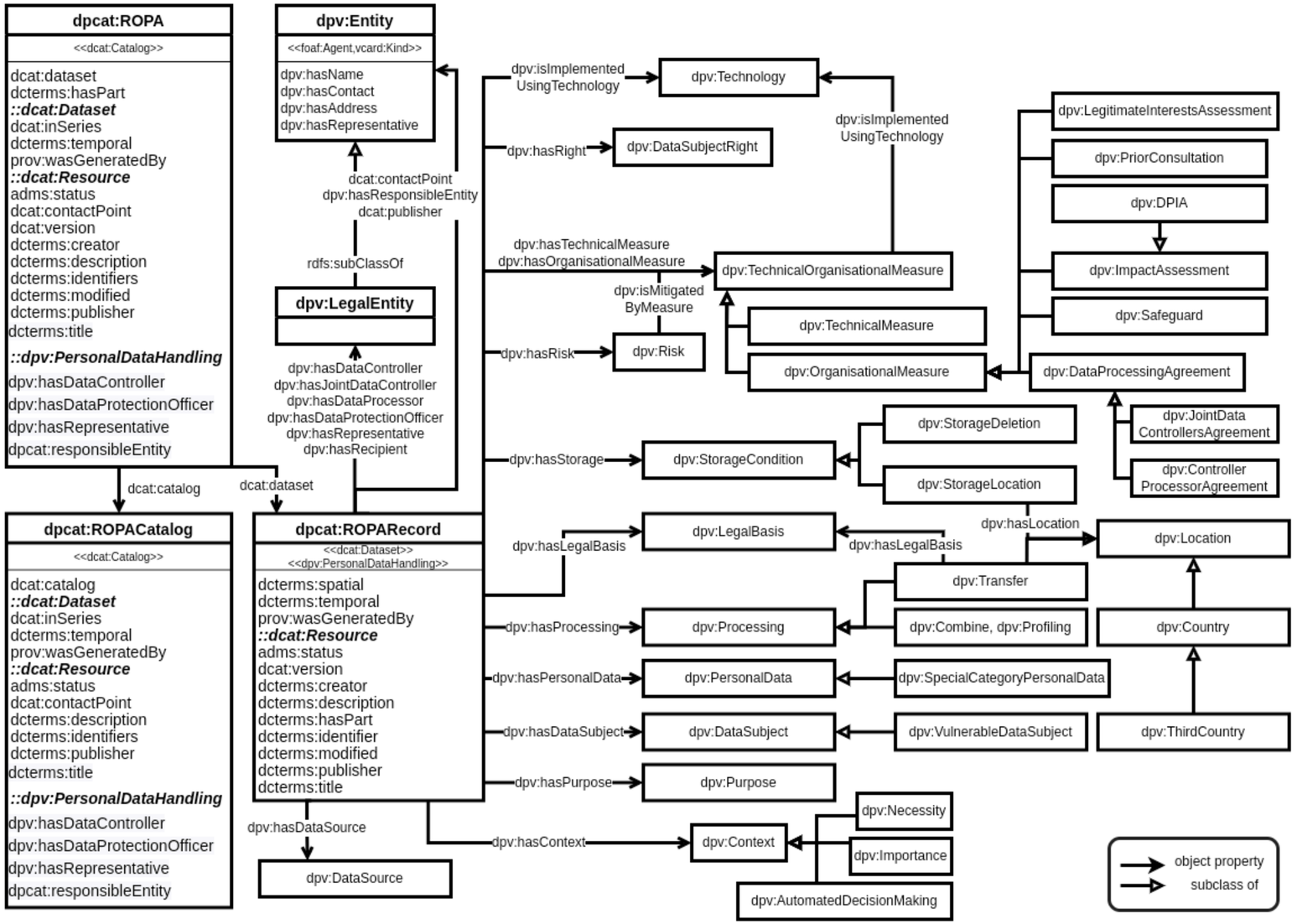
integrates legal metadata for GDPR processing records as 'catalogues'

