European Commission

Study on Interoperability of data processing services

Final report

Written by: Peter Kroon, Mark Reeve, Cédric Lebon, Ilsa Godlovitch

Repository development: Jan Droege, Dimitra Vasilia, Davide Casarin

November 2025

WIK CONSULT DECISION ETUDES & CONSEIL SCHUMAN ASSOCIATES

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate E — Future Networks
Unit E.2 — Cloud and Software

Contact: Leire Orue-Echevarria

E-mail: CNECT-E2@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Study on Interoperability of data processing services

Final report

Directorate-General for Communications Networks, Content and Technology

2025

Manuscript completed in November 2025

This document has been prepared for the European Commission however it reflects the views only of the authors, and the European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2025

PDF ISBN 978-92-68-33847-6 doi:10.2759/4466080 KK-01-25-154-EN-N

Abstract

The Data Act seeks to address barriers to cloud switching and supports interoperability. In this context, the Data Act envisages the establishment of a repository for the publication of harmonised standards and open interoperability specifications.

WIK Consult, Decision Etudes & Conseil and Schuman Associates were tasked with assisting the Commission in establishing this repository and preparing for the publication of references therein, in particular by elaborating processes and criteria to identify potential standards and specifications which could meet the requirements laid down in the Data Act.

The study contains a first screening of possible candidates that could be considered for inclusion in the repository as well as identifying areas for which new standards development or approval could be considered due to gaps in the availability of compliant standards and specifications. The study team also developed specifications for the online platform on the Europa server, the Digital Strategy website section. This online repository will include approved standards and specifications for interoperability of data processing services, which thereafter become mandatory for providers of data processing services.

Résumé

Le règlement sur les données (« Data Act ») vise à lever les obstacles au changement de services de traitement de données et à améliorer l'interopérabilité. Dans ce contexte, le Data Act prévoit la création d’un répertoire destiné à la publication des normes harmonisées ou des spécifications ouvertes d’interopérabilité.

WIK Consult, DECISION Études & Conseil et Schuman Associates ont été mandatés pour aider la Commission à créer ce répertoire et à préparer la publication des références qui y figureront, notamment en élaborant des processus et des critères permettant d'identifier les normes et spécifications susceptibles de répondre aux exigences fixées par le Data Act.

L'étude propose une première analyse des candidats potentiels pouvant être pris en considération pour inclusion dans le répertoire, ainsi que l’identification des domaines pour lesquels l’élaboration ou l’approbation de nouvelles normes pourrait être envisagée en raison de lacunes dans la disponibilité de standards et de spécifications adaptés. L'équipe d'étude a également conçu les caractéristiques techniques de la plateforme en ligne hébergée sur les serveurs Europa, dans la section « Digital Strategy ». Ce répertoire en ligne rassemblera les normes et spécifications approuvées pour l'interopérabilité des services de traitement des données, qui deviendront obligatoires pour les prestataires concernés une fois publiées.

Contents

Figures

Tables

Abbreviations

Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data (the Data Act)

Platform as a Service (PaaS)

Software as a Service (SaaS)

WIK-Consult (WIK)

Cloud Service Provider (CSP)

Cloud Service Customer (CSC)

Information and Communication Technology (ICT)

Standard Developing Organisation (SDO)

European Standard Developing Organisation (ESO)

Regulation (EU) 1025/2012, (the ‘Standardisation Directive’)

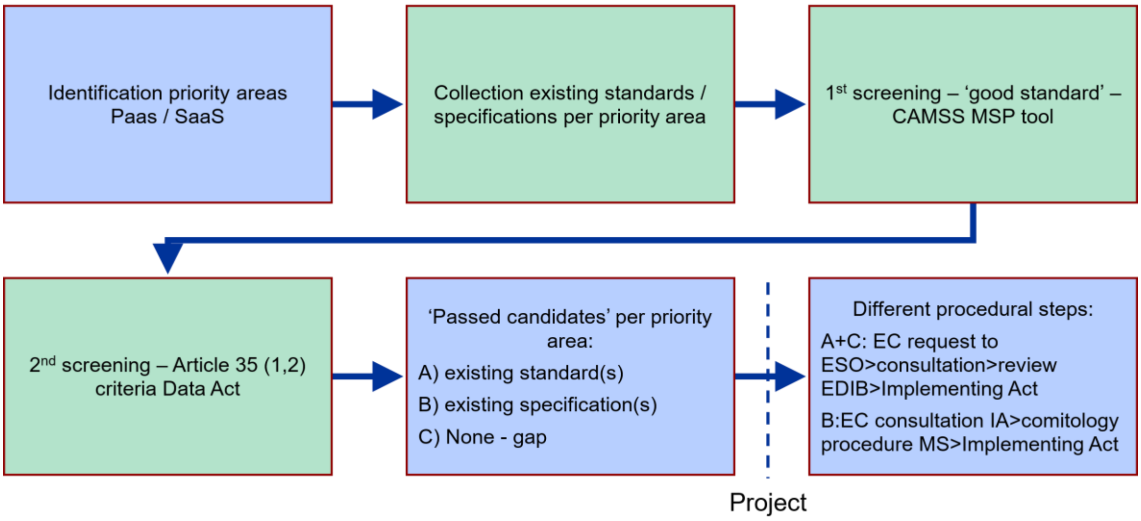
Regulation (EU) No 182/2011 (the ‘comitology regulation’).

1. Executive summary

The Data Act seeks to address barriers to cloud switching and supports interoperability. In this context, the Data Act envisages the establishment of a repository for the publication of harmonised standards and open interoperability specifications (following procedures described in Article 35). Article 30 of the Data Act further requires that providers of Platform as a Service (PaaS) and Software as a Service (SaaS) cloud services must ensure compatibility with the standards and specifications referenced in the repository.

The aim of the study is first to assist the Commission in operationalising the requirements on standards and specifications in regard to interoperability from the Data Act, Article 35(1) and (2). Secondly to support the establishment of the online repository and thirdly to prepare for the publication of references therein, in particular by identifying existing harmonised standards and open interoperability specifications that meet the requirements laid down in the Data Act. The study also seeks to identify areas for which new standards development or approval could be considered due to gaps in the availability of compliant standards and specifications.

The procedures that were followed to identify potentially relevant candidates for the repository are shown in the following diagram.


Identification priority areas Paas / SaaS
Collection existing standards / specifications per priority area
1st screening – 'good standard' – CAMSS MSP tool
2nd screening – Article 35 (1,2) criteria Data Act
'Passed candidates' per priority area:
A) existing standard(s)
B) existing specification(s)
C) None - gap
Different procedural steps:
A+C: EC request to ESO>consultation>review EDIB>Implementing Act
B:EC consultation IA>comitology procedure MS>Implementing Act
Project

Source: WIK-Consult.

ESO = EU Standardisation Organisation, EDIB = EU Data Innovation Board, IA = Implementing Act.

Firstly, priority areas were identified with reference to stakeholder feedback and market data. Subsequently, the study team collected existing standards and open interoperability specifications in the areas identified.

Thereafter, the study team developed a structured set of criteria reflecting the technical and functional obligations of Article 35(1) and (2), grouped under five main categories: portability of digital assets, interoperability between data processing services, no adverse impact on security and integrity, not hindering innovation, and functional equivalence. As the Data Act also refers to criteria of Annex II to Regulation (EU) No 1025/2012 on European standardisation, collected standards and specifications were subject firstly to screening based on criteria established in the context of CAMSS ([1]). Those passing this assessment were subject to a complete screening against the other criteria established in Article 35 of the Data Act based on a typology and evaluation system developed by experts from DECISION and WIK-Consult. This process enabled the identification of a first set of candidates which could potentially be considered for inclusion in the Data Act repository.

The study team then highlighted potential gaps where there could be a case to develop additional harmonised standards by European standardisation bodies. As not all gathered standards and specifications could be fully assessed during the period of the project, the study team also highlighted potential candidates that could be subject to a full evaluation and advised on a future process that could be followed to identify candidate standards and specifications for inclusion in the repository at a later stage.

The process involved a number of steps where stakeholders' input was invited. This included exploratory interviews, an online stakeholder survey and a workshop conducted on 20 March 2025. Following this process, and as a result of stakeholder feedback, priority was given to identifying and screening generic (rather than sector-specific) standards, and to focus on PaaS rather than SaaS cloud services, which were considered more case specific where standardisation is more likely to raise concerns around innovation.

The following open specifications were recommended for inclusion in the repository:

- As there is no technical overlap, both the generic **Open API** specification and **SECA** specification can be made mandatory.
- The **OCI** and **Oasis TOSCA** specifications relate to different aspects of container orchestration & Kubernetes; OCI on containerization and TOSCA on the topology and orchestration. Hence both can be included in the repository.
- **XML** and **JSON** could be candidates for inclusion. However, due to certain overlaps between them, further consideration is needed as to whether both can be made mandatory. In this context, it is also relevant to note that

([1]) CAMSS refers to the Common Assessment Method for Standards and Specifications. https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss preferences for one or the other differ as regards vertical industry segments.

- **SQL** could potentially be included, but should be further investigated as there are multiple versions of SQL (many CSPs and new database management systems have extended the SQL language and created new versions) and it is not clear what the impact would be of mandating one version.

As regards candidates for further screening or for new standards development, the study team concluded that:

- The remaining 11 candidates identified which were not subject to a full screening during the project, should be subject to a full screening. Particular attention should be given to the Oauth standard and the OIDC open specification, which are the de facto standards for delegated authentication and the SAML standard, which is widely used for federated sign-on.
- European SDO’s could investigate the possible development of a harmonized European standard for federated and delegated identity and access management as it is foundational to all Data Act provisions (it is a pre-requisite for secure interoperability). It would be built on top of the OIDC, OAuth and SAML open specifications. This would require:
  - Performing a second stage of screening of the IAM open specifications to ensure they meet the Data Act requirements;
  - Developing a standard for IAM portability and federation across Data Spaces, covering mechanisms for cross-trust domain identity exchange, policy enforcement, and credential portability;
  - Defining common European metadata and ontology models for IAM, supporting semantic interoperability and cross domain discoverability of identities, roles and access policies; and
  - Defining interoperability profiles and conformance testing procedures in order to ensure interoperability between sovereign and hyperscale cloud environments.

The conclusions of the study provide an input which could inform decisions made by the European Commission to issue a draft Implementing Act listing standards and specifications which should be included in the Data Act Repository, to pursue further screening to assess Data Act Article 35 conformity and/or potentially to instruct European SDOs to develop harmonised European standards.

In parallel to the identification of potential candidates for inclusion in the repository, Schuman Associates developed specifications for the online platform on the Europa server, the Digital Strategy website section. This section will host the repository, once relevant standards and specifications have been approved for inclusion. Schuman Associates worked closely with the European Commission to develop the look and the feel of this section of the website. Given the need for future growth and expansion of the data set it was designed in such a way to allow the Commission to add and expand on the screened standards in the future.

2. Introduction and methodology

2.1. Context of the study

The Data Act [2] aims to tackle barriers to cloud switching and multi-cloud usage. One of these barriers is a lack of interoperability between cloud service providers (CSPs) and/or on-premises Information and communication technology (ICT) infrastructure.

In order to address this concern, Article 30(3) Data Act requires providers of data processing services offering PaaS and SaaS to ensure compatibility with **harmonised standards and common specifications** based on open interoperability specifications that have been published in a central Union repository. In accordance with Article 35(8) Data Act, they are required to ensure compatibility within 12 months after the publication of such standards and specifications in the repository.

The repository will be available online [3] and will contain “harmonised standards” and “common specifications”. See Annex 8 for the graphical lay-out of the online repository.

Harmonised standards as referred to in the Data Act are either drafted in response to a request from the Commission by European standardisation organisations (SDOs) or created via the inclusion of an existing harmonized standard in the online repository after it has been established that it complies with all criteria in the Data Act. [4]

On the other hand, “common specifications” as referred to in the Data Act are existing open interoperability specifications which will have to be adopted through an Implementing Act converting them into common specifications and later on, adopted for the inclusion in the repository via another Implementing Act [5]. Open interoperability specifications do not require a formal standardisation process

[2] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act).

[3] The repository will be hosted on europa.eu.

[4] A ‘harmonised standard’ is defined in Regulation (EU) No 1025/2012: A European standard developed by a recognised European Standards Organisation like CEN, CENELEC, or ETSI following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies use these harmonised standards to demonstrate that their products, services, or processes comply with relevant EU legislation.

[5] See Data Act, Article 2(41 and 42). Open interoperability specifications are technical specifications in the field of ICT which are performance-oriented towards achieving interoperability between data processing services. See also Recital 100, which describes the 2 step approach.

(like standards) and can be the outcome of informal agreements between industry groups, for example on data formats to use when exchanging between different services of the same type. However, in order for such a specification to be included in the central Union's repository, it would need to go through a screening procedure to ensure compliance with the requirements listed in the Data Act.

2.2. Objectives and methodology

The main purpose of the study is to operationalise the criteria specified in the Data Act and put in place the central Union standards repository for the interoperability of data processing services. The study also highlights standards and specifications for future evaluation and assesses whether there are areas for which new standards development or approval could be considered due to gaps in the availability of compliant standards and specifications.

The steps taken by the study team are listed below:

- First, we reviewed the relevant articles of the Data Act to understand the relationship between the Articles and the formal requirements.
- Drawing on this analysis, we outlined the formal procedural steps that could be taken in order to identify candidate standards or specifications for the inclusion in the online repository. In elaborating these procedures, the study also reviewed the validation processes used by standards development organisations (SDOs) to understand if these could be (partially) used as a baseline for the envisaged Data Act process.
- Thereafter, we elaborated on the criteria needed to demonstrate compliance with the Data Act requirements. In doing so, we have drawn on explanations in recitals in the regulation, literature, and existing compliance checklists.
- The resulting criteria were tested by using them for the screening of the first batch of standards and specifications, identified through desk research or suggested by stakeholders in the context of interviews and the online survey conducted for this study.
- Finally, by following the identified selection procedure, we determined a number of provisional candidates for inclusion in the repository, as well as highlighting standards / specifications which should be screened in a second phase, and gaps, that is, priority areas in which no compliant standards or specifications were identified and for which initiatives to develop new standards could be considered.

- The criteria and processes pursued as well as the identified candidates for inclusion in the repository and possible areas for new standards initiatives were presented in an online workshop held on 20 March 2025. Stakeholders were requested to provide input via an online polling tool. - +The results of this exercise were used to confirm or amend the proposed approach as well as to validate whether the selected candidate standards and open specifications were appropriate.

In parallel with the elaboration of criteria and screening of standards and specifications, the study team developed the structure for the online platform which will serve as the Repository of harmonised standards and open interoperability specifications that are considered compliant and approved for inclusion in the Repository in accordance with the Data Act.

2.3. Structure

The study is structured as follows:

- Chapter 2 describes how we operationalised the criteria set out in Article 35 of the Data Act to provide a framework under which standards and specifications could be evaluated to assess their compliance with the conditions established for inclusion in the Repository
- Chapter 3 discusses the processes that were used in the study to prioritise amongst candidate standards and thereafter to evaluate shortlisted candidates to assess which could be proposed for possible inclusion in the Repository. It also discusses how these processes could be adapted to allow the process to be repeated following the conclusion of this study.
- Based on the processes described above, Chapter 4 identifies priority areas based on PaaS and SaaS service types.
- Chapter 5 provides a mapping of identified standards and open specifications against the priority areas and provides the outcomes from the initial compliance assessment against the criteria described in chapter 2; and
- Chapter 6 provides recommendations for standards and specifications to be included in the repository as well as identifying gaps where new standards development could be considered.
    - The report includes a number of Annexes. These cover:
    - Annex 1 – Literature research regarding categories of cloud functions
    - Annex 2 – Proposed categories for PaaS/SaaS service types
    - Annex 3 – Online survey

- Annex 4 – Interview guidelines
- Annex 5 – Reviewed standardization processes of SDOs
- Annex 6 – Criteria and means of verification
- Annex 7 – Full list of gathered standards/ specification/ Tools/ other
- Annex 8 – Evaluation sheet – step 2 screening – Open API
- Annex 9 – Repository Mock-up
- Annex 10 – CAMSS MSP Reference
- Annex 11 – Least Applicable Criteria in the Second Screening

3. Criteria to evaluate standards and specifications for compliance with Article 35 of the Data Act

In this chapter, we provide an overview of the requirements that need to be met for inclusion in the Repository of harmonized standards and open interoperability specifications under the Data Act. We then elaborate on the criteria referred to in Article 35 (1,2) Data Act as well as Annex II of Regulation (EU) No 1025/2012 on European standardization with a view to describing how they could be operationalised for the purposes of evaluating possible candidates for inclusion in the Repository.

3.1. Legal requirements from the Data Act

The provisions in the Data Act which relate to standards and specifications for cloud interoperability are articles 23, 30, 34 and 35. In addition, Regulation (EU) 1025/2012 (Standardisation Directive), Annex II, is referenced in Article 35(3) of the Data Act.

Article 23 notes that the aim of the obligations is to remove obstacles for an effective switching between data processing service providers covering the same service type or using several CSPs at the same time.

Article 30 describes the technical aspects of switching, distinguishing between data processing services providing scalable and elastic computing resources limited to **infrastructural** elements such as servers, networks and the virtual resources necessary for operating the infrastructure and 'all other data processing services', which provide access to the **operating services, software and applications**.

The obligations on data processing service providers are then split based on this distinction:

- Related to **infrastructure** elements: obligation to facilitate that the customer, after switching to a data processing service covering the same service type, achieves functional equivalence in the use of the destination data processing service (Article 30(1)).
- Related to Operating Systems **(OS), software and applications:**
  - Obligation to make open interfaces available to an equal extent to all customers and concerned destination providers of data processing services, free of charge, to facilitate data portability and interoperability (and hence switching, Article 30(2)).
  - Obligation to ensure compatibility with common open interoperability specifications or harmonised standards for

interoperability as published in a central standards repository at least 12 months after these are published by the EU Commission (Article 30(3)).

- Obligation to update the online register hosted by the data processing service provider specifying details on data structures, data formats, relevant standards and open interoperability specification (Article 30(4) and 26(b))
- Obligation to export all exportable data, at the request of the cloud customer, in a structured, commonly used and machine-readable format in case there is switching between data processing services of the same type, and no common specifications and standards have been published (Article 30 (5)).

Article 34 complements Article 30 by stating that the above obligations should not only enable customers to switch from one data processing service provider to another but also to be able to use them in-parallel in a so-called multi-cloud set-up (see also Recital 99).

Article 35 (1) then defines the specific requirements for the common specifications and harmonised standards (in the repository) for the purpose of enabling interoperability of data processing services in relation to OS, software and applications (or in other words at the PaaS, SaaS level). These are to:

- 1 a) achieve, where technically feasible, interoperability between different data processing services that cover the same service type;
- 1 b) enhance portability of digital assets between different data processing services that cover the same service type;
- 1 d) not have an adverse impact on the security and integrity of data processing services and data;
- 1 e) be designed in such a way so as to allow for technical advances and the inclusion of new functions and innovation in data processing services.

Article 35 (2) further notes that open interoperability specifications and harmonised standards shall adequately address:

- (a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability;
- (b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;
- (c) the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

In addition, the following clarifications are provided in recitals:

- Recital 100 states that these harmonised standards and common specifications should consider the needs of Small Medium Enterprises (SME).
- Recital 103 clarifies that common specifications should only be adopted as fall-back solution to facilitate compliance with the requirements in Article 35 (1,2) when the standardisation process is blocked or delayed. However, the function and role of standardisation bodies should be respected. Furthermore, it states that common specifications can be sector specific as *'…common specifications in different sectors could be adopted…on the basis of specific needs of those sectors.'*
- Recital 98 explains that those data processing services for which the majority of functions is custom-built to respond to specific customer needs are not covered under these (interoperability) obligations. However, if the data processing services provider decides to deploy these specific functions at scale, then the (interoperability) obligations do apply.

Article 35 (3) of the Data Act also requires open interoperability specifications to comply with Annex II of Regulation 1025/2012 ([6]) (Standardisation Regulation). This Annex describes the requirements of technical specifications in the field of ICT in general.

Article 35 (4 to 8) lastly describes the process whereby existing standards and/or open interoperability specifications can be formalized into harmonised standards and common specifications and after publication in the central Union repository become obligatory to comply with within 12 months.

Hence the obligation to comply with the harmonised standards and common specifications on interoperability included in the central repository applies for data processing services regarding OS, software and applications and for the same service type.

3.2. Proposed taxonomy of cloud functions to enable testing criteria for the 'same service type'

As described above, the obligations in Article 35 (1a, 1b) on enabling interoperability of data processing services and portability of digital assets for PaaS and SaaS apply for the same service type. Article 2, Data Act defines same service type as '...sharing the same primary objective, data processing service

[6] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

model and main functionalities.'. As the scope of the interoperability obligations in this study is mainly restricted to PaaS and SaaS, we sought to identify literature which classified cloud functions delivered over the PaaS and SaaS service model with a view to developing a taxonomy against which to categorise the service types addressed.

Literature was researched with publication date from 2009 onwards until 2024 using Google search / Google Scholar and search criteria 'taxonomy for PaaS/SaaS categories' and 'functional categories for PaaS / SaaS cloud services'. The resulting list of relevant publications on identified categories of cloud functions/features was reviewed. More details on the literature are provided in Annex 1. This includes a detailed mapping of cloud services from leading vendors, which could be used for future reviews of service types or when assessing whether cloud services from different providers belong to 'the same service type'.

The identified categories of cloud functions/features were compared to assess which list provides the most comprehensive overview and to verify if certain categories were missing or named differently. Discrepancies were then reviewed internally by technical experts in the Team. Lastly, a more aggregated list was established to define the 'service types' for PaaS/SaaS cloud services as applied in the Data Act. The resulting Table 2-1 below is proposed to be used to determine whether interoperability and portability of digital assets obligations for harmonised standards and common specifications relate to the 'same service type', as applied by the Data Act. See Annex 2 for this list including descriptions for the groupings from the literature.

Table 1 – Proposed list of 'service types' to verify the scope of certain obligations from the Data Act.

Cloud Tier	Service Type	Group
PaaS	Machine Learning Platforms	AI & Machine Learning
PaaS	AI Development Tools	AI & Machine Learning
PaaS	Pre-trained AI Services	AI & Machine Learning
PaaS	Data Labelling & Training	AI & Machine Learning
PaaS	Analytics & Big Data	Analytics & Big Data
PaaS	Data Lakes	Analytics & Big Data
PaaS	Big Data Processing	Analytics & Big Data
PaaS	Real-time Analytics	Analytics & Big Data
PaaS	Data Warehousing	Analytics & Big Data
PaaS	Blockchain Platforms	Blockchain
PaaS	Smart Contract Development	Blockchain
PaaS	Blockchain Networking	Blockchain
PaaS	Cryptography Services	Blockchain
SaaS	Customer Relationship Management (CRM)	Business Applications

Cloud Tier	Service Type	Group
SaaS	Enterprise Resource Planning (ERP)	Business Applications
SaaS	Human Capital Management (HCM)	Business Applications
SaaS	Supply Chain Management	Business Applications
PaaS	Containers & Kubernetes	Compute
PaaS	Serverless Functions	Compute
IaaS	Batch & High-Performance Computing	Compute
IaaS	File Systems	Data Storage
PaaS	Relational Databases	Databases
PaaS	NoSQL Databases	Databases
PaaS	In-memory Databases	Databases
PaaS	Database Migration Services	Databases
PaaS	Integrated Development Environments (IDE)	Developer Tools
PaaS	Continuous Integration & Deployment (CI/CD)	Developer Tools
Transversal	Source Control	Developer Tools
Transversal	Observability & Logging Tools	Developer Tools
Transversal	Application deployment	Developer Tools
Transversal	App Development Platforms	Developer Tools
PaaS	Service Integration	Enterprise Integration
PaaS	API Management	Enterprise Integration
PaaS	Enterprise Messaging	Enterprise Integration
PaaS	Business Process Automation	Enterprise Integration
PaaS	Web Hosting & Web App Services	Front-end Web & Mobile
PaaS	Content Management Systems	Front-end Web & Mobile
PaaS	Mobile App Services & Frameworks	Front-end Web & Mobile
PaaS	Web Security	Front-end Web & Mobile
PaaS	Progressive Web Apps	Front-end Web & Mobile
PaaS	Front-end Frameworks & Libraries	Front-end Web & Mobile
Transversal	Mobile Backend-as-a-Service (MBaaS)	Front-end Web & Mobile
Transversal	Mobile Analytics	Front-end Web & Mobile
Transversal	User Engagement Tools	Front-end Web & Mobile
PaaS	Game Development Platforms	Gaming
PaaS	Multiplayer Servers	Gaming
PaaS	Real-time Game Analytics	Gaming
PaaS	Game Asset Management	Gaming
PaaS	IoT Device Management	Internet of Things
PaaS	IoT Data Analysis	Internet of Things
PaaS	Edge Computing	Internet of Things
PaaS	IoT security	Internet of Things
Transversal	Systems administration	Management & Governance
Transversal	Data Storage	Management & Governance

Cloud Tier	Service Type	Group
Transversal	Infrastructure Automation	Management & Governance
Transversal	Cost Management	Management & Governance
Transversal	Resource Organization	Management & Governance
Transversal	Governance & Compliance Tools	Management & Governance
Transversal	Migration Tools	Migration & Hybrid Cloud
Transversal	Hybrid Cloud Platforms	Migration & Hybrid Cloud
Transversal	Disaster Recovery	Migration & Hybrid Cloud
SaaS	Hybrid Recovery	Migration & Hybrid Cloud
Iaas	Media Conversion & Encoding	Multimedia Services
Iaas	Media Storage & Delivery	Multimedia Services
Iaas	Interactive Media Services	Multimedia Services
Iaas	Media Analytics	Multimedia Services
SaaS	Robotic Process Automation (RPA)	Robotics
SaaS	Robotics Management	Robotics
SaaS	Robotic Development Kits	Robotics
SaaS	Robot Telemetry & Analytics	Robotics
Transversal	Data Protection	Security & Identity
Transversal	Identity & Access Management (IAM)	Security & Identity
Transversal	Threat Detection	Security & Identity
Transversal	Compliance Management	Security & Identity
Transversal	Cloud Security Posture Management	Security & Identity
PaaS	Serverless Functions & Events	Serverless
PaaS	VR/AR Development Platforms	VR / AR
Transversal	VR/AR Content Creation & Management	VR / AR
Transversal	VR/AR Hardware & Device Support	VR / AR
Transversal	Mixed Reality Services	VR / AR
Transversal	Spatial Computing & Environmental Understanding	VR / AR
SaaS	Collaboration & Productivity	Workplace solutions
SaaS	Endpoint Security	Workplace solutions
IaaS	Virtual Desktops	Workplace solutions
IaaS	Remote App Streaming	Workplace solutions

3.3. Operationalisation of the criteria to assess compliance with Article 35 of the Data Act

The next step was to operationalize the criteria derived from Article 35(1), (2), and (3) of the Data Act, the latter referencing Annex II of Regulation (EU) No 1025/2012. These criteria serve as the basis for screening both existing standards and specifications, as well as newly drafted harmonised standards on interoperability, to assess their suitability for inclusion in the Union's central repository.

To ensure a structured and effective screening process, we categorized the criteria into two groups:

- **Governance and Coherence Criteria** (Article 35(3), referring to Annex II of Regulation 1025/2012): These criteria assess whether a standard or specification meets fundamental quality and governance requirements, such as openness, transparency, and procedural robustness, represented by points 2 and 3 of Annex II of Regulation 1025/2012. This serves as the first screening phase.
- **Operational Compliance Criteria** (Article 35(1) and (2)): These criteria assess compliance with interoperability and portability requirements, including the facilitation of digital asset portability across data processing services of the same service type, ensuring security and data integrity, and enabling technological innovation.

The process pursued for assessing candidate standards and specifications against the requirements of the Data Act is fully described in section 4. However, for the purposes of explaining how the criteria were identified and structured, it is relevant to note that we adopted a two-step approach to assess the compliance of standards and specifications with the requirements of Article 35 of the Data Act. This methodological choice was made for reasons of efficiency. First, given the significant number of candidate standards and open specifications gathered (more than 100), and the large number of criteria involved in the full evaluation, it was necessary to introduce an initial filtering step. The purpose of this first screening is to quickly eliminate non-relevant or non-compliant standards based on high-level coherence and governance criteria, derived from Annex II (Articles 2 and 3) of Regulation (EU) No 1025/2012.

Only the standards that pass this first screening proceed to the second phase—referred above as the Operational Compliance Criteria. This second phase is a more in-depth assessment that evaluates compliance with Article 35(1) and (2) of the Data Act. It also integrates the remaining CAMSS MSP ([7]) criteria not covered in the first screening—particularly those related to market acceptance and requirement, in line with the structure of the CAMSS MSP methodology. The core of this second phase is based on a structured set of operationalised criteria, which were developed to translate the legal obligations of the Data Act into verifiable dimensions of compliance.

[7] CAMSS is the common assessment method for standards and specifications by the European Commission in the context of interoperability issues and solutions for European public services. The multi-stakeholder platform (MSP) provides guidance to public administrations to assess among others the compliance of interoperability specifications. See also https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-multi-stakeholder-platform-msp-scenario/camss-assessment-msp-scenario-quick-user-guide

3.3.1. CAMSS MSP Criteria

We based our approach on CAMSS Assessment MSP Scenario Methodology v4.0.0 (See Annex 10 for detailed CAMSS criteria)

In the context of this study, we reviewed the full CAMSS MSP criteria set to identify those most relevant for assessing standards and open specifications under Article 35 of the Data Act.

The use of the CAMSS tool was explicitly foreseen in the Terms of Reference for the study, and the methodology has already been applied and validated in previous European Commission work. Moreover, CAMSS criteria directly map to the requirements of Annex II of Regulation (EU) No 1025/2012, which forms the legal basis for assessing the governance and procedural quality of ICT standards or specifications under Article 35(3) of the Data Act. It is a structured and widely recognised framework and therefore provided a reliable and coherent starting point for our assessment.

However, not all CAMSS criteria were used. Certain criteria were considered out of scope for this specific study, as they go beyond the legal requirements of Annex II of Regulation (EU) No 1025/2012. The criteria that were left out for this study are as follows:

- There are public references (especially policies or in procurement) of the respective specification made by public authorities.
- Does the specification address and facilitate interoperability between public administrations?
- Is there evidence that the adoption of the specification positively impacts one or several of the following: organisational processes, the environment, the administrative burden, the disability support, cross-border services, public policy objectives, societal needs?
- Is the specification largely independent of specific platforms or technologies?

3.3.2. First Screening – Based on Extracted Criteria from CAMSS MSP

The first screening phase applies a preliminary filter designed to quickly eliminate non-relevant standards and specifications from the list of candidates.

This pre-screening step relies on a subset of criteria extracted from the CAMSS MSP assessment. These criteria focus primarily on the governance and development process of standards, as well as their coherence with existing and future European standardisation efforts.

The objective is to ensure that only standards meeting minimum quality and transparency requirements proceed to the more comprehensive evaluation phase. This approach enables the study team to concentrate efforts on standards with sufficient maturity and procedural credibility.

The following CAMSS MSP criteria were selected for use in this first screening phase:

Table 2 – Re-use of Art 2 and 3 questions from CAMSS MSP Scenario to assess partially Annex II of Regulation 1025/2012 for step 1 screening

Criterion Categories	Questions [8]
Coherence with existing and future European standards	Does the technical specification or standard cover areas different from areas addressed by technical specifications being under consideration to become a European standard?
	Is the adoption of new European Standards which cover the same areas as the proposed specification (or standard) foreseen within a reasonable timeframe?
	Are there existing European standards with market uptake which cover the same areas as the proposed specification (or standard) being assessed?
	If yes, are the existing standards becoming obsolete? (optional)
Governance & development process	Is the Standards Developing Organisation a non-profit organisation?
	Is participation in the creation process of the specification open to all interested parties (e.g. organisations, companies, and individuals)?
	Are the specifications approved in a decision-making process which aims to reach consensus?
	Is relevant documentation of the development and approval process of the specification archived and identified?
	Is information on (new) standardisation activities widely announced through suitable and accessible means?
	All relevant stakeholders can formally appeal or raise objections to the development and approval of specifications?
Maintenance, availability & intellectual property	Does the specification have a defined maintenance and support process?
	Is the specification publicly available for implementation and use on reasonable terms?
	Is the specification licensed on a (F)RAND basis?
	Is the specification licensed on a royalty-free basis?

In line with the CAMSS MSP methodology, each criterion is scored individually based on the responses provided for the specification being assessed:

+1: The specification is compliant with the criterion ("Yes")

–1: The specification is not compliant with the criterion ("No")

0: The criterion is not applicable or insufficient information is available ("Not applicable" or "Not answered")

[8] CAMSS MSP.

The “Not applicable” option is used only in cases where the criterion is clearly outside the scope of the specification or cannot be meaningfully assessed due to lack of information.

For each category, the total score corresponds to the sum of individual criterion scores, and the compliance level per section is determined using a conversion table (see MSP Scenario Compliance Level Conversion Table below).

Table 3 – MSP Scenario Compliance Level Conversion Table

	Compliance Level			
Section	1	2	3	4
Market acceptance	-2 to -3	-1 to 0	1 to 2	3
Coherence Principle	-4 to -2	-1 to 0	1 to 2	3 to 4
Attributes	-6 to -4	-3 to 0	1 to 3	4 to 6
Requirements	-9 to -6	-5 to -1	0 to 4	5 to 9

Source: CAMSS Assessment Multi-Stakeholder Platform (MSP) Scenario.

The original CAMSS MSP conversion table was designed for a much larger number of criteria than those retained for this study. To ensure coherence, an amended version of the table has been developed for this study, recalibrating the compliance thresholds according to the actual number of questions per category:

- Coherence: 3 criteria (maximum score = 3)
- Attributes (Governance): 6 criteria (maximum score = 6)
- Requirements (Maintenance, Availability & Intellectual Property): 4 criteria (maximum score = 4)

Only the standards and open specifications reaching the maximum compliance to Annex II of Regulation (EU) No 1025/2012 are eligible to proceed to the second screening phase. Therefore, the assessment focuses on those achieving Level 4 compliance, ensuring that only items demonstrating full alignment with governance, coherence, and maintenance requirements advance to the operational compliance assessment under the Data Act.

To reach Level 4 in each category, the following minimum scores are required:

- Coherence: compliance with all 3 criteria
- Attributes (Governance): compliance with at least 4 of 6 criteria
- Requirements (Maintenance, Availability & Intellectual Property): compliance with at least 3 of 4 criteria

The table below presents the amended compliance scale used in this study. Only standards and open specifications achieving Level 4 in all three categories proceed to the second screening phase, which focuses on operational compliance with the Data Act.

Table 4 – Amended CAMSS compliance level for the step 1 (Annex II) compliance check – based on the reduced number of criteria

Step 1	Compliance Level				
Section	**1**	**2**	**3**	**4**	
Market acceptance	not applicable				
Coherence Principle	-3 to -2	-1 to 0	1 to 2	3	minimum score: 3
Attributes	-6 to -4	-3 to 0	1 to 3	4 to 6	minimum score: 4
Requirements	-4 to -2	-1 to 0	1 to 2	3 to 4	minimum score: 3

Source: DECISION Études & Conseil, WIK-Consult, CAMSS Assessment Multi-Stakeholder Platform (MSP) Scenario.

