

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

Harshvardhan J. Pandit

*ADAPT Centre, Dublin City University
National Standards Authority Ireland (NSAI)
Chair, W3C Data Privacy Vocabularies and
Controls Community Group (DPVCG)*

Email:

*harshvardhan.pandit@adaptcentre.ie
me@harshp.com*

Jan Lindquist

*Swedish Institute for Standards (SIS),
Stockholm, Sweden
Co-Editor ISO/IEC TS 27560:2023*

Email:

jan@linaltec.com

Georg P. Krog

*Chief Legal Counsel
& Co-Founder of Signatu AS, Oslo, Norway
Member DPVCG*

Email:

georg@signatu.com

A Story in 3 Parts

Past

Standardisation of “**Notice & Consent**” under ISO and GDPR

Present

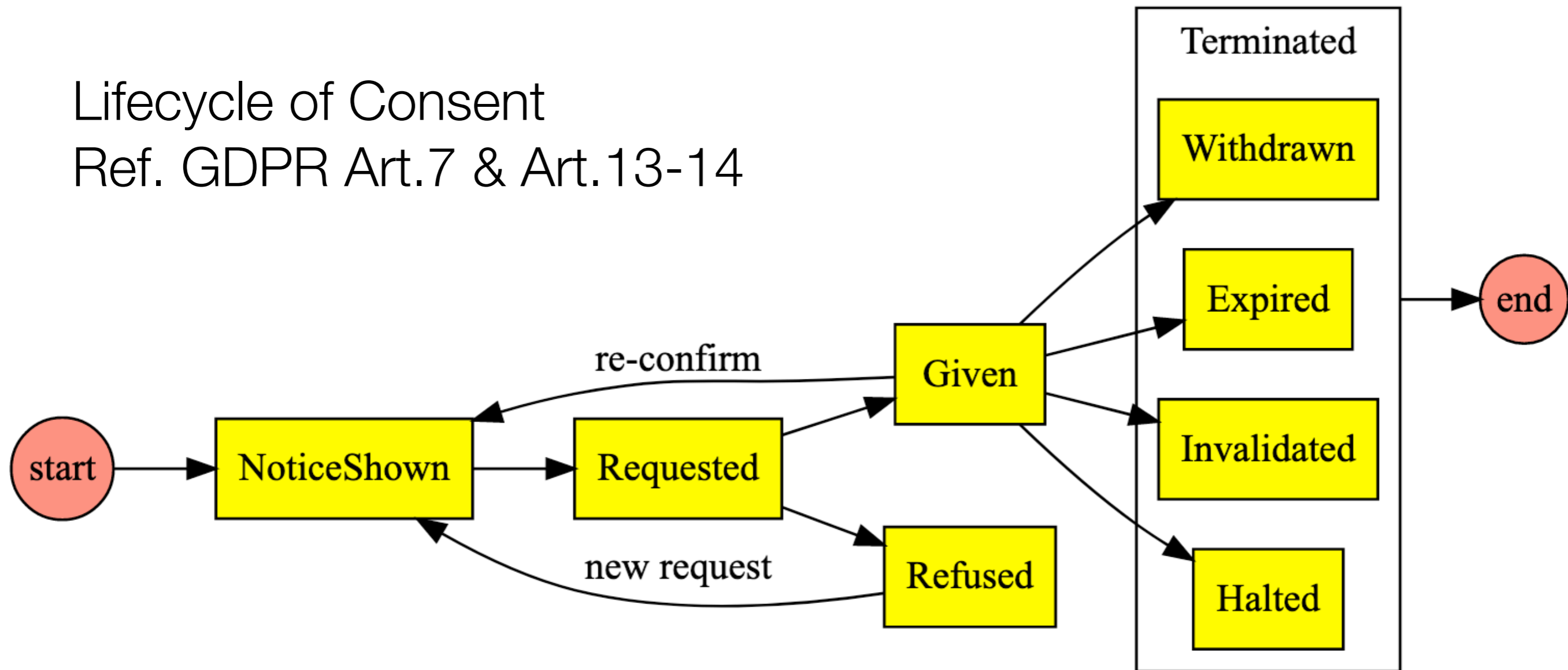
Developing Practical Solutions to Implement Notice & Consent using something called the **Data Privacy Vocabulary (DPV)**