based on analysis of all DPAs in EU

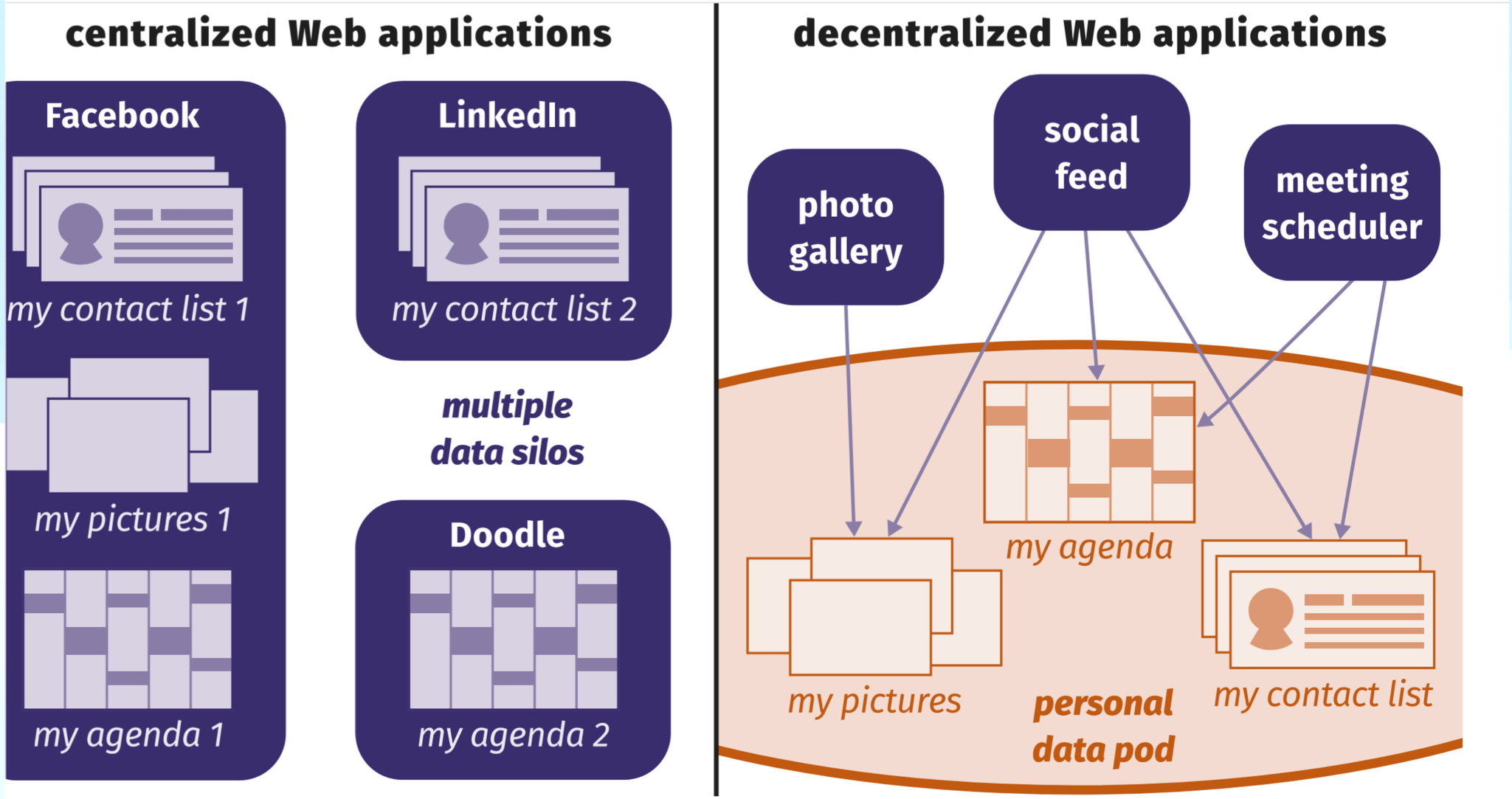
extensible, customisable, interoperable

can be used to query, import, export

for inter- and intra- org. processes



Centralisation vs Decentralisation



SOLID: A Decentralised Web

https://solidproject.org/

Centralised

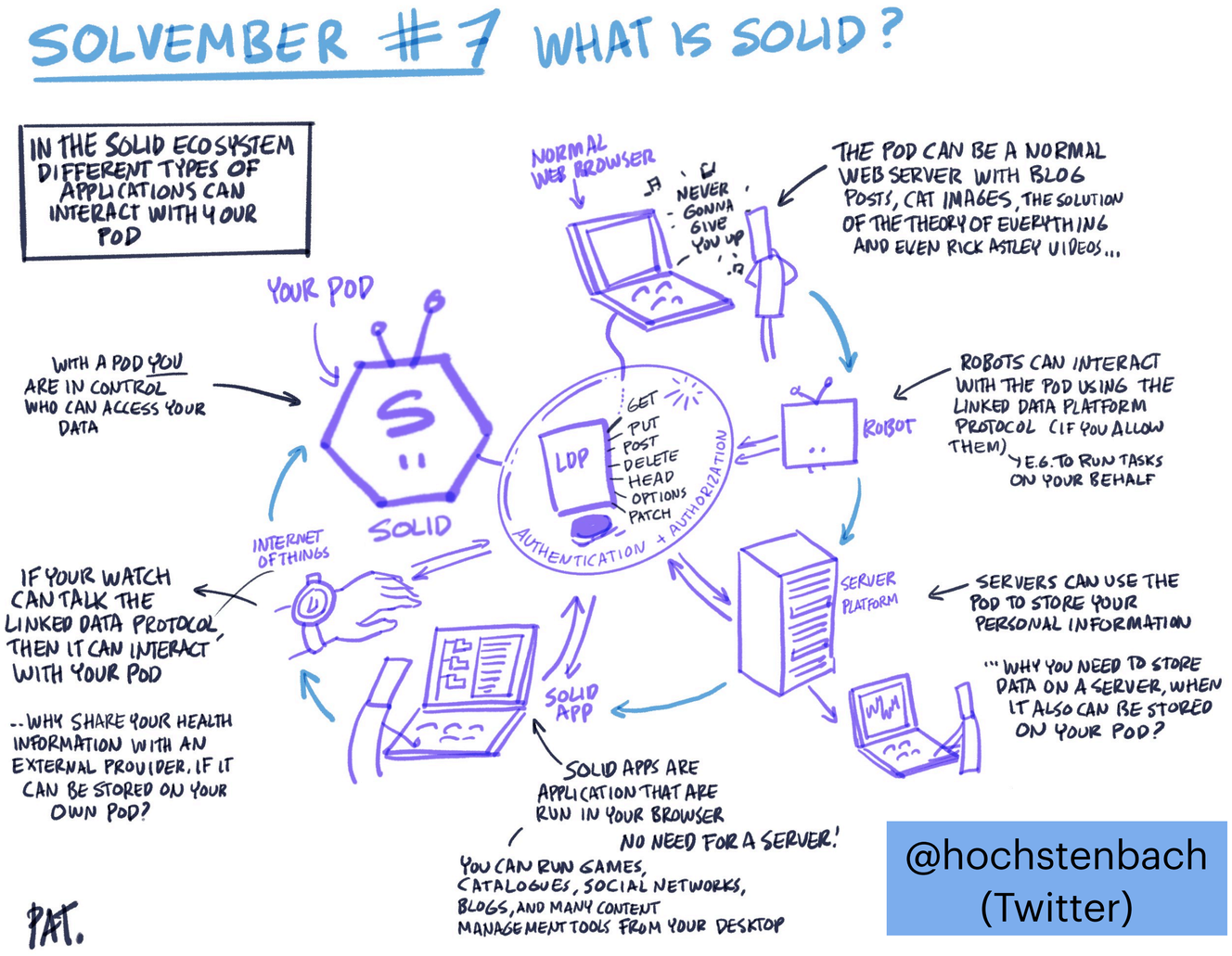
- Companies decide how to collect, store data
- Companies decide how/where to use it
- Companies offer you choices and controls

