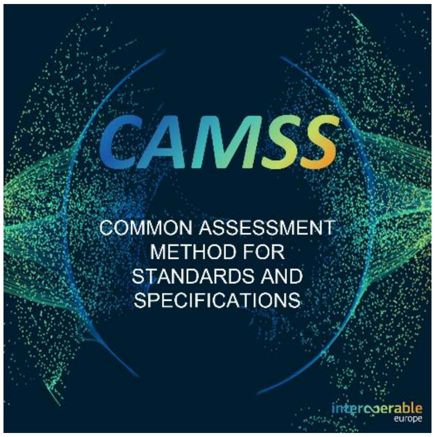

ASSESSMENT SUMMARY v1.0.0

Data Privacy Vocabulary (DPV)[1]

World Wide Web Consortium (W3C)[2]

[1] DPV: https://w3c.github.io/dpv/primer/

[2] W3C: https://www.w3.org/

Change Control

Modification	Details
Version 1.0.0	
Initial version	

TABLE OF CONTENT

1. Introduction

The present document is a summary of the assessment of the **DPV** carried out by CAMSS using the CAMSS Assessment EIF scenario[3]. The purpose of this scenario is to assess the compliance of a standard or specification with the European Interoperability Framework (EIF)[4].

2. Assessment Summary

The **Data Privacy Vocabulary (DPV)** provides a vocabulary and ontology for expressing information related to processing of personal data, entities involved and their roles, details of technologies utilised, relation to laws and legal justifications permitting its use, and other relevant concepts based on privacy and data protection.

DPV aims to act as a core framework of 'common concepts' that can be extended to represent specific laws, domains, or applications. It also enables the expressing of machine-readable metadata about the use and processing of personal data based on legislative requirements such as the General Data Protection Regulation (GDPR).

The specification has been developed by World Wide Web Consortium (W3C), which is an international community concerned with evolving the World Wide Web by developing protocols and guidelines to ensure and enhance its growth.

2.1. EIF Interoperability Principles

Interoperability principles are fundamental behavioural aspects that drive interoperability actions. They are relevant to the process of establishing interoperable European public services. They describe the context in which European public services are designed and implemented.

The specification does not support the principles setting context for EU actions on interoperability:

- **Subsidiarity and proportionality**
  There is no Member State that includes the DPV in their national catalogue with Their National Interoperability Framework (NIF) in alignment with the three categories 1. Conceptual model for integrated public services provision, 2. interoperability layers, and 3. interoperability principles.

The specification fully supports the principles setting context for EU actions on interoperability:

- **Openness**
  DPV is a Core Vocabulary, and as such, the specification enables data portability and the transmission of personal data in an interoperable way. Personal data and open data are compatible in the sense that users can decide where to store their data and what use this data might have.

[3] CAMSS Assessment EIF Scenario: https://ec.europa.eu/eusurvey/runner/CAMSSAssessmentEIFScenario6

[4] ISA2 programme: https://ec.europa.eu/isa2/eif_en

The development process has been carried out by W3C[5] to make it accessible to the different stakeholders and it also includes a public review. Moreover, the Data Privacy Vocabulary Community Group (DPVCG) is the developer community that maintains this specification. It is important mentioning that DPV Final Community Group Report has been delivered in August 2024.

It is interesting to remark that DPV has support from interest groups that are involved in the development of cross-border initiatives. DPV is publicly available for free on W3C's webpage[6] , and It is licensed on a royalty-free basis for its implementation or study.

- **Transparency**

  DPV is based on European Union legislative requirements such as the GDPR, which aims to harmonize data privacy laws across Europe. Therefore, public administrations benefit from the definition of a data model based on this regulation given that it promotes the transparency of the procedures and personal data handled by public administrations, as it is intended to ease proof of compliance against laws regarding data privacy.

  By creating a standardised taxonomy for data privacy concepts and terms, the DPV is enabling the exposure of interfaces as it is intended to enhance semantic interoperability about personal data processing and enable data portability for data subjects.

  Therefore, the DPV promotes the comprehensibility of administrative procedures by providing a clear vocabulary that defines all levels at which personal data will be processed.

- **Reusability**

  While it uses the EU's General Data Protection Regulation (GDPR) as a guiding source for the creation and interpretation of concepts, the ambition and scope of DPV are to provide a broad globally useful vocabulary that can be extended to jurisdiction or domain-specific applications, making it a versatile data model adaptable to multiple business domains.

- **Technological neutrality and data portability**

  DPV is independent of any specification and does not rely on any technology or platform. Moreover, the DPV data model and taxonomy can be adapted to the specific needs of organisations, allowing for partial implementations and for customisations depending on the requirements of the particular context where it is intended to be applied. The specification also provides extension mechanisms for its concepts, to align them with other existing taxonomies. DPV also models the legal aspects of data portability, linking them with technical aspects of electronic data exchange.

[5] W3C process document: https://www.w3.org/2018/Process-20180201/#Policie

[6] DPV on Github: https://w3c.github.io/dpv/primer/

***The specification supports the principles related to generic user needs and expectations*:**

- **User-centricity**
  DPV enables expressing machine-readable metadata about use and processing of personal data based on legislative requirements such as the GDPR. Modelling of the GDPR concepts by the DPV contributes to the once-only principle given that it is meant to be an interoperable vocabulary for representing information about the use and processing of personal data.

- **Inclusion and accessibility**
  The purpose of DPV is not related to e-accessibility. Therefore, this criterion is considered not applicable to this specification.

- **Security and privacy**
  The motivation of DPV is to provide a 'data model' or a 'taxonomy' of concepts that act as a vocabulary for the interoperable representation and exchange of information about personal data and its processing. Therefore DPV is an active enabler of the secure exchange and processing of data, insofar as it refers what measures and regulations are in place (such as GDPR) and points out the compliance of legal obligations to ensure data protection.