3.3.3. Second Screening – Based on Operationalised Requirements of the Data Act and Remaining CAMSS MSP Criteria

Standards and specifications that pass the first screening are then subject to a second, more detailed assessment, referred to as the Operational Compliance Criteria phase. This phase is composed of two complementary components:

1. Remaining CAMSS MSP Criteria (Relevant to Article 35(3) of the Data Act)

To complete the assessment of compliance with Article 35(3), this phase includes the remaining CAMSS MSP criteria not covered in the first screening. These additional criteria relate primarily to market acceptance and quality alignment and serve to complete the evaluation framework established by Annex II of Regulation (EU) No 1025/2012.

The CAMSS criteria used in this phase are presented in the following table:

Table 5 – Re-use of Art 1 and 4 questions from CAMSS MSP Scenario to assess remaining aspects of Annex II of Regulation 1025/2012

Criterion Categories	Questions
Market Acceptance	The technical specification or standard has been used for different implementations by different vendors/suppliers.
	The implementation of the technical specification or standard does not hamper interoperability with implementations that are currently based on existing European or international standards.
Quality	Has the specification sufficient detail, consistency, and completeness for the use and development of products and services?

2. Operationalised Criteria Based on Article 35(1) and (2) of the Data Act

In parallel, the study team developed a set of operationalised criteria to assess compliance with the more technical and functional obligations outlined in Article 35(1) and (2) of the Data Act. Two sets of criteria were developed, one to assess standards and one to assess open specifications.

To translate these legal obligations into practical assessment tools, each requirement was broken down into the following thematic categories and subcategories:

Table 6 – Operationalisation of requirements from Article 35(1,2)

Criterion Categories	Criterion Sub Categories
Portability of digital assets	Semantic Interoperability
	Syntactic Interoperability
Interoperability between data processing services	Policy Interoperability
	Operational Interoperability
	Behavioural Interoperability
	Technical Interoperability
No adverse impact on security and integrity	System security and integrity
Not hindering innovation	Extensibility and Adaptability
	Openness and flexibility
Functional Equivalence	Consistent service-level behaviour

To determine whether a standard or open specification successfully passes the second screening phase, a structured weighting and scoring system was designed. Drawing on the CAMSS MSP methodology ([9]), this system ensures compliance with Article 35 of the Data Act by combining individual criterion scores, category-level thresholds, and an assessment strength indicator.

(i) Scoring system per criterion and category

Each criterion is scored as follows:

- 1 if the standard or specification is fully compliant
- 0.5 if partially compliant
- –1 if not compliant
- 0 if not applicable

[9] Especially on the section on result visualisation, scoring and interpretation: https://interoperable-europe.ec.europa.eu/collection/common-assessment-method-standards-and-specifications-camss/solution/camss-assessment-multi-stakeholder-platform-msp-scenario/results-visualisation-and-interpretation

Each category's compliance score is computed by dividing the sum of scores by the number of applicable criteria, according to the formula below:

$$Score_{Category} = \frac{\mathrm{Count}_{\mathrm{full\ compliance}} + Count_{partial\ compliance} + Count_{not\ compliant}}{Number\ of\ applicable\ criteria} * 100$$

A final score is also calculated across all categories using the same method, according to the formula below:

$$Final\ Score = \frac{\mathrm{Sum\ Score}_{\mathrm{Category}}}{Total\ Number\ of\ aaplicable\ criteria} * 100$$

(ii) Category thresholds based on legal obligations

To determine whether a standard or specification is compliant within a category, minimum thresholds were defined based on the legislative wording in Article 35(1). The analysis of wording used in the legal text reveals two distinct groups of obligations with different levels of strictness.

The first group covers the following categories:

- Article 35(1a) – Interoperability between data processing services
- Article 35(1b) – Portability of digital assets
- Article 35 (1c) – Functional equivalence

The obligations in these categories are expressed using wording such as "shall achieve… where technically feasible", "shall enhance", and "shall facilitate". This wording makes the requirements mandatory but allows some flexibility. The qualifier "where technically feasible" in both Article 35(1a and 1c) acknowledges that in certain cases, full compliance may not be possible due to inherent technical constraints. The wording "enhance" in Article 35(1b) requires measurable improvement in portability but does not imply that full portability must be achieved from the outset. Because these obligations allow for limited exceptions or progressive improvement, the minimum compliance threshold is set at 80%. This value was defined following a sensitivity analysis conducted on the assessed sample, which demonstrated that an 80% cut-off separates broadly applicable interoperability standards from narrower, implementation-specific technologies, such as SQL for instance.

The second group covers the following categories:

- Article 35(1d) – No adverse impact on the security and integrity
- Article 35(1e) – Not hindering innovation

The obligations in these categories are expressed without any qualifier that would allow partial compliance. In Article 35(1d), the wording "shall not have" establishes an unconditional prohibition. Any adverse impact on security or integrity is incompatible with the legislative intent and would disqualify the standard or specification. Similarly, Article 35(1e) uses the wording “shall be designed” without any conditional phrasing, making it a near-absolute requirement aimed at ensuring that standards and specifications remain future-proof and capable of incorporating innovation over time. Because these obligations are absolute in nature, the compliance threshold is set at 100%.

The remaining CAMSS MSP Criteria have a compliance threshold of 100% as well, considering the wording of Article 35(3).

If a standard or specification exceeds the threshold in a given category, it is considered fully compliant for that category. However, if it meets the threshold but is based on a low number of applicable criteria (below 50% coverage), it is considered only partially compliant. This distinction between full and partial compliance is intended to indicate the breadth of coverage of the standard or specification within the category. Items falling below the threshold are deemed not compliant, while those with no applicable criteria are marked as Not Applicable.

(iii) Applicability of criteria on the reviewed standard or specification

In addition to per-category compliance, an assessment strength score is calculated to reflect the extent to which a standard or open specification addresses the full range of interoperability criteria. This score is calculated as the ratio of applicable criteria to the total number of possible criteria. It serves as an indicator of the breadth of interoperability aspects covered by a given standard or open specification. A lower applicability score generally reflects that the specification is focused on a narrow or specific dimension of interoperability (e.g. syntactic interoperability only), while a higher score indicates that the specification addresses a broader range of interoperability requirements across multiple categories.

Annex 5 provides the means of verification used for each criterion in the assessment.

The full list of operationalised criteria is detailed below.

Criteria for Standards

Portability of digital assets

A standard must ensure that digital assets can be transferred and interpreted consistently across platforms by meeting the following criteria:

Semantic Interoperability

Define or support semantic models and structures that enable interoperability between heterogeneous systems.

Define principles, capabilities or framework requirements to provide specifications for data mappings or conversion methods between different formats

Define principles, capabilities or framework requirements to define metadata descriptors to ensure accurate data interpretation across different platforms and services

Define principles, capabilities or framework requirements to enforce the use of widely accepted vocabularies to improve data understanding

Syntactic Interoperability

Define principles, capabilities or framework requirements to define a common data model in order to ensure semantic consistency across services

Interoperability Between Data Processing Services

A standard must enable seamless interactions between different cloud providers and data processing services by fulfilling the following criteria:

Operational Interoperability

Define principles or reference models that enable synchronization of data and consistency management and integrity across multiple providers or systems

Facilitate workload portability by providing a common approach to describing and deploying workloads across cloud environments.

Provide framework requirements or set of principles to support secure and standardized data exchanges between interoperable systems.

Enable multi-provider and multi-cloud interoperability by supporting deployment across heterogeneous cloud platforms.

Policy Interoperability

Provide framework requirements for expressing and aligning policies such as access rights, consent, and usage conditions across systems or domains.

Behavioural Interoperability

Define reference interaction models or protocols that ensure consistent behaviour and service interaction across implementations

Technical Interoperability

Define principles, capabilities or framework requirements to specify schema validation mechanisms to guarantee data integrity

Support interoperability by referencing or relying on open and standardized network communication protocols.

Define principles, capabilities or framework requirements to define serialization and deserialization mechanisms to ensure data consistency across different services

Define principles, capabilities or framework requirements to enforce authentication mechanisms that are deployed at least on 2 different cloud provider platforms.

Define principles, capabilities or framework requirements to specify protocols and apis for secure and structured data transfer

Define principles, capabilities or framework requirements to mandate the use of machine-readable data formats in order to ensure seamless data exchange

No Adverse Impact on Security and Integrity

System security and integrity

A standard must not introduce security risks and must ensure data integrity:

Allow for the use of federated identity management approaches to enable secure authentication across cloud environments.

Define principles, capabilities or framework requirements to enforce mutual authentication for services.

Define requirements for secure and encrypted communication when accessing APIs, to ensure protection against unauthorized access and data tampering.

Not Hindering Innovation

Extensibility and Adaptability

A standard must support long-term evolution and adaptability:

Define principles, capabilities or framework requirements to allow incremental updates of data models in order to accommodate new use cases

Define extension mechanisms that enable third parties to augment or tailor its core functionality to specific needs.

Define principles, capabilities or framework requirements to support api versioning, modular extensions, and backward compatibility to allow continuous evolution

Define principles, capabilities or framework requirements to avoid restrictive dependencies that prevent flexible implementation and adaptation

Functional Equivalence (this category is optional as dedicated to IaaS)

Consistent Service-Level Behaviour

A standard must ensure that services function consistently across different environments:

Define principles, capabilities or framework requirements to require compatibility tests to ensure continuous service functionality

Define principles, capabilities, or framework requirements to enforce data integrity and support functional equivalence across services, ensuring that data remains consistent and unaltered during exchange, and that comparable services can perform equivalent operations reliably.

Criteria for Specifications

Portability of digital assets

A specification must ensure that digital assets can be transferred and interpreted consistently across platforms by meeting the following criteria:

Semantic Interoperability

Define mechanisms or interfaces for automating the translation or mapping of data between heterogeneous semantic models to enable interoperability.

Implement mechanisms or technologies such as structured mappings between formats

Incorporate mechanisms or technologies, such as the definition of metadata elements, to ensure that descriptive, technical, and access metadata are clearly specified.

Implement mechanisms or technologies such as Widely accepted vocabularies like DCAT-AP, Dublin Core, Schema.org, ISO 11179 or domain-specific ones are mandated

Make use of, or be compatible with, established vocabularies or ontologies to ensure semantic consistency across systems.

Syntactic Interoperability

Implement consistent data structures and use standardized serialization formats to ensure syntactic interoperability between systems.

Interoperability Between Data Processing Services

A specification must enable seamless interactions between different cloud providers and data processing services by fulfilling the following criteria:

Operational Interoperability

Support compatibility with open specifications that enable distributed identity management and federated access control (e.g., OAuth 2.0, OpenID Connect, DIDs).

Define mechanisms, protocols, or interfaces to synchronize data and maintain consistency across systems or cloud providers.

Define principles, capabilities or frameworks to support event-driven architectures to enable real-time interoperability

Define mechanisms for describing, transferring, and re-deploying workloads across cloud providers, including portable application descriptions or deployment artifacts that ensure compatibility and reusability

Define concrete protocols, data models, or interfaces that enable secure and interoperable data sharing between systems or organizations.

Define interfaces, models, or deployment descriptors that enable consistent deployment of applications across different cloud providers.

Policy Interoperability

Define mechanisms or formats for expressing and enforcing access, consent, or data usage policies in a machine-readable and interoperable manner.

Behavioural Interoperability

Define and document interface behaviours, workflows, and expected outcomes to ensure consistent interaction patterns across implementations.

Technical Interoperability

Implement mechanisms or technologies to verify data exchange rules, ensuring that APIs, databases, and file formats enforce data validation, integrity constraints, and conformance to defined schemas.

Define network communication using open and standardized protocols to ensure cross-system interoperability.

Define or use standardized serialization and deserialization formats to ensure consistent data exchange across services.

Implement authentication using widely adopted and open protocols

Implement mechanisms or technologies that allow for communication such as RESTful and Web-Based APIs

Define and use machine-readable data formats to enable automated and seamless data exchange between systems

<u>No Adverse Impact on Security and Integrity</u>

System security and integrity

A specification must not introduce security risks and must ensure data integrity:

Implement or define interfaces for federated identity management to enable secure cross-cloud authentication.

Implement mechanisms or technologies such as Cross-provider authentication (e.g., Identity Federation, Single Sign-On)

Implement secure and encrypted communication for all API interactions, using industry-standard protocols.

<u>Not Hindering Innovation</u>

A specification must support long-term evolution and adaptability:

Extensibility and Adaptability

Support the incremental evolution of data model versions to accommodate new use cases without disrupting existing implementations

Include defined extension points or interfaces to allow third parties to add custom functionalities or integrations.

Define mechanisms for API versioning and ensure backward compatibility to support long-term interoperability between systems.

Extensibility and Adaptability

Support modular and decentralized system architectures to enable flexible integration and deployment across diverse environments.

<u>Functional Equivalence</u> (this category is only applicable to IaaS)

Consistent Service-Level Behaviour

A specification must ensure that services function consistently across different environments:

Implement mechanisms or technologies such as API compatibility tests

Implement mechanisms or technologies such as Checksum validation, consistency checks

Implement mechanisms or technologies such as rollback mechanisms in case of migration failures

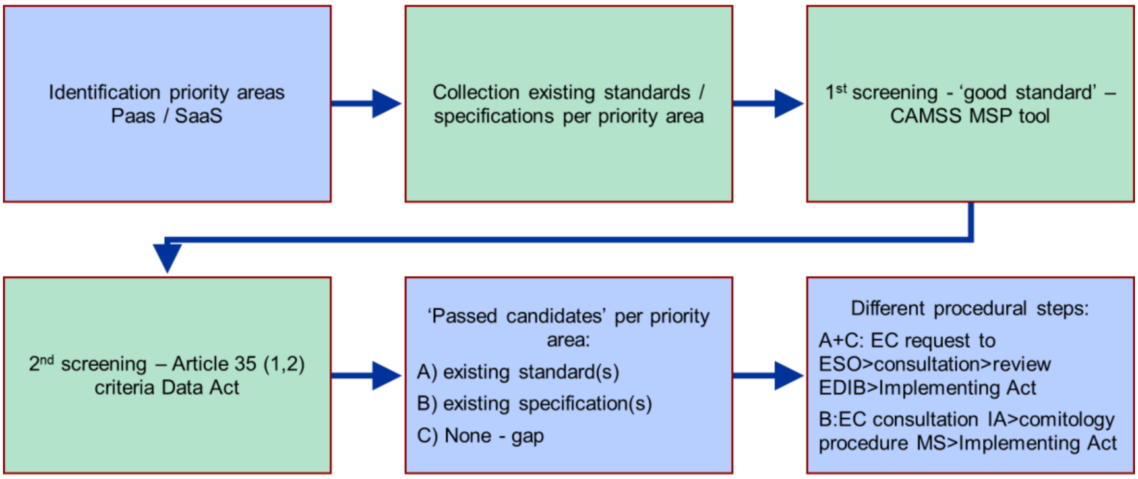
4. Recommended processes for identifying priority areas and screening of candidates to include in the repository

This chapter outlines the proposed processes to identify priority areas for further standardisation on interoperability and processes to be used for screening candidate standards and specifications for possible inclusion in the repository. These processes build on legal requirements from the Data Act and take into account best practice processes from European standard development bodies (which are described in Annex 5 – Reviewed standardization processes of SDOs).

4.1. Overview

The following diagram shows the overall process used by the study team (screening part in green).

Figure 1 – Overall process


Identification priority areas Paas / SaaS
Collection existing standards / specifications per priority area
1st screening - 'good standard' – CAMSS MSP tool
2nd screening – Article 35 (1,2) criteria Data Act
'Passed candidates' per priority area:
A) existing standard(s)
B) existing specification(s)
C) None - gap
Different procedural steps:
A+C: EC request to ESO>consultation>review EDIB>Implementing Act
B:EC consultation IA>comitology procedure MS>Implementing Act

Source: WIK-Consult.

ESO = EU Standardisation Organisation, EDIB = EU Data Innovation Board, IA = Implementing Act.

First, the priority areas were identified by looking at those segments of the European PaaS and SaaS cloud market, which could potentially benefit most from mandating additional interoperability standards and open specifications. This process is described in detail in the next paragraph 4.2.

Thereafter for those priority areas, the study team identified possible suitable candidate standards and open specifications based on input received from stakeholders in interviews, online survey, own desk research and finally from the online workshop ([10]). This resulted in a full list of gathered standards and specifications as listed in Annex 7 – Full list of gathered standards/ specification/ Tools/ other.

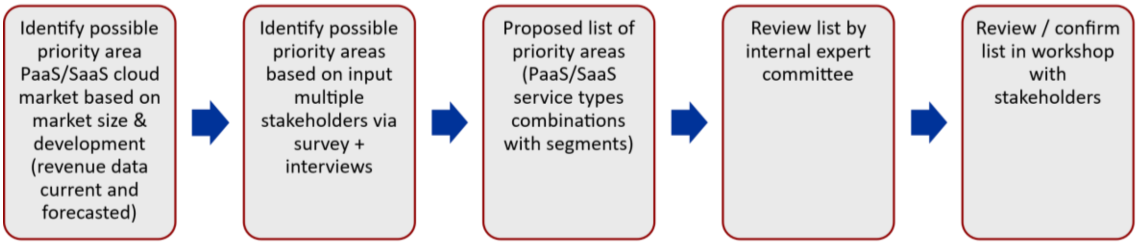
In coordination with the EC, a selection of standards and specifications was made for detailed screening (see the process of shortlisting in 4.3). For these candidates, the study team then conducted a screening process following the two-step approach described in detail in section 4.3.

The outcome of the screening could be that for a certain priority area there are either suitable candidate standards, and/or open specifications, or none. For the different outcomes there are different procedural steps foreseen in the Data Act leading towards either an Implementing Act for inclusion in the repository or a request to a European Standardisation Organisation (ESO) to draft a harmonised standard where there is a gap. These procedural steps are described in detail in section 4.4.

4.2. Process for identifying priority areas for standardisation

For this study, we applied the following process for determining the priority areas for further standardisation of interoperability of data processing services not related to infrastructure elements.

Figure 2 – Process applied for identifying priority areas


Identify possible priority area PaaS/SaaS cloud market based on market size & development (revenue data current and forecasted)
Identify possible priority areas based on input multiple stakeholders via survey + interviews
Proposed list of priority areas (PaaS/SaaS service types combinations with segments)
Review list by internal expert committee
Review / confirm list in workshop with stakeholders

Source: WIK-Consult.

First the economic significance of cloud market segments in the European PaaS and SaaS was considered by looking at the current market size based on available market data ([11]).

Thereafter, stakeholders were specifically asked in an online survey what they consider to be priority areas for further standardisation in view of any problems they had experienced in undertaking cloud migration and/or in implementing multi-cloud strategies. Thereafter, interviews with selected stakeholders were

[10] Held on 20th of March 2025.

[11] Based on available market data from Statista.

used to verify if any area had been overlooked. This did not result in any change as the input from the interviews confirmed the priority areas from the online survey.

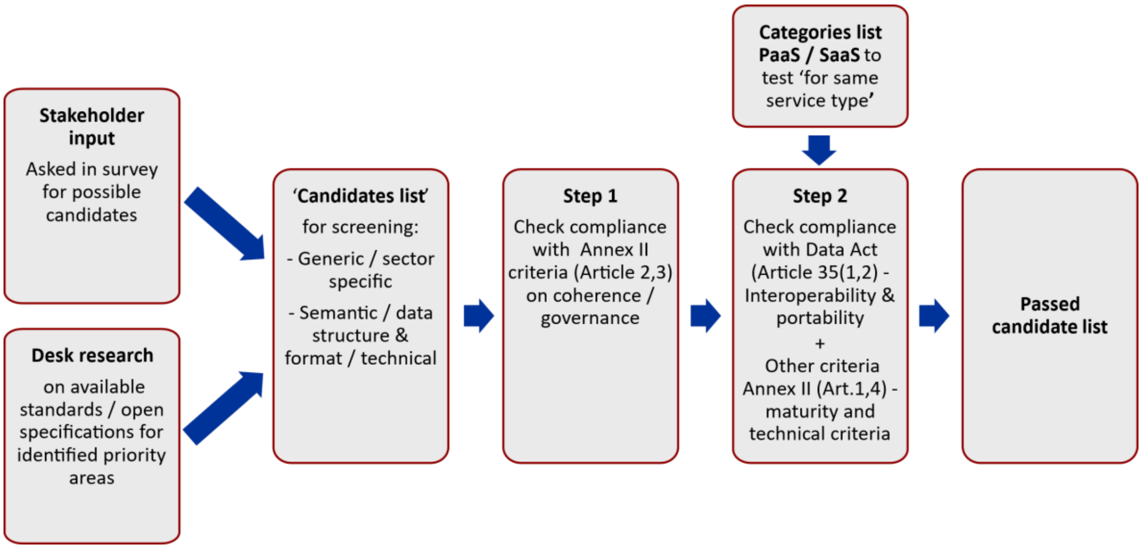
In order to rank the different categories, the relevant European market share per segment (expressed as %) and the % of respondents selecting a certain priority area were both taken into account. In this context, two scenarios were considered; an equal (50/50) weighting and a 75/25% weighting whereby more weight was assigned on the stakeholder input from the online survey. The 75/25 weighting was proposed to be used as the input from the online survey was more specific than the (rough) market segments based on available revenue data.

Finally, the proposed weighting and the resulting priority areas were discussed in the online workshop of 20th March 2025. At the workshop, 73% of stakeholders agreed with the recommended approach and the applied weight factors (45% versus 36% preferring different weighting factors). As regards the process for future assessment (after conclusion of the study), the majority of stakeholders indicated that this process should preferably be conducted as a combined effort involving the industry along with European standard bodies and the European Commission. More specifically, out of industry participants at the workshop 35% noted that cloud customers should be involved, 25% European standard bodies and 20% the European Commission. 9% indicated that cloud providers should be involved. Comments provided suggest that inputs from different stakeholder groups should be taken into account.

4.3. Process to shortlist candidates and screen for compliance

The following figure provides a full overview of the process that was used to shortlist and screen candidate standards and open interoperability specifications that were collected based on the priority areas identified following the process described in the previous section.

Figure 3 – Process to identify and screen candidates


Stakeholder input
Asked in survey for possible candidates
Desk research
on available standards / open specifications for identified priority areas
'Candidates list' for screening:
- Generic / sector specific
- Semantic / data structure & format / technical
Step 1
Check compliance with Annex II criteria (Article 2,3) on coherence / governance
Categories list PaaS / SaaS to test 'for same service type'
Step 2
Check compliance with Data Act (Article 35(1,2) - Interoperability & portability
+
Other criteria Annex II (Art.1,4) - maturity and technical criteria
Passed candidate list

Source: WIK-Consult.

The steps involved are further described below.

4.3.1. Gathering candidates and shortlisting

Standards and open specifications on interoperability for data processing services in the top priority areas (see above) were collected via desk research, interviews and an online survey. As this resulted in a long list of possible candidates (see Annex 7 – Full list of gathered standards/ specification/ Tools/ other), a further step was applied to produce a shortlist of candidates, which could then be subject to a screening process for compliance with the Data Act. The shortlisting process was conducted in consultation with the European Commission.

The main criteria used for shortlisting was the potential for wide application, and market acceptance, as indicated through widespread use across the industry, as well as suggestions from industrials. This was considered important, as inclusion in the Data Act repository results in a legal requirement for cloud service providers to make their services compatible with such standards (with the associated cost implications).

To ensure a focus on standards and specifications with a wide scope of application, focus was given to shortlisting standards and specifications which were generic and cloud centric (not backbone cloud). In addition, we considered, in particular for tools and technology platforms used to support interoperability in cloud environments, whether they had evolved into de facto standards, which were recognised across the industry and considered foundational to interoperability.

Implementation tools which have not been formalised as standards or specifications such as infrastructure management software, messaging services, or development tools, among others, were not shortlisted for screening.

For the purposes of this study, the shortlisting process was conducted in consultation with the European Commission. We also gave priority to those open specifications that were the most frequently mentioned across stakeholder engagement activities—including interviews, the online survey, and the March 2025 workshop, where participants were explicitly invited to propose additional specifications.

After the conclusion of this study (as recommended in the context of identifying priority areas), the process of shortlisting from amongst a wider list of standards and specifications could be coordinated by the European Commission with input from experts including cloud customers via a relevant forum or working group established for this purpose.

4.3.2. Process for screening shortlisted candidate standards and open specifications

Following the shortlisting, a two-step screening process was applied following the criteria set out in section 3.3. As previously noted, step 1 of the screening involved a review of compliance with criteria on coherence and governance (Article 2 and 3) from Annex II of Regulation 1015/2012.

The resulting prequalified list of passed candidate standards and/or open specifications (of Step 1 screening) were thereafter screened on their full compliance with the remaining Article 1 and 4 criteria from Annex II (maturity and technical specifications) and the new Article 35 (1,2) criteria of the Data Act (on interoperability and portability of data and applications).

The taxonomy of cloud functions as described in section 3.2 supported the identification of services of the ‘same service type’ for the purposes of screening.

In the online workshop of 20th of March 2025, this approach and operationalisation of screening criteria was proposed to stakeholders. A large majority of participants (80%) agreed with the proposed two-step screening. In addition, 83% of stakeholders in the workshop confirmed via polling the proposed re-use of the CAMSS MSP tool for step 1.

As regards the future process / responsibility for conducting the evaluation, stakeholders in the workshop agreed that checking compliance in step 1 should be carried out by the EC (35%) in conjunction with EU Standard Development Organisations (SDOs) (30%). 22% of stakeholders suggested that cloud customers should also be involved. For step 2 of the screening process, the polling results suggested a similar set-up with joint responsibility for the EC (41%) and EU SDOs (41%) with some involvement by cloud customers (22%).

The proposed taxonomy was also discussed in the workshop; for the maintenance of this list, stakeholders pointed towards international SDOs (30%), followed by the cloud industry itself (26%) and 22% for EU SDOs and 17% for the European Commission. Additional comments from workshop participants were that it is important to have cloud customers involved as they have the business domain knowledge and could initiate the insertion of new service types. Furthermore, a neutral oversight body should finally determine what is then 'same' service type, and this could best be done by EC/EU SDOs.

4.4. Procedural process to include standards and specifications in the repository

As described in the overall flow (see Figure 1); after candidate standards and open specifications have been identified and validated, the procedural steps will lead either towards the development of an Implementing Act to formalise an open specification such that it becomes a common specification based on an open specification or to possible requests to ESOs for the development of a harmonised standard ([12]) or eventually to the development of an Implementing Act to include harmonised standard and/or common specifications in the online repository.

In this regard, there are three different possible procedural streams depending on whether there are:

A) Validated candidate standards per priority area;

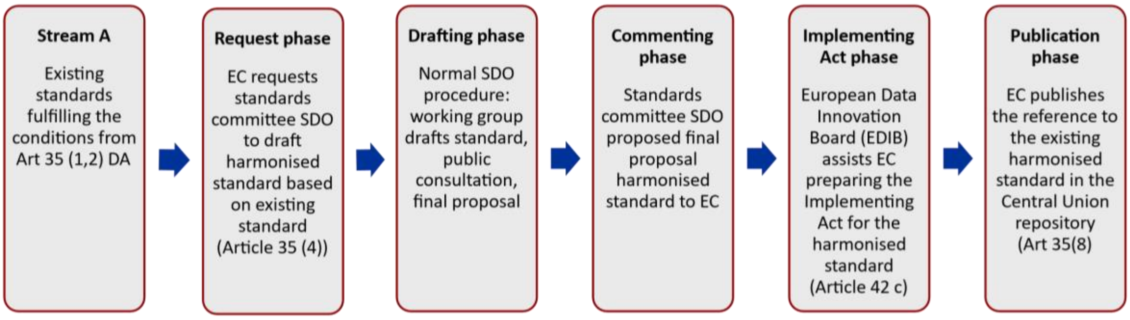
B) Validated candidate open specifications per priority area; or

C) None of both (requesting the development of new standards).

The following processes are described in the Data Act:

[12] See Article 35(4) and 35(5,6,7,8) of the Data Act.

Figure 4 – Procedural process for stream A (validated candidate standards)

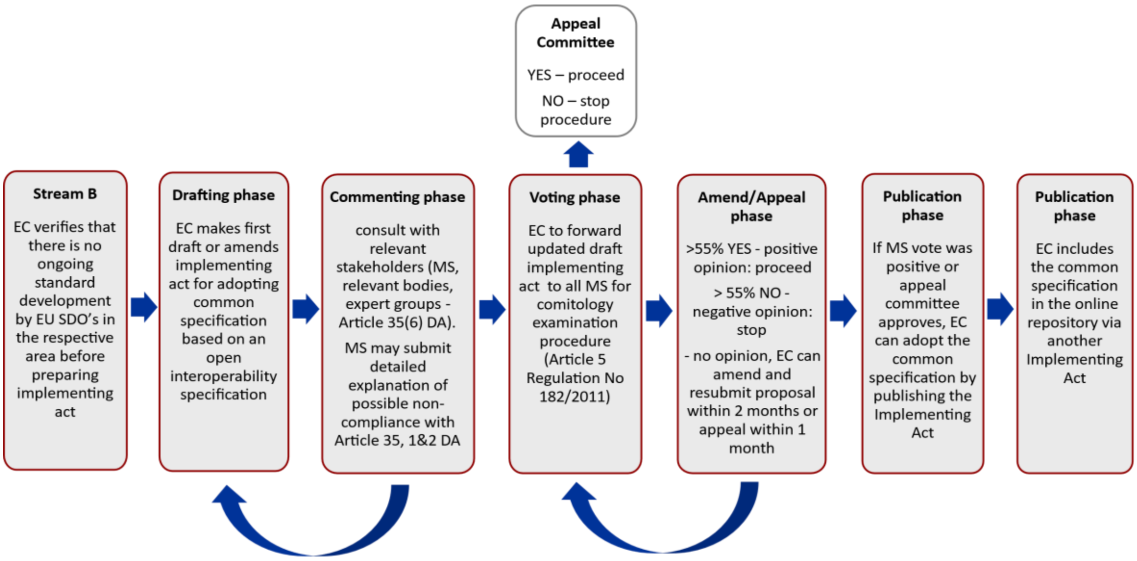

Stream A
Existing standards fulfilling the conditions from Art 35 (1,2) DA
Request phase
EC requests standards committee SDO to draft harmonised standard based on existing standard (Article 35 (4))
Drafting phase
Normal SDO procedure: working group drafts standard, public consultation, final proposal
Commenting phase
Standards committee SDO proposed final proposal harmonised standard to EC
Implementing Act phase
European Data Innovation Board (EDIB) assists EC preparing the Implementing Act for the harmonised standard (Article 42 c)
Publication phase
EC publishes the reference to the existing harmonised standard in the Central Union repository (Art 35(8)

Source: WIK-Consult.

In case there are validated candidates for open specifications, which could be transformed into a common specification, the EC first needs to verify whether there is no ongoing standard development in the respective area or the standard development is delayed (Recital 103 and Article 35,4 of the Data Act).

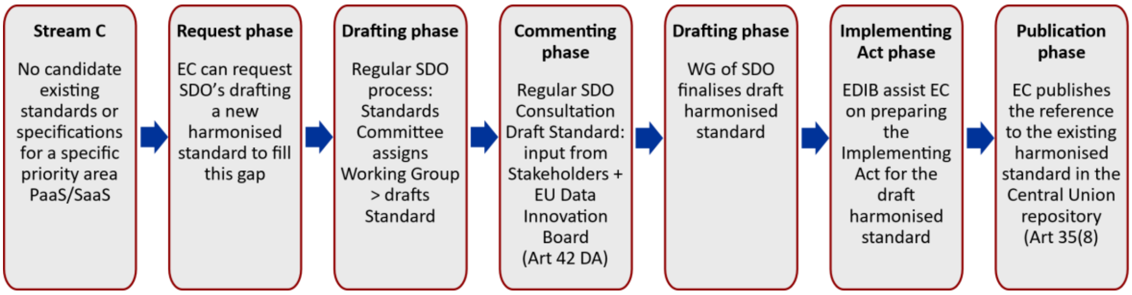
Thereafter, first an Implementing Act is required to convert the open specification into a common specification and then another Implementing Act is required to include the common specification in the online repository (and make it mandatory). See the following figure.

Figure 5 – Procedural process for stream B (validated candidate open specifications)


Appeal Committee
YES – proceed
NO – stop procedure
Stream B
EC verifies that there is no ongoing standard development by EU SDO's in the respective area before preparing implementing act
Drafting phase
EC makes first draft or amends implementing act for adopting common specification based on an open interoperability specification
Commenting phase
consult with relevant stakeholders (MS, relevant bodies, expert groups - Article 35(6) DA).
MS may submit detailed explanation of possible non-compliance with Article 35, 1&2 DA
Voting phase
EC to forward updated draft implementing act to all MS for comitology examination procedure (Article 5 Regulation No 182/2011)
Amend/Appeal phase
>55% YES - positive opinion: proceed
> 55% NO - negative opinion: stop
- no opinion, EC can amend and resubmit proposal within 2 months or appeal within 1 month
Publication phase
If MS vote was positive or appeal committee approves, EC can adopt the common specification by publishing the Implementing Act
Publication phase
EC includes the common specification in the online repository via another Implementing Act

Source: WIK-Consult.

Figure 6 – Procedural process for stream C (no candidates)


Stream C
No candidate existing standards or specifications for a specific priority area PaaS/SaaS
Request phase
EC can request SDO's drafting a new harmonised standard to fill this gap
Drafting phase
Regular SDO process: Standards Committee assigns Working Group > drafts Standard
Commenting phase
Regular SDO Consultation Draft Standard: input from Stakeholders + EU Data Innovation Board (Art 42 DA)
Drafting phase
WG of SDO finalises draft harmonised standard
Implementing Act phase
EDIB assist EC on preparing the Implementing Act for the draft harmonised standard
Publication phase
EC publishes the reference to the existing harmonised standard in the Central Union repository (Art 35(8)

Source: WIK-Consult.

5. Prioritising areas for further standardisation for PaaS and SaaS cloud services

This chapter sets out the conclusions of our preliminary analysis regarding priority areas for European PaaS and SaaS cloud services. See paragraph 4.2 for more details on the underlying process that was applied.

5.1. Prioritising based on market size

When considering market size, the starting point was the most detailed categorisation used by market research companies like Statista. Where data specific for the European market was available, this was used ([13]).

This early categorisation evolved into the more detailed categorisation used in the online survey into the even more detailed service type categories for PaaS services, which were developed later in the project. Where market definitions have been provided by Statista, these have been added below the tables, complemented with descriptions from the cloud experts. The most detailed product categories (and description) of the PaaS cloud market can be found in Annex 2 – Proposed categories for PaaS/SaaS service types. For the next review of priority areas, we recommend using the most detailed categorisation of the PaaS service types.

The market share percentages were used as an input to determine the segment relevance. In addition, the expected market size in 2029 was reviewed to verify if significant changes could be expected in this ranking. However, this did not appear to be the case. The following tables provide an overview of the ranking for PaaS and SaaS based on market size in 2024.