Decentralised

- You “control” where your data is stored
- You “control” how it is used by apps/services
- You offer choices and controls

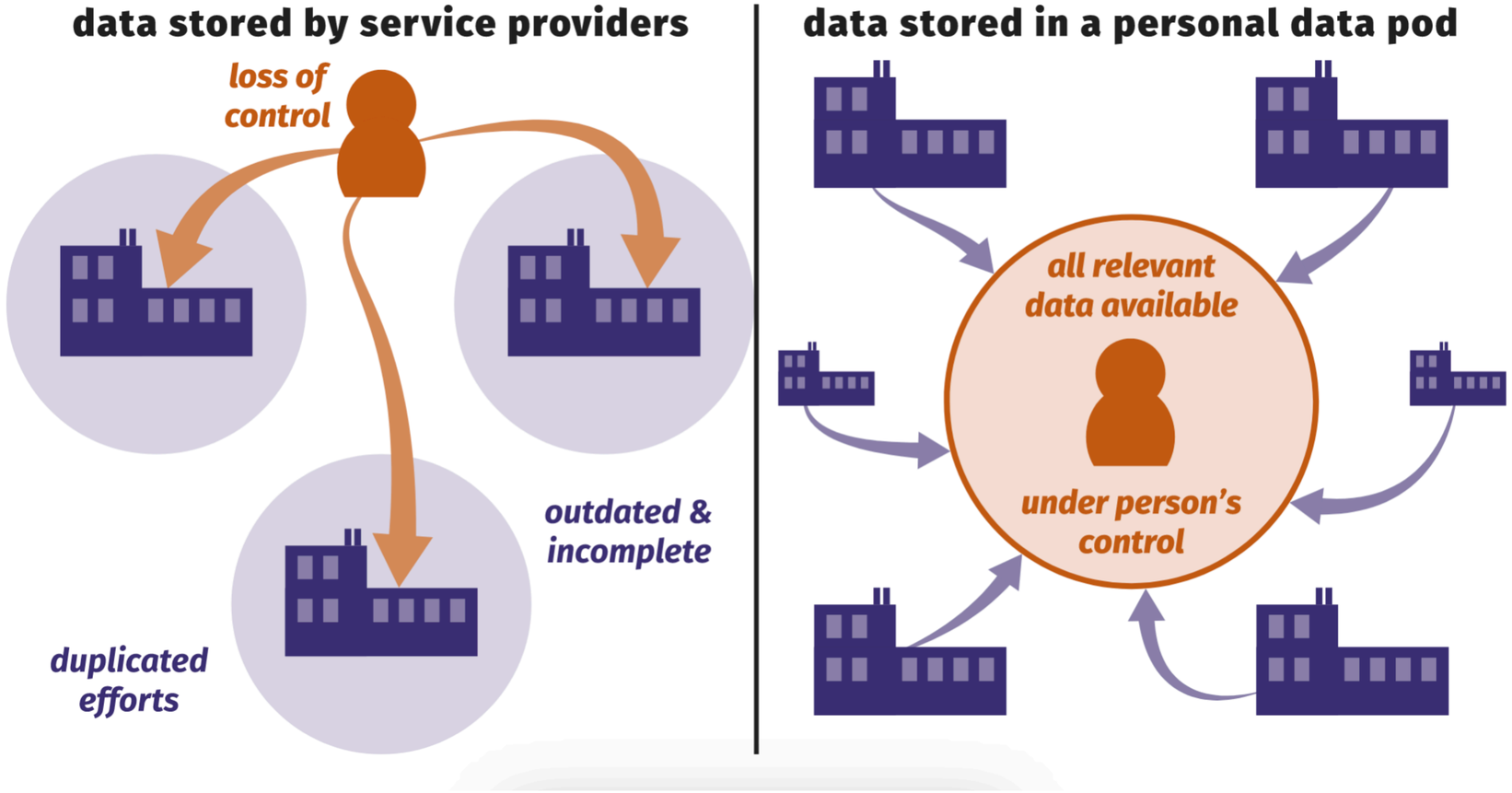
What will SOLID need to work?