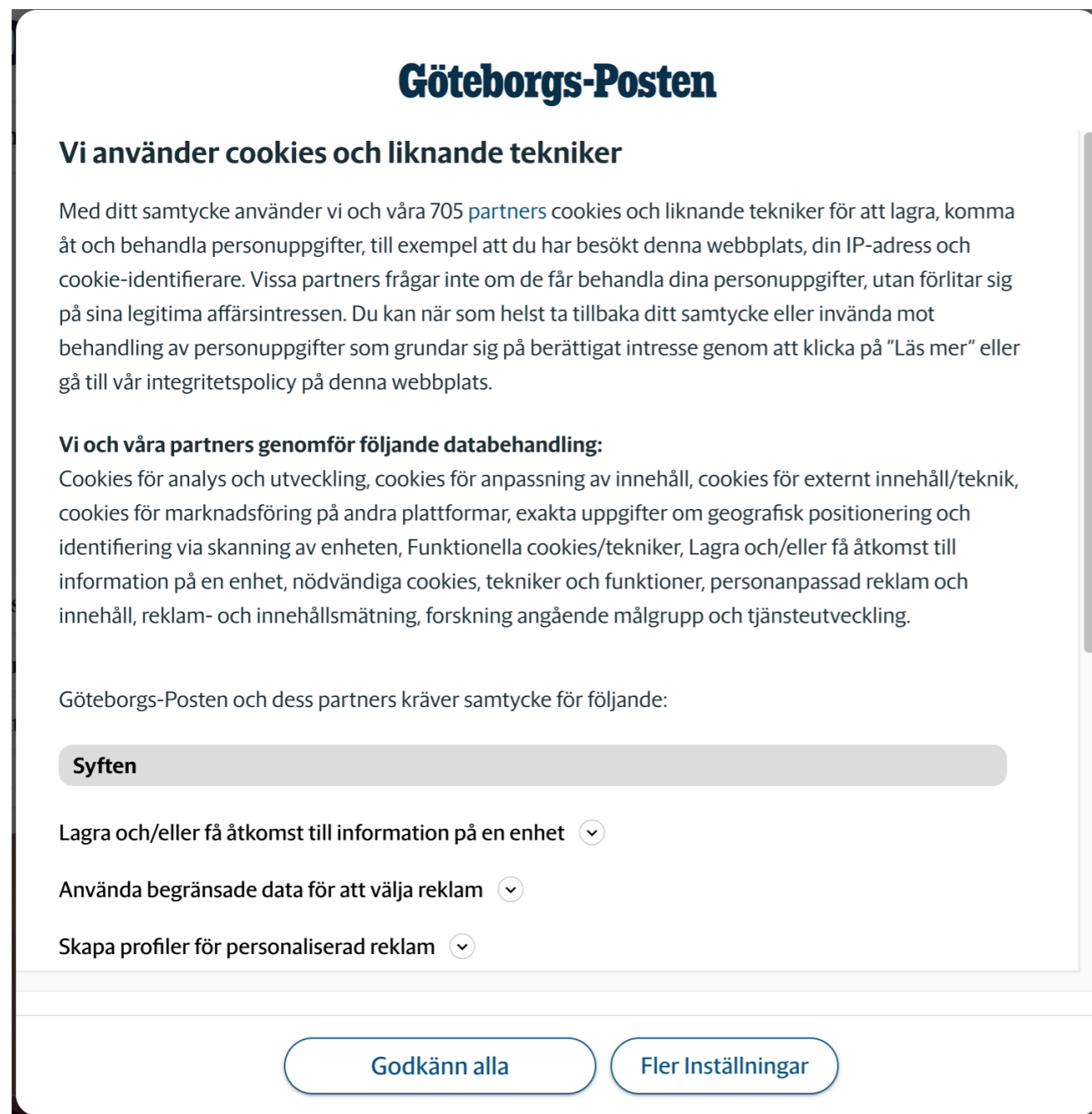
Future

Looking towards **future standards and regulations**
like DGA, eIDAS, EUDI, and more...

Lifecycle of Consent

Ref. GDPR Art.7 & Art.13-14





<https://www.gp.se/>

Hejsan!
Vad händer om du klickar på
Acceptera eller **Avvisa**?

Hello There!
What happens if you click on
Accept or **Reject**?

Challenges

Organisations / Data Controllers

- GDPR Art.7-3 clearly states “*the controller shall be able to demonstrate that the data subject has consented*”
- **How to maintain such Consent Records?**
- What Information must consent records contain for GDPR?
- How to produce such records? E.g. for audits and compliance?
- How to exchange consent records with others in an interoperable manner?

Individuals / Data Subjects

- Individuals have to repeat their consent interactions over and over again across websites and devices
- **Consent, once given or refused, just disappears ...**
- Accounts that could save consent are ‘tied’ to specific services
- Individuals have no way to retain a ‘record’ of what they consented to (or not)

Consent Receipt Specification

Version: 1.1.0
Document Date: 2018-02-20
Editors: Mark Lizar, David Turner
Contributors: Richard Beaumont, Chris Cooper, Sal D'Agostino, Rupert Graves, Iain Henderson, Mary Hodder, Harri Honko, Andrew Hughes, Tom Jones, Robert Lapes, Oliver Maerz, Eve Maler, Jim Pasquale, Samuli Tuoriniemi, John Wunderlich
Produced by: Consent & Information Sharing Work Group

To address this, the Kantara Initiative published the ‘**Consent Receipt**’ specification in 2018.

A ‘*consent receipt*’ is a digital receipt of the consent as a transaction - similar to how you receive a receipt after purchasing goods.

The receipt is proof of the consent interaction, and is an actionable artefact that can be used in future transactions with the same or different entities.



Photos by Karolina Kaboompic

INTERNATIONAL
STANDARD

ISO/IEC
29184:2020

Edition 1
2020-06

Information technology — Online
privacy notices and consent



Reference number
ISO/IEC 29184:2020

© ISO 2024

ISO/IEC 29184:2020

Information technology — Online privacy notices and consent

Published (Edition 1, 2020)

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

TECHNICAL
SPECIFICATION

ISO/IEC TS
27560:2023

Edition 1
2023-08

Privacy technologies — Consent record
information structure



Reference number
ISO/IEC TS 27560:2023

© ISO 2024

ISO/IEC TS 27560:2023

Privacy technologies — Consent record information structure

Published (Edition 1, 2023)