Table 7 – Ranking PaaS market segments based on market size in Europe (€ bln)

Paas

Service Type / Area – PaaS	2024	% of total
Application Development	40,8	61%
DevOps and CI/CD	11,5	17%
Database as a Service (DBaaS)	7,4	11%
Identity and Access Management (IAM)	4,95	7%

[13] Where only the worldwide size of a certain market segment was available via Statista, it was assumed that 24% of this applies for the European size (based on the total market size of the cloud market worldwide versus the market size of the cloud market in Europe). Overall size PaaS cloud market in Europe 41,44 bn USD in 2024 versus 171,8 bn USD worldwide (24%). Source: Platform as a Service - Europe | Statista Market Forecast

Service Type / Area – PaaS	2024	% of total
Middleware	2,14	3%
Integration Services	0,262	0%
Mobile Backend as a Service (MBaaS)	0,268	0%
	67,32	

Source: WIK-Consult based on Statista Market Insights via pro account.

Definitions applied:

- Application Development: development tools used by developers to design, create, test, and deploy applications. These applications can be anything from mobile apps and web-based software to complex enterprise applications. Examples of software solutions in the Application Development Software market include a wide range of tools and technologies, such as integrated development environments (IDEs), code editors, compilers, debuggers, testing and deployment tools, and programming languages. ([14])
- DevOps and CI/CD: PaaS solutions streamlining collaboration between software development and IT operations teams, fostering a culture of continuous integration and continuous delivery (CI/CD) of high-quality software. ([15])
- Database as a Service: solutions providing managed database (and related) services using public cloud platforms.
- Identity and Access Management: solutions ensuring availability of identity services like username and password or mobile SMS-based authentication, password managers, push apps, hardware security keys etc. ([16])

Table 8 – Ranking SaaS market segments based on market size in Europe (€ bln)

Saas

Service Type / Area – SaaS	2024	% of total
Enterprise Resource Planning (ERP)	53	32%
Healthcare SaaS Solutions	37,1	22%
Customer Relation Management (CRM)	19,6	12%
Project Management and Task Management	13,5	8%
Office Software	6,5	4%

[14] Statista Market Insights, Software -Application Development Software, Europe, December 2024. See https://www.statista.com/outlook/tmo/software/application-development-software/europe?currency=USD

[15] Statista Market Insights, Platform as a Service: Market data & Analysis, July 2024.

[16] Statista, Digital & Trands, Identity and Access Management, see (https://www.statista.com/study/117243/identity-and-access-management/

Service Type / Area – SaaS	2024	% of total
Business Intelligence (BI) and Analytics	6,3	4%
Learning Management Systems (LMS)	5	3%
Content Management Systems (CMS)	5	3%
Supply Chain and Inventory Management	4,5	3%
Human Resources Management Systems (HRMS)	3,37	2%
Collaboration and Communication Tools	3,37	2%
Construction and Design Software	2,46	1%
Marketing Automation	2	1%
E-commerce Platforms	1,78	1%
Security and Compliance	2	1%
	165,48	

Source: WIK-Consult based on Statista Market Insights via pro account.

Descriptions of applied market segments ([17]):

- Enterprise Resource Planning or Management (ERP/ERM): cloud-based platforms that integrate and manage core business operations such as finance, supply chain, procurement, and human resources. These solutions centralize data, automate workflows, and provide real-time insights to improve efficiency and decision-making across the organization.
- Healthcare SaaS Solutions: Software-as-a-Service applications tailored for the healthcare sector, including electronic health records (EHR), telemedicine platforms, patient engagement tools, and healthcare analytics. Helps to streamline administrative tasks.
- Customer Relationship Management (CRM): cloud-hosted systems for managing a company's interactions with customers and prospects. CRM SaaS platforms offer tools for sales pipeline management, marketing automation, customer support, and analytics to improve customer acquisition, retention, and satisfaction.
- Project Management & Task Management: SaaS platforms that enable teams to plan, track, and execute projects and individual tasks collaboratively. These tools often include Gantt charts, Kanban boards, time tracking, resource allocation, and integrations with other productivity software.
- Office Software: cloud-based productivity applications such as word processors, spreadsheets, presentation tools, email, and calendaring. They allow real-time collaboration, version control, and anywhere-access, replacing or complementing traditional desktop office suites.

[17] Based on chatgpt5, reviewed by expert.

- Business Intelligence & Analytics: SaaS solutions that collect, process, and visualize data to support decision-making. They include dashboards, data exploration tools, predictive analytics, and reporting features, enabling organizations to identify trends, measure KPIs, and uncover business opportunities.

Later on in the project, detailed service types (as described in section 3.2) were defined for the operationalisation of certain obligations on interoperability and portability of data, which overlap partially with certain market segments defined here (e.g. IAM and CI/CD).

5.2. Priority areas cited in the online survey and interviews

Particular consideration was also given to input from stakeholders. This was gathered via responses to the online survey which included specific questions asking respondents which areas should have priority for interoperability standards considering experienced problems with cloud migration and/or multi-cloud strategies ([18]).

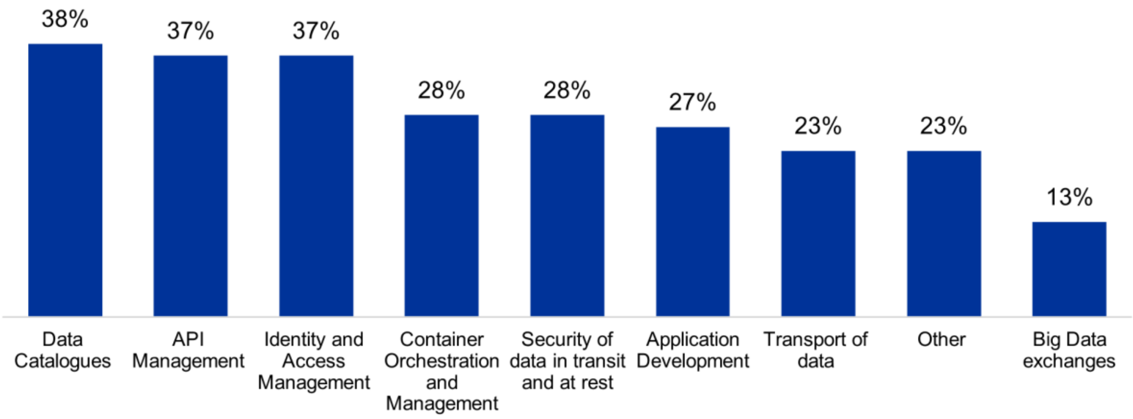
These questions were:

- Question 11: Considering the experienced problems asked for in the previous questions, what should be, in your opinion, the priority areas of the PaaS cloud market when reviewing standards and specifications to be included in the Union repository (and thereby making them mandatory)? Options: For Data Catalogue, Big Data Exchanges, For Application Development (DevOps, CI/CD etc..), For Database as a Service (DBaaS), For API Management, For Container Orchestration and Management, For Transport of data, For Identity and Access Management (IAM, For Security of data in transit and at rest, other – please describe).
- Question 12: Considering the experienced problems asked for in the previous questions, what should be, in your opinion, the priority areas of the SaaS cloud market when reviewing standards and specifications to be included in the Union repository (and thereby making them mandatory)? Options: For Enterprise Resource Planning (ERP) systems, For Customer Relation Management (CRM) systems, For Project / Task management systems, For Office Automation Software, for Financial and Accounting Software, For Business Intelligence (BI) and Analytics, Other in relation to data format and structure (please describe).

The following charts provide an overview of the responses given to these questions by stakeholders.

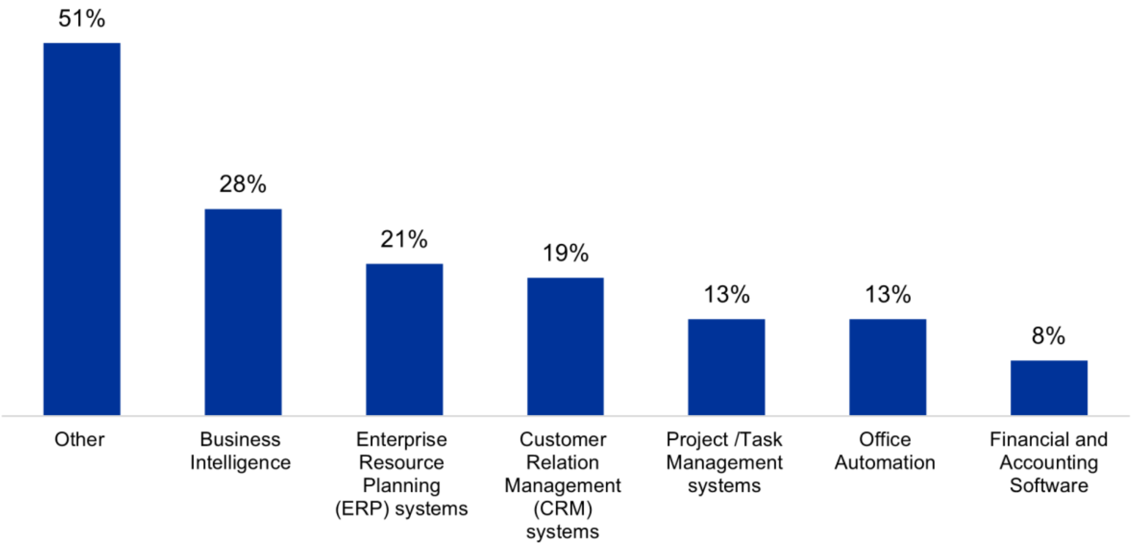
[18] See Annex 2, question 11 and 12.

Figure 7 – Priority areas – PaaS (Q11, all respondents)



Source: WIK-Consult Online survey on „Interoperability of data processing services" (12/12/2024-17/01/2025), N=60 (all respondents).

Figure 8 – Priority areas – SaaS (Q12, all respondents)



Source: WIK-Consult Online survey on „Interoperability of data processing services" (12/12/2024-17/01/2025), N=53 (all respondents).

For SaaS, the category 'Other' contained mainly remarks that SaaS solutions are very vendor specific and thus it was difficult to standardise without hindering innovation. Stakeholders suggested that any standardization efforts in this area should thus focus on mass market, generic SaaS solutions and not on dedicated SaaS solutions. However, some stakeholders suggested that even for the generic SaaS solutions, standardisation should be sector specific due to varying customer requirements. On the other hand, for open specifications no suggestions have been proposed by stakeholders.

The specific input for priority areas from the interviews (see Annex 3 for interview guidelines) was also reviewed to see if any area had been overlooked. However, no change was made as the input from the interviews was limited, as noted in the following table.

Table 9 – Priority areas from the interviews (sorted per stakeholder type)

Interviewee type	Prioritized segments
Hyperscalers	None
EU cloud providers	For PaaS: focus on general purpose apps (data service & data transfer was named multiple times), event triggering and Identity Access Management and API management. For SaaS: data analytics, observability and cybersecurity. But also, more focus on segment specifics.
Standard bodies	No priority areas for PaaS and SaaS Focus on large public sector Focus on data portability first and the basic PaaS services (including IaaS as these are still difficult to switch).
Industry Association	General segments: Industry, Media, transport & logistics, health and public safety & security
Customers	For SaaS: eCommerce, Data Analytics, Online File sharing, Observability and Cybersecurity.

Source: WIK-Consult, Interviews November – December 2024.

5.3. Conclusions regarding priority areas

Finally, in order to draw conclusions regarding areas to be prioritised, as discussed in section 4.2, we applied a 75% weighting on the stakeholder input from the online survey and a 25% weighting to ranking based on the relative size of the market segment.

Before finalising the weighting, we conducted a sensitivity test by reviewing the effect of changing the weights to 50/50. For PaaS, this did not result in a different order. For SaaS, the order changed slightly. The most significant change was that Healthcare moved down and fell below 10% while Office Automation moved up and lay above the 10%. The category ‘Other’ does not qualify as respondents highlighting this category did so to make comments as noted above. We concluded that changing the weighting would not have a material impact (in particular noting the preference of many stakeholders not to focus on SaaS) and retained the 75:25 split.

The resulting ranking based on this split (75% x stakeholder preference for specific area) + (25% x market share of relevant segment) is shown in following table.

Table 10 – Recommended priority areas for PaaS (in green)

Scenario 2: 75/25 stakeholder/market size

Overall ranking PaaS	
Application Development	35%
Identity and Access Management (IAM)	30%
Data Catalogues	29%
API Management	28%
Container Orchestration and Management	21%
Security of data in transit and in rest	21%
Transport of data	17%
Big Data Exchanges	4%
DevOps and CI/CD	10%
Database as a Service (DBaaS)	3%

Source: WIK-Consult.

Table 11 – Recommended priority areas for SaaS

Scenario 2: 75/25 stakeholder/market size

Overall ranking SaaS	
Other	38%
Enterprise Resource Planning (ERP) systems	24%
Business Intelligence	22%
Customer Relation Management (CRM)	17%
Project Management and Task Management	12%
Office Automation	11%
Financial and Accounting Software	6%
Healthcare SaaS Solutions	6%

Source: WIK-Consult.

These rankings of priority areas, as well as comments made in the interviews regarding priority areas for PaaS and SaaS were discussed in the workshop of 20th March 2025. In this context we proposed to refrain from establishing priority areas (and reviewing standards and specifications) for the SaaS market as the majority of responses in our online survey had cautioned against standardising specific SaaS solutions (including those relating to specific sectors) for the time being. 76% of stakeholders agreed with this proposal when asked via online polling in the workshop.

During the workshop, we proposed to focus for the first review on the top 4 priority areas of the PaaS market, i.e. Application Development, Identity and Access Management, Data Catalogues and API management. A majority of stakeholders agreed with this suggestion in the polling (66%).

However, several stakeholders indicated that Container Orchestration and Security of Data were also relevant. To reflect this input, the scope was expanded to include the top seven categories in the PaaS market—adding Container orchestration and Security of Data, as well as Transport of Data, for which the percentage of support was close to that of the two previously mentioned categories. Its inclusion ensures that all PaaS categories with more than 15% of stakeholder support were considered in the initial assessment.

6. Screening of standards and specifications against the operationalised criteria

This chapter describes which identified standards and specifications were considered for screening and how these map against the priority areas identified in chapter 4. It also describes the results of the step 1 and step 2 screening verifying the compliance with the Data Act criteria as described in section 3.3.

6.1. Approach

Standards and specifications were identified through multiple sources. A key source of information came from stakeholder engagement, including interviews and the online survey. Respondents were directly asked about applicable standards and specifications, with targeted questions ensuring that only those relevant to cloud interoperability were considered. Prior to the interviews, preliminary desk research was conducted, allowing for the identification of a first list of standards for validation and ensuring a more focused discussion.

The desk research included a review of publications and databases from key SDOs such as OASIS, IETF, ISO/IEC, and ETSI, with particular attention to specific working groups such as ISO/IEC JTC 1 or JTC 38, the joint technical committees focusing on information technology and cloud computing. Additionally, standards foundational to interoperability – such as those defining taxonomy, data formats, and protocols – were examined, as these elements provide the basis for achieving cloud interoperability. Reports conducting preliminary mappings of cloud standards, such as ETSI SR 003 392 V2.1.1 (2016-02), were also reviewed to cross-check and validate the selection of relevant standards.

Following the initial identification, several types of standards/specifications were excluded from the evaluation, following the logic described in section 4.3.1:

- Technology tools and software platforms that do not constitute formal standards, unless they have evolved into widely adopted de facto standards (e.g. Kubernetes, S3-compatible APIs), in which case they were kept and assessed on a case-by-case basis.
- Mechanisms, reference frameworks, governance models, and organisational names (e.g. "ETSI NFV", "Webhooks", "Web 3") that do not represent standalone technical specifications.
- Vertical-sector-specific standards, which were identified but set aside for potential future evaluation, given the additional complexity and context-specificity they entail.

Among the remaining items, a priority level was assigned to each standard or specification based on its relevance to the seven identified priority areas: Application Development, Identity and Access Management (IAM), Data Catalogues, API Management, Container Orchestration and Management, Security of data in transit and at rest, and Transport of data. Items directly addressing these areas were considered high priority for the following screening phases. The priority standards and specifications were identified following consultation with the Commission.

Thereafter, following the process described in section 4.3.2, a first screening exercise was then performed based on a subset of the CAMSS screening process in order to identify which amongst them were valid candidates for the full screening.

6.2. Standards and specifications identified

In addition to the interviews and survey, desk research was conducted to compile a comprehensive list of candidate standards and specifications. The following tables present the full set of inputs received through stakeholder engagement, including interviews and the online survey. These entries reflect stakeholders' broad interpretation of relevant standards and specifications and therefore include some items that fall outside the scope of this study.

At the time of data collection, the categorisations applied were the original ‚service types‘, which were later updated and made more granular. The online survey split possible candidates between generic and sector specific. The generic candidates were further split into three categories: a) data format, structure and semantic and b) technical and c) foundational aspects. [19]

[19] The initial classification of the generic standards into the categories of data format, structure & semantics, technical aspects, and foundational aspects was established as an interim measure to support the prioritisation and processing of the standards and open specifications during the early stages of the project. These categories were defined as follows:

- Data format, structure & semantics: standards that define how data is structured, formatted, modeled, or semantically described to ensure it can be understood and exchanged consistently across systems (e.g. JSON Schema, RDF, DCAT).
- Technical aspects: standards that specify the protocols, interfaces, APIs, and mechanisms enabling systems to communicate, exchange, and secure data (e.g. OpenAPI, OAuth 2.0, MQTT).
- Foundational aspects: standards that provide cross-cutting frameworks, principles, or reference architectures that underpin interoperability but do not directly prescribe specific formats or protocols (e.g. FAIR Principles, ISO 8000, the European Interoperability Framework).

This approach was intended to remain in place only until the key priority areas were formally agreed upon during the workshop held in March. With these priority areas now defined, the original classification serves primarily as contextual information and is no

A refined list of standards and open specifications — limited to those meeting the definition and scope of this study — in the priority areas, is presented at the end of this subsection, following a filtering step to exclude entries such as tools, organisations, or concepts that do not qualify as formal standards or specifications.

longer considered a determinant for subsequent steps. The survey conducted prior to the workshop was based on these initial categories and therefore reflects this provisional methodology. Should a new survey be conducted in the future, it would instead leverage the formally defined priority areas to ensure consistency and alignment with the agreed framework.

Table 12 – Proposed candidate standards and specifications – input from interviews

		Proposed standards& specifications for formalisation													
	General remarks	Data structure / storage	Data Catalogue / observability	Data space	Data exchange/ transfer	IOP and data portability	Containerisation	IAM / security	Monitoring	Messaging	API management	Protocol buffers	Data visualisation	Data & Analytics	Other
Hyperscalers	CNCF					ISO/IEC 19941:2017									
EU cloud provider	CNCF	AWS S3 - defacto standard. any other low level standards	Data Catalog from W3C	eclipse foundation (defacto standard)	EDIFACT, Apache Arrow data format. ORNEX (open network exchange)	ISO/IEC 19941:2017	Kubernetes Kubernetes + defacto standards: Docker, Cri-o, Podman, Open container initiative (OCI), Helm, Istio	Open ID Connect (OIDC), Online Authorisation (OAuth 2.0), SAML	Promo-theus (open source)	Kafka. CNCF Kafka, NATS for non critical large volume messaging	Open API Open API for REST API + async API for event driven APIs	Google	Grafana	Azure Data Bricks, ML Flow Delta lake, Open telemetry	eCalendar, WebDav solace, cloud events (meta data)
Industry Association	standards from SDO's (3GPP, ETSI, ITU). Relevant projects: Camara, Silva, Nephio														
Cloud customer		CSV, XML, JSON	Active Directory		Simple Object Access Protocol (SOAP), HTTP			Security Assertion Markup Language (SAML), Oauth OIDC, Lightweight Directory Access Protocol (LDAP), HTTPS		Kafka	Rest API				
Standard bodies	Smart Applications REFerence (SAREF). Semantic interoperability. From ETSI TC SmartM2M. See ETSI TS 103 264.					ISO/IEC 19941:2017									

Source: WIK Consult based on interviews.

The following tables (Table 13 to Table 17) present the full, unfiltered set of inputs received from stakeholders via the online survey. While many of the responses refer to relevant standards and open specifications, some entries fall outside the scope of the study—such as references to organisations, implementation mechanisms, or concepts. These inputs were collected through open-ended questions and therefore reflect a broad interpretation of what stakeholders considered relevant. At this stage, all suggestions are displayed exactly as provided by respondents, before any filtering is applied. These include, for example, references to CAMSS in response to a question asking for sector-specific standards and specifications or implementation mechanisms where the survey specifically asked for generic technical standards or specifications. All entries are presented here for transparency, but the study team reviewed each item to determine its relevance and retain only those meeting the definition of a standard or open specification for the screening phases described below.

In most tables, the column headers represent the type of stakeholder (e.g. cloud provider, customer, or standardisation organisation). However, in Table 14 and Table 15, the columns refer to thematic groupings used to structure the responses.

Table 13 – Proposed generic candidate standards/specifications – data format, structure, semantic from online survey

PaaS in general	Customer	EU CSP	Hyperscaler	SDO	Unspecified
ISO/IEC 19941:2017	✓	✓	✓		
ISO/IEC 22123-1:2021	✓				
ISO/IEC 22123-2:2023	✓				
ISO/IEC 22123-3:2023	✓				
On2M2M for IoT	✓	✓			
17826:2022 (CDMI)		✓			
OGC API standards				✓	
IEEE 2302-2021 (SIIF)				✓	
Open Telemetry				✓	
ISO/IEC 19503:2005 XML					✓
ISO/IEC 5140:2023					✓
ISO/IEC TR 23188					✓
ISO/IEC TR 3445					✓
ISO/IEC 17826:2022 (a)					✓
openEHR					✓
FHIR					✓
ISO13606					✓
SNOMED CT					✓
LOINC					✓
ICD10					✓
ICD11					✓

PaaS in general	**Customer**	**EU CSP**	**Hyperscaler**	**SDO**	**Unspecified**
ORPHA					✓
HPO					✓
RxNorm					✓
YAML, JSON, SQL, XML					✓
For specific PaaS	Customer	EU CSP	Hyperscaler	SDO	Unspecified
NIST SP 800-145 & 53, IETF RFC 6749 (OAuth 2.0 open standard for access delegation	✓	✓			
IETF RFC 8259	✓				
ISO/IEC 11179	✓				
IEEE 1616.1-2023 Standard for Data Storage Systems for Automated Driving (Mobility).				✓	
For specific SaaS	Customer	EU CSP	Hyperscaler	SDO	Unspecified
ISO 10303 - Automation Systems and Integration – Product Data Representation and Exchange (STEP)				✓	

Source: WIK-Consult Online survey on „Interoperability of data processing services" (12/12/2024-17/01/2025).

Table 14 – Proposed candidate standards/specifications – technical aspects – from online survey

Generic standards on technical aspects

Data Catalogues	**API Mgt**	**Container Orchestr.**	**DBaaS**	**Appl. Dev.**	**Big Data Exchange**
W3C DCAT V3	GraphQL	Kubernetes (OCI)	ISO/IEC 9075	NIST 800-204D	Apache Avro
ETIS ISG CIM	OpenAPI	OpenSVC	Mariadb	EIRA/eGovERA	Parquet
Smart Data Model	gRPC	OpenStack	Mongodb	ITestBed	Apache Arrow
SHACL	SAML specification	IEEE 2301-2020	SQL Db standards		Apache Hudi
Semic GeoDCAT-AP V3	Odata	Docker (OCI)	openEHR AQL		
DPROD	ISO/IEC 30102:2012	Open Container Initiative			
HL7 FHIR	oas V3.1	ISO/IEC 19944-1:2020			
	IEEE 2302-2021				
	Camarea API specs				
	HL7 FHIR				
	SMART on FHIR				

Source: WIK-Consult Online survey on „Interoperability of data processing services" (12/12/2024-17/01/2025).

Table 15 – Generic candidate standards/specifications – foundational aspects-from online survey

Identity and Access Management (IAM)	Customer	EU CSP	Hyperscaler	SDO	Unspecified
W3C SSI	✓				
OAuth	✓	✓	✓	✓	✓
SAML	✓	✓	✓		✓
DID	✓				
Web 3	✓				
SCIM	✓	✓	✓		✓
FIDO	✓	✓			✓
WebAuthn	✓	✓			
OIDC	✓	✓	✓		✓
ADFS			✓		
Entra ID			✓		
W3C Webauthn			✓		
X.509 (IETF RFC 5280)			✓		
OpenID4VCI			✓		
OpenID4VP			✓		
IEEE 2302-2021				✓	
PKI					✓
JWT					✓
Transport of data	**Customer**	**EU CSP**	**Hyperscaler**	**SDO**	**Unspecified**
ETSI ISG CIM	✓				
Apache Kafka	✓	✓		✓	✓
Apache Pulsar	✓				
MQTT	✓	✓			
AMQP	✓				
OAI-PMH	✓				
RabbitMQ		✓			
JSON over HTTP/TLS		✓			
ISO/IEC 19944-1			✓		
IEEE 2302-2021				✓	
Security of data in transit and at rest	**Customer**	**EU CSP**	**Hyperscaler**	**SDO**	**Unspecified**
TLS	✓	✓			
ISO/IEC 27017/27018	✓	✓			
BSI TR	✓				
New PQC standards (NIST)	✓	✓			
RFC 5246					✓

Other area	Customer	EU CSP	Hyperscaler	SDO	Unspecified
HELM charts	✓				
Ansible	✓				
OASIS-TOSCA	✓				
ISO/IEC 19941:2017	✓	✓			
Minio S3	✓	✓	✓	✓	
Open Source		✓			
IPv6			✓		

Source: WIK-Consult Online survey on „Interoperability of data processing services” (12/12/2024-17/01/2025).

Table 16 – Cited sector-specific candidate standards and specifications – from online survey

Sector specific standards

Manufacturing	Healthcare	Finance	Public sector	Smart Living	Energy	Mobility
COVESA VSS	Fast Healthcare Interoperability Resources (FHIR)	DORA	ETSI ISG CIM	ETSI ISG CIM	IEC 62325 Series	IEEE 1616.1-2023
Asset Administration Shell	openEHR	ISO 20022	web3	MQTT	web3	DATEX 2
OPC UA	ISO 27799	web3	EIRA	MATTER.		TPEG
	ISO/IEEE 11073-x family	AMQP	eGovERA			MobilityDCAT
	ISO13606.		ITestBed			
			CAMSS			
			ELIS			
			ELAP			
			EIF			

Source: WIK-Consult Online survey on „Interoperability of data processing services” (12/12/2024-17/01/2025).

Table 17 – Other cited standards or open interoperability specifications that may be relevant for a first review – from online survey

Standards or open interoperability specifications	Customer	EU CSP	Hyperscaler	SDO	Unspecified
LUDX	✓				
kubernetes	✓				
CAPI	✓				
Kepler	✓				
Web3	✓				
STEP ISO 10303		✓			
ISO/IEC 19941:2017		✓			
ISO/IEC 5140:2024		✓			
Open Virtualization Format (OVF)			✓		
Logboek dataverwerkingen				✓	
Data space protocol					✓

Source: WIK-Consult Online survey on „Interoperability of data processing services” (12/12/2024-17/01/2025).

Table 18 – Gathered standards from Desk Research

Standard / specification	Description
OData	REST-based data access protocol
ISO/IEC 12207	Software lifecycle processes
GraphQL	API query language
ISO/IEC 27018	Cloud privacy and data protection
Oasis STIX	Cyber threat intelligence
Oasis TAXII	Cyber threat data transport
Oasis PKCS	Public key cryptography
Oasis TOSCA	Topology of cloud based web services, their components, relationships, and the processes that manage them
OCI	Container runtime and image formats — ensures portability of workloads across Kubernetes, Docker, etc.
CBOR	Binary data serialization format
Webhooks	Event-driven API callback mechanism
YAML	Human-readable data serialization format
RFC 6455 Websocket Protocol	Bidirectional communication
RFC 9556 IoT Devices cloud connectivity	Cloud connectivity for IoT devices
CEN/TS 18026:2024	Cybersecurity requirements for cloud services
ISO/IEC 17203:2017	Information technology — Open Virtualization Format (OVF) specification
ISO/IEC 19086-2:2018	Cloud computing — Service level agreement (SLA) framework
ISO/IEC 19831:2015	Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol — An Interface for Managing Cloud Infrastructure

Source: DECISION Études & Conseil.

The table below presents the refined list of standards and open specifications that fall within the identified priority areas. These items were retained after the filtering process, which excluded entries that did not meet the study's definition of a formal standard or open specification.

Item	Link	Version
Standards		
ISO 19941:2017	https://www.iso.org/standard/66639.html	2017
Oauth/ IETF RFC 6749	https://datatracker.ietf.org/doc/html/rfc6749	2.31
CBOR (IETF RFC 8949)	https://datatracker.ietf.org/doc/html/rfc8949	2020
ISO/IEC 27018:2019	https://www.iso.org/standard/76559.html	2019
CDMI (Cloud Data Management Int.)/ ISO/IEC 17826:2022	https://www.iso.org/standard/76559.html	2019
RFC 6455 Websocket Protocol	https://datatracker.ietf.org/doc/html/rfc6455	2011
RFC 9556 IoT Devices cloud connectivity	https://datatracker.ietf.org/doc/rfc9556/	2024
ISO/IEC 17203:2017	https://www.iso.org/standard/72081.html	2017

Item	Link	Version
oneM2M	https://www.onem2m.org/technical/published-specifications	
OGC API standards	https://ogcapi.ogc.org/	
IEEE 2302-2021 (SIIF)	https://standards.ieee.org/ieee/2302/7056/	2022
ISO/IEC 19503:2005	https://www.iso.org/standard/32622.html	2005
ISO/IEC 11179	https://www.iso.org/standard/78914.html	2023
IEEE 1616.1-2023	https://standards.ieee.org/ieee/1616.1/10939/	2023
ISO 10303	https://www.iso.org/fr/standard/83105.html	2024
TLS/ RFC 8446	https://datatracker.ietf.org/doc/html/rfc8446	2018
ISO/IEC 27017/27018	https://www.iso.org/standard/43757.html	2015
Specifications		
Oasis PKCS	https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=pkcs11	3.1
OIDC (OpenID Connect)	https://openid.net/developers/discover-openid-and-openid-connect/	2014
SAML	https://docs.oasis-open.org/security/saml/v2.0/	2.0 (2005)
GraphQL	https://graphql.org/	2021
Open API	https://spec.openapis.org/oas/latest.html	3.1.1 (2024)
Protocol Buffers	https://protobuf.dev/	
Async API	https://www.asyncapi.com/docs/reference/specification/v3.0.0	3.0.0
OData	https://docs.oasis-open.org/odata/	4.02
Open Container Initiative (OCI)	https://specs.opencontainers.org/	1.0 (1, 0 & 2)
CloudEvents	https://cloudevents.io/	
AMQP (ISO/IEC 19464)	https://www.oasis-open.org/standard/amqp/	1.0
MQTT (ISO/IEC 20922)	https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.html	5.0
JSON/ IETF RFC 8259	https://datatracker.ietf.org/doc/html/rfc8259	2017
XML	https://www.w3.org/TR/xml/	1.0 (Fifth Edition)
Oasis STIX	https://www.oasis-open.org/standard/6426/	2.1
Oasis TAXII	https://www.oasis-open.org/standard/taxii-version-2-1/	2.1
CEN/TS 18026:2024		
OASIS TOSCA	https://www.oasis-open.org/standard/tosca-yaml-v1-3-os/	1.3 (2020)
W3C SSI / DID	https://www.w3.org/TR/did-1.0/	2023
SCIM	https://datatracker.ietf.org/doc/html/rfc7643	2015
FIDO	https://fidoalliance.org/specifications-overview/	
W3C/ FIDO WebAuthn	https://www.w3.org/TR/webauthn-3/	2025 (level 3, 2021 for Level 2)
X.509 (IETF RFC 5280)	https://datatracker.ietf.org/doc/html/rfc5280 & https://datatracker.ietf.org/doc/html/rfc6818	

Item	Link	Version
OpenID4VCI	https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html	draft 2025
OpenID4VP	https://openid.net/specs/openid-4-verifiable-presentations-1_0.html	draft 2025
IPv6	https://www.rfc-editor.org/rfc/rfc8200.html	2017
CSV	https://datatracker.ietf.org/doc/html/rfc4180	2005
Other (Tools, Platform)		
Cri-O	https://cri-o.io/	1.32
Docker	https://docs.docker.com/get-started/docker-overview/	N/A
Podman	https://docs.podman.io/en/latest/	5.5
Helm	https://helm.sh/docs/	3.17
S3 Api	https://docs.aws.amazon.com/AmazonS3/latest/API/Type_API_Reference.html	01/03/2006
NATS	https://nats.io/	2.11
ML Flow	https://mlflow.org/	3.2
Istio	https://istio.io/	1.26
ADFS	https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview	
Entra ID (formerly Azure AD)	https://learn.microsoft.com/en-us/entra/identity/	
Apache Pulsar	https://pulsar.apache.org/	4.0.x
RabbitMQ	https://www.rabbitmq.com/docs	4.1.x
kubernetes	https://kubernetes.io/releases/	
CAPI	https://github.com/kubernetes-sigs/cluster-api/releases	

6.3. Assessment against CAMSS criteria (step 1 screening)

Based on the priorities and exclusions identified in chapter 4, standards and specifications within the top seven priority areas identified in Section 5.3 were selected for pre-screening. These priority areas were:

- Application Development
- Identity and Access Management (IAM)
- Data Catalogues
- API Management
- Container orchestration
- Security of data
- Transport of data

However, since collected standards and specifications regarding Application Development consisted exclusively of tools, it was also excluded from further evaluation (considered relevant but lower priority versus the other standards and specifications).

As a result, a list of 18 standards was considered to be relevant for the pre-screening on the selected criteria from CAMSS (see below table). Of this list, 16 passed the step 1 screening against the CAMSS criteria. In coordination with the Commission, a subset of 9 standards/ open specifications were further selected for the extensive step 2 screening.

Table 19 – Pre-selected candidates for pre-screening with CAMSS

Standards / Specifications	Priority area	Result of step 1 screening	Selected for step 2 screening
SAML (specification) [20]	Identity and Access Management	Passed	
OIDC (specification)	Identity and Access Management	Passed	
OAuth (specification)	Identity and Access Management	Passed	
OCI (specification)	API Management	Passed	✓
Open API (specification)	API Management	Passed	✓
SECA (specification)	API Management	Passed	✓
Async API (specification)	API Management	Passed	
Odata (standard/ specification)	API Management	Passed	
GraphQL (specification)	API Management	Passed	
OASIS-TOSCA (standard/specification)	Container Orchestration	Passed	✓
S3 API (specification)	Transport of data	Failed – controlled by Amazon, no open process to participate or raise objections. Also, specification not licensed on Frand [21] or royalty free basis	
XML (specification)	Transport of data	Passed	✓
JSON (specification)	Transport of data	Passed	✓
CSV (specification)	Transport of data	Passed	✓
CDMI (standard)	Transport of data	Passed	
SQL (specification)	Transport of data / Database as a Service	Passed	
ISO IEC 19941-2017	Transport of data	Failed - specification not free to access. ISO does not commit to royalty free licensing	

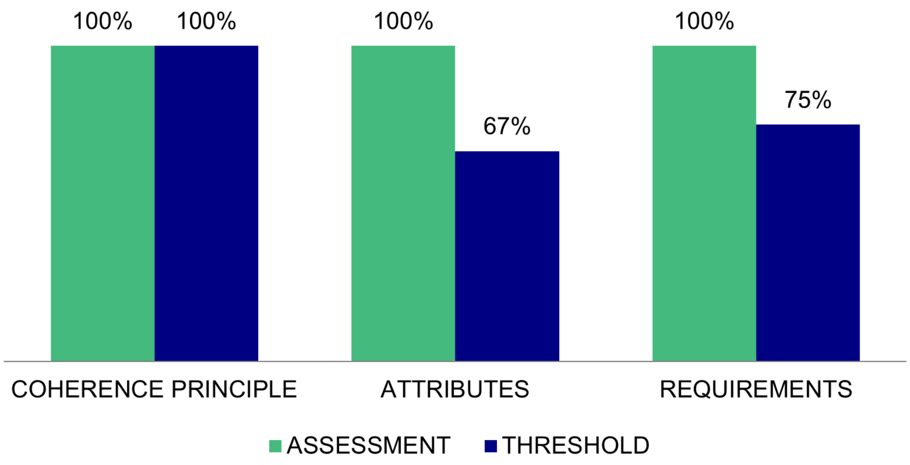
[20] SAML (Security Assertion Markup Language) was not further assessed under the operationalised criteria of Article 35 of the Data Act, as its functional role in enabling federated identity and cross-domain authentication is already addressed by OpenID Connect (OIDC), which would be a more suitable candidate.