- A new way to express privacy and preferences
- User-friendly UI/UX *without dark patterns*
- Legal enforcement to make companies respect negotiation of user preferences and settings



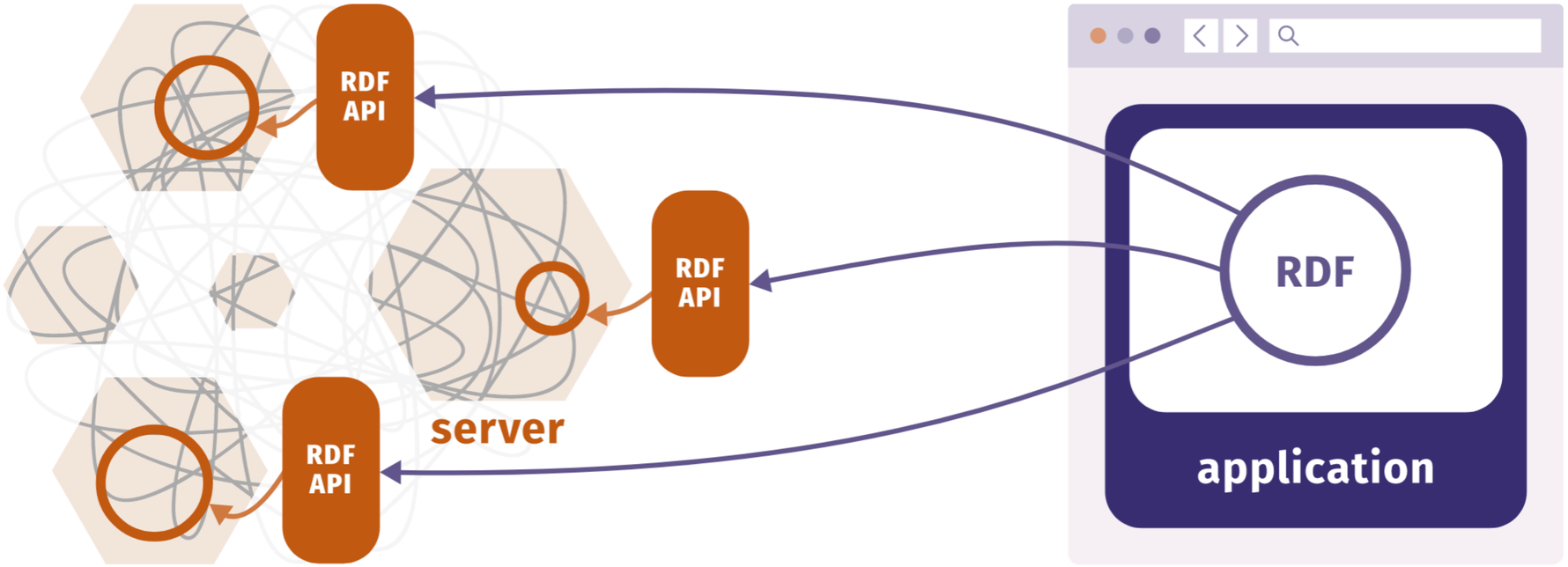
Solid - Inversion of Control

Every piece of data created *by* a person or *about* them, is stored in a data pod.