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

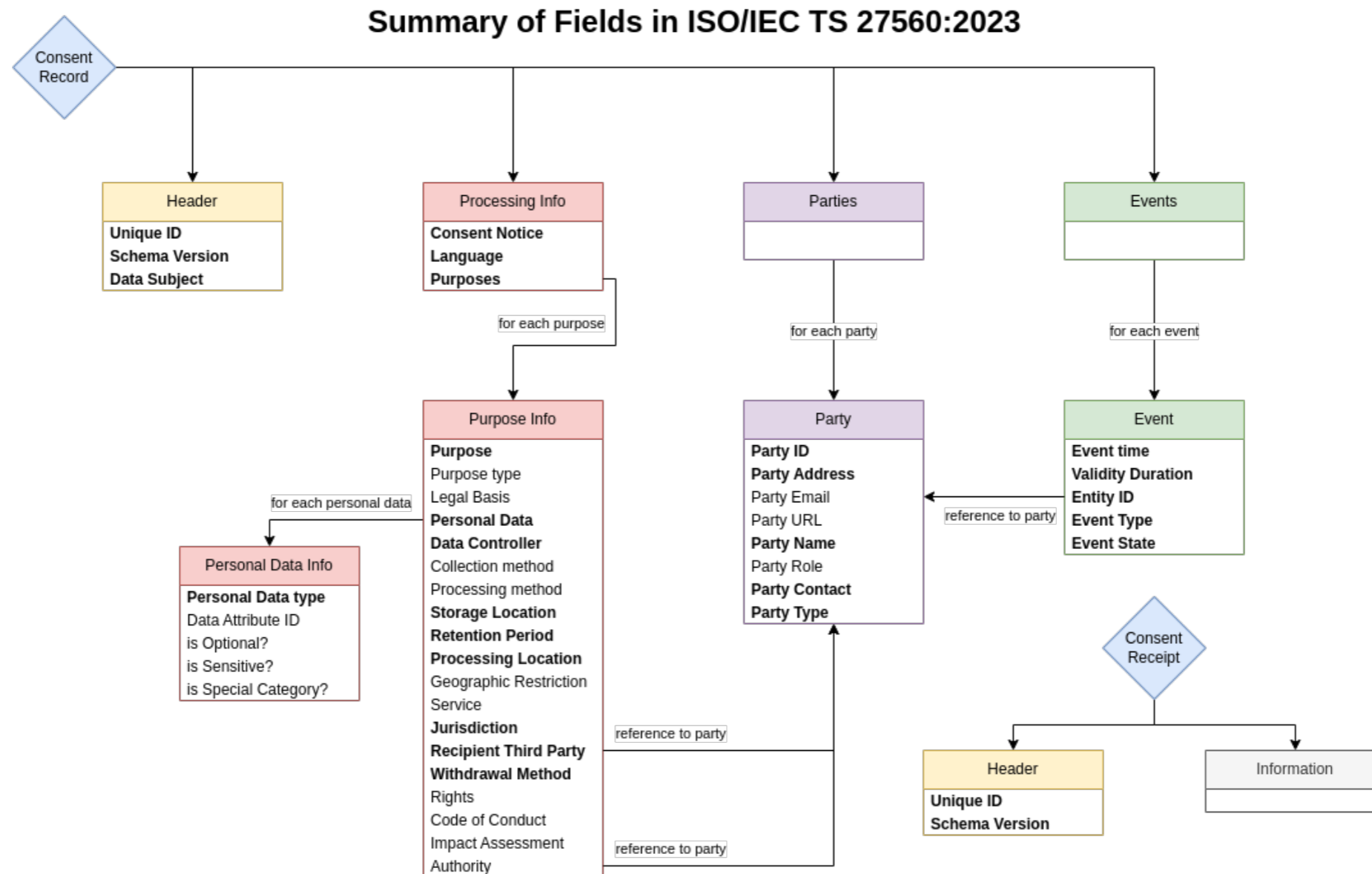
1. Maintaining a **Consent Record**
2. Providing a record of consent to the Data Subject as a **Consent Receipt**
3. Exchange of consent information between information systems
4. Managing the life cycle of recorded consent information

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

Practical Problems ~~Challenges~~ Challenges

1. How will ISO/IEC 29184:2020 and ISO/IEC TS 27560:2023 work with the GDPR?
2. If an Organisation uses these standards - to what extent do they support requirements for valid consent?
3. How to practically create consent records/receipts?
4. How will consent records/receipts work with the upcoming legal frameworks of DGA, eIDAS, and EUDI?

1. How will ISO/IEC 29184:2020 and ISO/IEC TS 27560:2023 work with the GDPR?



Consent Records contain information about processing, entities, and consent events

Is this information in accordance with the GDPR? Is it sufficient?

Table 2. Mapping information requirements across ISO/IEC TS 27560:2023, ISO/IEC 29184:2020 and EU GDPR. For GDPR, numbers without prefixes are Articles, and with prefix R are Recitals

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

ISO/IEC TS 27560:2023	ISO/IEC 29184:2020	EU GDPR
3.1 consent	—	4–11 definition of consent
3.2 consent receipt	Annex B	R42, 7–1 demonstrating consent
3.3 consent record	—	R42, 7–1, 13, 14, 30 recording information related to consent
3.4 consent type	5.4.3 Informed and freely given consent. 3.1 explicit consent	R32, R43, 6–1a, 9–2a conditions for consent. R42 demonstrating consent. 8 child’s consent. 9–2a explicit consent
6.2 recordkeeping for privacy notices and consent	—	R42, 7–1, 13, 14, 30 recording and demonstrating consent
6.2.2.1 presentation of notice	5.2.2 providing notice, 5.2.3 appropriate expression, 5.2.7 appropriate forms, 5.2.9 accessibility	R32, R42, R43, R58, 7–2 notice for consent
6.2.2.2 timeliness of notice	5.2.5 appropriate timing	R32, R42, R43, R60, 7–2, 13, 14 notice for providing information and requesting consent. R61, 13–2 14–3 timing of notice. R62 exceptions
6.2.2.3 obtaining consent	5.2.7 appropriate forms	R42, 7–1 record of consent
6.2.2.4 time and manner of consent	5.2.6 appropriate locations	R32, R42, R43, 7–2
6.2.2.5 technical implementation	—	R42, 7–1, 13, 14, 30 maintaining information for demonstrating consent
6.2.2.6 unique reference	5.2.8 ongoing reference	
6.2.2.7 legal compliance	—	

This work was carried out during the 27560 development process in ISO

2. If an Organisation uses these standards - to what extent do they support requirements for valid consent?

ISO/IEC TS 27560:2023

- All fields required by GDPR regarding consent are present in the standard (this paper).
- GDPR does have the concept of a 'consent record' (Art.7-1) but does not have the concept of a "consent receipt"

* Art.15 Right of Access is similar.
* However, if consent = personal data, and it is 'given' by the data subject, then maybe Art.20 Data Portability means we should be able to receive a copy of it?