[21] Frand = Fair, reasonable and non-discriminatory

Standards / Specifications	Priority area	Result of step 1 screening	Selected for step 2 screening
Apache Iceberg (specification)	Transport of data / Big data exchanges	Passed	✓

As an example, the following figure shows the results of the assessment of the step 1 screening for the OCI specification. As displayed in the graph, OCI meets the requirements in each category, and therefore qualifies for the broader step 2 screening on the operationalised criteria from the Data Act.

Figure 9 – Example of step 1 screening results for OCI



Source: Decision.

6.4. Assessment against operationalised criteria (step 2 screening)

In the second phase of the assessment, the selected standards and specifications were validated against the operationalised criteria (developed to evaluate compliance with Article 35(1) and (2) of the Data Act, see also Section 2.3).

The nine selected standards/ open specifications, which passed the step 1 screening, were reviewed in the step 2 screening to determine their level of compliance with the full set of operationalised criteria across all thematic categories (portability, interoperability, security, innovation, and functional equivalence).

Only those standards/specifications where all relevant criteria were at least partially or fully compliant with a certain threshold per category (e.g. portability of digital assets ([22]) were considered passed. This only applied to:

- Open API (100% compliance score on relevant criteria)
- OCI (98%)
- Oasis TOSCA (100%)
- SECA (97%)
- XML (100%)
- JSON (93%)

An example of the evaluation sheet of Open API has been included in Annex 8 – Evaluation sheet – step 2 screening – Open API.

The CSV specification had a score of 43% with several non-compliant categories (portability of digital assets, interoperability between data processing services, Not hindering innovation and Market acceptance & quality). The same applies for the Apache Iceberg with a compliance score of 23%.

([22]) All categories are: portability of digital assets, Interoperability between data processing services, No adverse impact on security and integrity, Not hindering innovation, Functional Equivalence, Market acceptance & quality.

7. Recommended actions in relation to implementation of the Data Act, Article 35

This chapter provides an overview of recommendations regarding candidates for inclusion in the Repository along with possible areas that could benefit from new standardization initiatives based on a gap analysis.

7.1. Recommendations regarding inclusion in the repository

As previously described, generic (applicable for all sectors or also called transversal) standards and specifications were selected for screening from amongst those proposed in the interviews, online survey and identified through own desk research.

Following the workshop, it was decided that the focus should be on PaaS related standards and specifications. As regards SaaS candidates, these were left out for this first assessment due to the high chance of being sector specific, which makes it more difficult to standardise without hindering innovation as noted by many stakeholders and EU cloud providers. Stakeholders further noted that the formalisation of sector specific standards and specifications should be customer led and preferably by groups representing a large part of the sector. Another pragmatic aspect considered was that sector specific standards and specifications might change more frequently than generic ones and hence require more frequent review / maintenance in the repository.

After screening the PaaS related generic candidates on compliance, the conclusion reached in the previous chapter was that there were no candidate PaaS related standards on interoperability aspects which passed the complete compliance screening. However, there were seven PaaS related open interoperability specifications, which did pass the compliance screening, namely Open API and SECA in respect to API Management, OCI and Oasis TOSCA in respect to Containers & Kubernetes and XML and JSON for Transport of data.

Before converting these generic open specifications into common specifications via an Implementing Act, it needs to be ensured that there is no ongoing or planned standard development by EU SDO's. If this is confirmed by EU SDO's, the EC can draft the Implementing Act and start consulting all relevant stakeholders on proposed common specifications. Although the Data Act prioritises harmonised standards (where available, under development or planned) above common specifications, it is not prescriptive as to whether in the absence of harmonised standards, further harmonised standards should be developed, or available open specifications should be used.

Once the common specifications are adopted, another Implementing Act can be introduced to include them in the repository, making these common specifications for interoperability mandatory. As the selected (and reviewed) candidates are all generic, they should apply to all service types. Before mandating however, it is important to verify that there is no overlap or conflict. Taking this into account, we recommend the following:

- As there is no technical overlap, both the generic **Open API** specification and **SECA** specification can be made mandatory.
- The **OCI** and **Oasis TOSCA** specifications relate to different aspects of container orchestration & Kubernetes; OCI on containerization and TOSCA on the topology and orchestration. Hence both can be included in the repository.
- **XML** and **JSON** could be candidates for inclusion. However, due to certain overlaps between them, further consideration is needed as to whether both can be made mandatory. In this context, it is also relevant to note that preferences for one or the other differ as regards vertical industry segments.
- **SQL** could potentially be included, but should be further investigated as there are multiple versions of SQL (many CSPs and new database management systems have extended the SQL language and created new versions) and it is not clear what the impact would be of mandating one version.

7.2. Recommendations regarding further analysis and new areas for standards development

During the course of the project, stakeholders were asked in interviews and via an online survey about areas where they consider there are gaps as regards interoperability standards or open interoperability specifications for data processing services. A gap was described as an area where it would be appropriate for the EU Commission to ask standard bodies to develop harmonised standards on interoperability and data portability for PaaS and Saas cloud services.

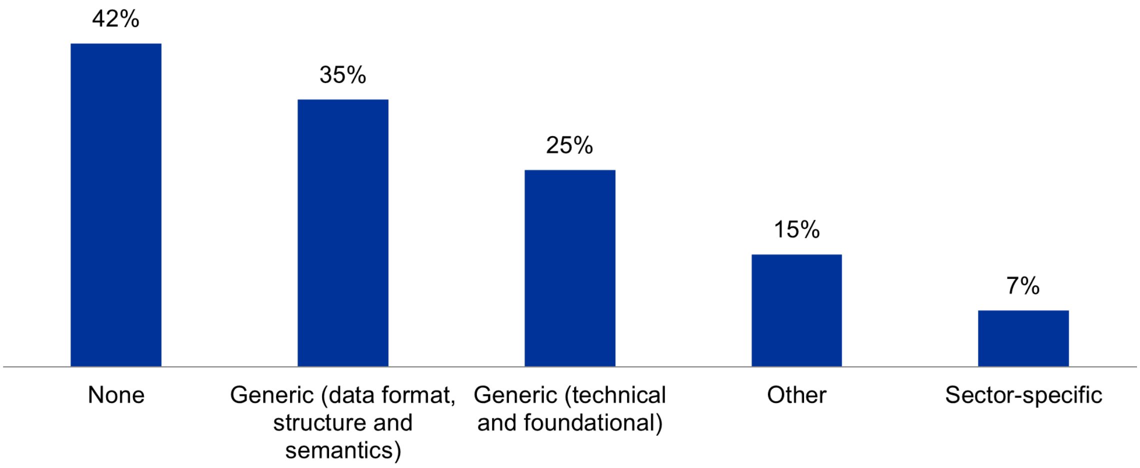
The following paragraph summarises stakeholders' main input from the online survey regarding the potential gap areas. Thereafter, we explain how we have 'mapped' this input onto the identified high-priority areas to highlight the specific aspect of interoperability concerned. Next, per defined priority area, we mapped the identified candidates (standards and open interoperability specifications) to see where there might be an indicated gap by stakeholder, but no possible candidates for inclusion in the repository. In such a situation, the development of a new harmonised standard could be warranted.

It should be noted that within the timeframe of this study it was not possible to perform a full compliance screening (step 1 and step 2) of all identified candidate standards and specifications. Thus, there might be a priority area where it may be advisable to first finish the (step 2) screening of certain candidates, before being able to conclude whether or not the development of a new harmonised standard by EU SDO's is required. Lastly, we added insights from the screening of existing suitable standards and open specifications in case a candidate 'closely failed'. Some of the screened candidates failed only on the basis that they did not comply with certain criteria, which could potentially be resolved. Improving compliance on these specific aspects could most likely lead to easier and faster adoption of a suitable harmonised standard or open interoperability specification compared with the process of developing a new harmonised standard from scratch.

7.2.1. Input online survey on perceived gaps

As can be seen in below figure, in the online survey, many respondents (42%) indicated that there were no gaps warranting further standard development. However, the majority of respondents (60%) pointed to gaps for generic standards or open specifications. Of this group, the majority (35%) pointed towards **data format, structure and semantics** and the second group (25%) to **technical and foundational** aspects.

Figure 10 – Possible GAPs warranting standards development, all respondents



Source: WIK-Consult Online survey on „Interoperability of data processing services" (12/12/2024-17/01/2025).

N=55 (all respondents). Q19: Indicate in which areas you consider there are gaps (no existing standards or open interoperability specifications which are candidates for formalisation) for which it would be appropriate for the EU Commission to ask standard bodies to develop harmonised standards on interoperability and data portability for PaaS and SaaS cloud services.

In addition, there was a group 'other' (15%) which was mostly critical towards standard development by a repository as they considered that this would undermine the industry's innovation and that absence of industry standards may also indicate healthy industry progression. Furthermore, this group pointed towards existing standardisation bodies and open-source communities, saying that they would be best placed to address any gaps that may arise.

The smallest group respondents (7%) indicating that there might be sector-specific gaps in interoperability standards, argued on the one hand that sector specific standards are needed (e.g. in telecommunication sector) but also that for the most part generic standards and specifications for interoperability and data portability are sufficient. Furthermore, this group noted that because of the (sector) specificity the standardisation here should be customer-led to avoid dominant vendors imposing their specifications.

These responses were similar across the subgroups 'Customer', 'Cloud provider' and 'Standardization Organisations', except for 'Hyperscalers' who mainly indicated the categories 'Other' and 'None'.

Respondents were also asked to **describe the reason** why the specific gap areas were chosen.

For the largest category 'generic - data format, structure and semantics' standards for the **data exchange between data spaces** were noted as an area in which further standardisation would be desirable.

- Customers highlighted the need to standardise semantic relationships, metadata and property-of-properties.
- A CSP suggested that that the first priority should be to develop semantic standards, before format. Other EU cloud providers pointed to evidence management storage for automatic audit of security compliance and standard data format definitions that make it possible to exchange data between similar services.

For the second largest category 'generic - technical and foundational', identity and access management (IAM) was mentioned as a gap.

- Cloud customers specified this further by noting that there is a gap in relation to common authentication and authorization mechanisms for industrial integration across different cloud services, open (cross platform) interfaces and APIs to enable data portability and interoperability between different providers and/or vendor solutions. In addition, minimal interoperability mechanisms (MIMs) for Data spaces were mentioned ().
- EU cloud providers see gaps regarding standards for similar capabilities/service offerings. e.g. GAIA-X ontology. Furthermore, they noted that there is a need for new ways to store data and re-engineer

database approaches for database-as-a-service as the current tech stacks are not well suited.

- Hyperscalers see a missing aspect in the field of workload movement which is not only limited to containers but also includes bare metal and virtual machines. Virtual machines are a foundation for which the data format of a VM image should be standardized like the open virtualization format (OVF).

7.2.2. Screened candidates and gaps per priority area

The following table, repeated from section 5.3, shows the identified priority areas for interoperability for PaaS cloud services. As described, these were used to 'map' the input from the online survey and the identified candidates. As previously explained, these priority areas are focused on PaaS and therefore this comparison of indicated gaps and identified candidate standards and open specifications is restricted to PaaS services. Recommendations are provided for each category below.

Table 20 – Recommended priority areas for PaaS (in green)

Scenario 2: 75/25 stakeholder/market size

Overall ranking PaaS	
Application Development	35%
Identity and Access Management (IAM)	30%
Data Catalogues	29%
API Management	28%
Container Orchestration and Management	21%
Security of data in transit and in rest	21%
Transport of data	17%
Big Data Exchanges	4%
DevOps and CI/CD	10%
Database as a Service (DBaaS)	3%

Source: WIK-Consult.

Application Development

- **Input from online survey**: there was no specific input in the online survey.
- **Identified candidates for this priority area**: as noted before, since collected standards and specifications regarding Application Development consisted exclusively of tools, which had a lower priority, and were excluded from screening.
- **Recommendation**: despite being the highest ranked priority area, stakeholders did not seem to perceive that there was a gap in

interoperability standards in this area. We therefore do not recommend any specific action at this time in relation to the development or formalisation of standards.

Identity and Access Management (IAM)

- **Input from online survey**: IAM is clearly mentioned as a gap area, as well as common authentication and authorization mechanism for industrial automation.
- **Identified candidates for this priority area**: there were 11 candidates for IAM (see below table). Of these, 2 were preselected in coordination with the Commission (OIDC, SAML) for step 1 screening and both passed. However, they were not selected for step 2 screening and therefore we cannot recommend any standard or specification for this priority area at this time. Considering that this is the second ranked priority area and the input from the survey, this should be considered a gap that potentially needs to be addressed by identifying candidates for inclusion in the repository and/or recommending new standard development by European SDO's.
- Recommendations:
  - We recommend that all 11 candidates identified should be subject to a full screening (many of them were only screened on step 1 requirements). Particular attention should be given to the Oauth standard and the OIDC open specification, which are the de facto standards for delegated authentication and the SAML standard, which is widely used for federated sign-on.
  - Furthermore, European SDO's could investigate the possible development of a harmonized European standard for federated and delegated identity and access management as it is foundational to all Data Act provisions (it is a pre-requisite for secure interoperability). It would be built on top of the OIDC, OAuth and SAML open specifications. This would require:
    - To perform the second stage of screening of the IAM open specifications to ensure they meet the Data Act requirements;
    - To develop a standard for IAM portability and federation across Data Spaces, covering mechanisms for cross-trust domain identity exchange, policy enforcement, and credential portability;
    - To define common European metadata and ontology models for IAM, supporting semantic interoperability and cross domain discoverability of identities, roles and access policies; and

- To define interoperability profiles and conformance testing procedures in order to ensure interoperability between sovereign and hyperscale cloud environments.

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
Oauth/ IETF RFC 6749	Transversal	Standard	Identity & Access Management	OAuth 2.0 is a widely adopted authorization protocol
OIDC (OpenID Connect)	Transversal	Specification	Identity & Access Management	OIDC is built on top of OAuth 2.0 and used for authentication (not just authorization). Standard for federated identity and single sign-on (SSO).
SAML	Transversal	Specification	Identity & Access Management	XML-based framework for authentication and authorization
W3C SSI / DID	Transversal	Specification	Identity & Access Management	For decentralized, privacy-preserving digital identity. Core to SSI ecosystems, identity wallets, and trust frameworks — emerging in cloud identity use cases.
SCIM	Transversal	Specification	Identity & Access Management	Identified in priority areas by stakeholders. standardized protocol for managing user identity in cloud apps. Enables automatic provisioning/deprovisioning between identity providers and SaaS platforms.
FIDO	Transversal	Specification	Identity & Access Management	Identified in priority areas by stakeholders. defines passwordless authentication protocols, including biometrics and security keys.
W3C/ FIDO WebAuthn	Transversal	Specification	Identity & Access Management	Part of the FIDO2 suite. It's a W3C standard for public key-based web authentication in browsers and applications.
ADFS	Transversal	Tools	Identity & Access Management	An enterprise identity federation system supporting SAML and OIDC. Enables SSO and claims-based access control in Microsoft and hybrid cloud environments.
Entra ID (formerly Azure AD)	Transversal	Tools	Identity & Access Management	Microsoft's cloud identity platform.
OpenID4VCI	Transversal	Specification	Identity & Access Management	Extension of oAuth
OpenID4VP	Transversal	Specification	Identity & Access Management	Extension of oAuth

Analysis of gaps for Data Catalogues

- **Input from the online survey**: multiple possible standards / specifications relating to this category were named in the survey (W3C Dcat V3, ETIS ISG CIM, Smart Data Model, SHACL, Semic GeoDCAT-AP V3, DPROD, HL7 FHIR). Data catalogues were not specifically mentioned as a gap area. However, generic standards in respect to data format, structure and semantics have been indicated as a key are of focus for possible standard development.

- **Identified candidates for this priority area**: the initial screening resulted in 2 relevant candidates for Data catalogues. These are listed in the table below. In coordination with the Commission, none of these were preselected for screening, so it is not possible to say at this time whether there are candidates which should be considered as priorities and would pass screening.
- **Recommendation**: we recommend to verify with stakeholders whether the 2 possible candidates have market acceptance and should be screened for consideration for inclusion in the repository. In addition, European SDO's could be asked to develop standards regarding data format, structure and semantics for Data catalogues.

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
ISO/IEC 11179	PaaS	Standard	Data Catalogues	Defining and managing metadata registries, widely used in data governance, data integration, and semantic interoperability.
OAI-PMH	Transversal	Protocol	Data Catalogues	Open-source message broker that implements AMQP. used protocol for harvesting metadata from repositories. Especially relevant in open science, digital libraries, and semantic web applications.

Analysis of gaps for API Management

- **Input from the online survey**: no specific input was provided on gaps related to API Management. However, data semantics is indicated as the main focus area in the online survey. Standardised data semantics together with standardised data models are crucial for API management.
- **Identified candidates for this priority area**: the initial screening resulted in 6 relevant candidates (see below table) to which the SECA specification was later added after stakeholder input. The Open API specification both passed the step 1 and 2 screening. However, there is currently insufficient market information available on SECA. On the one hand, it could qualify as a relevant candidate, as it was developed by major EU industry players, which supports its potential market importance. On the other hand, given its recency, there are no clear indications yet of whether it will achieve broader adoption.
- **Recommendation**: Formally, no gaps as there are candidates identified for inclusion in the repository. However, European SDO's could be asked to investigate possible new standard development in the area of data models and semantic for API management. The study team recommends treating SECA as a promising but still immature candidate, given that its

specifications are evolving and not yet stabilized, and its governance mechanisms have yet to be broadly demonstrated. If omitted, existing frameworks such as GAIA-X, CISPE, and CNCF provide partial compensation. Once mature, SECA could make a significant contribution to strengthening the EU's cloud sovereignty and interoperability landscape.

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
GraphQL	PaaS	Specification	API & API Management	Identified in priority areas by stakeholders. Query language and runtime for APIs
Open API	PaaS	Specification	API & API Management	Identified in priority areas by stakeholders. standard, machine-readable interface for RESTful APIs
Async API	PaaS	Specification	API & API Management	Identified in priority areas by stakeholders. for defining asynchronous event-driven APIs, like OpenAPI is for REST
OData	PaaS	Specification	API & API Management	Identified in priority areas by stakeholders. Enables interoperable data access via APIs. OASIS Standard
CloudEvents	PaaS	Specification	API & API Management	Defines a standardized event format for cloud-native event-driven systems. CNFC
OGC API standards	PaaS	Standard	API & API Management	Define RESTful web service interfaces for geospatial data (features, coverages, maps)

<u>Analysis of gaps for Container Orchestration and Management</u>

- **Input from the online survey**: no specific input on gaps related to Container orchestration and management was provided.
- **Identified candidates for this priority area**: the initial screening resulted in 6 candidates (see below table) of which 2 (OCI and Oasis TOSCA) were selected and step 1 and 2 screened. Both passed, so could be included in the repository.
- **Recommendation:** No gap identified. Both OCI and Oasis TOSCA specifications can be included in the repository as they relate to different aspects of container orchestration & Kubernetes; OCI on containerization and TOSCA on the topology and orchestration).

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
Cri-O	PaaS	Tools	Container Orchestration and Management	Tool or Technology Platform, not exclusively a standard / specification
Docker	PaaS	Tools	Container Orchestration and Management	Tool or Technology Platform, not exclusively a standard / specification

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
Podman	PaaS	Tools	Container Orchestration and Management	Tool or Technology Platform, not exclusively a standard / specification
Helm	PaaS	Tools	Container Orchestration and Management	Tool or Technology Platform, not exclusively a standard / specification
Open Container Initiative (OCI)	PaaS	Specification	Container Orchestration and Management	OCI defines interoperable container formats and runtime behaviors. OCI Runtime Specification, OCI Image Specification, OCI Distribution Specification
OASIS TOSCA	PaaS	Specification	Container Orchestration and Management	Modeling language to define cloud application topologies and orchestrate deployment across multiple providers. Used to automate deployment and lifecycle of complex apps.

Analysis of gaps for Security of data in transit and in rest

- **Input online survey**: no specific input on gaps related to Security of data in transit and in rest was provided.
- **Identified candidates for this priority area**: the initial screening resulted in 10 candidates (see below table) of which none were selected for screening. As this is one of the priority areas, this is an area which could warrant further investigation by stakeholders and European SDO's.
- Recommendation:
  - we recommend verifying with stakeholders and European SDO's whether there is a need to mandate standards or specifications in this area either via inclusion in the repository, or via new standard development. We propose to start with the following:
    - Develop a European Key Management Services (KMS) Portability Standard covering a common API for Customer-Managed Keys (CMK) lifecycle, envelope-encryption metadata profile, and audit requirements, then specify conformance tests and certification criteria.
    - Specify an Encrypted Data Packaging format for objects, datasets or virtual machines (including Open Virtualisation Format (OVF) encryption profile), enabling portable data encryption across providers.

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
Istio	PaaS	Tools	Security of Data in Transit and at Rest	Tool or Technology Platform, not exclusively a standard / specification
Oasis PKCS	Transversal	Specification	Security of Data in Transit and at Rest	Cryptographic messaging, encryption, and signing
ISO/IEC 27018:2019	Transversal	Standard	Security of Data in Transit and at Rest	Not specific to the cloud. Defines controls for protecting personal data in public clouds, complementing ISO/IEC 27001/27002.
Oasis STIX	Transversal	Specification	Security of Data in Transit and at Rest	Cybersecrutiy related ==> Not in stakeholder top priorities. standard format for sharing cyber threat intelligence, widely used in SOCs and cloud threat monitoring.
Oasis TAXII	Transversal	Specification	Security of Data in Transit and at Rest	Used to exchange cyber threat intelligence (CTI) data, often alongside STIX. It defines secure sharing protocols, making it a security-focused transport mechanism.
EN ISO/IEC 27017:2021	Transversal	Harmonised Standard	Not applicable, Security of Data in Transit and at Rest	Defines security practices tailored for cloud environments, especially in multi-tenant and shared infrastructure contexts.
NIST SP 800-145 & 53	Transversal	Standard	Not applicable, Security of Data in Transit and at Rest	SP 800-145 defines cloud computing models (IaaS, PaaS, SaaS). SP 800-53 provides security and privacy controls
X.509 (IETF RFC 5280)	Transversal	Specification	Security of Data in Transit and at Rest	Defines the structure of digital certificates (used in TLS, S/MIME, etc.)
TLS/ RFC 8446	Transversal	Standard	Security of Data in Transit and at Rest	TLS is the core protocol for securing data in transit over the internet, including HTTPS, SMTP, IMAP, etc.
ISO/IEC 27017/27018	Transversal	Standard	Not Applicable, Security of Data in Transit and at Rest	Governance. 27017: InfoSec controls for cloud service providers and customers. 27018: Privacy protection of personal data in public clouds.

Analysis of gaps for Transport of data

- **Input from the online survey**: customers emphasized the need to ensure a data exchange that includes semantic relationships, metadata and property-of-properties.
- **Identified candidates for this priority area**: the initial screening resulted in 21 candidates, which is the highest number for any priority area (see table below).

  - 7 of the candidates were selected for screening, ISO/IEC 17203:2017 OVF was excluded as it was less relevant for cloud interoperability and Apache Iceberg was added to the list based on stakeholder input. Of the 8 selected, 2 failed the step 1 screening (S3 API and ISO 19941-2017); the first one as it is closed source, managed exclusively by AWS without FRAND or royalty free licensing and the second one as ISO does not commit to royalty free licensing.
  - 5 were selected for extensive step 2 screening (XML, JSON, CSV, SQL and Apache Iceberg). CSV and Apache failed, but XML and JSON passed with a high compliance score (92-100%). Note, the number of applicable criteria was however quite low (between 21 and 36%), but this should not be a problem as a certain specification can only relate to certain aspects of cloud interoperability addressed in the Data Act and hence not all criteria are relevant.

- **Recommendation:** the ISO standard failed in the step 1 screening due to a (minor) aspect (paid documentation). It may be appropriate to review whether this could be accepted and converted into a European standard. This could be work for a European SDO. Although the XML/JSON specifications passed, we recommend reviewing for which sectors there should apply before mandating them. We recommend not to include SQL for now as each CSP seems to have its own version. In addition, European SDO's could investigate possible standard development related to data format and structures which enable the exchange of data between similar service types of data processing services.

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
S3 Api	PaaS	De Facto Standard	Transport of Data	
ISO 19941:2017	Transversal	Standard	Transport of Data	
CBOR (IETF RFC 8949)	PaaS	Standard	Transport of Data	Backbone interoperability. Compact binary format used to serialize data for transmission
Protocol Buffers	PaaS	Specification, Tools	Transport of Data	Identified in priority areas by stakeholders. language-neutral serialization format
CDMI (Cloud Data Management Int.)/ ISO/IEC 17826:2022	PaaS	Standard	Transport of Data	Defines a RESTful interface for managing cloud storage and data
AMQP (ISO/IEC 19464)	PaaS	Specification	Transport of Data	Messaging protocol for secure and reliable message transport. Formalized as an ISO/OASIS standard.
MQTT (ISO/IEC 20922)	PaaS	Specification	Transport of Data	Lightweight messaging protocol optimized for IoT, cloud-native messaging. OSAIS/ ISO IEC

Standard or Specification	Cloud Tier	Tool / True Standard	Priority Areas	Comments
RFC 6455 Websocket Protocol	Transversal	Standard	Transport of Data	Enables bidirectional, real-time communication over a single TCP connection
RFC 9556 IoT Devices cloud connectivity	PaaS	Standard	Transport of Data	Defines best practices and models for connecting IoT devices to cloud platforms
JSON/ IETF RFC 8259	PaaS	Specification	Transport of Data	Widely used data interchange format in cloud systems
XML	PaaS	Specification	Transport of Data	Common format in enterprise systems and cloud-based document/data exchanges
CEN/TS 18026:2024	Transversal	Technical Specification	Transport of Data	Provides structured data flow descriptions between cloud roles (e.g., providers, customers), promoting interoperability and traceability of cloud data exchange
ISO/IEC 17203:2017	Transversal	Standard	Transport of Data	Focuses on the semantic and technical aspects of cloud portability — migration, interoperability between services and clouds.
oneM2M	PaaS	Standard/ Framework	Transport of Data	Global standard for IoT interoperability, enabling communication and data sharing between devices and clouds
IEEE 2302-2021 (SIIF)	Transversal	Standard	Transport of Data	Defines a framework for intercloud interoperability, addressing federation, trust, identity, and service portability between cloud platforms.
SQL	Transversal	Standard/ Scripting Language	Transport of data/ Database as a Service (DBaaS)	Tool or Technology Platform, not exclusively a standard / specification
IEEE 1616.1-2023	PaaS	Standard	Transport of Data	Vertical segment: automotive. Defines data exchange standards for vehicle-to-everything (V2X) communication
ISO 10303	SaaS	Standard	Transport of Data	Vertical segment: tranversal industry. Defines a mechanism to exchange product manufacturing data. Widely used in CAD/PLM systems
IPv6	Transversal	Specification	Transport of Data	Foundational internet protocol for network addressing, replacing IPv4
CSV	Transversal	Specification/ Scripting Language	Transport of Data	

As a last comment on the gap analysis, we note that while we made use of the priority areas identified for this purpose, it would be better for the next assessment to use the defined service types (and grouping) instead of the (rougher) market-based priority areas. Stakeholders are likely to have more specific input per service type. Moreover, stakeholders noted in the workshop that they would be willing to be consulted in updating these service types due to the dynamic character of the cloud markets and to ensure that their expertise is considered.

Literature

Al-Sayed et al (2020). M.M. Al-Sayed, H.A. Hassan and F.A. Omara, CloudFNF: An ontology structure for functional and non-functional features of cloud services, Journal of Parallel and Distributed Computing (2020), doi: https://doi.org/10.1016/j.jpdc.2020.03.019.

Jula and Othman (2013). A. Jula, E. Sundararajan, Z. Othman, “Cloud computing service composition: A systematic literature review,” Expert systems with Applications, vol. 41, issue 8, pp. 3809-3824, 2014. https://doi.org/10.1016/j.eswa.2013.12.017.

Komchak (2024). Khomchak, M. (2024). A Comprehensive Taxonomy of Modern Public Cloud Services for Infrastructure Selection. *International Journal of Computing*, *23*(3), 468-475. https://doi.org/10.47839/ijc.23.3.3667.

Kostoska et al (2016). Kostoska, M., Gusev, M., & Ristov, S. (2016, September). An overview of cloud interoperability. In *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)* (pp. 873-876). IEEE.

Nickerson (2013). Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, *22*(3), 336-359. Paper removed as of 24 January 2024 at request of the author.

Rimal et al (2009). Rimal, B. P., Choi, E., & Lumb, I. (2009, August). A taxonomy and survey of cloud computing systems. In 2009 fifth international joint conference on INC, IMS and IDC (pp. 44-51).

Rosian and Hagenhoff (2021). M. Rosian, P. Hagenhoff, B. Otto, (2021). Towards a Holistic Cloud Computing Taxonomy: Theoretical & Practical Findings. In AMCIS. Proceedings of the Twenty-Seventh Americas Conference on Information Systems AMCIS’2021, Montreal, Canada, 2021, pp. 1-10

Sikeridis and Rimal (2017). D. Sikeridis, I. Papapanagiotou, B. P. Rimal, M. Devetsikiotis, “A comparative taxonomy and survey of public cloud infrastructure vendors,” arXiv preprint arXiv:1710.01476, 2017.

Annex 1 – Literature research regarding categories of cloud functions

Literature was researched with publication date from 2009 onwards until 2024 using Google search / Google Scholar and search criteria ‘taxonomy for PaaS/SaaS categories’ and ‘functional categories for PaaS / SaaS cloud services’.

The following articles were selected based on their ‘fit’ and reviewed:

- Rimal, B. P., Choi, E., & Lumb, I. (2009, August). A taxonomy and survey of cloud computing systems. In *2009 fifth international joint conference on INC, IMS and IDC* (pp. 44-51). Ieee.
- A. Jula, E. Sundararajan, Z. Othman, “Cloud computing service composition: A systematic literature review,” Expert systems with Applications, vol. 41, issue 8, pp. 3809-3824, 2014. https://doi.org/10.1016/j.eswa.2013.12.017.
- D. Sikeridis, I. Papapanagiotou, B. P. Rimal, M. Devetsikiotis, “A comparative taxonomy and survey of public cloud infrastructure vendors,” arXiv preprint arXiv:1710.01476, 2017.
- Al-Sayed et al (2020). M.M. Al-Sayed, H.A. Hassan and F.A. Omara, CloudFNF: An ontology structure for functional and non-functional features of cloud services, Journal of Parallel and Distributed Computing (2020), doi: https://doi.org/10.1016/j.jpdc.2020.03.019 .
- Rosian and Hagenhoff (2021). M. Rosian, P. Hagenhoff, B. Otto, (2021). Towards a Holistic Cloud Computing Taxonomy: Theoretical & Practical Findings. In AMCIS. Proceedings of the Twenty-Seventh Americas Conference on Information Systems AMCIS’2021, Montreal, Canada, 2021, pp. 1-10.
- Komchak (2024). Khomchak, M. (2024). A Comprehensive Taxonomy of Modern Public Cloud Services for Infrastructure Selection. International Journal of Computing, 23(3), 468-475. https://doi.org/10.47839/ijc.23.3.3667

The literature shows that from the beginning of the cloud market, there have been efforts to provide a taxonomy for cloud services, mainly to assist potential customers in the selection and comparison process.

Starting with Rimal et al (2009) providing a rudimentary categorization for cloud services starting with the layered architecture of cloud services (Hardware as a Service, IaaS, PaaS, SaaS). Their main categories for PaaS/SaaS were ([23]):

- Computing Architecture
- Virtualisation Management
- Service (runtime interpreter)
- Load balancing
- Fault tolerance
- Interoperability (between different platforms)
- Storage (model)
- Security
- Programming Framework

Jula and Othman (2013) performed a systematic literature review using an extensive taxonomy to assist in the selection and optimisation of cloud services with a focus on the three service models (SaaS, PaaS, IaaS) and the four deployment models (private cloud, public cloud, community cloud and hybrid cloud). They found in the literature that response time, availability and reliability are the main parameters beside cost. No complete taxonomy was published however.

Sikeridis and Rimal (2017) also aimed to assist the procurement of cloud services by providing a taxonomy by looking at the offered services of four dominant cloud vendors in 2017 (AWS, MS, Google, IBM). Following functional categories were identified for PaaS/SaaS:

- Big data management (analysis)
- Data Pipelines (for enabling streaming services)
- Machine Learning
- Language processing & Speech recognition AI
- Image recognition AI

And in addition, from their Table XI ([24]):

- Identity & Access Management
- Security Assessment
- Hardware Based Security / Secure Key Management

[23] Table 3. Cloud computing PaaS and SaaS Provider, Page 50.

[24] Table XI- Additional services, Page 18.

- Directory Services / Single & Multi-Factor Authentication
- Network Security & Firewall
- Management Tools
- Monitoring, Logging, Error reporting
- Software Development
- Deployment Templates
- API Management
- Mobile App Development
- Mobile App Testing & Analytics
- IOT Platform & Development Solutions

Al-Sayed et al (2020) reviewed the existing taxonomies and proposed a more comprehensive cloud ontology focusing on three dimensions: 1) functionality classification, 2) non-functional features (QoS, configuration) and 3) representation of semantic relations. The focus shifts here from layer-based classifications to functional classification. For the operationalisation of the interoperability obligation in the Data Act, the functional classification is relevant. When in the future, specific use cases are also used to specify even more detailed service types, QoS properties like reliability, performance (via latency, response time and throughput) and availability (via time to repair might become relevant ([25]).

The authors defined following functional categories:

- Data Governance, consisting out of Data Migration, Data portability, Data Interoperability and Data and Information Protection.
- Data Storage consisting out of File Storage, Block Storage, Object Storage, Data Center, Recovery and Back-up and Streaming and Multimedia.
- Data Manipulation and Analysis consisting of: Big Data Analysis, Business Intelligence, Real-time Search and Analytics Engine, Web Log Analyzer and General Data Analysis.
- Business functions like Business Project Management, Business Resource management, Productivity, but also Enterprise Resource Planning (ERP) and Integration.
- Development and Testing Functionalities like Application Design and Modelling, Application Development: and Deployment.

([25]) See para 5.3 of Al-Sayed et al (2020).