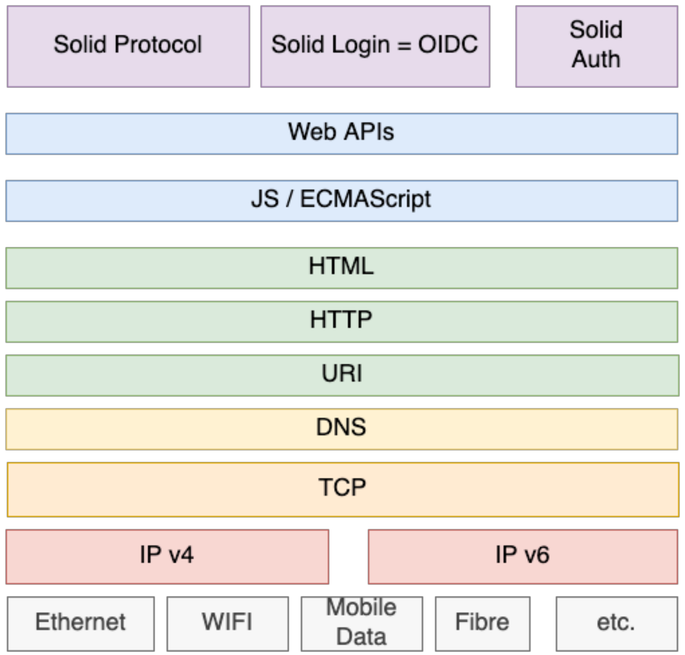


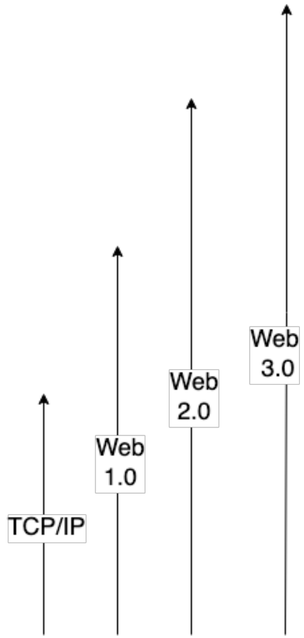
Solid - RDF ‘data standard’

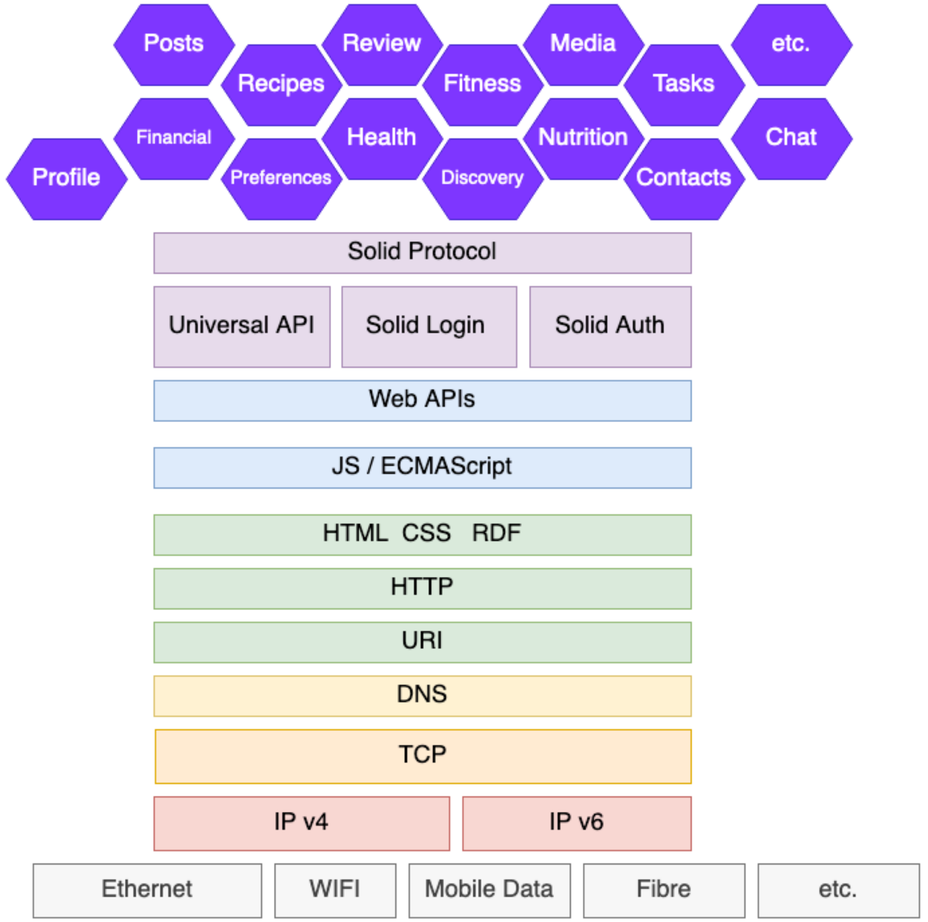
Each data pod exposes its part as RDF through a Web API.