ISO/IEC 29184:2020

"The comparison shows that 29184 and GDPR have similar requirements, and that 29184 meets these in several cases. However, 29184 fails to meet two important requirements in GDPR regarding 'freely given' consent and use of 'explicit consent' as a legal basis."

"Comparison of notice requirements for consent between ISO/IEC 29184:2020 and GDPR" by Pandit and Krog - Journal of Data Protection & Privacy (2021)

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’

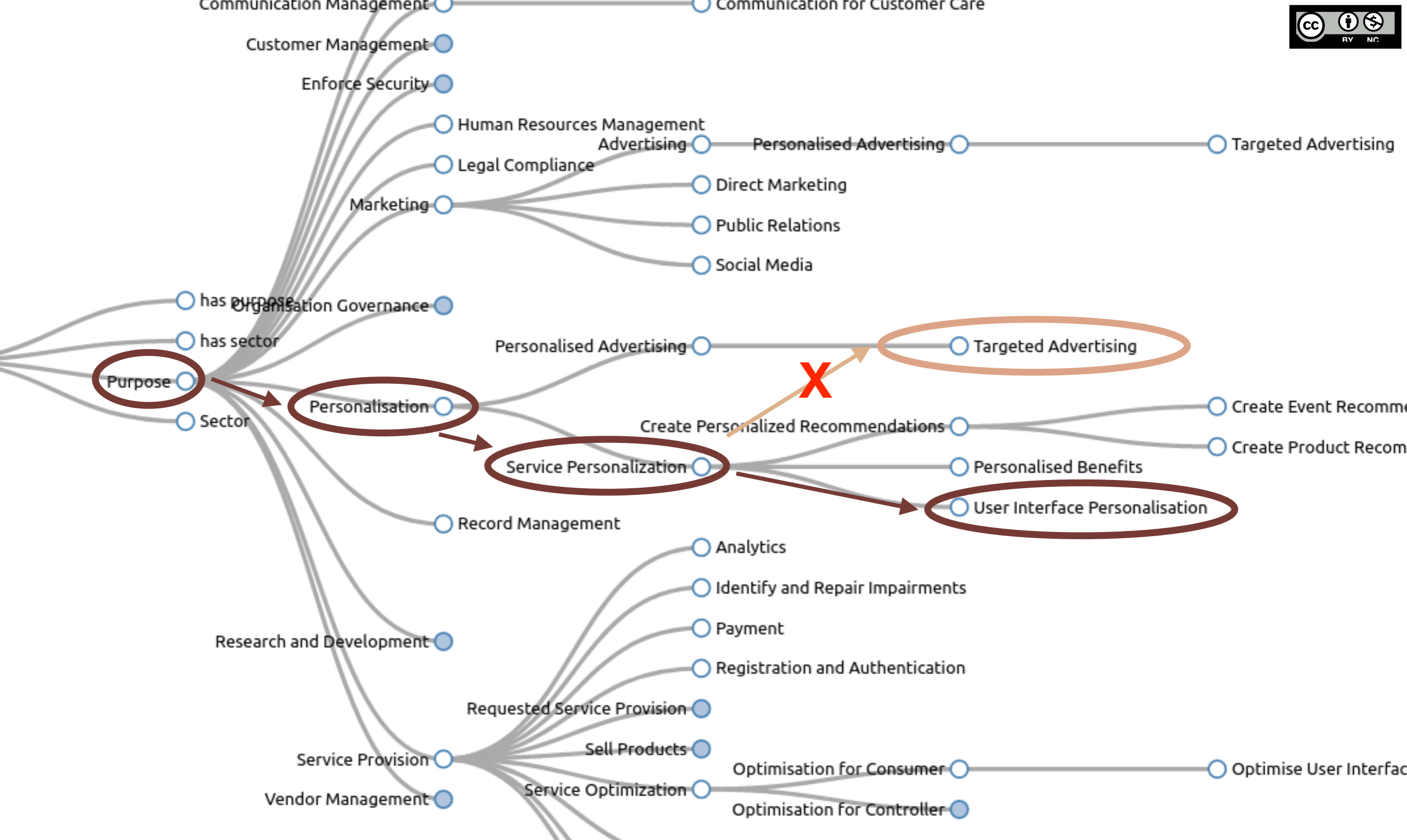


Semantics

Data Privacy Vocabulary (DPV)