- User Supporting Functionalities like Cloud Broker, Cloud Service Discovery (CSD), Service Management and Systems Administration.
- Cloud Management Systems (CMS) with Cloud Business Support Functions, Operational Support Functions, Service Transition Management, Service Operation Management and Continual Service Improvement (CSI).

Rosian and Hagenhoff (2021) also developed a cloud computing taxonomy based on structured literature review and empirical validation via workshops with participants from the industry and science. They followed the taxonomy development method according to Nickerson et al (2013) based on 7 consecutive steps. First, they defined key characteristics of cloud computing and chose meta-dimensions based on the Kano model of customer satisfaction (basic needs, performance needs and Attractive needs). This is reflected in following table. However, no specific categorisation was published.

Final Cloud Computing Taxonomy Roslan et al (2021)

Meta-Dimension (MD$_n$)	Dimension (D$_{nm}$)	Characteristics (C$_{nmk}$)			
Basic needs	Deployments	Private	Public	Hybrid	Community
	Services	IaaS	PaaS	SaaS	
	Pricing	On-Demand	Subscription	Freemium	
Performance needs	Security	Infrastructure	Application	IAM	Data
	Governance	Policies	SLAs		
	Compliance	Certifications	Regulation	Frameworks	
Attractive needs	Adapted Trends	Big Data	IoT	AI	Digital Twin
	Cloud Trends	Multi-Cloud	Cloud-Native		

Source: Rosian et al (2021), Table 2. Final Cloud Computing Taxonomy, Page 4.

Komchak (2024) developed a comprehensive taxonomy of cloud services based on an extensive literature research of existing taxonomies, solutions provided by the leading providers of cloud services worldwide and definitions on service models from NIST. Starting point was the identification of the 12 worldwide leading cloud vendors based on market share and other parameters such as service offering, innovation, customer feedback and global footprint ([26]). This was used as basis for further development of the taxonomy. Thereafter, the service portfolios were analysed to identify commonalities and unique offerings. For this review, following criteria were used: primary function, usage & popularity, inter-dependability, (similar) scalability and security & compliance.

([26]) AWS, MS Azure, Google Cloud Platform, Alibaba Cloud, Oracle Cloud Infrastructure, Tencent Cloud, IBM Cloud, OVH cloud, Rackspace Technology, Salesforce, SAP and Huawei Cloud.

This led to the following list of 24 key cloud features:

- Compute
- Storage
- Databases
- Networking
- Developer Tools
- Analytics & Big Data
- AI & Machine learning
- Security & Identity
- IoT
- Migration & hybrid Cloud
- Management & Governance
- Mobile Services
- Enterprise Integration
- End User Computing
- Front-end Web Services
- Business Applications
- Blockchain
- Gaming
- Multimedia Services
- Content Delivery Networks (CDN)
- Satellite Services
- Robotics
- Quantum Computing
- VR/AR

These key cloud features were further split in sub-categories. Annex 2 provides an overview of the detailed categories according Komchak (2024) including a useful mapping against the current service offering of the leading vendors. This detailed mapping exercise could be used for future reviews when it is necessary to compare services from different providers to assess whether they belong to ‘the same service type’.

Following table shows the result of Komchak's mapping of cloud service offerings from the 8 leading providers worldwide.

Detailed mapping of 2024 cloud offerings on the functional subcategories of Komchak (2024)

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Compute				
Virtual Machines	EC2	Azure VM	Compute Engine	Elastic Compute Service (ECS)
Containers & Kubernetes	EKS, ECS	AKS	Kubernetes Engine	Container Service for Kubernetes
Serverless Functions	Lambda	Azure Functions	Cloud Functions	Function Compute
Batch & High-Performance Computing	AWS Batch, EC2 Spot Instances	Azure Batch	Preemptible VMs	Batch Compute
Storage				
Object Storage	S3	Blob Storage	Cloud Storage	OSS
Block Storage	EBS	Disk Storage	Persistent Disk	Block Storage
File Systems	EFS	Azure Files	Filestore	NAS
Cold & Archival Storage	Glacier, S3 IA	Cool and Archive Blob Storage	Nearline, Coldline, Archive	Cold Archive
Databases				
Relational Databases	RDS, Aurora	Azure SQL Database	Cloud SQL	ApsaraDB RDS
NoSQL Databases	DynamoDB	Cosmos DB	Firestore, Bigtable	Table Store
In-memory Databases	ElastiCache	Azure Cache for Redis	Memorystore	ApsaraDB for Redis
Database Migration Services	DMS	Azure Database Migration Service	BigQuery Data Transfer Service	DTS
Networking				
Virtual Private Cloud (VPC)	VPC	Virtual Network (VNet)	VPC	Virtual Private Cloud
Content Delivery Network (CDN)	CloudFront	Azure CDN	Cloud CDN	Alibaba Cloud CDN
Load Balancing	Elastic Load Balancing (ELB)	Load Balancer	Load Balancer	Server Load Balancer
Network Security & Firewalls	Security Groups, NACLs, WAF	Azure Firewall, Network Security Groups	Cloud Armor, Firewall Rules	Security Center
Developer Tools				

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Integrated Development Environments (IDE)	Cloud9	Azure DevOps Services, Visual Studio	Cloud Code	Cloud IDE
Continuous Integration & Deployment (CI/CD)	CodePipeline, CodeBuild	Azure Pipelines	Cloud Build	CodePipeline
Source Control	CodeCommit	Azure Repos	Cloud Source Repositories	CodeSource
Monitoring & Logging Tools	CloudWatch, CloudTrail	Azure Monitor, Log Analytics	Stackdriver (Cloud Monitoring & Logging)	ARMS, Log Service
Analytics & Big Data				
Data Lakes	S3, Lake Formation	Azure Data Lake Storage	Cloud Storage, Dataproc	Data Lake Storage
Big Data Processing	EMR	Azure HDInsight, Databricks	Dataproc, Dataflow	E-MapReduce
Real-time Analytics	Kinesis	Azure Stream Analytics	Dataflow, Pub/Sub	Stream Compute
Data Warehousing	Redshift	Azure Synapse Analytics	BigQuery	MaxCompute
AI & Machine Learning				
Machine Learning Platforms	SageMaker	Azure Machine Learning	AI Platform Training, AI Platform Prediction	Machine Learning Platform for AI
AI Development Tools	Deep Learning AMIs	Azure Machine Learning Studio	AI Hub, AI Platform Notebooks	PAI Studio
Pre-trained AI Services	Rekognition, Polly, etc.	Azure Cognitive Services	Vision AI, Speech-to-Text, etc.	Image Search, Intelligent Speech Recognition
Data Labeling & Training	SageMaker Ground Truth	Azure Machine Learning Data Labeling	AI Platform Data Labeling	Data Annotation
Security & Identity				
Identity & Access Management (IAM)	IAM	Azure Active Directory	Identity & Access Management (IAM)	Resource Access Management (RAM)
Threat Detection	GuardDuty	Azure Security Center, Sentinel	Security Command Center, Event Threat Detection	Threat Detection Service
Data Protection	Key Management Service (KMS), Secrets Manager	Azure Key Vault, Disk Encryption	Key Management Service, Secret Manager	KMS, Secret Manager

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Compliance Management	Config, Macie	Azure Policy, Blueprints	Cloud Asset Inventory, Security Health Analytics	Cloud Config
IoT				
IoT Device Management	IoT Core	Azure IoT Hub	Cloud IoT Core	IoT Platform
IoT Data Analysis	IoT Analytics	Azure Stream Analytics	Cloud IoT Core	IoT Platform
Edge Computing	Greengrass, Wavelength	Azure IoT Edge	Edge TPU, Anthos	Link Edge
IoT Security	IoT Defender	Azure Security Center for IoT	Cloud IoT Core	IoT Platform
Migration & Hybrid Cloud				
Migration Tools	Migration Hub, Server Migration Service	Azure Migrate	Migrate for Compute Engine	Migration Platform
Hybrid Cloud Platforms	Outposts	Azure Arc, Azure Stack	Anthos	Hybrid Cloud
Disaster Recovery	Disaster Recovery	Azure Site Recovery	Cloud Disaster Recovery	Hybrid Backup Recovery
Hybrid Connectivity	Direct Connect, VPN	Azure ExpressRoute, VPN Gateway	Cloud Interconnect, Cloud VPN	Express Connect, VPN Gateway
Management & Governance				
Infrastructure Automation	CloudFormation, OpsWorks	Azure Resource Manager, Bicep	Deployment Manager, Cloud Composer	ROS, Terraform Provider
Cost Management	Cost Explorer, Budgets	Azure Cost Management and Billing	Cost Management tools	Cloud Cost Management
Resource Organization	Organizations, Control Tower	Azure Management Groups, Blueprints	Resource Manager, Folders	Resource Directory
Governance & Compliance Tools	Config, Service Catalog	Azure Policy, Blueprints	Policy Intelligence, Security Command Center	Cloud Config, Cloud Governance Dashboard
Mobile Services				
Mobile Backend-as-a-Service (MBaaS)	AWS Amplify	Azure Mobile Apps	Firebase	mPaaS
App Development Platforms	AWS Mobile	Azure Mobile Apps	Firebase, App Engine	Mobile Development Platform

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Mobile Analytics	AWS Mobile Analytics	Azure Mobile Engagement	Firebase Analytics	mPaaS
User Engagement Tools	Pinpoint	Azure Notification Hubs	Firebase Cloud Messaging	Mobile Push
Enterprise Integration				
Service Integration	AppFlow, Step Functions	Logic Apps	Cloud Composer	Integration Service
API Management	API Gateway	Azure API Management	Apigee API Platform	API Gateway
Enterprise Messaging	SNS, SQS	Azure Service Bus	Pub/Sub	Message Service
Business Process Automation	Step Functions	Logic Apps, Power Automate	Cloud Workflows	BPM Platform
End User Computing				
Virtual Desktops	WorkSpaces	Azure Virtual Desktop	Google Workspace	E-Desktop Service
Collaboration Tools	Chime	Teams (part of Office 365)	Google Workspace	Alibaba WorkMail
Remote App Streaming	AppStream 2.0	Azure RemoteApp	n/a	n/a
Workspace Security	WorkDocs	Intune	Google Workspace Security Center	n/a
Front-end Web & Mobile				
Web Hosting	Lightsail	Azure Web Apps	App Engine	Web App Service
Mobile Web Services	Amplify	Azure Mobile Apps	Firebase Hosting	mPaaS
Progressive Web Apps	n/a	n/a	Firebase	n/a
Web Security	WAF & Shield	Azure Web Application Firewall	Web Security Scanner	Web Application Firewall
Business Applications				
Customer Relationship Management (CRM)	n/a	Dynamics 365 for Sales	n/a	n/a
Enterprise Resource Planning (ERP)	n/a	Dynamics 365	n/a	n/a

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Human Capital Management (HCM)	n/a	Dynamics 365 Human Resources	n/a	n/a
Supply Chain Management	n/a	Dynamics 365 Supply Chain Management	n/a	n/a
Blockchain				
Blockchain Platforms	Managed Blockchain	Azure Blockchain Service	Cloud Spanner (for certain applications)	Blockchain as a Service
Smart Contract Development	n/a	n/a	n/a	n/a
Blockchain Networking	n/a	Azure Blockchain Workbench	n/a	n/a
Cryptography Services	KMS, CloudHSM	Azure Key Vault	Cloud Key Management Service	KMS
Gaming				
Game Development Platforms	n/a	PlayFab	n/a	Game Development Platform
Multiplayer Servers	n/a	PlayFab Multiplayer	n/a	n/a
Real-time Game Analytics	n/a	PlayFab Insights	n/a	n/a
Game Asset Management	n/a	PlayFab Content	n/a	n/a
Multimedia Services				
Media Conversion & Encoding	Elastic Transcoder	Azure Media Services		ApsaraVideo for VOD
Media Storage & Delivery	S3, CloudFront	Azure Blob Storage, Azure CDN	Cloud Storage, Cloud CDN	OSS, Alibaba Cloud CDN
Interactive Media Services	Interactive Video Service	n/a	n/a	n/a
Media Analytics	Kinesis Video Streams	Azure Video Analyzer	n/a	n/a
Content Delivery Networks (CDN)				
Content Distribution	CloudFront	Azure CDN	Cloud CDN	Alibaba Cloud CDN
Content Acceleration	CloudFront	Azure Front Door	Cloud CDN	Alibaba Cloud CDN
Edge Caching	CloudFront	Azure CDN	Cloud CDN	Alibaba Cloud CDN
Traffic Management	Route 53, Global Accelerator	Azure Traffic Manager	Cloud Load Balancing	Alibaba Cloud DNS

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Satellite Services				
Satellite Connectivity	AWS Ground Station	n/a	n/a	n/a
Data Processing & Analysis	n/a	n/a	n/a	n/a
Earth Observation	n/a	n/a	n/a	n/a
Ground Station Management	AWS Ground Station	n/a	n/a	n/a
Robotics				
Robotic Process Automation (RPA)	n/a	Azure Logic Apps	n/a	Robotic Process Automation
Robotics Management	RoboMaker	n/a	n/a	n/a
Robotic Development Kits	RoboMaker	n/a	n/a	n/a
Robot Telemetry & Analytics	n/a	n/a	n/a	n/a
Quantum Computing				
Quantum Processors & Hardware	Braket	Azure Quantum	n/a	n/a
Quantum Algorithms	Braket	Azure Quantum	n/a	n/a
Quantum Networking	n/a	n/a	n/a	n/a
Quantum Security	n/a	n/a	n/a	n/a
VR/AR				
VR/AR Development Platforms	n/a	Azure Remote Rendering, Azure Mixed Reality Services	n/a	n/a
VR/AR Content Creation & Management	n/a	Azure Mixed Reality Services	n/a	n/a
VR/AR Hardware & Device Support	n/a	HoloLens, Azure Kinect DK	n/a	n/a
Mixed Reality Services	n/a	Azure Mixed Reality Services	n/a	n/a

Groups & subgroups	Amazon Web Services (AWS)	Microsoft Azure	Google Cloud Platform	Alibaba Cloud
Spatial Computing & Environmental Understanding	n/a	Azure Spatial Anchors	n/a	n/a

Groups & subgroups	Oracle Cloud Infrastructure	Tencent Cloud	Google Cloud Platform	OVHcloud
Compute				
Virtual Machines	OCI Compute	CVM	Compute Engine	Public Cloud Instances
Containers & Kubernetes	Oracle Kubernetes Engine	Tencent Kubernetes Engine	Google Kubernetes Engine	Managed Kubernetes® Service
Serverless Functions	Oracle Functions	SCF	Cloud Functions	—
Batch & High-Performance Computing	Batch Processing Service	BatchCompute	Cloud Dataflow, Cloud Dataproc	—
Storage				
Object Storage	Object Storage	COS	Cloud Storage	Object Storage
Block Storage	Block Volume	Cloud Block Storage	Persistent Disk	Block Storage
File Systems	File Storage	CFS	Filestore	—
Cold & Archival Storage	Archive Storage	Cloud Object Storage - Infrequent Access	Cloud Storage Nearline, Coldline, Archive	Cold Storage
Databases				
Relational Databases	Oracle Database, MySQL, Autonomous Database	TencentDB for MySQL, TencentDB for MariaDB, TencentDB for PostgreSQL	Cloud SQL	Managed Databases: MySQL
NoSQL Databases	Oracle NoSQL Database	TencentDB for MongoDB	Firestore, Cloud Bigtable	—
In-memory Databases	Oracle Coherence, Autonomous Database with in-memory	TencentDB for Redis	Memorystore	—
Database Migration Services	Oracle Data Pump, Oracle GoldenGate	Data Transmission Service (DTS)	Cloud Data Transfer, BigQuery Data Transfer Service	—
Networking				
Virtual Private Cloud (VPC)	Virtual Cloud Network	Virtual Private Cloud	VPC Network	vRack
Content Delivery Network (CDN)	Oracle Cloud CDN	Tencent Cloud CDN	Cloud CDN	OVHcloud Content Delivery Network
Load Balancing	Load Balancing	Cloud Load Balancer	Cloud Load Balancing	Load Balancers
Network Security & Firewalls	Web Application Firewall, Network Security Groups	Cloud Firewall	Cloud Armor, Firewall Rules	OVHcloud Firewall Network

Groups & subgroups	Oracle Cloud Infrastructure	Tencent Cloud	Google Cloud Platform	OVHcloud
Developer Tools				
Integrated Development Environments (IDE)	Oracle Developer Service	Cloud Development Suite	Cloud Shell, Cloud Code	—
Continuous Integration & Deployment (CI/CD)	Oracle Visual Builder	Tencent Cloud Continuous Integration	Cloud Build	—
Source Control	—	Tencent Cloud CodeHub	Cloud Source Repositories	—
Monitoring & Logging Tools	Oracle Cloud Monitoring, Oracle Cloud Logging	Cloud Monitor	Stackdriver Monitoring, Stackdriver Logging	OVHcloud Logs Data Platform
Analytics & Big Data				
Data Lakes	Oracle Big Data Service	Cloud Native Data Lake	BigQuery, Dataproc	—
Big Data Processing	Oracle Data Flow	Batch Compute	Cloud Dataflow, Cloud Dataproc	—
Real-time Analytics	Oracle Stream Analytics	Real-Time Compute	Datastream, Dataflow	—
Data Warehousing	Oracle Autonomous Data Warehouse	TencentDB for Data Warehouse	BigQuery	—
AI & Machine Learning				
Machine Learning Platforms	Oracle Big Data Service	Cloud Native Data Lake	BigQuery, Dataproc	—
AI Development Tools	Oracle Data Flow	Batch Compute	Cloud Dataflow, Cloud Dataproc	—
Pre-trained AI Services	Oracle Stream Analytics	Real-Time Compute	Datastream, Dataflow	—
Data Labeling & Training	Oracle Autonomous Data Warehouse	TencentDB for Data Warehouse	BigQuery	—
Security & Identity				
Identity & Access Management (IAM)	Identity and Access Management	CAM (Cloud Access Management)	Identity and Access Management	OVHcloud Identity and Access Management
Threat Detection	Oracle Cloud Guard	Threat Detection Service	Security Command Center, Event Threat Detection	—
Data Protection	Oracle Data Safe	Data Backup	Cloud Data Loss Prevention	OVHcloud Backup
Compliance Management	Oracle Compliance Documentations	Cloud Compliance	Security and Compliance tools	—

Groups & subgroups	Oracle Cloud Infrastructure	Tencent Cloud	Google Cloud Platform	OVHcloud
IoT				
IoT Device Management	Oracle IoT Fleet Monitoring	IoT Device Management	Cloud IoT Core	—
IoT Data Analysis	Oracle IoT Data Science	IoT Data Explorer	Cloud IoT Core Data Analytics	—
Edge Computing	Oracle IoT Edge	Edge Computing	Cloud IoT Edge	—
IoT Security	Oracle IoT Security Analytics	IoT Security Solutions	Cloud IoT security features	—
Migration & Hybrid Cloud				
Migration Tools	Oracle Cloud Lift	Cloud Migration	Migrate for Compute Engine	OVHcloud Migrate
Hybrid Cloud Platforms	Oracle Cloud@Customer	Tencent Cloud Hybrid Cloud	Anthos	OVHcloud Private Cloud
Disaster Recovery	Oracle Cloud Disaster Recovery	Disaster Recovery	Disaster Recovery	OVHcloud Disaster Recovery Plan
Hybrid Connectivity	Oracle FastConnect	Direct Connect	Cloud Interconnect	OVHcloud Connect
Management & Governance				
Infrastructure Automation	Oracle Resource Manager	Service Automation	Deployment Manager	OVHcloud Managed Kubernetes
Cost Management	Oracle Cost Management Cloud	Cloud Cost Management	Cost Management	OVHcloud Cost Insights
Resource Organization	Resource Manager	Resource Directory	Cloud Resource Manager	—
Governance & Compliance Tools	Oracle Cloud Compliance and Governance	Governance	Policy Intelligence	—
Mobile Services				
Mobile Backend-as-a-Service (MBaaS)	—	Mobile Tencent Cloud	Firebase (part of GCP)	—
App Development Platforms	Oracle Mobile Hub	Cloud Mobile Application Platform	Firebase Cloud Functions	—
Mobile Analytics	Oracle Infinity	Mobile Tencent Cloud Analytics	Firebase Analytics	—
User Engagement Tools	—	Mobile Tencent Cloud Messaging	Firebase Cloud Messaging	—
Enterprise Integration				
Service Integration	Oracle Integration Cloud	Cloud Integration Platform	Cloud Endpoints	—

Groups & subgroups	Oracle Cloud Infrastructure	Tencent Cloud	Google Cloud Platform	OVHcloud
API Management	Oracle API Gateway	API Gateway	Apigee API Platform	—
Enterprise Messaging	Oracle Messaging Cloud Service	Cloud Message Queue	Cloud Pub/Sub	OVHcloud Messaging Service
Business Process Automation	Oracle Integration Cloud	Cloud Workflow	Cloud Composer	—
End User Computing				
Virtual Desktops	Oracle Secure Global Desktop	Virtual Desktop Infrastructure	Google Workspace	—
Collaboration Tools	Oracle Collaboration Suite	Tencent Meeting	Google Workspace	OVHcloud Collaborative Tools Suite
Remote App Streaming	—	Cloud Virtual Desktop	App Streaming	—
Workspace Security	Oracle CASB Cloud Service	—	BeyondCorp	—
Front-end Web & Mobile				
Web Hosting	Oracle Content and Experience	Cloud Virtual Machine	App Engine	OVHcloud Web Hosting
Mobile Web Services	Oracle Mobile Cloud Service	Mobile Tencent Cloud	Firebase Hosting	—
Progressive Web Apps	—	—	Firebase for PWAs	—
Web Security	Oracle Cloud WAF	Web Application Firewall	Web Security Scanner	OVHcloud Web Security
Business Applications				
Customer Relationship Management (CRM)	Oracle CX Cloud	Cloud CRM	Google Workspace with CRM integrations	—
Enterprise Resource Planning (ERP)	Oracle ERP Cloud	—	Google Workspace with ERP integrations	—
Human Capital Management (HCM)	Oracle HCM Cloud	—	Google Workspace with HCM integrations	—
Supply Chain Management	Oracle SCM Cloud	—	Google Workspace with SCM integrations	—
Blockchain				
Blockchain Platforms	Oracle Blockchain Platform	Blockchain Service	Cloud Blockchain	—

Groups & subgroups	Oracle Cloud Infrastructure	Tencent Cloud	Google Cloud Platform	OVHcloud
Smart Contract Development	—	Blockchain Contract Development	Cloud Blockchain Ethereum API	—
Blockchain Networking	—	Blockchain Network	—	—
Cryptography Services	Oracle Key Management	Key Management Service	Cloud Key Management Service	OVHcloud Key Management Service
Gaming				
Game Development Platforms	—	Tencent Cloud Game Solution	Firebase for Games	—
Multiplayer Servers	—	Tencent Cloud Game Server	Agones (with Kubernetes)	—
Real-time Game Analytics	—	Tencent Cloud Game Player Analysis	Firebase Analytics for Games	—
Game Asset Management	—	Tencent Cloud COS (as part of game solution)	Cloud Storage for Firebase	—
Multimedia Services				
Media Conversion & Encoding	—	Tencent Cloud Media Processing Service	Cloud Video Intelligence	—
Media Storage & Delivery	Oracle Cloud Storage	Tencent Cloud Media Storage	Google Cloud Storage	OVHcloud Object Storage
Interactive Media Services	—	Tencent Cloud Interactive Media Streaming	Anvato	—
Media Analytics	—	Tencent Cloud Media Data Analysis	Video Intelligence API	—
Content Delivery Networks (CDN)				
Content Distribution	Oracle Cloud Content and Experience	Tencent Cloud CDN	Cloud CDN	OVHcloud Content Delivery Network
Content Acceleration	—	Tencent Cloud CDN	—	—
Edge Caching	—	Tencent Cloud CDN Edge Caching	Cloud CDN Edge Caching	OVHcloud CDN Edge Servers
Traffic Management	Oracle Traffic Management	Tencent Cloud Traffic Management	Traffic Director	OVHcloud Load Balancer
Satellite Services				
Satellite Connectivity	—	—	—	—

Groups & subgroups	Oracle Cloud Infrastructure	Tencent Cloud	Google Cloud Platform	OVHcloud
Data Processing & Analysis	—	Tencent Cloud Data Processing	BigQuery GIS	—
Earth Observation	—	—	Earth Engine	—
Ground Station Management	—	—	—	—
Robotics				
Robotic Process Automation (RPA)	—	—	Cloud Robotics Core	—
Robotics Management	—	—	Cloud Robotics Core	—
Robotic Development Kits	—	—	—	—
Robot Telemetry & Analytics	—	—	—	—
Quantum Computing				
Quantum Processors & Hardware	—	—	—	—
Quantum Algorithms	—	—	—	—
Quantum Networking	—	—	—	—
Quantum Security	—	—	—	—
VR/AR				
VR/AR Development Platforms	—	Tencent Cloud VR	ARCore, VR SDK	—
VR/AR Content Creation & Management	—	Tencent Cloud VR	Poly	—
VR/AR Hardware & Device Support	—	—	ARCore for device support	—
Mixed Reality Services	—	—	—	—
Spatial Computing & Environmental Understanding	—	—	ARCore Depth API	—

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
Compute				
Virtual Machines	Rackspace Managed VMs	Heroku Dynos	SAP Cloud Platform Virtual Machines	ECS (Elastic Cloud Server)
Containers & Kubernetes	Rackspace Kubernetes-as-a-Service	Salesforce Kubernetes-based Services	SAP Gardener	CCE (Cloud Container Engine)
Serverless Functions	—	Salesforce Functions	SAP Cloud Platform Functions	FunctionGraph
Batch & High-Performance Computing	—	—	SAP High-Performance Analytic Appliance (HANA)	BatchCompute
Storage				
Object Storage	Rackspace Cloud Files	—	SAP Cloud Platform Object Store	OBS (Object Storage Service)
Block Storage	Rackspace Cloud Block Storage	—	—	EVS (Elastic Volume Service)
File Systems	—	—	SAP Cloud Platform File Store	SFS (Scalable File Service)
Cold & Archival Storage	—	—	—	OBS Infrequent Access
Databases				
Relational Databases	Rackspace Database	Salesforce Database Services	SAP HANA	RDS (Relational Database Service)
NoSQL Databases	—	Salesforce Big Objects	SAP Cloud Platform NoSQL	DCS (Distributed Cache Service)
In-memory Databases	—	—	SAP HANA	GaussDB for IMDB
Database Migration Services	Rackspace Database Migration	Salesforce Data Migration	SAP Data Services	DTS (Data Transfer Service)
Networking				
Virtual Private Cloud (VPC)	Rackspace Private Cloud	—	SAP Cloud Platform Cloud Foundry Environment	VPC
Content Delivery Network (CDN)	Rackspace CDN	Salesforce Content Delivery	SAP Cloud Platform CDN	Content Delivery Network
Load Balancing	Rackspace Load Balancers	—	SAP Cloud Platform Load Balancer	ELB (Elastic Load Balance)

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
Network Security & Firewalls	Rackspace Managed Security	Salesforce Shield	SAP Cloud Platform Application Runtime	Anti-DDoS
Developer Tools				
Integrated Development Environments (IDE)	—	Salesforce Developer Tools (like Developer Console)	SAP Web IDE	CloudIDE
Continuous Integration & Deployment (CI/CD)	Rackspace DevOps	Salesforce DevOps Center	SAP Cloud Platform Continuous Integration & Delivery	CodeHub & Pipeline
Source Control	—	Salesforce DX	SAP Cloud Platform Git Service	CodeHub
Monitoring & Logging Tools	Rackspace Monitoring	Salesforce Event Monitoring	SAP Cloud Platform Alert Notification	Cloud Eye
Analytics & Big Data				
Data Lakes	—	—	SAP Data Intelligence	Data Lake Insight
Big Data Processing	—	—	SAP Data Hub	MRS (MapReduce Service)
Real-time Analytics	—	Salesforce Einstein Analytics	SAP HANA Real-time Analytics	StreamLink
Data Warehousing	—	—	SAP BW/4HANA	GaussDB for DW
AI & Machine Learning				
Machine Learning Platforms	—	Einstein Platform	SAP Leonardo Machine Learning	ModelArts
AI Development Tools	—	Einstein Developer Tools	—	ModelArts SDK
Pre-trained AI Services	—	Einstein Voice, Einstein Vision	—	AI Cloud Services
Data Labeling & Training	—	—	—	Data Labeling & Annotation Service
Security & Identity				
Identity & Access Management (IAM)	Rackspace Identity	Salesforce Identity	SAP Cloud Identity Service	Identity and Access Management

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
Threat Detection	—	Event Monitoring	—	IDS/IPS
Data Protection	Rackspace Privacy and Data Protection	Salesforce Shield	SAP Data Protection	Data Encryption Service
Compliance Management	Rackspace Compliance Assistance	Salesforce Compliance	SAP Cloud Compliance	Compliance Center
IoT				
IoT Device Management	—	IoT Cloud	SAP Leonardo IoT	IoT Device Management
IoT Data Analysis	—	Einstein Analytics for IoT	SAP Leonardo IoT Edge	StreamLink
Edge Computing	—	—	SAP Leonardo Edge Computing	Edge Computing IoT
IoT Security	—	Salesforce IoT Security	—	IoT Security
Migration & Hybrid Cloud				
Migration Tools	Rackspace Migration	—	SAP Cloud Platform Migration	SMS (Server Migration Service)
Hybrid Cloud Platforms	Rackspace Hybrid Cloud	—	SAP Cloud Platform	Huawei Hybrid Cloud
Disaster Recovery	Rackspace Disaster Recovery	—	SAP Cloud Platform Disaster Recovery	Disaster Recovery Service
Hybrid Connectivity	Rackspace Connectivity	—	SAP Cloud Platform Connectivity	VPN, Direct Connect
Management & Governance				
Infrastructure Automation	—	—	SAP Cloud Platform Automation	CloudFormation
Cost Management	Rackspace Cost Optimization	—	SAP Cloud Platform Cost Management	Cost Management Center
Resource Organization	—	—	SAP Cloud Platform Cockpit	Resource Management
Governance & Compliance Tools	—	Salesforce Governance	SAP Cloud Platform Compliance	Governance, Risk, and Compliance
Mobile Services				
Mobile Backend-as-a-Service (MBaaS)	—	Salesforce Mobile Services	SAP Cloud Platform Mobile Services	mPaaS

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
App Development Platforms	—	Salesforce Mobile SDK	SAP Cloud Platform SDK for iOS/Android	DevCloud
Mobile Analytics	—	Salesforce Analytics Cloud	SAP Fiori	Mobile Analytics
User Engagement Tools	—	Marketing Cloud	SAP Cloud Platform Engagement	Push Service
Enterprise Integration				
Service Integration	Rackspace Service Integration	MuleSoft Anypoint Platform	SAP Cloud Platform Integration	ServiceStage
API Management	—	Salesforce API Management	SAP Cloud Platform API Management	API Gateway
Enterprise Messaging	—	Salesforce Messaging	SAP Cloud Platform Enterprise Messaging	Message & Notification Service
Business Process Automation	—	Salesforce Flow	SAP Intelligent Business Process Management	FlowEngine
End User Computing				
Virtual Desktops	—	—	—	Cloud Desktop
Collaboration Tools	—	Salesforce Quip	SAP Jam Collaboration	—
Remote App Streaming	—	—	—	AppStream
Workspace Security	—	Salesforce Shield	SAP Cloud Platform Security	Workspace Security
Front-end Web & Mobile				
Web Hosting	Rackspace Web Hosting	Salesforce Sites	SAP Cloud Platform Web IDE	Web Hosting
Mobile Web Services	—	Salesforce Mobile	SAP Cloud Platform Mobile	mPaaS
Progressive Web Apps	—	—	SAP Cloud Platform PWA	—
Web Security	Rackspace Managed Security	Salesforce Shield	SAP Web Dispatcher	Web Application Firewall
Business Applications				

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
Customer Relationship Management (CRM)	—	Salesforce Sales Cloud, Service Cloud	SAP CRM	—
Enterprise Resource Planning (ERP)	—	—	SAP S/4HANA	—
Human Capital Management (HCM)	—	Work.com	SAP SuccessFactors	—
Supply Chain Management	—	—	SAP Integrated Business Planning	—
Blockchain				
Blockchain Platforms	—	Salesforce Blockchain	SAP Cloud Platform Blockchain	BCS (Blockchain Service)
Smart Contract Development	—	—	—	BCS IDE
Blockchain Networking	—	—	—	BCS Network
Cryptography Services	—	Salesforce Platform Encryption	—	Key Management Service
Gaming				
Game Development Platforms	—	—	—	Game Hosting
Multiplayer Servers	—	—	—	Game Server Hosting
Real-time Game Analytics	—	—	—	Game Analysis
Game Asset Management	—	—	—	—
Multimedia Services				
Media Conversion & Encoding	—	—	—	Media Transcoding
Media Storage & Delivery	Rackspace Cloud Files	Salesforce CMS	—	Content Delivery Network
Interactive Media Services	—	—	—	Real-time Communication
Media Analytics	—	—	—	Media Analysis
Content Delivery Networks (CDN)				

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
Content Distribution	Rackspace CDN	—	SAP Cloud Platform CDN	Content Delivery Network
Content Acceleration	—	—	—	Content Delivery Network (for acceleration)
Edge Caching	—	—	—	Content Delivery Network (caching capabilities)
Traffic Management	—	—	—	Traffic Management System
Satellite Services				
Satellite Connectivity	—	—	—	—
Data Processing & Analysis	—	—	—	—
Earth Observation	—	—	—	—
Ground Station Management	—	—	—	—
Robotics				
Robotic Process Automation (RPA)	—	Salesforce RPA (Einstein Automate)	—	—
Robotics Management	—	—	—	—
Robotic Development Kits	—	—	—	—
Robot Telemetry & Analytics	—	—	—	—
Quantum Computing				
Quantum Processors & Hardware	—	—	—	—
Quantum Algorithms	—	—	—	—
Quantum Networking	—	—	—	—
Quantum Security	—	—	—	—
VR/AR				
VR/AR Development Platforms	—	—	SAP Cloud Platform VR/AR services	—
VR/AR Content Creation & Management	—	—	—	—

Groups & subgroups	Rackspace Technology	Salesforce	SAP	Huawei Cloud
VR/AR Hardware & Device Support	—	—	—	—
Mixed Reality Services	—	—	SAP Cloud Platform Mixed Reality	—
Spatial Computing & Environmental Understanding	—	—	—	—

Annex 2 – Proposed categories for PaaS/SaaS service types

Cloud Tier	Service Type	Group	Detailed explanation
PaaS	Machine Learning Platforms	AI & Machine Learning	Services, platforms and tools to develop, deploy, and manage artificial intelligence and machine learning models and applications *1
PaaS	AI Development Tools	AI & Machine Learning	Frameworks and platforms for building AI models.
PaaS	Pre-trained AI Services	AI & Machine Learning	APIs and tools offering ready-to-use AI capabilities.
PaaS	Data Labeling & Training	AI & Machine Learning	Services for preparing and annotating datasets for AI.
PaaS	Analytics & Big Data	Analytics & Big Data	Services, platforms and tools that assist in processing, analyzing, and visualizing vast datasets to derive insights, including data lakes and real-time analytics tools *1
PaaS	Data Lakes	Analytics & Big Data	Centralized repositories for storing structured and unstructured data.
PaaS	Big Data Processing	Analytics & Big Data	Services for analyzing and processing large-scale datasets.
PaaS	Real-time Analytics	Analytics & Big Data	Tools for analyzing data as it is generated.
PaaS	Data Warehousing	Analytics & Big Data	Centralized systems optimized for querying and reporting on large datasets.
PaaS	Blockchain Platforms	Blockchain	Blockchain platforms and services supporting the creation, deployment, and management of blockchain networks and application *1
PaaS	Smart Contract Development	Blockchain	Tools for creating blockchain-based contracts.
PaaS	Blockchain Networking	Blockchain	Services for deploying and managing blockchain networks.
PaaS	Cryptography Services	Blockchain	Tools to secure data using encryption techniques.
SaaS	Customer Relationship Management (CRM)	Business Applications	Business Applications are cloud-based applications designed for specific business operations like CRM, ERP, and HCM. *1
SaaS	Enterprise Resource Planning (ERP)	Business Applications	Integrated software for managing business processes.
SaaS	Human Capital Management (HCM)	Business Applications	Tools for managing employee-related processes.
SaaS	Supply Chain Management	Business Applications	Platforms for optimizing supply chain operations.
PaaS	Containers & Kubernetes	Compute	Services, providing raw processing power. This encompasses virtual machines, containers, serverless computing, and other computational resources.*1
PaaS	Serverless Functions	Compute	Event-driven compute service that runs code without managing servers.