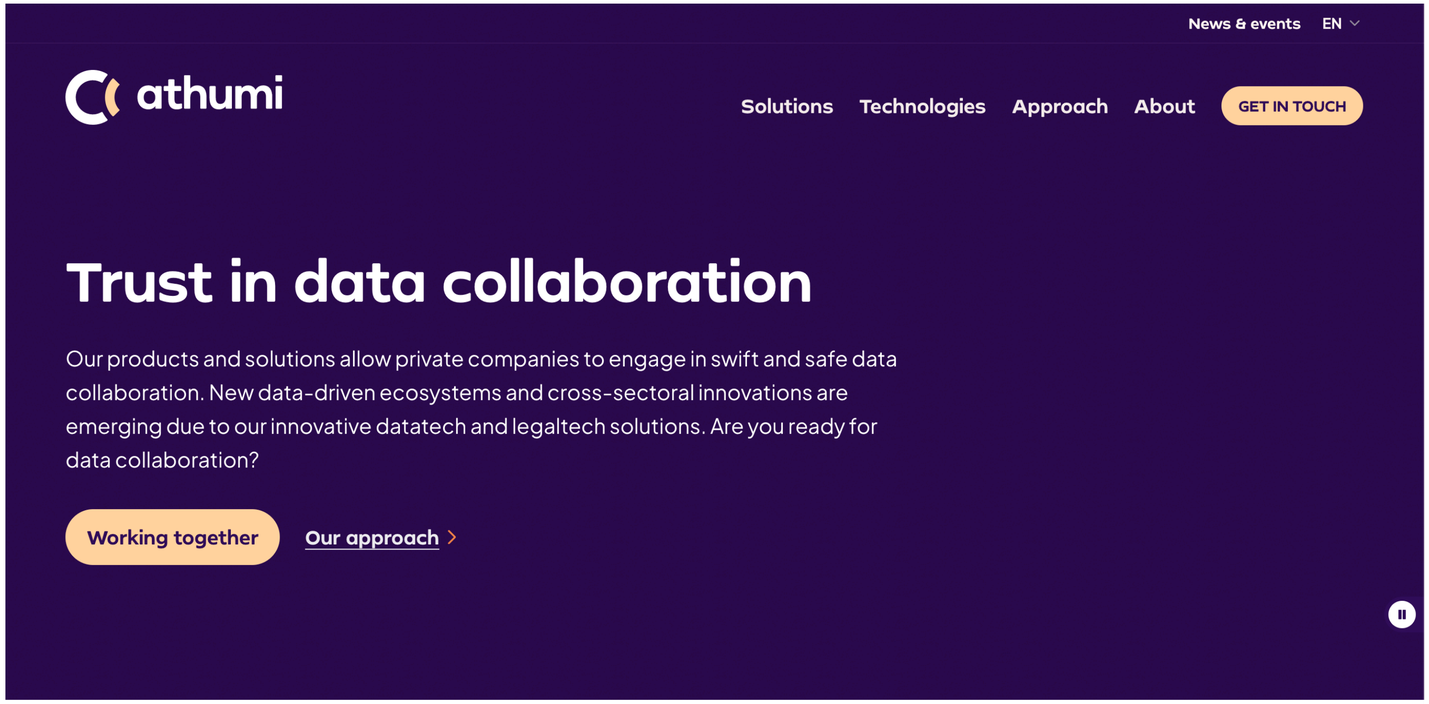
Web 3.0







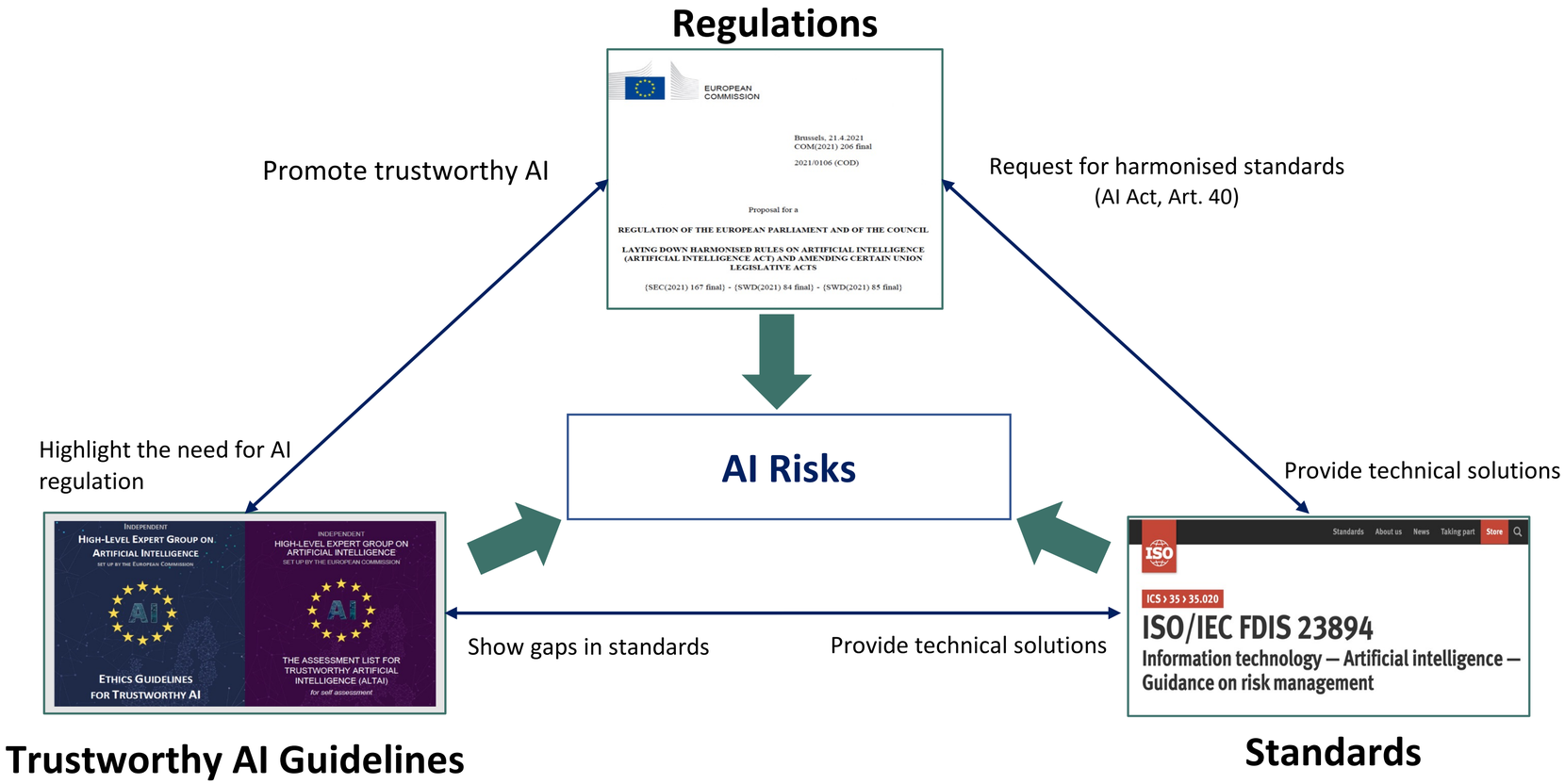
Flanders (Belgium) - a Pod for every Citizen