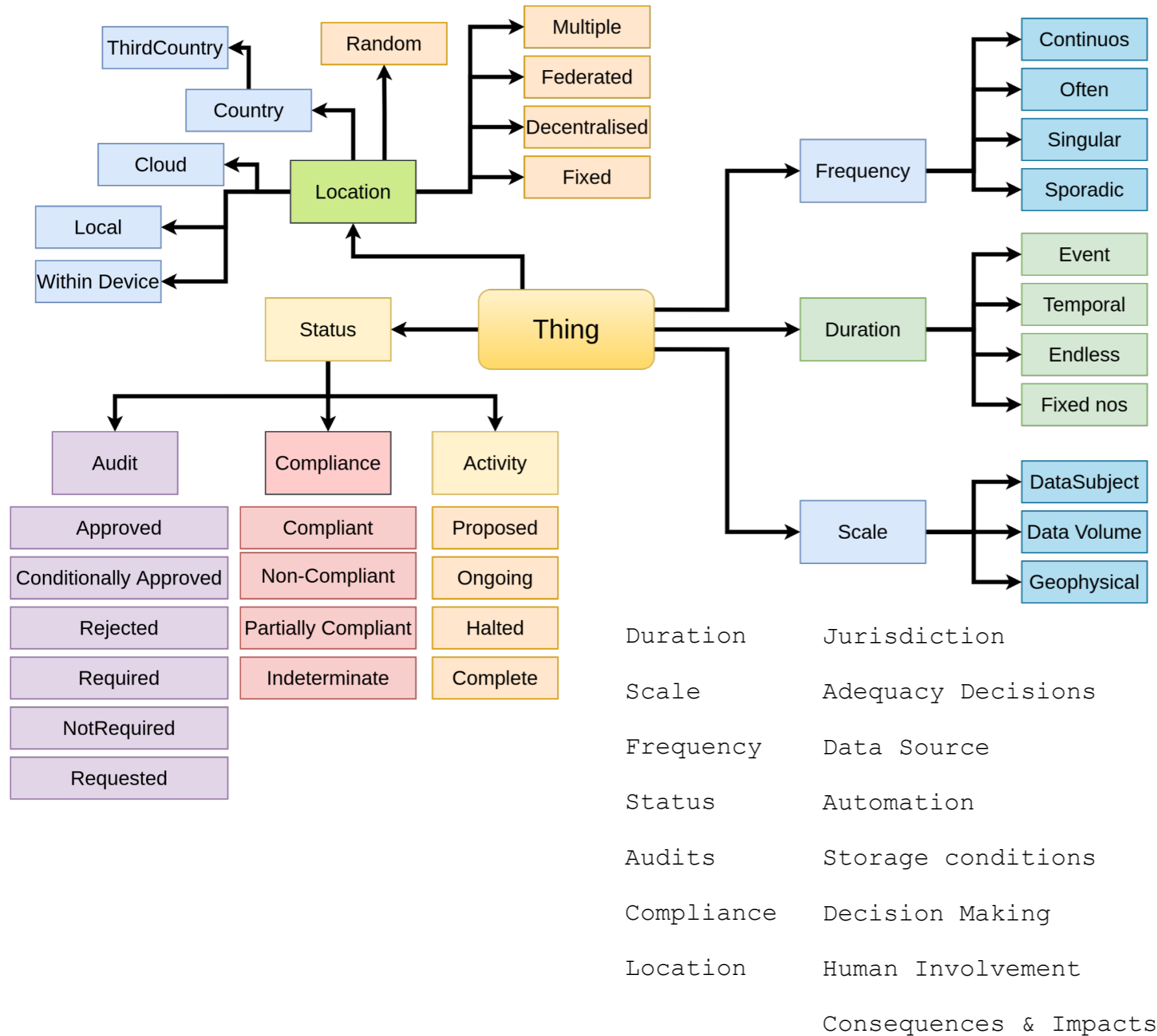
<https://dpvcg.org/>

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



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

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



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

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

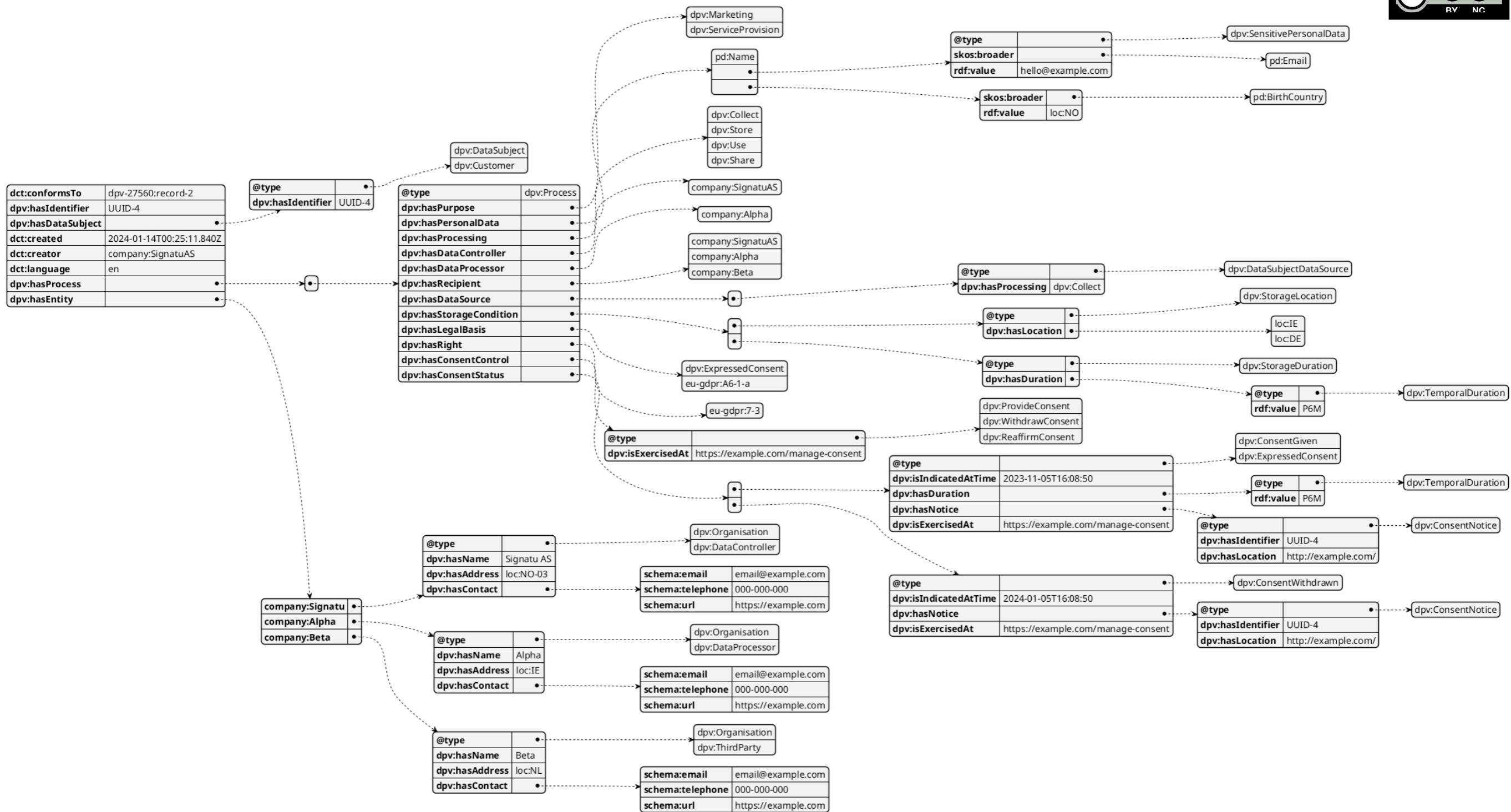
From: Implementing ISO/IEC TS 27560:2023 Consent Records and Receipts for GDPR and DGA