Cloud Tier	Service Type	Group	Detailed explanation
IaaS	Batch & High Performance Computing	Compute	Services for running large-scale, compute-intensive workloads.
IaaS	File Systems	Data Storage	Cloud-based storage systems for organizing and accessing files.
PaaS	Relational Databases	Databases	Services related to structured and unstructured data storage, retrieval, and management, including relational, NoSQL, and specialized database systems *1
PaaS	NoSQL Databases	Databases	Databases optimized for non-relational, unstructured, or semi-structured data.
PaaS	In-memory Databases	Databases	Databases that store data in RAM for ultra-fast access.
PaaS	Database Migration Services	Databases	Tools to transfer databases between platforms or environments.
PaaS	Integrated Development Environments (IDE)	Developer Tools	Services, platforms and tools designed to streamline the coding, deploying, and managing of applications and services in the cloud *1
PaaS	Continuous Integration & Deployment (CI/CD)	Developer Tools	Services automating code integration, testing, and deployment.
Transversal	Source Control	Developer Tools	Version control systems for managing code changes.
Transversal	Observability & Logging Tools	Developer Tools	Services to monitor, log, and analyze application performance.
Transversal	Application deployment	Developer Tools	Tools and platforms for releasing applications to production.
Transversal	App Development Platforms	Developer Tools	Services for creating and deploying applications.
PaaS	Service Integration	Enterprise Integration	Enterprise Integration solutions that allow seamless integration of cloud services with existing enterprise applications, databases, and systems *1
PaaS	API Management	Enterprise Integration	Platforms for designing, deploying, and monitoring APIs.
PaaS	Enterprise Messaging	Enterprise Integration	Messaging systems for reliable communication between services.
PaaS	Business Process Automation	Enterprise Integration	Tools to automate repetitive business workflows.
PaaS	Web Hosting & Web App Services	Front-end Web & Mobile	Front-end Web & Mobile solutions for developing, hosting, and managing web-based and mobile interfaces *1
PaaS	Content Management Systems	Front-end Web & Mobile	Platforms for creating and managing digital content.
PaaS	Mobile App Services & Frameworks	Front-end Web & Mobile	Tools for building and managing mobile applications.

Cloud Tier	Service Type	Group	Detailed explanation
PaaS	Web Security	Front-end Web & Mobile	Services to protect web applications from threats.
PaaS	Progressive Web Apps	Front-end Web & Mobile	Web applications with app-like features and offline support.
PaaS	Front-end Frameworks & Libraries	Front-end Web & Mobile	Pre-built code libraries for building user interfaces.
Transversal	Mobile Backend-as-a-Service (MBaaS)	Front-end Web & Mobile	Mobile Services tools and platforms specifically designed for the development, deployment, and management of mobile applications *1
Transversal	Mobile Analytics	Front-end Web & Mobile	Tools to track and analyze mobile app usage.
Transversal	User Engagement Tools	Front-end Web & Mobile	Platforms to improve customer interaction and retention.
PaaS	Game Development Platforms	Gaming	Gaming cloud solutions catering to the gaming industry, including game hosting, multiplayer frameworks, and analytics. *1
PaaS	Multiplayer Servers	Gaming	Hosting solutions for online multiplayer games.
PaaS	Real-time Game Analytics	Gaming	Tools for tracking live game performance and player activity.
PaaS	Game Asset Management	Gaming	Platforms to store and organize game resources.
PaaS	IoT Device Management	Internet of Things	IoT platforms and services tailored to support the development, deployment, and management of Internet of Things devices and applications *1
PaaS	IoT Data Analysis	Internet of Things	Tools for processing and analyzing IoT-generated data.
PaaS	Edge Computing	Internet of Things	Computing resources located close to data sources for faster processing.
PaaS	IoT security	Internet of Things	Security solutions for IoT devices and networks.
Transversal	Systems administration	Management & Governance	Tools for managing IT infrastructure and systems.
Transversal	Data Storage	Management & Governance	Services for storing and managing digital data.
Transversal	Infrastructure Automation	Management & Governance	Management & Governance services that assist businesses in monitoring, managing, and optimizing their cloud resources and applications *1
Transversal	Cost Management	Management & Governance	Tools for tracking and optimizing cloud spending.
Transversal	Resource Organization	Management & Governance	Services for structuring and grouping cloud assets.
Transversal	Governance & Compliance Tools	Management & Governance	Platforms to enforce policies and regulatory compliance.

Cloud Tier	Service Type	Group	Detailed explanation
Transversal	Migration Tools	Migration & Hybrid Cloud	Migration & Hybrid Cloud tools and services designed to help businesses migrate to the cloud and manage hybrid (on-premises and cloud) architectures *1
Transversal	Hybrid Cloud Platforms	Migration & Hybrid Cloud	Platforms integrating on-premises and cloud resources.
Transversal	Disaster Recovery	Migration & Hybrid Cloud	Services to restore operations after system failures.
SaaS	Hybrid Recovery	Migration & Hybrid Cloud	Recovery solutions combining cloud and on-premises systems.
Iaas	Media Conversion & Encoding	Multimedia Services	Multimedia Services are related to the creation, storage, processing, and streaming of multimedia content *1
Iaas	Media Storage & Delivery	Multimedia Services	Services for storing and distributing media files.
Iaas	Interactive Media Services	Multimedia Services	Platforms for delivering interactive digital experiences.
Iaas	Media Analytics	Multimedia Services	Tools for analyzing media consumption and engagement.
SaaS	Robotic Process Automation (RPA)	Robotics	Robotics platforms and tools tailored for the development, control, and management of robotic systems *1
SaaS	Robotics Management	Robotics	Platforms to control and monitor robotic systems.
SaaS	Robotic Development Kits	Robotics	Hardware and software kits for building robots.
SaaS	Robot Telemetry & Analytics	Robotics	Tools for monitoring robot performance and data.
Transversal	Data Protection	Security & Identity	Security & Identity services ensuring data protection, identity management, threat detection, and compliance in the cloud environment *1
Transversal	Identity & Access Management (IAM)	Security & Identity	Services to control user access to resources.
Transversal	Threat Detection	Security & Identity	Systems that identify and respond to security threats.
Transversal	Compliance Management	Security & Identity	Tools to ensure adherence to regulations and policies.
Transversal	Cloud Security Posture Management	Security & Identity	Services to monitor and improve cloud security settings.
PaaS	Serverless Functions & Events	Serverless	Cloud functions triggered by events without server management.
PaaS	VR/AR Development Platforms	VR / AR	VR/AR cloud platforms and tools designed for the creation, deployment, and management of virtual and augmented reality experiences *1

Cloud Tier	Service Type	Group	Detailed explanation
Transversal	VR/AR Content Creation & Management	VR / AR	Tools for developing and managing VR/AR content.
Transversal	VR/AR Hardware & Device Support	VR / AR	Services supporting VR/AR devices and accessories.
Transversal	Mixed Reality Services	VR / AR	Platforms blending virtual and real-world experiences.
Transversal	Spatial Computing & Environmental Understanding	VR / AR	Technologies to understand and interact with physical spaces.
SaaS	Collaboration & Productivity	Workplace solutions	Services focused on providing cloud-based user desktops, apps, and collaboration tools *1
SaaS	Endpoint Security	Workplace solutions	Protection for devices accessing a network.
IaaS	Virtual Desktops	Workplace solutions	Cloud-hosted desktop environments accessible remotely.
IaaS	Remote App Streaming	Workplace solutions	Services that deliver applications to users over the internet.

*1 Descriptions from Literature - Komchak (2024).

Some of the descriptions were partly generated using AI tools and subsequently reviewed, updated, and validated by our cloud experts

Annex 3 – Online survey

Survey questionnaire

Interoperability of data processing services

Study for the European Commission
DG Directorate-General for Communications
Networks, Content and Technology (DG CNECT)

No. 2024-016 in the context the framework contract for the provision
of studies and related services on digital policy issues -
CNECT/2022/OP/0036

WIK-Consult GmbH

WIK CONSULT

Schumann Associates

SCHUMAN ASSOCIATES

Decision - Études & Conseil

DECISION ETUDES & CONSEIL

Bad Honnef, 11.12.2024

1. Background of the study

WIK-Consult together with Decision and Schuman Associates carry out a study for the European Commission on Interoperability of data processing services.

The aim of the study is to assist the Commission in performing a first review of existing standards and open interoperability specifications that meet the requirements laid down in the Data Act, and therefore could be considered (after a thorough scrutiny process) for inclusion in the central Union repository.

The Data Act ([27]) tackles barriers to cloud switching and multi-cloud use. One of these barriers is a lack of interoperability between cloud providers and/or on-site systems. Article 30, paragraph 3 of the Data Act requires providers of data processing services **not** related to infrastructural elements (so PaaS and SaaS ([28]) cloud services) to ensure compatibility with harmonised standards and common specifications based on open interoperability specifications that are laid down in a central Union repository within 12 months after their publication in said repository. ([29]) Other obligations on cloud service providers to increase interoperability and thereby remove obstacles for effective switching include: Making open interfaces available to an equal extent to all their customers and relevant destination providers free of charge (Article 30(2)); maintaining an updated online register detailing their data structure and format and which harmonised standards and common specifications these comply with (Article 30(4)); and – for service types where no harmonised standards and common specifications are published in the repository - making available exportable data in a structured, commonly used and machine-readable format (Article 30(5)).

In the context of the Data Act, harmonised standards mean a standard as defined in Article 2, point (1)(c), of Regulation (EU) No 1025/2012. A harmonised standard is a European standard developed by a recognised European Standards Organisation: CEN, CENELEC, or ETSI. It is created following a request from the European Commission to one of these organisations. Manufacturers, other economic operators, or conformity assessment bodies can use harmonised standards to demonstrate that products, services, or processes comply with relevant EU legislation. Open interoperability specifications are technical specifications in the field of information and communication technologies which are performance-oriented towards achieving interoperability between data processing services. Open interoperability specifications do not require a formal standardisation process and can be the outcome of informal agreements between industry groups, for example on data formats to use when exchanging between different services of the same type.

With this survey, we would like to understand your views in particular regarding:

[27] See https://digital-strategy.ec.europa.eu/en/policies/data-act

[28] Platform as a Service / Software as a Service.

[29] For the more far reaching obligations on providers of IaaS services see Art. 30 paragraph 1 of the Data Act.

- Which **type** of standards and technical specification regarding interoperability of cloud services should be **prioritised** when it comes to inclusion in the repository. We note that priority areas should be chosen based on their relevance in addressing problems currently experienced when switching cloud provider and/or building multi-cloud environments;
- Which interoperability standards and specifications that **exist** at international, European and national level should be **considered as candidates** for inclusion in the repository;
- Your judgement of the **level of maturity and any shortcomings** of these proposed standards and specifications; and
- Any **gaps** in the availability of **existing standards and open specifications** regarding interoperability of cloud services that may justify the Commission launching a standardisation request to a European standardisation organisation.

Information gathered via the survey will be aggregated with that of other respondents to keep your response anonymous. The aggregated information may be displayed in the study report, for example in the form of charts or tables.

Questions marked with an * are required to be filled as they are essential.

2. Your details and preferences

1. Could you please provide your name (purely for purposes of any required follow-up, and to check that no duplicate responses have been provided) [text field]
2. Could you please provide your email address (see above) [text field]
3. Which company or organization do you represent? [text field]
4. Which of the following category best describes the role of your company or organization [checkbox] [End user, cloud service provider, association representing end-users, association representing cloud service providers, standardisation organisation/specifications setting organisation, other- text field
5. In which industry domain(s) is your company or organisation active? check boxes as multiple sectors possible + option other + text field
6. What is the European turnover of your organization [insert ranges]
7. We will organise a **workshop** in March 2025 with the aim of discussing and validating our preliminary findings with stakeholders. Please click the checkbox to indicate if you would be interested in participating. [insert checkbox].
8. Please indicate if you would like to receive information about other events and studies organised by WIK-Consult [insert checkbox]

9. Please confirm that you consent for us to process personal data in the context of the survey, for the purpose of validating responses and to make further contact in the cases described above. [checkbox]

3. **What are the priority areas in the PaaS/SaaS cloud market for reviewing which standards and specifications on interoperability and portability to be included in the repository?**

Introduction

According to the Data Act, the focus of provisions regarding the potential inclusion of standards and specifications in the online repository is on Platform as a Service (PaaS) and Software as a Service (SaaS). Infrastructure as a Service (IaaS) is not in scope of these provisions.

When we ask about your opinion about **priority areas**, we ask you to focus on areas where you see problems with migrating PaaS/SaaS cloud environments and/or building multi-cloud environments, which could be improved by requiring cloud service providers to ensure compatibility with certain existing standards and/or informal technical specifications across industries, or creating new standards, where gaps might exist.

10. Have you experienced problems with migration or multi-cloud strategies due to a lack of standardisation of **data semantics (interpretation) or syntactic (format, structure)** and **technical and foundational** aspects (like data transport, identity managment or API management) for Paas/SaaS cloud services and if so in which scenario? Options: Yes/NO + check box in which areas: migrating data from one cloud environment to another / migrating applications from one cloud environment to another / building a multi-cloud environment, other + text field

11. Considering the experienced problems asked for in the previous questions, what should be, in your opinion, the priority areas of the PaaS cloud market when reviewing standards and specifications to be included in the Union repository (and thereby making them mandatory)?

☐ For Data Catalogue

Big Data exchanges

☐ For Application Development (DevOps, CI/CD, etc…)

☐ For Database as a Service (DBaaS)

☐ For API management

☐ For Container Orchestration and Management

☐ For Transport of data

☐ For Identity and Access Management (IAM)

☐ For Security of data in transit and at rest

☐ Other– please describe

12. Considering the experienced problems asked for in the previous questions, what should be, in your opinion, the priority areas of the SaaS cloud market when reviewing standards and specifications to be included in the Union repository (and thereby making them mandatory)?

☐ For Enterprise Resource Planning (ERP) systems

☐ For Customer Relation Management (CRM) systems

☐ For Project / Task Management systems

☐ For Office Automation Software

☐ For Financial and Accounting Software

☐ For Business Intelligence (BI) and Analytics

☐ Other in relation to data format and structure – please describe

4. **Which existing generic standards and specifications should be considered for inclusion in the repository?**

As the distinction between PaaS and SaaS cloud services is becoming fluid and the Data Act has similar obligations relating to both categories, in the following questions, we have distinguished between **generic (sector agnostic)** and **sector specific** standards and specifications. We also distinguish between the data **semantic (interpretation), syntactic (format) and technical and** foundational (core principles on communication, data exchange and interworking) **aspects** of standards and specifications.

There are already certain generic standards and specifications on data format, structure and semantics which seek to support interoperability and portability for PaaS/SaaS. For example ISO/IEC 19941:2017, 17826:2022 (CDMI) and CNCF provide robust foundations to structure the services on the semantic structure and interfacing.

13. Are there existing international, European or national standards or open interoperability specifications relating to PaaS/SaaS on data format, structure and semantics that should be considered for inclusion in the repository? If so, please list them. [text Yes for PaaS in general, Yes for specific PaaS (please specify)– multi text fields, Yes for SaaS in general, Yes for specific SaaS (please specify) -multiple text fields, No

In addition to generic standards and specifications on data format, structure and semantics described above, standards and specifications to support interoperability and portability may also cover **technical** and **foundational** aspects like data catalogues, API, container orchestration and data transport.

There are already certain standards and specifications on technical aspects for PaaS/SaaS for the purpose of interoperability and portability. For example ISO/IEC 17826:2022 (CDMI) CDMI .

In the following questions, we ask you to identify any international, European or national standards or open interoperability specifications covering these aspects that should be considered for inclusion in the repository.

14. Please indicate for which of the following **technical** aspects, if any, you consider that there may be a case to include harmonised standards or open interoperability specifications in the EU Data Act repository? If so, please cite any existing standards or specifications that in your view should be included in the repository? Some examples are given. You are free to cite any of these examples or identify others for specific areas (e.g. for PaaS only) in the text field.

☐ For Data Catalogue and Big Data exchanges (e.g. W3C Dcat version 3,) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For Big Data exchanges (e.g. Apache Avro and Parquet) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For Application Development [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For Database as a Service (e.g ISO/IEC 9075 for SQL Database standards that apply to both IaaS & PaaS Database products) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For API management (e.g. GraphQL) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For Container Orchestration and Management (e.g. Kubernetes) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐Other in relation cloud development environments – please describe [open text]

☐ None

15. Please indicate for which of the following **foundational** (related to core principles on communication, data exchange and interworking) aspects, if any, you consider that there may be a case to include harmonised standards or open interoperability specifications in the EU Data Act repository? If so, please cite any existing standards or specifications that in your view should be included in the repository? Some examples are given. You are free to cite any of these examples or identify others.

☐ For Transport of data (e.g Apache Kafka) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For Identity and Access Management (IAM) e.g OAuth, SAML, etc…) [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ For Security of data in transit and at rest (e.g RFC 5246 for TLS or ISO/IEC 27017/27018)

[checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐ Other in relation to foundational layers – please describe [open textbox]

☐ None

5. Which existing sector specific standards and specifications should be considered for inclusion in the repository?

Introduction:

Certain sectors with a high level of data exchange and/or integration of cloud environments, have developed sector specific standards and/or specifications resolving interoperability and portability issues.

We have identified in certain industry segments existing standards for cloud interoperability, data and application portability. For example:

- For Manufacturing: VSSo standard for Vehicle Signal Specifications;
- For Finance: ISO 20022 which normalizes data interchange between institutions; and
- For Healthcare: Fast Healthcare Interoperability Resources facilitating interoperability between legacy and modern platforms.

16. Please indicate for which sector(s), if any, you consider that there is a case to include standards or open interoperability specifications in the EU repository? If so, please cite any existing standards or specifications that in your view should be included in the repository?

☐For Industry [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Healthcare [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Finance [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Public sector [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Smart Living [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Energy [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Mobility [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Agriculture [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Professional services [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐For Retail & Wholesale [checkbox + (where box is checked) Please list the harmonised standards or open interoperability specifications that you consider should be included in the repository [open text]

☐Other– please describe [open textbox]

[checkbox- none]

17. If you have indicated one of more sectors above, please describe why certain sectors need sector specific standards and specifications for interoperability and portability instead of generic ones. Textfield

18. Please also indicate **any other standards or open interoperability specifications** at national, European or international level that are not in the list, but may be relevant for a first review.

6. Perceived gaps in formal standards

We asked you before which areas of cloud interoperability and portability (generic, sector specific, syntactic, semantic, technical) should be reviewed with priority when considering candidates for inclusion in the repository.

However, it could be that for a certain area and/or aspect there are **no existing** harmonised standards, but also no suitable other standards or open interoperability specifications which satisfy the requirement of the Data Act enabling interoperability and data portability for PaaS and SaaS cloud services (so called white spots). In this case, the European Commission could ask standard bodies to **develop certain harmonised standards to cover these gaps**.

19. Please indicate in which areas you consider there are such gaps and it would be appropriate for the EU Commission to ask standard bodies to develop harmonised standards on interoperability and data portability for PaaS and SaaS cloud services?
    a. Generic (data format, structure and semantics) [checkbox + (where box is checked) Please describe the request that you consider should be made to develop harmonised standards in the area where you consider that such standards are missing] [open text]
    b. Generic (**technical** and **foundational)** [checkbox + (where box is checked) Please describe the request that you consider should be made to develop harmonised standards in the area where you consider that such standards are missing] [open text]
    c. Sector-specific [checkbox + (where box is checked) Please describe the request that you consider should be made to develop harmonised standards in the area where you consider that such standards are missing] [open text]
    d. Other. Please describe the request that you consider should be made to develop harmonised standards in the area that they are missing

{none] checkbox

7. Features for the Union online repository tool

Introduction

When certain standards or open specifications are deemed suitable to be applied across the EU, they will be included in the Union online repository and hence become mandatory across the EU.

The functions of this online repository and how stakeholders may search for standards and specifications is also under consideration.

20. Please evaluate from the following list, what are in your opinion the most important parameters while searching for relevant interoperability standards and specifications in the online repository. Rank the most important at the top (by clicking on it and shifting) and the least important at the bottom.

☐ Eu harmonised standards vs common specifications?

☐ Generic vs sector specific standards and specifications?

☐ Interoperability aspect: transport, syntactic, semantic, behavior, policy

☐ Data portability aspects (syntactic, semantic, policy)

☐ Application portability aspects (syntactic, instruction, meta data, behaviour, policy)

☐ Functions in cloud development environments: application development, DevOps and CI/CD, DBaaS, IAM, API management, Container Orchestration and management, Security, Other.

☐ Technical aspects: data transport, IAM, API management, Container Orchestration and management, Security, Other

☐Developer and developer type. In addition to the name of the body behind the standard it will be necessary to specify which type of body is involved e.g. industry association, public standards body

This was the last question. By clicking on the button 'Next', you will proceed to the next screen, where you have to click the button 'Exit' in order to save your input.

Thank you for your input and participation to this survey on interoperability for data processing services.

We hope to see you at our workshop in March 2025.

Annex 4 – Interview guidelines

Interview guideline

Interoperability of data processing services

Study for the European Commission
DG Directorate-General for Communications
Networks, Content and Technology
(DG CNECT)

No. 2024-016 in the context the framework contract for the provision of studies and related services on digital policy issues - CNECT/2022/OP/0036

WIK-Consult GmbH

Schumann Associates

Decision - Études & Conseil

Bad Honnef, 9.10.2024

Task	Topic	Questions	Options to guide responses
0	Introduction	Could you please introduce your organisation briefly and explain in which context you develop, provide and/or make use of cloud computing services, with a focus on PaaS and SaaS?	
1	Priority PaaS and SaaS services for standards	To identify priority sectors that the repository would deal with: Could you please highlight what **priority you would give to each of the following service types** as regards the establishment or formal recognition of harmonised standards and/or open interoperability specifications? In answering this question, please take into account the following factors: Where do you know of relevant standards and specifications? Where would a move towards greater interoperability be particularly necessary? Are there any other relevant service types that should be considered?	Common PaaS types include: • General purpose application services • Data Services • Events & Triggering Systems • Data transfer, exposure & transformation services Common SaaS types include: • Productivity, Collaboration & Communication • ERP • Customer Relationship Management • Project Management • Human Resources • e-Commerce • Data & Analytics • Content Management • Service Desk • Online File Sharing • Content Creation • Whiteboarding • Cybersecurity & Observability
2	Existing international, European and national standards / specifications that are considered promising, important and relevant	Could you please identify any **existing international, European or national standards** which you consider to meet the criteria set out in Article 35 Data Act and should in your view be included in a first Implementing Act for inclusion in the repository? While standards have undergone a standardisation process, the Data Act also recognizes the value of convergence towards open interoperability specifications outside of formal standardisation processes, for example in industry consortia. Could you please identify any **existing open interoperability specifications** which you consider to meet the criteria set out in Article 35 Data Act?	

Task	Topic	Questions	Options to guide responses
2	For the candidates you proposed, what is the level of maturity?	For the harmonised standards and open interoperability specifications you just highlighted, could you please rate their **maturity level** with reference to the options shown? Do you agree with these criteria to assess maturity levels? Would you suggest adding any other criteria to assess the maturity of a standard or interoperability specification?	• Publication of the standard at regulatory level • Standard overlap assessed with other existing national, multi-national, sector specific standards • Translation of the standard into functional, non-functional requirements • Technical implementation specifications of the standard published • Technical implementation of the standard deployed to early adopters • Technical implementation of the standard broadly deployed:
2	Perceived compatibility of identified standards and specifications with Data Act requirements Interpretation of DA requirements and processes to assess compatibility	For the harmonised standards and open interoperability specifications that you highlighted previously, to what extent do you consider that they are **compatible with the criteria established in the Data Act** (see those shown)? How could compliance best be assessed? The DA requires compliant standards / specifications to be "secure" and "open to innovation". How can these concepts best be elaborated and assessed? Compliant interoperability specifications and standards should also meet the criteria set out in Annex II of the Regulation 1025/2012 on European standardisation. How should the concepts of "**accepted by the market**", and developed by a non-profit making organisation in a process characterised by "**openness, consensus and transparency**" best be elaborated in the context of data processing services? Are there useful examples that can be taken from the application of Annex II in other areas? **What process should be followed** to check whether standards and open interoperability specifications meet the DA criteria and should therefore be considered for inclusion in the repository? Are you familiar with the CAMSS process for verifying the compliance of specifications against the criteria of Annex II of 1025/2012? Would this be a useful example?	1. Open interoperability specifications and harmonised standards for the interoperability of data processing services shall: (a) achieve, where technically feasible, interoperability between different data processing services that cover the **same service type;** (b) enhance portability of digital assets between different data processing services that cover the same service type; (c) facilitate, where technically feasible, functional equivalence between different data processing services referred to in Article 30(1) that cover the same service type; (d) **not have an adverse impact on the security and integrity** of data processing services and data; (e) be designed in such a way so as to **allow for technical advances and the inclusion of new functions and innovation** in data processing services. 2. Open interoperability specifications and harmonised standards for the interoperability of data processing services shall adequately address: (a) the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability; (b) the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability; (c) the cloud application aspects of application syntactic portability,

Task	Topic	Questions	Options to guide responses
			application instruction portability, application metadata portability, application behaviour portability and application policy portability. 3. Open interoperability specifications shall comply with Annex II to Regulation (EU) No 1025/2012
3	Perceived gaps in formal standards	We asked you before which you consider should be the top priority service types for the identification of open interoperability specifications and/or standards. Are there service types for which you consider that there are currently no existing DA compatible harmonised standards or open interoperability specifications? What could be possible **priority areas for new standardisation requests to be initiated by the EC? Are there existing open interoperability specifications that should in your view be formalised via a standardisation request?**	
2 & 4	Categorisation of open interoperability specifications and standards	Turning to the design of the repository as an online platform: What are the **most important parameters that you would want to use to be able to search of filter for relevant interoperability standards and specifications** on the repository. For example, how relevant would you consider the following?	**Objective** e.g. Interoperability between different services of the same service type; and/or Portability of digital assets. More specifically it could be specified which aspects are covered e.g. • Cloud functional and technical interoperability aspects (transport, syntactic, semantic, behavioural, policy) • Cloud data portability aspects (syntactic, semantic, policy) Other relevant criteria could include: • Status e.g. whether it is a formal standard or a common specification • Developer and developer type. In addition to the name of the body behind the standard it will be necessary to specify which type of body is involved e.g. industry association, public standards body • Service type: with reference e.g. to the types of service falling within the PaaS and SaaS categories e.g. as listed in Task 1 • Geographic area of application: whether the area of application is national, EU-wide, international or unspecified • Scope of application e.g. whether the standard is horizontal or focuses on specific sectors e.g. smart meters

Task	Topic	Questions	Options to guide responses
			• Status of approval e.g. whether the specification or standard has been approved or is still under development. • Degree of uptake e.g. the number and size of firms applying the given standard to the extent known

Annex 5 – Reviewed standardization processes of SDOs

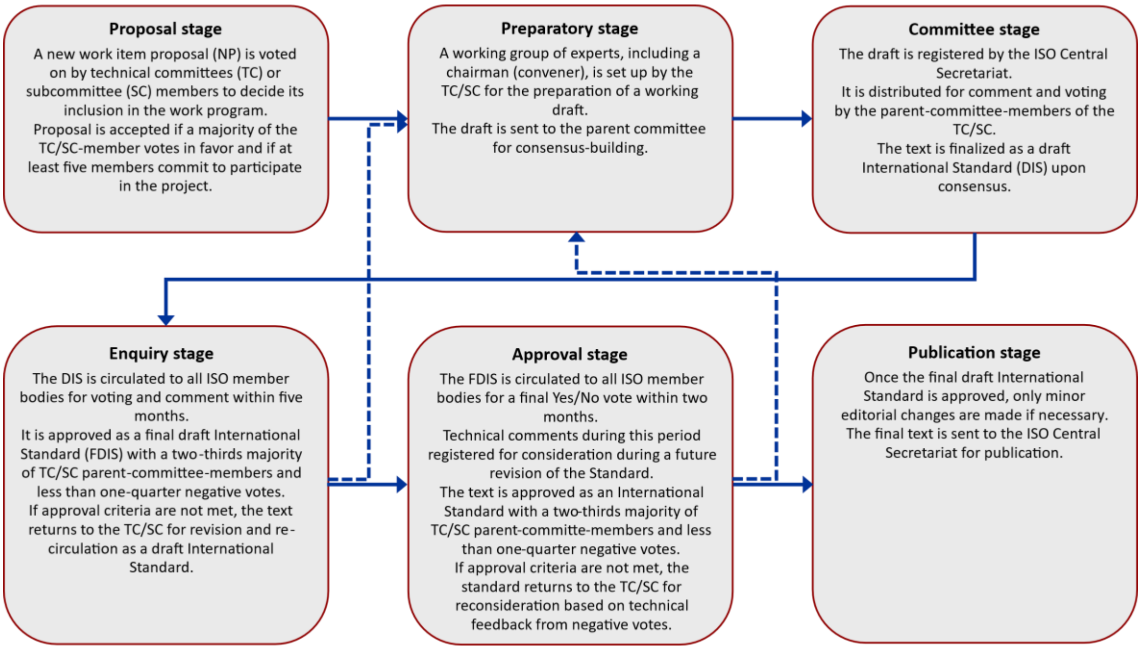
ISO standardization process

ISO develops six main categories of deliverables the **ISO Standards**, the **ISO/PAS Publicly Available Specifications**, the **ISO/TS Technical Specifications**, the **ISO/TR Technical Reports**, the **International Workshop Agreements/ IWA** and the **ISO Guides**.

When a stakeholder group expresses its requirement for a need for a standard to one of ISO's national members, the proposal is submitted to the relevant ISO technical committee or a new technical committee is established to cover a potential new field of activity. ([30])The majority support of the participating members of the ISO technical committee, amongst other criteria, verifies the "global relevance" of the proposed item. ([31])

International Standards are developed by ISO technical committees (TC) and subcommittees (SC) by a six-step process: ([32])

Process diagram for six-step process of ISO



Proposal stage
A new work item proposal (NP) is voted on by technical committees (TC) or subcommittee (SC) members to decide its inclusion in the work program.
Proposal is accepted if a majority of the TC/SC-member votes in favor and if at least five members commit to participate in the project.

Preparatory stage
A working group of experts, including a chairman (convener), is set up by the TC/SC for the preparation of a working draft.
The draft is sent to the parent committee for consensus-building.

Committee stage
The draft is registered by the ISO Central Secretariat.
It is distributed for comment and voting by the parent-committe-members of the TC/SC.
The text is finalized as a draft International Standard (DIS) upon consensus.

Enquiry stage
The DIS is circulated to all ISO member bodies for voting and comment within five months.
It is approved as a final draft International Standard (FDIS) with a two-thirds majority of TC/SC parent-committee-members and less than one-quarter negative votes.
If approval criteria are not met, the text returns to the TC/SC for revision and re-circulation as a draft International Standard.

Approval stage
The FDIS is circulated to all ISO member bodies for a final Yes/No vote within two months.
Technical comments during this period registered for consideration during a future revision of the Standard.
The text is approved as an International Standard with a two-thirds majority of TC/SC parent-committe-members and less than one-quarter negative votes.
If approval criteria are not met, the standard returns to the TC/SC for reconsideration based on technical feedback from negative votes.

Publication stage
Once the final draft International Standard is approved, only minor editorial changes are made if necessary.
The final text is sent to the ISO Central Secretariat for publication.

Source: WIK, based on Poustourli (2016): European and International Workshop Agreements: A Brief Example in Security Research Areas.

[30] Wirtanen, Salo (2009): Risk Management by Hygienic Design and Efficient Sanitation Programs.

[31] Wirtanen, Salo (2009): Risk Management by Hygienic Design and Efficient Sanitation Programs.

[32] Poustourli (2016): European and International Workshop Agreements: A Brief Example in Security Research Areas.

At the outset, each ISO deliverable is assigned to a standards development track. This track determines the timeframe of the project (18, 24, or 36 months) as it passes through the various stages to publication ([33]).

ISO's International Workshop Agreements (IWAs) are documents produced through a workshop meeting, rather than the full ISO technical committee process. Stakeholders do not have to address a national delegation and can directly participate in developing an IWA. Nevertheless, to give the project credibility, an ISO member body is assigned to help organize and run the workshop. The process should not take longer than 12 months ([34]).

ISO's IWAs are short-track processes, experiences here could be used to avoid that the envisaged process for the selection of candidate standards and specifications for the Data Act is not taking longer than necessary.

IEEE standardization process

IEEE standards are classified as **Standards** (documents with mandatory requirements), **Recommended Practices** (documents in which procedures and positions preferred by IEEE are presented), **Guides** (documents in which alternate approaches to good practices are suggested but no explicit recommendations are made) or **Trial-Use** (documents in effect for no more than three years. The documents can be a Standard, Recommended Practices or Guide).