athumi – your reliable partner for data collaboration

We are a newly public company bound by a statutory mandate to process personal and sensitive corporate data in a smart and secure way, ensuring that all who share their data through our services and partners retain full control and transparency.

Efforts Addressing AI Risks



AIRO Requirements

Describing High-Risk AI Systems

Questions to identify whether an AI system is high-risk according to Annex III

Question	concept	Relation with AISystem
What techniques are utilised in the system?	**AI Technique**	usesAITechnique
What domain is the system intended to be used in?	**Domain**	isAppliedWithinDomain
What is the intended purpose of the system?	**Purpose**	hasPurpose
What is the application of the system?	**AI Application**	hasApplication
Who is the intended user of the system?	**AI User**	hasAIUser
Who is the subject of the system?	**AI Subject**	hasAISubject
In which environment is the system used?	**Environment Of Use**	isUsedInEnvironment

ANNEX I
ARTIFICIAL INTELLIGENCE TECHNIQUES AND APPROACHES referred to in Article 3, point 1

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

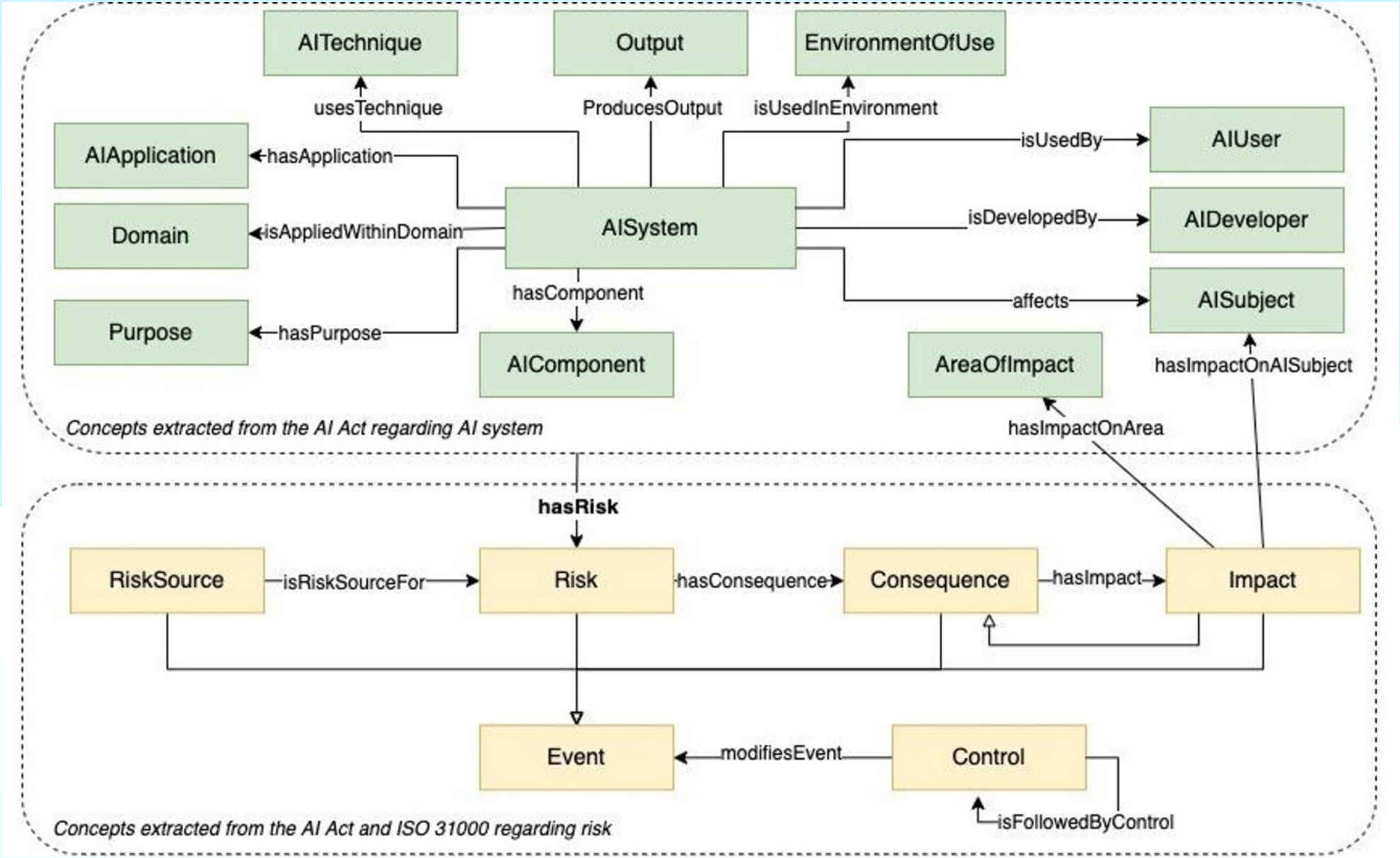
(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

(c) Statistical approaches, Bayesian estimation, search and optimization methods.