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:StorageDeletion	
Processing Condition	0..*	dpv:ProcessingCondition, dpv:ProcessingLocation, 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 Steps

- Propose ISO/IEC TS 27560:2023 be made FREE for access and use given its utility *(REQUEST SUBMITTED)*
- Using ISO/IEC TS 27560:2023 within the EU Legal Framework —> Propose it be adopted as EN *(ONGOING)*
- Promote use of 29184:2020 and TS 27560:2023 to Industry and Data Protection Authorities *(HAPPENING NOW???)*
- Promote “consent receipts” for rights management *(ONGOING)*
- Create a technical specification for industry to implement records/receipts in their systems *(ONGOING)*

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

Create Data Processing Specification-September 4, 2024

 Add legal basis as GDPR consent

The legal basis for processing under GDPR is "consent".

Here is the final summary of the Data Processing Specification:

- **Name:** UIP
- **Purpose:** UI Personalisation for ease of use
- **Purpose Category:** dpv:UserInterfacePersonalisation
- **Data:** Name
- **Personal Data Categories:** pd:Name
- **Legal Basis:** GDPR Consent

Shall I proceed to create this Data Processing Specification?

2 Represent with DPV

Purpose description

UI Personalisation for ease of use

Purpose Categories (DPV)

User Interface Personalisation

Technical Service Provision

dpv:Purpose / dpv:TechnicalServiceProvision ([reference](#))

Purposes associated with managing and providing technical processes and functions necessary for delivering services

User Interface Personalisation

dpv:Purpose / dpv:UserInterfacePersonalisation ([reference](#))

D: Purposes associated with personalisation of interfaces presented to the user


3 Generate Notice


Service Personalisation of UI Interface


UI Personalisation Off

[Detailed information and settings](#)

What is the purpose of collecting data?	Which data do we collect?	What is the legal basis of the purpose?	What is the benefit for you?	Who receives the data?
UI Personalisation	Name	Art.6(1-a) consent	Ease of use	Acme Read more

 I'M OK WITH THAT

 REJECT

 MODIFY SETTINGS

4 Generate Consent Records with Events

```

{
  "dpv:hasConsentStatus": [ 2 items
    {
      "@type": string "dpv:ConsentRequested"
      "dpv:isIndicatedAtTime": string "2024-09-04T06:02:25.443Z"
      "dpv:isIndicatedBy": string "company:665"
    }
    {
      "@type": string "dpv:ConsentGiven"
      "dpv:isIndicatedBy": string "253"
      "dpv:isIndicatedAtTime": string "2024-09-04T06:02:25.443Z"
    }
  ]
}

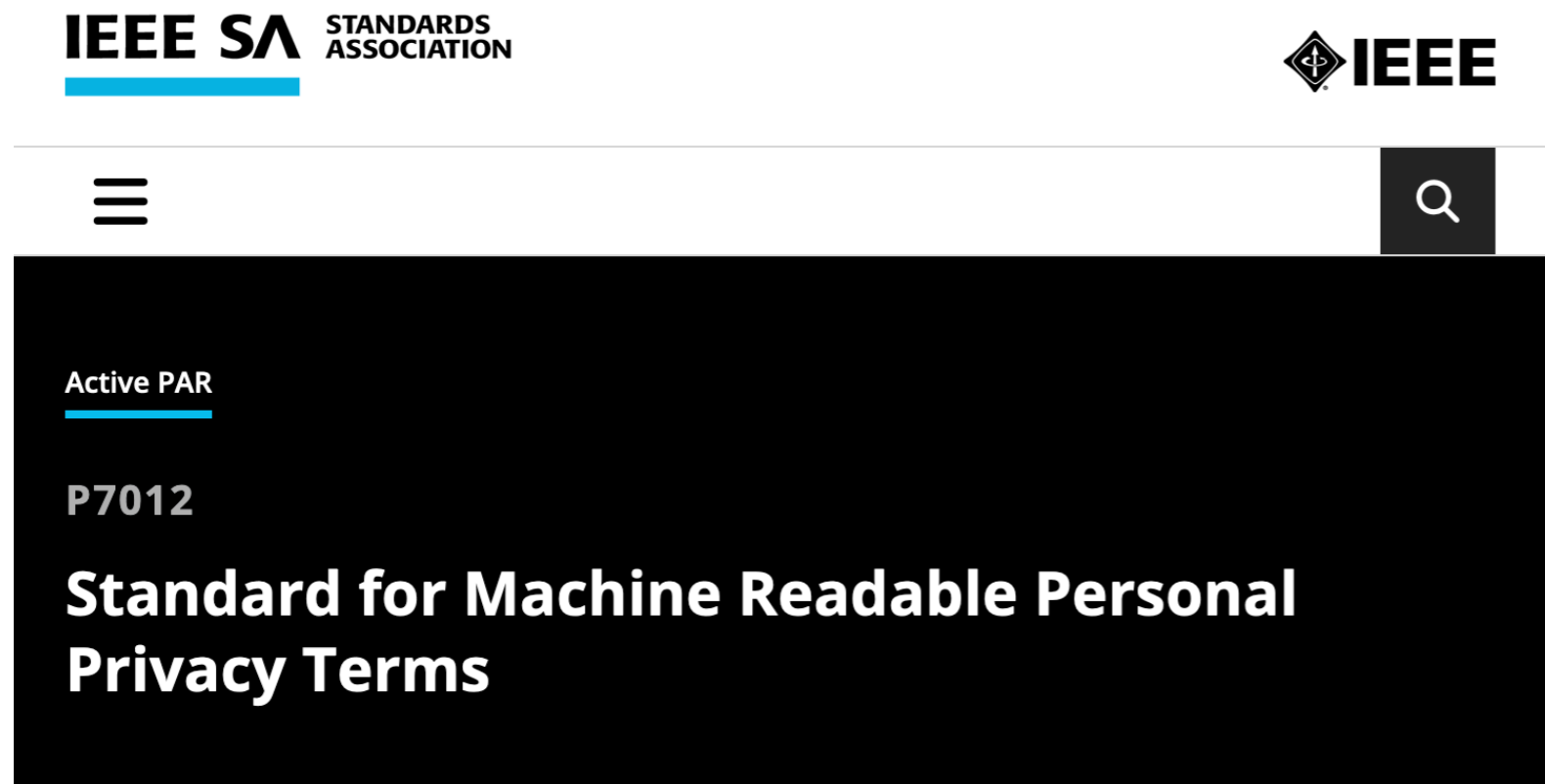
```