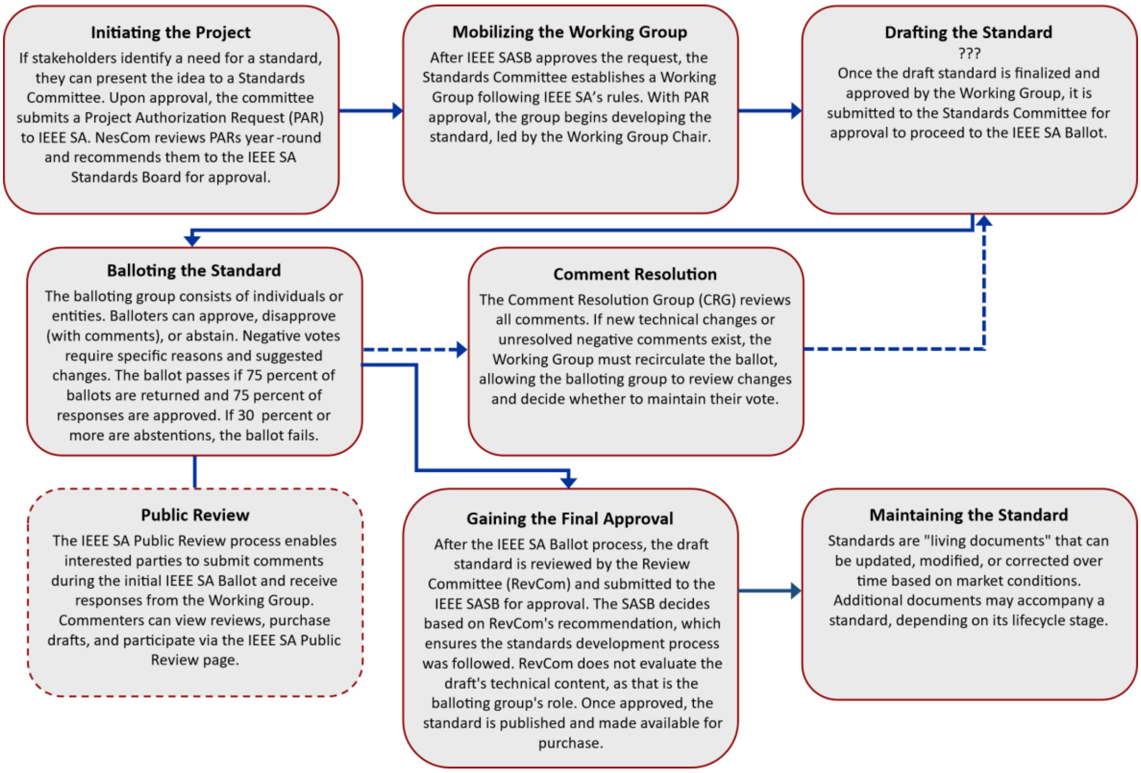
The development of an IEEE standard takes place in six stages: ([35])

[33] https://www.iso.org/stages-and-resources-for-standards-development.html

[34] Poustourli (2016): European and International Workshop Agreements: A Brief Example in Security Research Areas.

[35] https://standards.ieee.org/develop/initiating-project/

Process diagram for six-step process of IEEE



Initiating the Project

If stakeholders identify a need for a standard, they can present the idea to a Standards Committee. Upon approval, the committee submits a Project Authorization Request (PAR) to IEEE SA. NesCom reviews PARs year-round and recommends them to the IEEE SA Standards Board for approval.

Mobilizing the Working Group

After IEEE SASB approves the request, the Standards Committee establishes a Working Group following IEEE SA's rules. With PAR approval, the group begins developing the standard, led by the Working Group Chair.

Drafting the Standard

???

Once the draft standard is finalized and approved by the Working Group, it is submitted to the Standards Committee for approval to proceed to the IEEE SA Ballot.

Balloting the Standard

The balloting group consists of individuals or entities. Balloters can approve, disapprove (with comments), or abstain. Negative votes require specific reasons and suggested changes. The ballot passes if 75 percent of ballots are returned and 75 percent of responses are approved. If 30 percent or more are abstentions, the ballot fails.

Comment Resolution

The Comment Resolution Group (CRG) reviews all comments. If new technical changes or unresolved negative comments exist, the Working Group must recirculate the ballot, allowing the balloting group to review changes and decide whether to maintain their vote.

Public Review

The IEEE SA Public Review process enables interested parties to submit comments during the initial IEEE SA Ballot and receive responses from the Working Group. Commenters can view reviews, purchase drafts, and participate via the IEEE SA Public Review page.

Gaining the Final Approval

After the IEEE SA Ballot process, the draft standard is reviewed by the Review Committee (RevCom) and submitted to the IEEE SASB for approval. The SASB decides based on RevCom's recommendation, which ensures the standards development process was followed. RevCom does not evaluate the draft's technical content, as that is the balloting group's role. Once approved, the standard is published and made available for purchase.

Maintaining the Standard

Standards are "living documents" that can be updated, modified, or corrected over time based on market conditions. Additional documents may accompany a standard, depending on its lifecycle stage.

Source: WIK, based on https://standards.ieee.org/develop/initiating-project/.

European SDOs processes (CEN, CENELEC, ETSI)

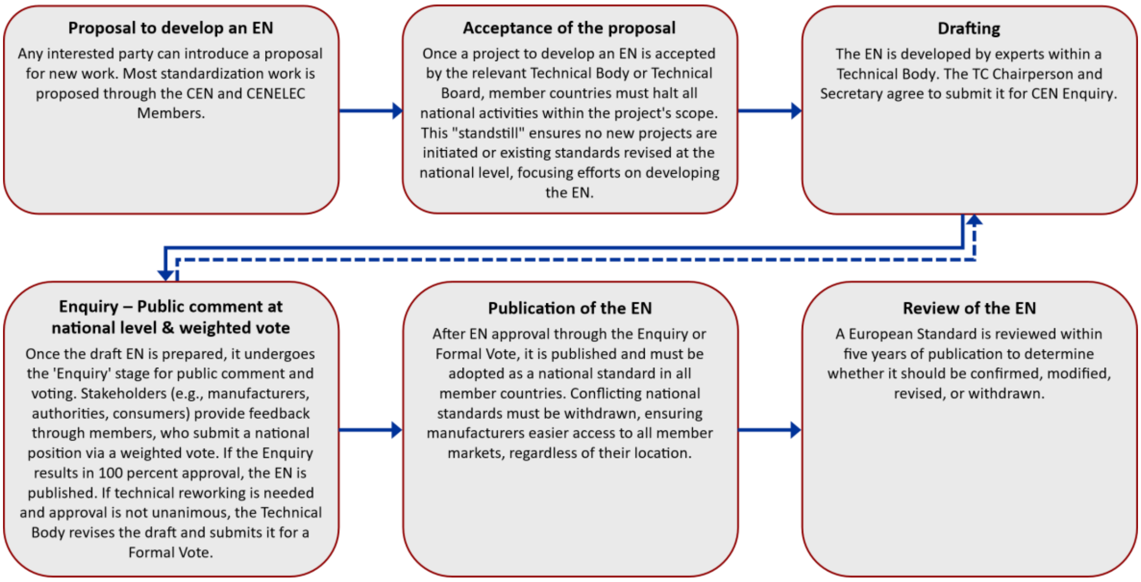
European Standards are developed by the three European SDOs: CEN, CENELEC and ETSI. The technical basis of a new standard is established through Pre-Normative Research (PNR). For new and emerging areas of technology a 'pre-standard', such as a Publicly Available Specification (PAS) or Technical Specification (TS) is prepared ([36]).

The development of a CEN/CENELEC standard takes place in six stages: ([37])

([36]) Poustourli (2016): European and International Workshop Agreements: A Brief Example in Security Research Areas.

([37]) https://standards.ieee.org/develop/initiating-project/

Process diagram for six-step process of CEN/CENELEC standard



Proposal to develop an EN

Any interested party can introduce a proposal for new work. Most standardization work is proposed through the CEN and CENELEC Members.

Acceptance of the proposal

Once a project to develop an EN is accepted by the relevant Technical Body or Technical Board, member countries must halt all national activities within the project's scope. This "standstill" ensures no new projects are initiated or existing standards revised at the national level, focusing efforts on developing the EN.

Drafting

The EN is developed by experts within a Technical Body. The TC Chairperson and Secretary agree to submit it for CEN Enquiry.

Enquiry – Public comment at national level & weighted vote

Once the draft EN is prepared, it undergoes the 'Enquiry' stage for public comment and voting. Stakeholders (e.g., manufacturers, authorities, consumers) provide feedback through members, who submit a national position via a weighted vote. If the Enquiry results in 100 percent approval, the EN is published. If technical reworking is needed and approval is not unanimous, the Technical Body revises the draft and submits it for a Formal Vote.

Publication of the EN

After EN approval through the Enquiry or Formal Vote, it is published and must be adopted as a national standard in all member countries. Conflicting national standards must be withdrawn, ensuring manufacturers easier access to all member markets, regardless of their location.

Review of the EN

A European Standard is reviewed within five years of publication to determine whether it should be confirmed, modified, revised, or withdrawn.

Source: WIK, based on https://boss.cen.eu/developingdeliverables/pages/en/pages/fv/.

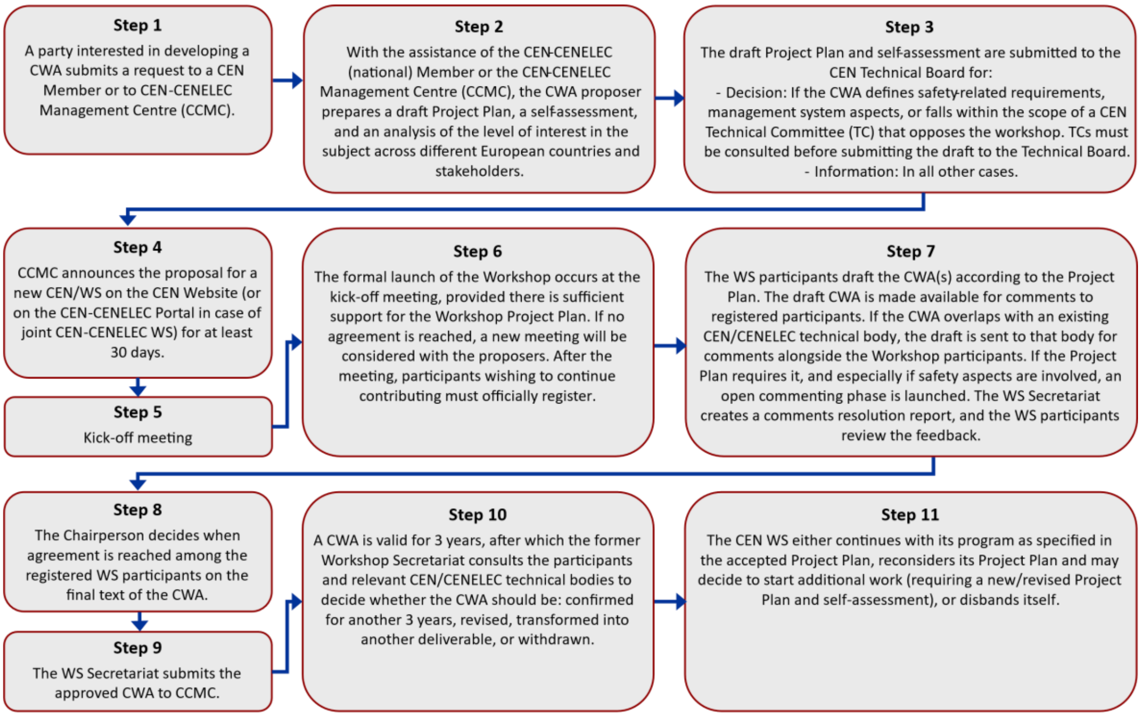
Besides **European Standards**, they produce **Technical Specifications** (TS), **Technical Reports** (TR), **Guides** and **CEN** and/or **CENELEC Workshop Agreements** (CWA).

A CWA is an agreement developed and approved in a CEN Workshop. The workshop is open to the direct participation of anyone with an interest in the development of the agreement (Participants may even be from outside Europe). It involves no obligation at national level. The development of a CWA lasts on average between 10-12 months. Nevertheless, it does not have the status of a European Standard but may not conflict with a European Standard ([38]). Notwithstanding the administrative requirements to implement a CWA, it is still one of the fastest options for an interested party to produce a type of standard.

The development of a CWA from CEN CENELEC needs 11 steps:

([38]) Poustourli (2016): European and International Workshop Agreements: A Brief Example in Security Research Areas.

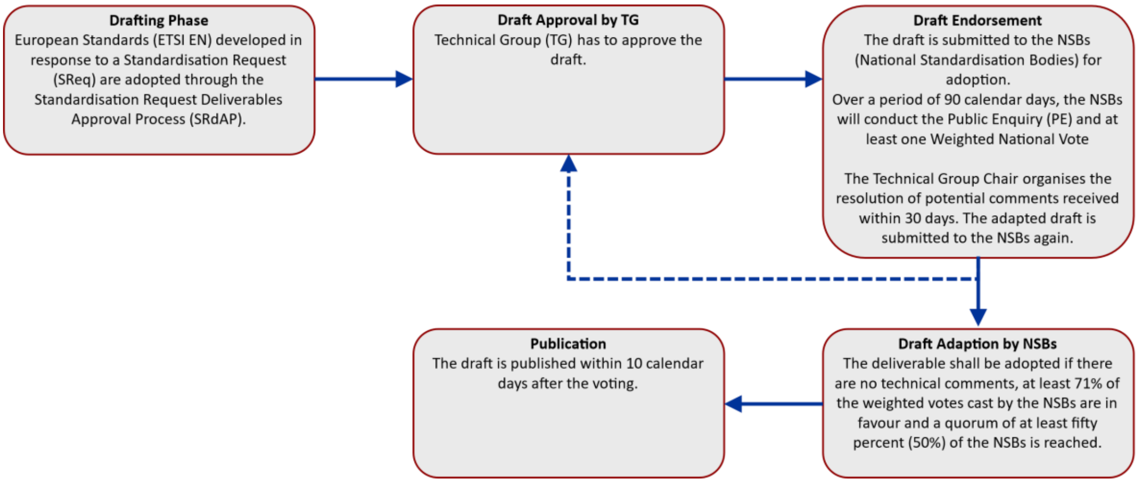
Process diagram for eleven-step process of a CWA from CEN CENELEC


Step 1
A party interested in developing a CWA submits a request to a CEN Member or to CEN-CENELEC Management Centre (CCMC).
Step 2
With the assistance of the CEN-CENELEC (national) Member or the CEN-CENELEC Management Centre (CCMC), the CWA proposer prepares a draft Project Plan, a self-assessment, and an analysis of the level of interest in the subject across different European countries and stakeholders.
Step 3
The draft Project Plan and self-assessment are submitted to the CEN Technical Board for:
- Decision: If the CWA defines safety-related requirements, management system aspects, or falls within the scope of a CEN Technical Committee (TC) that opposes the workshop. TCs must be consulted before submitting the draft to the Technical Board.
- Information: In all other cases.
Step 4
CCMC announces the proposal for a new CEN/WS on the CEN Website (or on the CEN-CENELEC Portal in case of joint CEN-CENELEC WS) for at least 30 days.
Step 5
Kick-off meeting
Step 6
The formal launch of the Workshop occurs at the kick-off meeting, provided there is sufficient support for the Workshop Project Plan. If no agreement is reached, a new meeting will be considered with the proposers. After the meeting, participants wishing to continue contributing must officially register.
Step 7
The WS participants draft the CWA(s) according to the Project Plan. The draft CWA is made available for comments to registered participants. If the CWA overlaps with an existing CEN/CENELEC technical body, the draft is sent to that body for comments alongside the Workshop participants. If the Project Plan requires it, and especially if safety aspects are involved, an open commenting phase is launched. The WS Secretariat creates a comments resolution report, and the WS participants review the feedback.
Step 8
The Chairperson decides when agreement is reached among the registered WS participants on the final text of the CWA.
Step 9
The WS Secretariat submits the approved CWA to CCMC.
Step 10
A CWA is valid for 3 years, after which the former Workshop Secretariat consults the participants and relevant CEN/CENELEC technical bodies to decide whether the CWA should be: confirmed for another 3 years, revised, transformed into another deliverable, or withdrawn.
Step 11
The CEN WS either continues with its program as specified in the accepted Project Plan, reconsiders its Project Plan and may decide to start additional work (requiring a new/revised Project Plan and self-assessment), or disbands itself.

Source: WIK, based on Poustourli (2016): European and International Workshop Agreements: A Brief Example in Security Research Areas.

The development of a European Standard (EN) from ETSI needs five steps:

Process diagram for five-step process of European Standard (EN) from ETSI


Drafting Phase
European Standards (ETSI EN) developed in response to a Standardisation Request (SReq) are adopted through the Standardisation Request Deliverables Approval Process (SRdAP).
Draft Approval by TG
Technical Group (TG) has to approve the draft.
Draft Endorsement
The draft is submitted to the NSBs (National Standardisation Bodies) for adoption.
Over a period of 90 calendar days, the NSBs will conduct the Public Enquiry (PE) and at least one Weighted National Vote
The Technical Group Chair organises the resolution of potential comments received within 30 days. The adapted draft is submitted to the NSBs again.
Draft Adaption by NSBs
The deliverable shall be adopted if there are no technical comments, at least 71% of the weighted votes cast by the NSBs are in favour and a quorum of at least fifty percent (50%) of the NSBs is reached.
Publication
The draft is published within 10 calendar days after the voting.

Source: WIK, based on https://ocgwiki.etsi.org/index.php?title=ETSI_Standards_Making_Process_Guide.

Besides ETSI EN (European Standard), ETSI also produces other types of deliverables, namely ETSI TS (ETSI Technical Specification) and ETSI TR (ETSI Technical Report), ETSI ES (ETSI Standard) and ETSI EG (ETSI Guide), ETSI SR (ETSI Special Report) as well as ETSI GS (ETSI Group Specification) and GR (ETSI Group Report).

Annex 6 – Criteria and means of verification

1) First screening

The means of verification in this screening are the same as defined in the CAMSS MSP Methodology:

Coherence principle

Criterion 4 (A4) – Does the technical specification or standard cover areas different from areas addressed by technical specifications being under consideration to become a European standard? (i.e. technical specifications provided by a non-formal standardisation organisation, that is other than CEN, CENELEC, or ETSI can be under consideration to become a European standard or alternatively an identified technical specification). In order to justify this criterion, research shall be carried out in several steps.

- First, the areas covered by the assessed specification and the number of SDOs and Technical Committees related to it shall be determined.
- Then these SDOs and Technical Committees' documentation shall be reviewed to find out if there is any mention of any specification being proposed to become a European standard, and that could cover any of the areas covered by the assessed specification.
- After this the documentation emitted by CEN, CENELEC, ETSI, and any other concerning European institutions shall be analysed to establish if any other specification that covers the same area as the assessed specification has been proposed to become a European standard.
    - https://www.cenelec.eu/
    - https://www.cen.eu/Pages/default.aspx
    - http://www.etsi.org/standards

Criterion 5a (A5a) – Is the adoption of new European Standards which cover the same areas as the proposed specification (or standard) foreseen within a reasonable timeframe?

"Reasonable timeframe" shall be understood merely as the fact that the specification has already been published in the documentation of any competent European institution as a specification proposed for becoming a European standard.

Criterion 5b (A5b) – Are there existing European standards with market uptake which cover the same areas as the proposed specification (or standard) being assessed?

In order to justify this criterion, research shall be carried out in ETSI/CEN/CENELEC or any other relevant European institution's repositories to check if there is any European standard that covers the same areas as the assessed specification. In case there is a match, the specification(s) shall be analysed to determine if it has market uptake.

- https://www.cenelec.eu/
- https://www.cen.eu/Pages/default.aspx
- http://www.etsi.org/standards

Governance

Criterion 6 (A6) – Is the standards developing organisation a non-profit organisation?

In order to justify this criterion, research shall be carried out regarding the SDO that owns the proposed specification to state if it is a non-profit-making organisation. Examples of non-profit organisations developing standards and specifications are the World Wide Web Consortium and the Internet Engineering Task Force (IETF).

- W3C: https://www.w3.org/
- IETF: https://www.ietf.org/

Criterion 8 (A8) – Are the specifications approved in a decision-making process which aims to reach consensus?

In order to justify this criterion, research shall be carried out on the process of development of the assessed specification. This research will aim to state if the process objective – and thereby the approval methodology – is the common consensus and to what degree. The justification will consist of a justified statement (YES/NO) and a brief description of the process. It can normally be found within the specification documentation or the SDO's website.

Criterion 9 (A9) – Is relevant documentation of the development and approval process of the specification archived and identified?

In order to justify this criterion, the repositories from the SDO that owns the specification shall be examined to determine if the development and approval process of the specification are documented. It can normally be found within the specification documentation or the SDO's website.

Criterion 10 (A10) – Is information on (new) standardisation activities widely announced through suitable and accessible means?

To justify this criterion, research shall be carried out regarding the process of publication of the (new) standardisation activities to state if this information is widely announced through suitable and accessible means.

For this purpose, the following shall be considered:

- Widely announced: The open, repetitive, and non-discriminative dissemination of information shall be considered as widely announced.
- Suitable means: All specialized means such as investigation reports, specialized magazines, and bulletins belonging to public organisations with competencies in the subject shall be considered suitable.
- Accessible: All means open to the public, without discrimination of any kind towards users, shall be considered accessible.

This information can be found within the specification documentation or the SDO's website.

Criterion 11 (A11) – Can all relevant stakeholders formally appeal or raise objections to the development and approval of specifications?

In order to provide a justification for this criterion, research shall be carried out on the process of development of the assessed specification to state if all relevant stakeholders can formally appeal or raise objections to the development and approval of specifications. The justification for this criterion will consist of examples of guidelines of the development process or documentation containing formal objections made to it by relevant stakeholders.

For this purpose, the stakeholders that shall be considered relevant will be those whose input could have a direct impact on the development process of the specification or on those other stakeholders whose input could have a direct impact on the development process of the specification. This information can be found within the specification documentation or the SDO's website.

Maintenance, availability and intellectual property

Criterion 12 (A12) – Does the specification have a defined maintenance and support process?

In order to justify this criterion, the SDO that owns the assessed specification shall be analysed to determine if it has set a defined maintenance and support process. This information can be found within the specification documentation or the SDO's website.

Criterion 13 (A13) – Is the specification publicly available for implementation and use on reasonable terms?

In order to justify this criterion, the SDO that owns the assessed specification shall be analysed to determine if it provides the specification for its implementation by the public under reasonable terms, considering reasonable terms all those that are not more restrictive than the average ones from other SDOs or organisations belonging to the specific field of application of the assessed specification.

Criterion 14a (A14a) – Is the specification licensed on a (F)RAND basis?

In order to justify this criterion, the license under which the assessed specification is released shall be analysed to determine if it is compliant with the (F)RAND licensing terms. This information can be found within the specification documentation or the SDO's website.

Criterion 14b (A14b) – Is the specification licensed on a royalty-free basis?

In order to justify this criterion, the license under which the assessed specification is released shall be analysed to determine if it is royalty-free. This information can be found within the specification documentation or the SDO's website.

2) Second screening

Market acceptance and quality question (remaining criteria from CAMSS MSP Assessment)

Criterion 1 (A1) – The technical specification or standard has been used for different implementations by different vendors/suppliers

The justification for this criterion will consist of a collection of different products or projects that include implementations of the assessed specification and that are developed or carried out by different vendors or suppliers.

Criterion 2 (A2) – The implementation of the technical specification or standard does not hamper interoperability with implementations that are currently based on existing European or international standards

To assess this criterion, follow these simplified steps:

- Check the specification's documentation for any mention of interoperability issues with existing European or international standards.
- Identify which existing standards are used by or related to the assessed specification, and whether they have been referenced by the MSP.
- Evaluate whether these related standards have wide market acceptance.

- If widely accepted, it can be assumed they do not hamper interoperability.

Criterion 17 (A17) – Has the specification sufficient detail, consistency, and completeness for the use and development of products and services?

The means of verification for the Data Act operationalised criteria are detailed in the table below:

Criteria for specifications	Guidance to identify specifications
The specification shall define mechanisms or interfaces for automating the translation or mapping of data between heterogeneous semantic models to enable interoperability.	- Automated translation between formats (e.g., JSON-LD ↔ RDF, XML ↔ JSON) - Refer to transformation frameworks like XSLT (XML), RML (RDF), or JSON-LD context definitions - Supports APIs or middleware for real-time data translation (e.g., OpenAPI, SPARQL
The specification shall implement mechanisms or technologies such as structured mappings between formats	- Documents or tables that explicitly map fields or elements from one format to another (e.g., from XML to JSON, or from a proprietary format to a standard like DCAT). - Use of tools or languages that support format transformation (XSLT, JQ, ETL pipelines, etc...)
The specification shall incorporate mechanisms or technologies, such as the definition of metadata elements, to ensure that descriptive, technical, and access metadata are clearly specified.	- Clear documentation specifying the metadata elements used (e.g., Dublin Core, DCAT, METS) or sample records showing actual metadata entries (e.g., JSON-LD, XML, RDF) - Metadata validation tools/scripts that check completeness and conformity to the schema or evidence of interoperability with data catalogs, registries, or search tools.
The specification shall implement mechanisms or technologies such as Widely accepted vocabularies like DCAT-AP, Dublin Core, Schema.org, ISO 11179 or domain-specific ones are mandated	Widely accepted vocabularies like DCAT-AP, Dublin Core, Schema.org, ISO 11179 or domain-specific ones are mandated.
The specification shall make use of, or be compatible with, established vocabularies or ontologies to ensure semantic consistency across systems.	- Check if it mandates ISO 19941, IEC CIM, or similar - Verify Data Structure & Ontology: Look for predefined entities, attributes, and vocabularies - Assess Interoperability: Ensure mappings to external standards exist.
The specification shall implement consistent data structures and use standardized serialization formats to ensure syntactic interoperability between systems.	- Focuses on standardized schemas, message formats, data representations. - May refer to XML, JSON, RDF, ISO/IEC 11179, NGSI-LD, etc.
The open specification shall define mechanisms or formats for expressing and enforcing access, consent, or data usage policies in a machine-readable and interoperable manner.	- May include reference to XACML, UMA, ABAC models, or policy vocabularies. - Emphasis on semantics of access and control across entities.
The specification shall define and document interface behaviors, workflows, and expected outcomes to ensure consistent interaction patterns across implementations.	- Relates to API behavior, expected inputs/outputs, sequence diagrams, etc. -Example: ISO/IEC 19941 or ETSI NFV reference behavior between components.

Criteria for specifications	Guidance to identify specifications
The specification shall support compatibility with open specifications that enable distributed identity management and federated access control (e.g., OAuth 2.0, OpenID Connect, DIDs).	- Federated identity protocols (such as SAML, OAuth 2.0 or OpenID Connect) - Decentralized identity frameworks (e.g., Self-Sovereign Identity, DID, Verifiable Credentials)
The specification shall define mechanisms, protocols, or interfaces to synchronize data and maintain consistency across systems or cloud providers.	- Cross-provider synchronization APIs (e.g., Change Data Capture, Webhooks) - Timestamping & version control (e.g., ISO 8601 timestamps, blockchain for audit trails)
The standard shall define principles, capabilities or frameworks to support event-driven architectures to enable real-time interoperability.	- Event-driven protocols - Supports real-time message streaming - Ensures compatibility with pub/sub models
The specification shall define mechanisms for describing, transferring, and re-deploying workloads across cloud providers, including portable application descriptions or deployment artifacts that ensure compatibility and reusability.	References to ISO/IEC 19944-1, OCI or an equivalent framework
The specification shall define concrete protocols, data models, APIs or interfaces that enable secure and interoperable data sharing between systems or organizations.	Mandates open data-sharing frameworks (IDS, GAIA-X).
The specification shall define interfaces, models, or deployment descriptors that enable consistent deployment of applications across different cloud providers.	- API compatibility with open standards (e.g., OpenAPI, CloudEvents) - Mandates containerization and orchestration support (e.g., Docker, Kubernetes) - Includes identity and access federation (e.g., OAuth 2.0, OIDC, SAML)
The specification shall implement mechanisms or technologies to verify data exchange rules, ensuring that APIs, databases, and file formats enforce data validation, integrity constraints, and conformance to defined schemas.	- Formal schema definitions (e.g., JSON Schema, XML Schema, SQL constraints) - At API level : OpenAPI (Swagger) or RAML - At database level : primary key & foreign key constraints
The specification shall define network communication using open and standardized protocols to ensure cross-system interoperability.	- Application Layer: HTTP/HTTPS, WebSockets, MQTT - Messaging Protocols: XMPP, Kafka, NATS
The specification shall define or use standardized serialization and deserialization formats to ensure consistent data exchange across services.	- Schema-based serialization formats - Human-Readable file formats - Real-Time Serialization Mechanisms
The specification shall implement authentication using widely adopted and open protocols.	- Token-Based Authentication: OAuth 2.0, OIDC (OpenID Connect) - Enterprise & Federated Authentication : SAML - Mutual Authentication : mTLS (Mutual TLS Authentication)
The specification shall implement mechanisms or technologies such as RESTful and Web-Based APIs.	RESTful and Web-Based APIs

Criteria for specifications	Guidance to identify specifications
The specification shall define and use machine-readable data formats to enable automated and seamless data exchange between systems.	- At file level: generic formats: JSON, XML, CSV, and RDF - At database level: Avro, Parquet, Protobuf - On industrial segments - specific formats: GeoJSON, EDIâ€¦
The open specification shall implement or define interfaces for federated identity management to enable secure cross-cloud authentication.	Compliance with security standards of ISO/IEC 29115
The specification shall implement mechanisms or technologies such as Cross-provider authentication (e.g., Identity Federation, Single Sign-On).	Cross-provider authentication (e.g., Identity Federation, Single Sign-On)
The open specification shall implement secure and encrypted communication for all API interactions, using industry-standard protocols.	TLS 1.2 version of higher
The specification shall support the incremental evolution of data models to accommodate new use cases without disrupting existing implementations.	- Supports schema extensibility (e.g., JSON Schema, XML Schema, RDF). - Allows custom metadata fields without breaking core functionality.
The specification shall include defined extension points or interfaces to allow third parties to add custom functionalities or integrations.	- Defines an extension framework with clear guidelines for third-party integrations. - Supports open APIs, SDKs, or plug-in architectures for modular enhancements.
The specification shall define mechanisms for API versioning and ensure backward compatibility to support long-term interoperability between systems.	- Defines API versioning rules (e.g., URI-based, header-based, or semantic versioning). - Ensures backward compatibility by maintaining support for older versions.
The specification shall support modular and decentralized system architectures to enable flexible integration and deployment across diverse environments.	- Defines a modular framework allowing independent component integration. - Supports decentralized architectures (e.g., microservices, distributed systems).
The specification shall implement mechanisms or technologies such as API compatibility tests.	API compatibility tests
The specification shall implement mechanisms or technologies such as Checksum validation, consistency checks.	Checksum validation, consistency checks
The specification must implement mechanisms or technologies such as rollback mechanisms in case of migration failures.	Rollback mechanisms in case of migration failures
The specification shall implement mechanisms or technologies such as API compatibility tests.	API compatibility tests

Annex 7 – Full list of gathered standards/ specification/ Tools/ other

Standard or Specification	Source	Saas / PaaS / Transversal	Tool / True Standard
Cri-O	Interview	PaaS	Tools
Docker	Interview	PaaS	Tools
Podman	Interview	PaaS	Tools
Helm	Interview	PaaS	Tools
S3 Api	Interview	PaaS	De Facto Standard
Istio	Interview	PaaS	Tools
ISO 19941:2017	Interview	Transversal	Standard
Oasis PKCS	Desk Research	Transversal	Specification
Oauth/ IETF RFC 6749	Interview	Transversal	Standard
OIDC (OpenID Connect)	Interview	Transversal	Specification
SAML	Interview	Transversal	Standard/ Specification
CBOR (IETF RFC 8949)	Desk Research	PaaS	Standard
GraphQL	Desk Research	PaaS	Specification
Open API	Interview	PaaS	Specification
Protocol Buffers	Interview	PaaS	Specification, Tools
Async API	Interview	PaaS	Specification
OData	Desk Research	PaaS	Standard/ Specification
ISO/IEC 27018:2019	Desk Research	Transversal	Standard
Open Container Initiative (OCI)	Interview	PaaS	Standard/ Specification
CDMI (Cloud Data Management Int.)/ ISO/IEC 17826:2022	Interview	PaaS	Standard
CloudEvents	Interview	PaaS	Standard/ Specification
AMQP (ISO/IEC 19464)	Interview	PaaS	Specification
MQTT (ISO/IEC 20922)	Interview	PaaS	Specification
RFC 6455 Websocket Protocol	Desk Research	Transversal	Standard
RFC 9556 IoT Devices cloud connectivity	Desk Research	PaaS	Standard
JSON/ IETF RFC 8259	Interview	PaaS	Standard/ Specification
XML	Interview	PaaS	Standard/ Specification
Oasis STIX	Desk Research	Transversal	Standard/ Specification
Oasis TAXII	Desk Research	Transversal	Standard/ Specification

Standard or Specification	Source	Saas / PaaS / Transversal	Tool / True Standard
CEN/TS 18026:2024	Desk Research	Transversal	Standard/ Technical Specification
EN ISO/IEC 27017:2021	Desk Research	Transversal	Harmonised Standard
ISO/IEC 17203:2017	Desk Research	Transversal	Standard
OASIS TOSCA	Desk Research	PaaS	Standard/ Specification
oneM2M	Survey	PaaS	Standard/ Framework
OGC API standards	Survey	PaaS	Standard
IEEE 2302-2021 (SIIF)	Survey	Transversal	Standard/ Specification
SQL	Survey	Transversal	Standard/ Scripting Language
ISO/IEC 19503:2005	Survey	Transversal	Standard
NIST SP 800-145 & 53	Survey	Transversal	Standard/ Specification
ISO/IEC 11179	Survey	PaaS	Standard
IEEE 1616.1-2023	Survey	PaaS	Standard
ISO 10303	Survey	SaaS	Standard
W3C SSI / DID	Survey	Transversal	Specification
SCIM	Survey	Transversal	Specification
FIDO	Survey	Transversal	Specification
W3C/ FIDO WebAuthn	Survey	Transversal	Specification
ADFS	Survey	Transversal	Tools
Entra ID (formerly Azure AD)	Survey	Transversal	Tools
X.509 (IETF RFC 5280)	Survey	Transversal	Standard/ Specification
OpenID4VCI	Survey	Transversal	Specification
OpenID4VP	Survey	Transversal	Specification
OAI-PMH	Survey	Transversal	Standard/ Specification
TLS/ RFC 5246	Survey	Transversal	Standard
ISO/IEC 27017/27018	Survey	Transversal	Standard
IPv6	Survey	Transversal	Standard/ Specification
CSV	Survey	Transversal	Standard/ Scripting Language

Annex 8 – Evaluation sheet – step 2 screening – Open API

Criterion Category	Criterion Sub Category	Criteria	Specification evaluated	Assessment	Compliance Level	Gap Analysis / Justification
Portability of digital assets	Semantic Interoperability	The specification shall define mechanisms or interfaces for automating the translation or mapping of data between heterogeneous semantic models to enable interoperability.	OpenAPI	OpenAPI is aimed at syntactic interoperability, not semantic interoperability.	Not applicable	
Portability of digital assets	Semantic Interoperability	The specification shall implement mechanisms or technologies such as structured mappings between formats	OpenAPI	OpenAPI is aimed at syntactic interoperability, not semantic interoperability.	Not applicable	
Portability of digital assets	Semantic Interoperability	The specification shall incorporate mechanisms or technologies, such as the definition of metadata elements, to ensure that descriptive, technical, and access metadata are clearly specified.	OpenAPI	OpenAPI is aimed at syntactic interoperability, not semantic interoperability.	Not applicable	
Portability of digital assets	Semantic Interoperability	The specification shall implement mechanisms or technologies such as widely accepted vocabularies like DCAT-AP, Dublin Core, Schema.org, ISO 11179 or domain-specific ones are mandated	OpenAPI	OpenAPI is aimed at syntactic interoperability, not semantic interoperability.	Not applicable	
Portability of digital assets	Semantic Interoperability	The specification shall make use of, or be compatible with, established vocabularies or ontologies to ensure semantic consistency across systems.	OpenAPI	OpenAPI is aimed at syntactic interoperability, not semantic interoperability.	Not applicable	
Portability of digital assets	Syntactic interoperability	The specification shall implement consistent data structures and use standardized serialization formats to ensure syntactic interoperability between systems.	OpenAPI	Full support for standardized formats like JSON, YAML, and support for JSON Schema-based data structures ensures syntactic interoperability.	Full compliance	
Interoperability between data processing services	Policy Interoperability	The open specification shall define mechanisms or formats for expressing and enforcing access, consent, or data usage policies in a machine-readable and interoperable manner.	OpenAPI	OpenAPI is aimed at syntactic interoperability, not semantic interoperability.	Not applicable	
Interoperability between data processing services	Behavioural Interoperability	The specification shall define and document interface behaviors, workflows, and expected outcomes to ensure consistent interaction patterns across implementations.	OpenAPI	OpenAPI is request/response; event semantics belong to AsyncAPI or CloudEvents.	Not applicable	