ANNEX III
HIGH-RISK AI SYSTEMS REFERRED TO IN ARTICLE 6(2)

High-risk AI systems pursuant to Article 6(2) are the AI systems listed in any of the following areas:

1. Biometric identification and categorisation of natural persons:
   (a) AI systems intended to be used for the 'real-time' and 'post' remote biometric identification of natural persons;
2. Management and operation of critical infrastructure:
   (a) AI systems intended to be used as safety components in the management and operation of road traffic and the supply of water, gas, heating and electricity.
3. Education and vocational training:
   (a) AI systems intended to be used for the purpose of determining access or assigning natural persons to educational and vocational training institutions;
   (b) AI systems intended to be used for the purpose of assessing students in educational and vocational training institutions and for assessing participants in tests commonly required for admission to educational institutions.
4. Employment, workers management and access to self-employment:
   (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;
   (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.
5. Access to and enjoyment of essential private services and public services and benefits:
   (a) AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such


AITechnique
Output
EnvironmentOfUse
usesTechnique
ProducesOutput
isUsedInEnvironment
AIApplication
hasApplication
isUsedBy
AIUser
Domain
isAppliedWithinDomain
AISystem
isDevelopedBy
AIDeveloper
hasComponent
affects
AISubject
Purpose
hasPurpose
AIComponent
AreaOfImpact
hasImpactOnAISubject
Concepts extracted from the AI Act regarding AI system
hasImpactOnArea
hasRisk
RiskSource
isRiskSourceFor
Risk
hasConsequence
Consequence
hasImpact
Impact
Event
modifiesEvent
Control
isFollowedByControl
Concepts extracted from the AI Act and ISO 31000 regarding risk

Identification of High-Risk AI Systems

```
PREFIX airo: <https://w3id.org/AIRO#>
SELECT  ?system ?technique ?domain ?purpose
        ?application ?user ?subject ?environment
WHERE {
        ?system a airo:AISystem ;
                airo:usesTechnique ?technique ;
                airo:isUsedWithinDomain ?domain ;
                airo:hasPurpose ?purpose ;
                airo:hasApplication ?application ;
                airo:isUsedBy ?user ;
                airo:affects ?subject ;
                airo:isUsedInEnvironment ?environment . }
```

AIRO concept	
`AISystem`	uber's real time id check
`AITechnique`	machine learning techniques
`Domain`	employment
`Purpose`	biometric identification of drivers to decide on contract termination
`AIApplication`	facial recognition
`AIUser`	uber driver
`AISubject`	uber driver of bame background
`EnvironmentOfUse`	work related relations

1. Biometric identification and categorisation of natural persons:

   (a) AI systems intended to be used for the 'real-time' and 'post' re identification of natural persons;

4. Employment, workers management and access to self-employment:

   (a) AI systems intended to be used for recruitment or selection of natural persons, notably for advertising vacancies, screening or filtering applications, evaluating candidates in the course of interviews or tests;

   (b) AI intended to be used for making decisions on promotion and termination of work-related contractual relationships, for task allocation and for monitoring and evaluating performance and behavior of persons in such relationships.

- Manual analysis

High Risk

SHACL Shapes for Automatic Identification of High-Risk AI

- ”Rules” to determine whether AI satisfies conditions for being “high-risk”
- Choose your favourite flavour of rule languages & mechanisms

- We chose **SHACL**
- Why:
  - Flexible, Standardised
  - Extensible with plugins/features
  - Built-in documentation of outputs
  - Integrate to instead check outputs e.g. another rule engine

- We implement SHACL shapes for clauses defined in Annex III that determine high-risk
- Validation is to NOT satisfy the expressed criteria

```
1  @prefix dash: <http://datashapes.org/dash#> .
2  @prefix sh: <http://www.w3.org/ns/shacl#> .
3  @prefix airo: <https://w3id.org/AIRO#> .
4  @prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#> .
5  :AnnexIII-1
6      a sh:NodeShape ;
7      sh:targetClass airo:AISystem ;
8      sh:message "High-Risk AI System as per AI Act Annex III-1"@en ;
9      sh:description "Biometric Identification of Natural Persons"@en ;
10     sh:not [
11         a sh:PropertyShape ;
12         sh:path airo:hasPurpose ;
13         sh:class airo:BiometricIdentification; ] .
```

AI & Data

Regulating ~~Data~~

Harshvardhan J. Pandit | email: harshvardhan.pandit@adaptcentre.ie

CS7IS1 | 14 October 2024 | Trinity College Dublin

Slides available at: https://harshp.com/research/presentations