4. How will consent records/receipts work with the upcoming legal frameworks of DGA, eIDAS, and EUDI? for the Data Governance Act (DGA)

- DGA Article 25 obligates a “**Common Consent Form**”
—> this work will help!
- Standards based consent notice, record, and receipt
- DPV is the best State of the Art resource to implement it practically - and continuously updated for ~6 years
- Assist Data Intermediaries with **consent collection and recording**, and promote receipts for **transparency** and **accountability** for data reuse and altruism

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



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

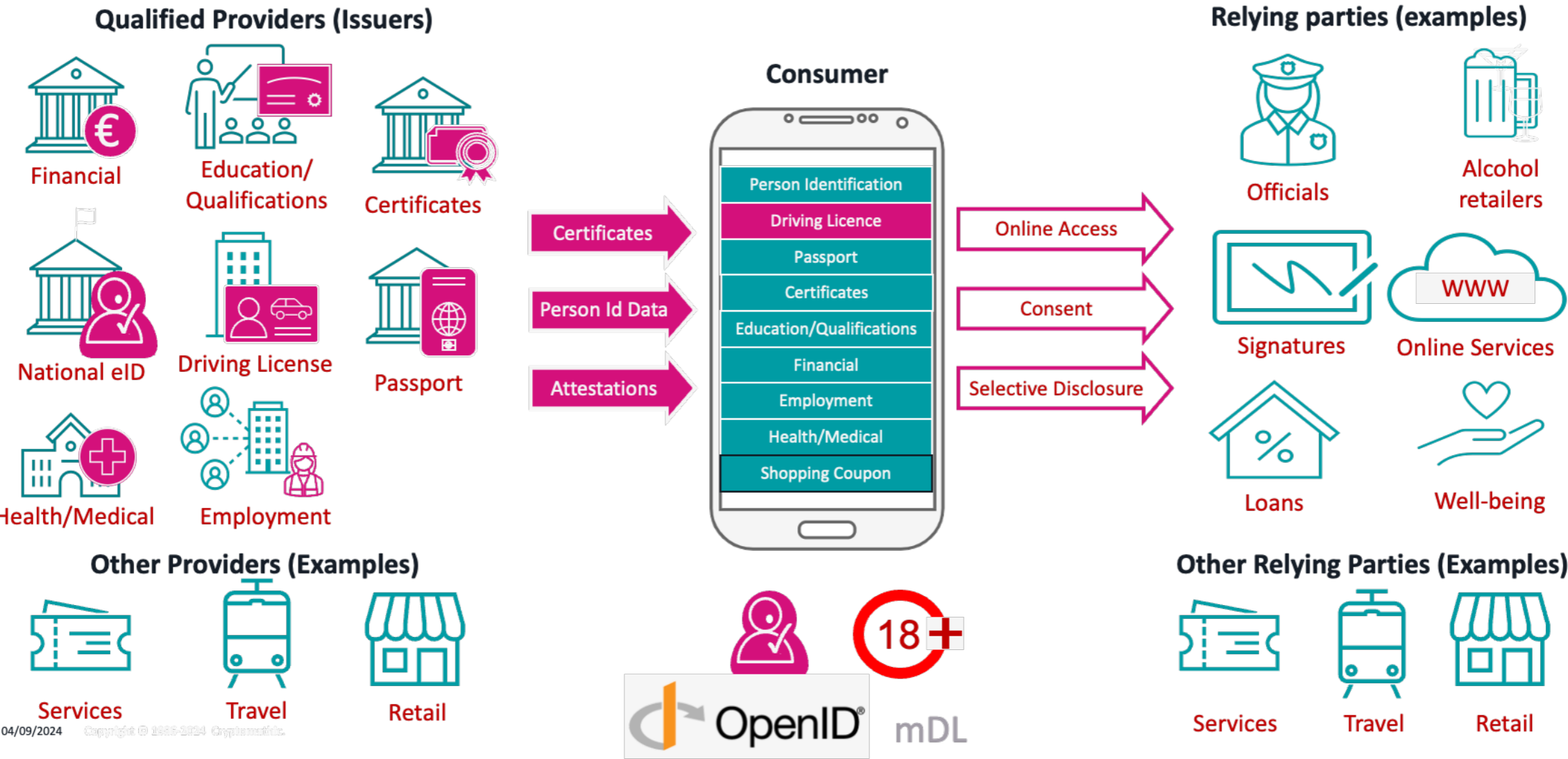
<https://standards.ieee.org/ieee/7012/7192/>