  The main goal of DPV is to develop a taxonomy of privacy terms, which include in particular terms from the new European General Data Protection Regulation (GDPR) in order to ease proof of compliance with the GDPR and related privacy protection regulations.

  DPV provides a taxonomy of technical and organisational measures for representing information about how the access to personal data is technically and organisationally protected, safeguarded, secured, or otherwise managed. By referring to what measures are in place (such as GDPR) DPV directly addresses issues about the access to data pointing to the compliance of legal obligations to ensure data protection.

- **Multilingualism**
  Given that the DPV aims to become a standard data model and vocabulary to be used across Europe, it is designed to support most of the languages used in the European Union.

***The specification fully supports the foundation principles for cooperation among public administrations*:**

- **Administrative Simplification**
  DPV provides the standard data that can be collected following European privacy regulations such as GDPR, thus, becoming an asset for digitalisation with conformity to such regulations, and fostering administrative simplification.

As it can be seen in the example of 'data protection aspects of online shopping - a use case'[7], DPV specifies the personal data that an order delivery has to take from the client, thus, ensuring efficient interactions between clients and citizens. For that matter, DPV can ease digitalisation and simplify the delivery of European public services.

- **Preservation of information**
  Although DPV is not directly related to the Preservation of information, it is still addressed when it comes to the modelling of the Context of Processing, indicating the regularity and temporal span of data restoration/backup mechanisms that guarantee that data is preserved.
  The purpose of DPV is not related to the long-term preservation of information; therefore, this criterion is not applicable to the specification.

- **Assessment of effectiveness and efficiency**
  There have been found some academic papers assessing the use of DPV in terms of efficiency. These documents describe the use of DPV personal data handling policies and information about consent or assess the effectiveness when it comes to the discovery of the relevant information in privacy policies through integrating the knowledge represented in the DPV with the information modelled in BabelNet.

2.2. EIF Interoperability Layers

The interoperability model which is applicable to all digital public services includes:

- Four layers of interoperability: legal, organisational, semantic and technical;
- A cross-cutting component of the four layers, 'integrated public service governance';
- A background layer, 'interoperability governance'.

The Specification supports the implementation of digital public services complying with the EIF interoperability model:

- **Interoperability governance**

  DPV can be mapped to the Eira Library of Interoperability Specifications (ELIS) in the "Privacy Policy", "Controlled Vocabulary" "Data", "Data Mapping Catalogue", "Metadata", "Open Data", "Hash Code", "Linked Open Data", "Linked Data in the Semantic View", "Data Model" and "Ontology" Semantic View as well as the "Privacy Framework" of the Organisational View.

  Although the DPV is not included in any catalogue, neither at the national nor the European level, it is nonetheless contributing to the development of the cross-border SPECIAL[8] project. In terms

[7] Data protection aspects of online shopping - a use case: https://www.w3.org/community/dpvcg/2019/12/12/data-protection-aspects-of-online-shopping-a-use-case/

[8] SPECIAL Project: https://specialprivacy.ercim.eu/

of implementation conformity, a “Development Guide” for the DPV can be found in the GitHub repository.

- **Legal Interoperability**

  Being in a low maturity level of development DPV is being developed under the guidelines proposed by W3C. Consequently, DPV is still not a standard nor is it in the W3C standards track, and it is not a European Standard.

- **Organisational interoperability**

  DPV defines a broad notion of semantics for providing a conceptual model of concepts and relationships between them. DPV can facilitate the modelling of personal data categories, and also provides a data model of concepts that act as a vocabulary for the interoperable representation and exchange of information about personal data and its processing. From this point of view, DPV is a good enabler for the modelling of business concepts.

  DPV also provides a data model of concepts that act as a vocabulary for the interoperable representation and exchange of information about personal data and its processing. It can help to facilitate interoperability agreements when it comes to applying privacy-friendly policies, as it represents concepts associated with privacy and data protection, primarily derived from GDPR.

- **Semantic Interoperability**

  As the SPECIAL project example shows, DPV is encouraging the creation of communities in European Platforms through the DPV Community Group where knowledge and data are shared to contribute to the regulation of data privacy. DPV can also be found in the GitHub repository, where any interested individual can participate in its development and raise issues about its implementation.

3. Assessment Results

This section presents an overview of the results of the CAMSS assessments for **DPV**. The CAMSS "Strength" indicator measures the reliability of the assessment by calculating the number of answered (applicable) criteria. On the other hand, the number of favourable answers and the number of unfavourable ones are used to calculate the "Automated Score" per category and an "Overall Score".

Category	Automated Score	Assessment Strength	Compliance Level
Principle setting the context for EU actions on interoperability	20/100 (20%)	100%	Ad-hoc
Core interoperability principles	1540/1700 (91%)	100%	Seamless
Principles related to generic user needs and expectations	1200/1200 (100%)	58%	Seamless
Foundation principles for cooperation among public administrations	500/500 (100%)	80%	Seamless
Interoperability layers*	660/1000 (66%)	100%	Sustainable
Overall Score	3320/3900 (85%)[9]	87%	

**The technical interoperability layer is covered by the criteria corresponding to the core interoperability principle ''Openness''.*

With a 87% of assessment strength, this assessment can be considered representative of the specification compliance with the EIF principles and recommendations.

The Overall Automated Score of 85% (3320/3900) demonstrates that the specification supports the European Interoperability Framework in the domains where it applies.

[9] See the "results interpretation" section of the CAMSS Assessment EIF Scenario Quick User Guide: https://joinup.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-eif-scenario/results-visualisation-and-interpretation