Using Consent Records / Receipts in EUDI Wallets

Ongoing work by Jan Lindquist



WALLET APP SERVICES

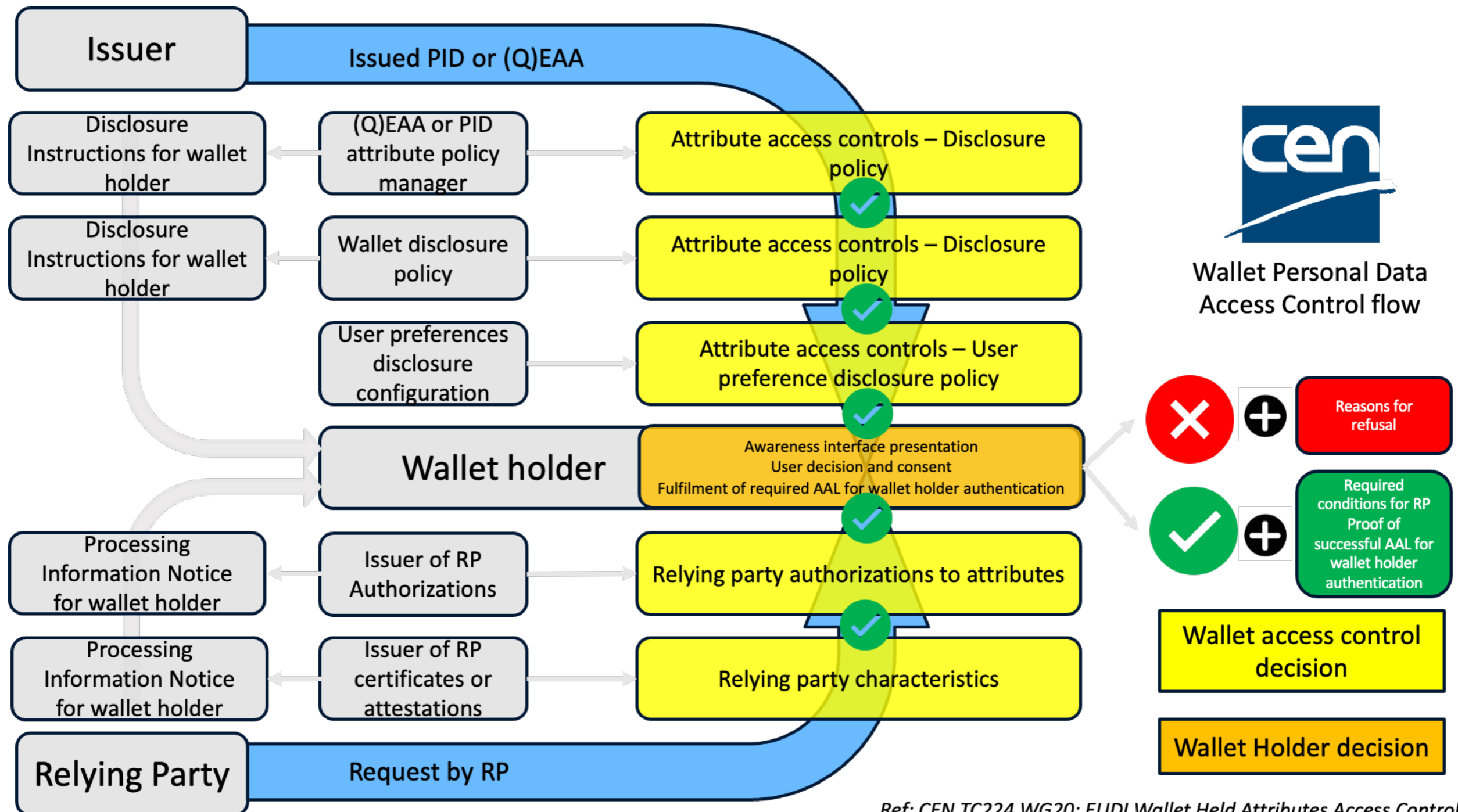


04/09/2024 Copyright © 1999-2024 Cryptomathic

2

Using Consent Records / Receipts in EUDI Wallets

Ongoing work by Jan Lindquist



Paper is Open Access

https://doi.org/10.1007/978-3-031-68024-3_12

Tack! / Thank you!

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

Harshvardhan J. Pandit

*harshvardhan.pandit@adaptcentre.ie
[me@harshp.com](https://harshp.com)*

Jan Lindquist

jan@linaltec.com

Georg P. Krog

georg@signatu.com

Check out Data Privacy Vocabulary (DPV) <https://dpvcg.org/>
W3C DPVCG is an open community group - we welcome you!

See you again at Noon to talk about the AI Act and AI Cards

Download this presentation at <https://harshp.com/research>