Criterion Category	Criterion Sub Category	Criteria	Specification evaluated	Assessment	Compliance Level	Gap Analysis / Justification
Interoperability between data processing services	Operational Interoperability	The specification shall support compatibility with open specifications that enable distributed identity management and federated access control (e.g., OAuth 2.0, OpenID Connect, DIDs).	OpenAPI	OpenAPI supports definition of security schemes including OAuth 2.0 and OpenID Connect via the securitySchemes object.	Full compliance	
Interoperability between data processing services	Operational Interoperability	The specification shall define mechanisms, protocols, or interfaces to synchronize data and maintain consistency across systems or cloud providers.	OpenAPI	Workload portability and deployment artefacts are outside OpenAPI;	Not applicable	
Interoperability between data processing services	Operational Interoperability	The standard shall define principles, capabilities or frameworks to support event-driven architectures to enable real-time interoperability	OpenAPI	OpenAPI is request-response focused. For event-driven APIs, the AsyncAPI specification is more suitable. We consider this not in scope of OpenAPI	Not applicable	
Interoperability between data processing services	Operational Interoperability	The specification shall define mechanisms for describing, transferring, and re-deploying workloads across cloud providers, including portable application descriptions or deployment artifacts that ensure compatibility and reusability	OpenAPI	OpenAPI does not describe deployment artifacts or workloads. It defines API interfaces only.	Not applicable	
Interoperability between data processing services	Operational Interoperability	The specification shall define concrete protocols, data models, APIs or interfaces that enable secure and interoperable data sharing between systems or organizations.	OpenAPI	OpenAPI defines interfaces and data models for APIs and supports secure schemes, enabling interoperable API definitions.	Full compliance	
Interoperability between data processing services	Operational Interoperability	The specification shall define interfaces, models, or deployment descriptors that enable consistent deployment of applications across different cloud providers.	OpenAPI	OpenAPI is not intended for describing deployment; does not cover deployment descriptors.	Not applicable	
Interoperability between data processing services	Technical Interoperability	The specification shall implement mechanisms or technologies to verify data exchange rules, ensuring that APIs, databases, and file formats enforce data validation, integrity constraints, and conformance to defined schemas.	OpenAPI	OpenAPI allows schema-based validation (using JSON Schema), enabling conformance checks for API inputs and outputs.	Full compliance	
Interoperability between data processing services	Technical Interoperability	The specification shall define network communication using open and standardized protocols to ensure cross-system interoperability.	OpenAPI	OpenAPI assumes use of HTTP(S), which is standardized and widely used, ensuring compatibility.	Full compliance	

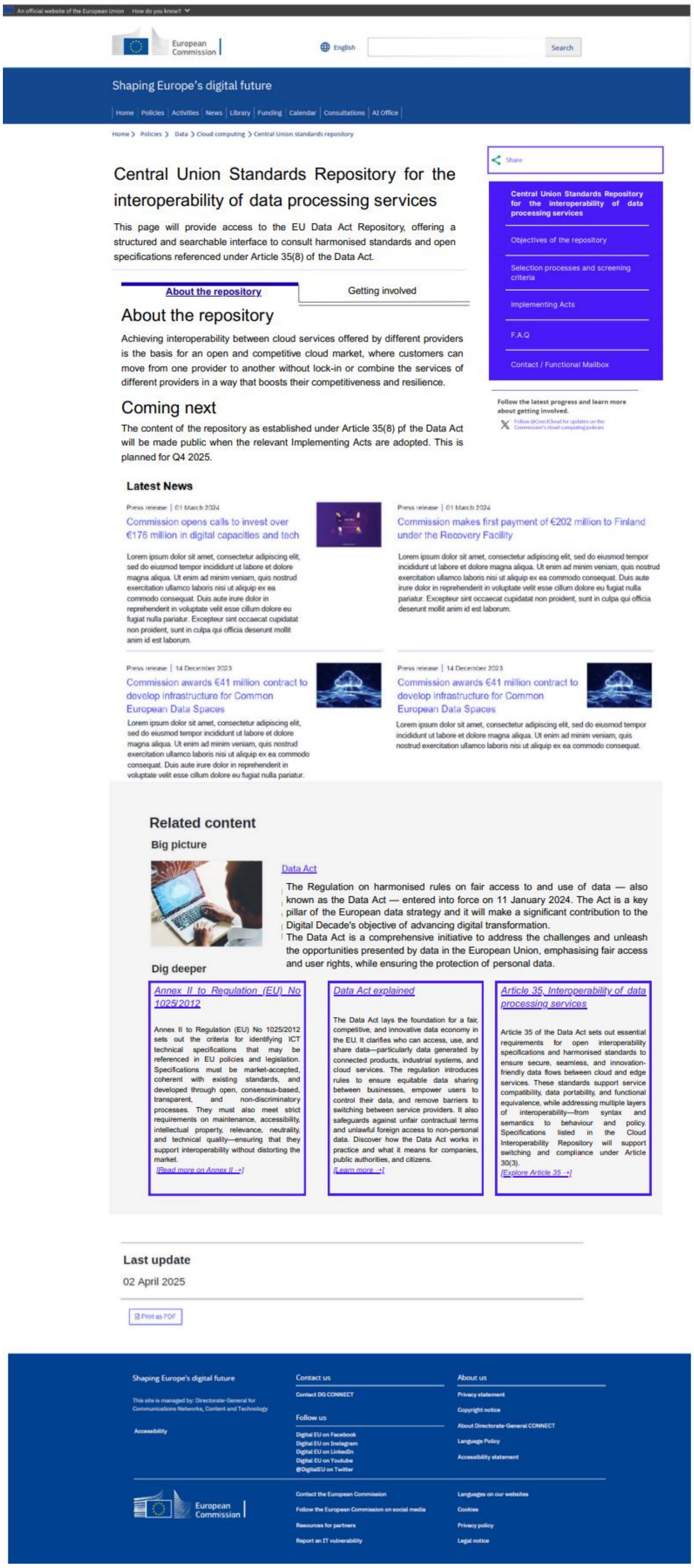
Criterion Category	Criterion Sub Category	Criteria	Specification evaluated	Assessment	Compliance Level	Gap Analysis / Justification
Interoperability between data processing services	Technical Interoperability	The specification shall define or use standardized serialization and deserialization formats to ensure consistent data exchange across services.	OpenAPI	OpenAPI supports JSON, XML and YAML formats and allows definition of content types (e.g., application/json), ensuring standard serialization.	Full compliance	
Interoperability between data processing services	Technical Interoperability	The specification shall implement authentication using widely adopted and open protocols	OpenAPI	Full support for OAuth2, OpenID Connect, API key, HTTP basic authentication—open and widely adopted protocols.	Full compliance	
Interoperability between data processing services	Technical Interoperability	The specification shall implement mechanisms or technologies such as RESTful and Web-Based APIs	OpenAPI	OpenAPI is primarily designed to describe RESTful APIs over HTTP(S).	Full compliance	
Interoperability between data processing services	Technical Interoperability	The specification shall define and use machine-readable data formats to enable automated and seamless data exchange between systems	OpenAPI	OpenAPI documents are machine-readable in JSON or YAML, and schemas are parseable to generate code, documentation, and clients.	Full compliance	
No adverse impact on security and integrity	System security and integrity	The open specification shall implement or define interfaces for federated identity management to enable secure cross-cloud authentication.	OpenAPI	OpenAPI allows the description of security schemes, including those for federated identity management, such as OAuth2 and OpenID Connect. However, it does not implement these interfaces itself; it provides a framework for their documentation.	Not applicable	OpenAPI is missing a profile/extension with normative conformance rules, IdP metadata and key sets, token/claim templates, and consent/usage-policy hooks to make federated identity machine-processable end-to-end.
No adverse impact on security and integrity	System security and integrity	The specification shall implement mechanisms or technologies such as Cross-provider authentication (e.g., Identity Federation, Single Sign-On)	OpenAPI	OpenAPI supports the documentation of cross-provider authentication mechanisms through its security schemes. However, it does not implement these mechanisms.	Not applicable	OpenAPI can describe cross-provider authentication. However, it relies on external implementations for actual functionality.
No adverse impact on security and integrity	System security and integrity	The open specification shall implement secure and encrypted communication for all API interactions, using industry-standard protocols.	OpenAPI	OpenAPI allows the specification of secure communication protocols (e.g., HTTPS) within API definitions but does not enforce or implement encryption itself.	Not applicable	OpenAPI enables the description of secure protocols but does not implement encryption mechanisms.

Criterion Category	Criterion Sub Category	Criteria	Specification evaluated	Assessment	Compliance Level	Gap Analysis / Justification
Not hindering innovation	Extensibility and Adaptability	The specification shall support the incremental evolution of data models to accommodate new use cases without disrupting existing implementations	OpenAPI	OpenAPI supports versioning and extensibility, allowing for the incremental evolution of APIs and data models.	Full Compliance	
Not hindering innovation	Extensibility and Adaptability	The specification shall include defined extension points or interfaces to allow third parties to add custom functionalities or integrations.	OpenAPI	OpenAPI supports specification extensions (vendor extensions) using the x- prefix, allowing third parties to add custom functionalities.	Full Compliance	
Not hindering innovation	Extensibility and Adaptability	The specification shall define mechanisms for API versioning and ensure backward compatibility to support long-term interoperability between systems.	OpenAPI	OpenAPI supports multiple versioning strategies, including URI versioning, header versioning, and query parameter versioning, aiding in maintaining backward compatibility.	Full Compliance	OpenAPI's support for various versioning methods ensures backward compatibility.
Not hindering innovation	Openness and flexibility	The specification shall support modular and decentralized system architectures to enable flexible integration and deployment across diverse environments.	OpenAPI	OpenAPI is agnostic to system architecture and can be used to describe APIs in modular and decentralized systems.	Full Compliance	
Functional Equivalence	Consistent service-level behavior	The specification shall implement mechanisms or technologies such as API compatibility tests	OpenAPI	Testing frameworks exist (Dredd, Spectral) but are not defined inside the open specification	Not applicable	
Functional Equivalence	Consistent service-level behavior	The specification shall implement mechanisms or technologies such as Checksum validation, consistency checks	OpenAPI	No checksum or signature features are included	Not applicable	
Functional Equivalence	Consistent service-level behavior	The specification must implement mechanisms or technologies such as rollback mechanisms in case of migration failures	OpenAPI	OpenAPI is a descriptive specification that doesn't tackle the technical implementation.	Not applicable	
Market Acceptance & quality	Market Acceptance	The technical specification or standard has been used for different implementations by different vendors/suppliers.	OpenAPI	OpenAPI is widely adopted across the industry, with numerous implementations by various vendors and suppliers.	Full Compliance	
Market Acceptance & quality	Market Acceptance	The implementation of the technical specification or standard does not hamper interoperability with implementations that are currently based on existing European or international standards.	OpenAPI	OpenAPI is designed to be compatible with existing standards and promotes interoperability across different systems and standards.	Full Compliance	
Market Acceptance & quality	Requirements	Has the specification sufficient detail, consistency, and completeness for the use and development of products and services?	OpenAPI	OpenAPI provides a comprehensive framework for defining APIs, offering sufficient detail, consistency, and completeness for product and service development.	Full Compliance	

Category	Score	Applicable criteria	Coverage	Score %	Results
Portability of digital assets	1	1	17%	100%	Partially compliant
Interoperability between data processing services	8	8	57%	100%	Compliant
No adverse impact on security and integrity	0	0			Not applicable
Not hindering innovation	4	4	100%	100%	Compliant
Functional Equivalence	0	0	0%	#DIV/0!	Not applicable
Market Acceptance & quality	3	3	100%	100%	Compliant
			Final Score	**100,00%**	
			Applicability of criteria	**48,48%**	

Annex 9 – Repository Mock-up

SEPTEMBER 2025 VERSION



Central Union Standards Repository for the interoperability of data processing services

This page will provide access to the EU Data Act Repository, offering a structured and searchable interface to consult harmonised standards and open specifications referenced under Article 35(8) of the Data Act.

About the repository
Getting involved

Central Union Standards Repository for the interoperability of data processing services

- Objectives of the repository
- Selection processes and screening criteria
- Implementing Acts
- F.A.Q
- Contact / Functional Mailbox

Follow the latest progress and learn more about getting involved.

Follow @CnectCloud for updates on the Commission's cloud computing policies

About the repository

Achieving interoperability between cloud services offered by different providers is the basis for an open and competitive cloud market, where customers can move from one provider to another without lock-in or combine the services of different providers in a way that boosts their competitiveness and resilience.

Coming next

The content of the repository as established under Article 35(8) pf the Data Act will be made public when the relevant Implementing Acts are adopted. This is planned for Q4 2025.

Latest News

Press release | 01 March 2024

Commission opens calls to invest over €176 million in digital capacities and tech

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 01 March 2024

Commission makes first payment of €202 million to Finland under the Recovery Facility

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Related content

Big picture

Data Act

The Regulation on harmonised rules on fair access to and use of data — also known as the Data Act — entered into force on 11 January 2024. The Act is a key pillar of the European data strategy and it will make a significant contribution to the Digital Decade's objective of advancing digital transformation.
The Data Act is a comprehensive initiative to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data.

Dig deeper

Annex II to Regulation (EU) No 1025/2012

Annex II to Regulation (EU) No 1025/2012 sets out the criteria for identifying ICT technical specifications that may be referenced in EU policies and legislation. Specifications must be market-accepted, coherent with existing standards, and developed through open, consensus-based, transparent, and non-discriminatory processes. They must also meet strict requirements on maintenance, accessibility, intellectual property, relevance, neutrality, and technical quality—ensuring that they support interoperability without distorting the market.

[Read more on Annex II →]

Data Act explained

The Data Act lays the foundation for a fair, competitive, and innovative data economy in the EU. It clarifies who can access, use, and share data—particularly data generated by connected products, industrial systems, and cloud services. The regulation introduces rules to ensure equitable data sharing between businesses, empower users to control their data, and remove barriers to switching between service providers. It also safeguards against unfair contractual terms and unlawful foreign access to non-personal data. Discover how the Data Act works in practice and what it means for companies, public authorities, and citizens.

[Learn more →]

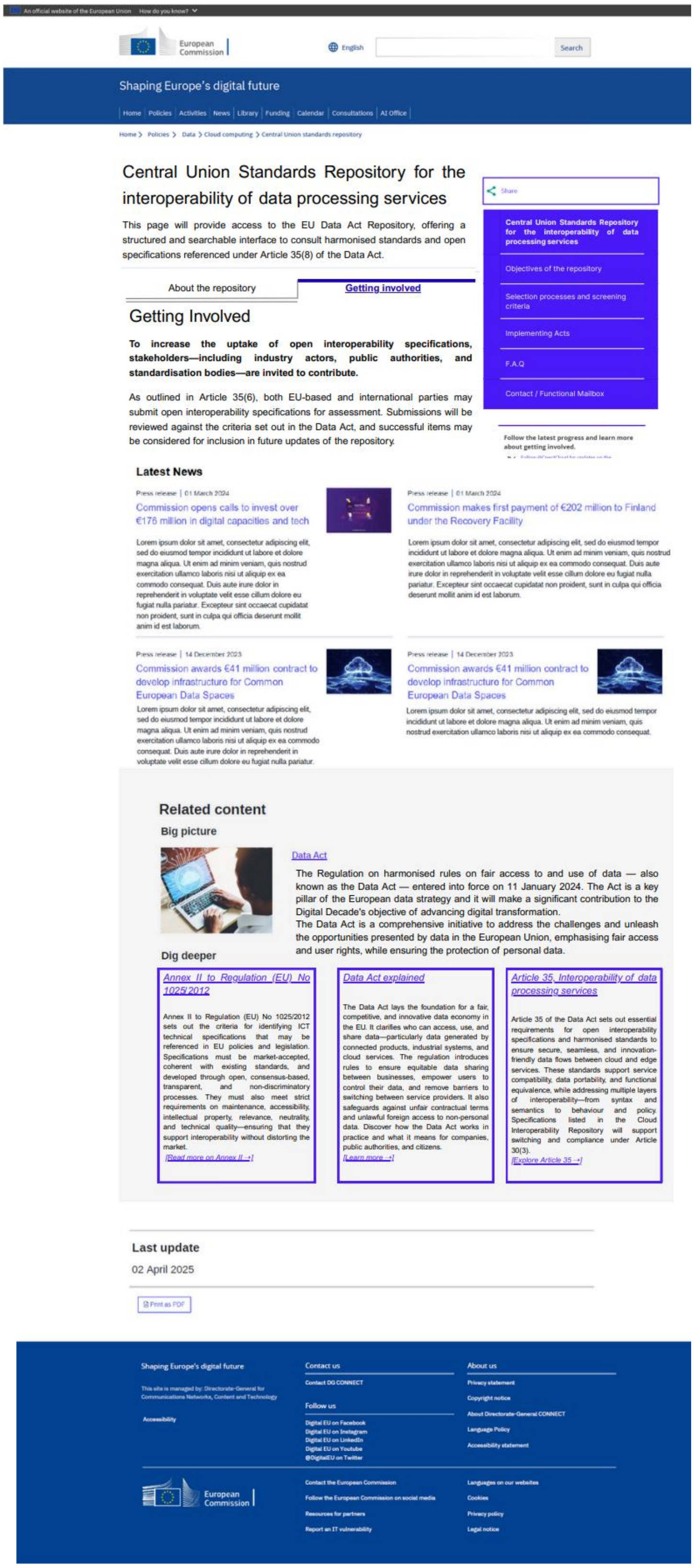
Article 35, Interoperability of data processing services

Article 35 of the Data Act sets out essential requirements for open interoperability specifications and harmonised standards to ensure secure, seamless, and innovation-friendly data flows between cloud and edge services. These standards support service compatibility, data portability, and functional equivalence, while addressing multiple layers of interoperability—from syntax and semantics to behaviour and policy. Specifications listed in the Cloud Interoperability Repository will support switching and compliance under Article 30(3).

[Explore Article 35 →]

Last update

02 April 2025



An official website of the European Union How do you know?
European Commission
English
Search
Shaping Europe's digital future
Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office
Home > Policies > Data > Cloud computing > Central Union standards repository
Share

Central Union Standards Repository for the interoperability of data processing services

This page will provide access to the EU Data Act Repository, offering a structured and searchable interface to consult harmonised standards and open specifications referenced under Article 35(8) of the Data Act.

Getting Involved

To increase the uptake of open interoperability specifications, stakeholders—including industry actors, public authorities, and standardisation bodies—are invited to contribute.

As outlined in Article 35(6), both EU-based and international parties may submit open interoperability specifications for assessment. Submissions will be reviewed against the criteria set out in the Data Act, and successful items may be considered for inclusion in future updates of the repository.

Central Union Standards Repository for the interoperability of data processing services
Objectives of the repository
Selection processes and screening criteria
Implementing Acts
F.A.Q
Contact / Functional Mailbox
Follow the latest progress and learn more about getting involved.
Follow @CnectCloud for updates on the

Latest News

Press release | 01 March 2024
Commission opens calls to invest over €176 million in digital capacities and tech
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 01 March 2024
Commission makes first payment of €202 million to Finland under the Recovery Facility
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 14 December 2023
Commission awards €41 million contract to develop infrastructure for Common European Data Spaces
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Press release | 14 December 2023
Commission awards €41 million contract to develop infrastructure for Common European Data Spaces
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Related content
Big picture
Data Act
The Regulation on harmonised rules on fair access to and use of data — also known as the Data Act — entered into force on 11 January 2024. The Act is a key pillar of the European data strategy and it will make a significant contribution to the Digital Decade's objective of advancing digital transformation.
The Data Act is a comprehensive initiative to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data.

Dig deeper
Annex II to Regulation (EU) No 1025/2012
Annex II to Regulation (EU) No 1025/2012 sets out the criteria for identifying ICT technical specifications that may be referenced in EU policies and legislation. Specifications must be market-accepted, coherent with existing standards, and developed through open, consensus-based, transparent, and non-discriminatory processes. They must also meet strict requirements on maintenance, accessibility, intellectual property, relevance, neutrality, and technical quality—ensuring that they support interoperability without distorting the market.
[Read more on Annex II →]

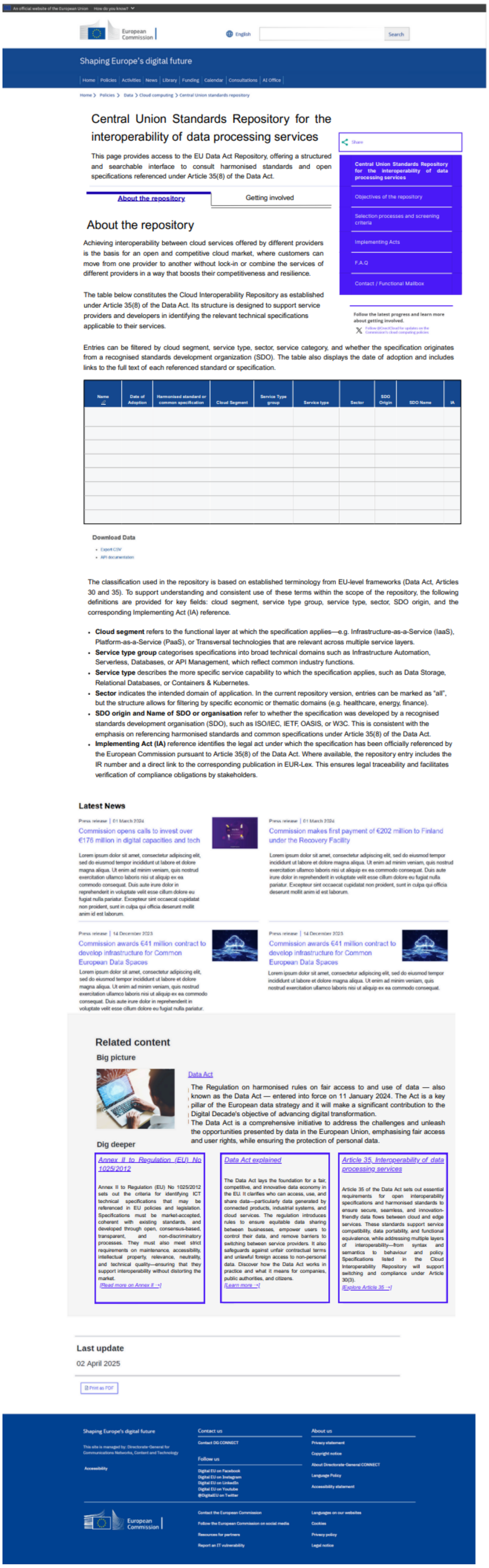
Data Act explained
The Data Act lays the foundation for a fair, competitive, and innovative data economy in the EU. It clarifies who can access, use, and share data—particularly data generated by connected products, industrial systems, and cloud services. The regulation introduces rules to ensure equitable data sharing between businesses, empower users to control their data, and remove barriers to switching between service providers. It also safeguards against unfair contractual terms and unlawful foreign access to non-personal data. Discover how the Data Act works in practice and what it means for companies, public authorities, and citizens.
[Learn more →]

Article 35, Interoperability of data processing services
Article 35 of the Data Act sets out essential requirements for open interoperability specifications and harmonised standards to ensure secure, seamless, and innovation-friendly data flows between cloud and edge services. These standards support service compatibility, data portability, and functional equivalence, while addressing multiple layers of interoperability—from syntax and semantics to behaviour and policy. Specifications listed in the Cloud Interoperability Repository will support switching and compliance under Article 30(3).
[Explore Article 35 →]

Last update
02 April 2025

Print as PDF
Shaping Europe's digital future
This site is managed by: Directorate-General for Communications Networks, Content and Technology
Accessibility
Contact us
Contact DG CONNECT
Follow us
Digital EU on Facebook
Digital EU on Instagram
Digital EU on LinkedIn
Digital EU on Youtube
@DigitalEU on Twitter
About us
Privacy statement
Copyright notice
About Directorate-General CONNECT
Language Policy
Accessibility statement
European Commission
Contact the European Commission
Follow the European Commission on social media
Resources for partners
Report an IT vulnerability
Languages on our websites
Cookies
Privacy policy
Legal notice

VERSION OF THE WEBSITE AFTER THE ADOPTION OF THE IMPLEMENTING ACTS



Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > Policies > Data > Cloud computing > Central Union standards repository

Central Union Standards Repository for the interoperability of data processing services

This page provides access to the EU Data Act Repository, offering a structured and searchable interface to consult harmonised standards and open specifications referenced under Article 35(8) of the Data Act.

- Central Union Standards Repository for the interoperability of data processing services
- Objectives of the repository
- Selection processes and screening criteria
- Implementing Acts
- F.A.Q
- Contact / Functional Mailbox

Follow the latest progress and learn more about getting involved.

Follow @CnectCloud for updates on the Commission's cloud computing policies

About the repository | Getting involved

About the repository

Achieving interoperability between cloud services offered by different providers is the basis for an open and competitive cloud market, where customers can move from one provider to another without lock-in or combine the services of different providers in a way that boosts their competitiveness and resilience.

The table below constitutes the Cloud Interoperability Repository as established under Article 35(8) of the Data Act. Its structure is designed to support service providers and developers in identifying the relevant technical specifications applicable to their services.

Entries can be filtered by cloud segment, service type, sector, service category, and whether the specification originates from a recognised standards development organization (SDO). The table also displays the date of adoption and includes links to the full text of each referenced standard or specification.

Name	Date of Adoption	Harmonised standard or common specification	Cloud Segment	Service Type group	Service type	Sector	SDO Origin	SDO Name	IA

Download Data

- Export CSV
- API documentation

The classification used in the repository is based on established terminology from EU-level frameworks (Data Act, Articles 30 and 35). To support understanding and consistent use of these terms within the scope of the repository, the following definitions are provided for key fields: cloud segment, service type group, service type, sector, SDO origin, and the corresponding Implementing Act (IA) reference.

- **Cloud segment** refers to the functional layer at which the specification applies—e.g. Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or Transversal technologies that are relevant across multiple service layers.
- **Service type group** categorises specifications into broad technical domains such as Infrastructure Automation, Serverless, Databases, or API Management, which reflect common industry functions.
- **Service type** describes the more specific service capability to which the specification applies, such as Data Storage, Relational Databases, or Containers & Kubernetes.
- **Sector** indicates the intended domain of application. In the current repository version, entries can be marked as "all", but the structure allows for filtering by specific economic or thematic domains (e.g. healthcare, energy, finance).
- **SDO origin and Name of SDO or organisation** refer to whether the specification was developed by a recognised standards development organisation (SDO), such as ISO/IEC, IETF, OASIS, or W3C. This is consistent with the emphasis on referencing harmonised standards and common specifications under Article 35(8) of the Data Act.
- **Implementing Act (IA)** reference identifies the legal act under which the specification has been officially referenced by the European Commission pursuant to Article 35(8) of the Data Act. Where available, the repository entry includes the IR number and a direct link to the corresponding publication in EUR-Lex. This ensures legal traceability and facilitates verification of compliance obligations by stakeholders.

Latest News

Press release | 01 March 2024

Commission opens calls to invest over €176 million in digital capacities and tech

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 01 March 2024

Commission makes first payment of €202 million to Finland under the Recovery Facility

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Related content

Big picture

Data Act

The Regulation on harmonised rules on fair access to and use of data — also known as the Data Act — entered into force on 11 January 2024. The Act is a key pillar of the European data strategy and it will make a significant contribution to the Digital Decade's objective of advancing digital transformation.
The Data Act is a comprehensive initiative to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data.

Dig deeper

Annex II to Regulation (EU) No 1025/2012

Annex II to Regulation (EU) No 1025/2012 sets out the criteria for identifying ICT technical specifications that may be referenced in EU policies and legislation. Specifications must be market-accepted, coherent with existing standards, and developed through open, consensus-based, transparent, and non-discriminatory processes. They must also meet strict requirements on maintenance, accessibility, intellectual property, relevance, neutrality, and technical quality—ensuring that they support interoperability without distorting the market.

[Read more on Annex II →]

Data Act explained

The Data Act lays the foundation for a fair, competitive, and innovative data economy in the EU. It clarifies who can access, use, and share data—particularly data generated by connected products, industrial systems, and cloud services. The regulation introduces rules to ensure equitable data sharing between businesses, empower users to control their data, and remove barriers to switching between service providers. It also safeguards against unfair contractual terms and unlawful foreign access to non-personal data. Discover how the Data Act works in practice and what it means for companies, public authorities, and citizens.

[Learn more →]

Article 35, Interoperability of data processing services

Article 35 of the Data Act sets out essential requirements for open interoperability specifications and harmonised standards to ensure secure, seamless, and innovation-friendly data flows between cloud and edge services. These standards support service compatibility, data portability, and functional equivalence, while addressing multiple layers of interoperability—from syntax and semantics to behaviour and policy. Specifications listed in the Cloud Interoperability Repository will support switching and compliance under Article 30(3).

[Explore Article 35 →]

Last update

02 April 2025

Print as PDF

Shaping Europe's digital future

This site is managed by: Directorate-General for Communications Networks, Content and Technology

Accessibility

Contact us

Contact DG CONNECT

Follow us

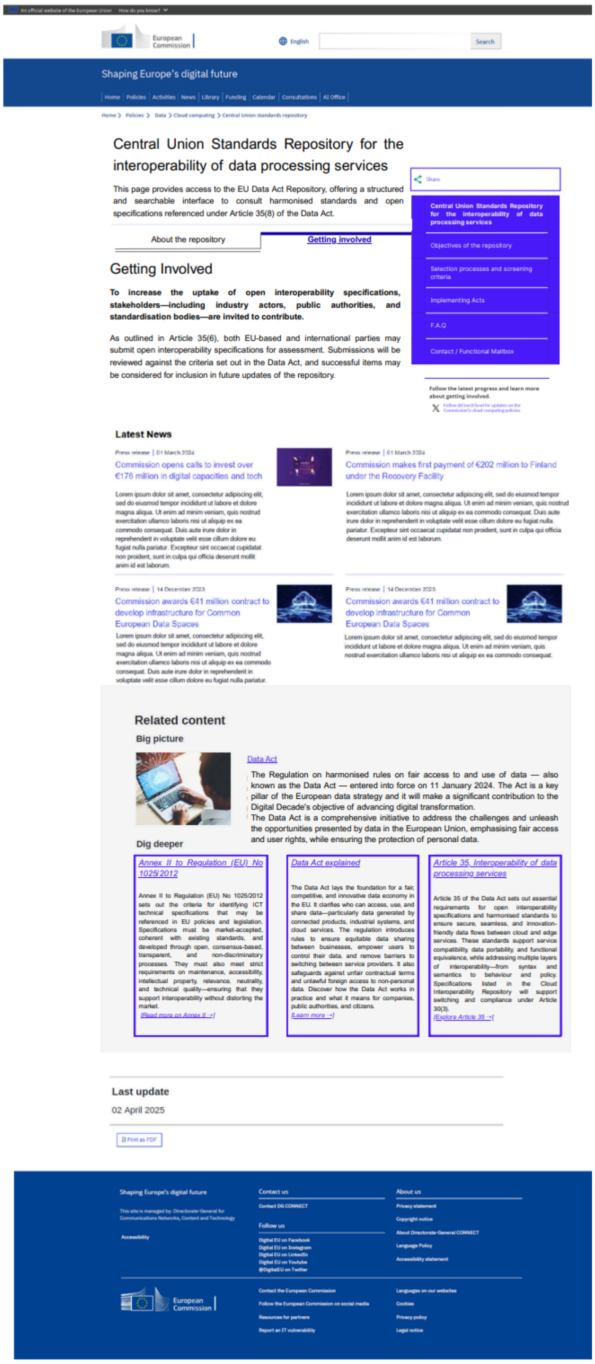
Digital EU on Facebook
Digital EU on Instagram
Digital EU on LinkedIn
Digital EU on Youtube
@DigitalEU on Twitter

About us

Privacy statement
Copyright notice
About Directorate-General CONNECT
Language Policy
Accessibility statement

Contact the European Commission
Follow the European Commission on social media
Resources for partners
Report an IT vulnerability

Languages on our websites
Cookies
Privacy policy
Legal notice



Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office

Home > Policies > Data > Cloud computing > Central Union standards repository

Central Union Standards Repository for the interoperability of data processing services

This page provides access to the EU Data Act Repository, offering a structured and searchable interface to consult harmonised standards and open specifications referenced under Article 35(8) of the Data Act.

- Central Union Standards Repository for the interoperability of data processing services
- Objectives of the repository
- Selection processes and screening criteria
- Implementing Acts
- F.A.Q
- Contact / Functional Mailbox

About the repository | Getting involved

Getting Involved

To increase the uptake of open interoperability specifications, stakeholders—including industry actors, public authorities, and standardisation bodies—are invited to contribute.

As outlined in Article 35(6), both EU-based and international parties may submit open interoperability specifications for assessment. Submissions will be reviewed against the criteria set out in the Data Act, and successful items may be considered for inclusion in future updates of the repository.

Follow the latest progress and learn more about getting involved.

Follow @CnectCloud for updates on the Commission's cloud computing policies

Latest News

Press release | 01 March 2024

Commission opens calls to invest over €176 million in digital capacities and tech

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 01 March 2024

Commission makes first payment of €202 million to Finland under the Recovery Facility

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Related content

Big picture

Data Act

The Regulation on harmonised rules on fair access to and use of data — also known as the Data Act — entered into force on 11 January 2024. The Act is a key pillar of the European data strategy and it will make a significant contribution to the Digital Decade's objective of advancing digital transformation.
The Data Act is a comprehensive initiative to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data.

Dig deeper

Annex II to Regulation (EU) No 1025/2012

Annex II to Regulation (EU) No 1025/2012 sets out the criteria for identifying ICT technical specifications that may be referenced in EU policies and legislation. Specifications must be market-accepted, coherent with existing standards, and developed through open, consensus-based, transparent, and non-discriminatory processes. They must also meet strict requirements on maintenance, accessibility, intellectual property, relevance, neutrality, and technical quality—ensuring that they support interoperability without distorting the market.

[Read more on Annex II →]

Data Act explained

The Data Act lays the foundation for a fair, competitive, and innovative data economy in the EU. It clarifies who can access, use, and share data—particularly data generated by connected products, industrial systems, and cloud services. The regulation introduces rules to ensure equitable data sharing between businesses, empower users to control their data, and remove barriers to switching between service providers. It also safeguards against unfair contractual terms and unlawful foreign access to non-personal data. Discover how the Data Act works in practice and what it means for companies, public authorities, and citizens.

[Learn more →]

Article 35, Interoperability of data processing services

Article 35 of the Data Act sets out essential requirements for open interoperability specifications and harmonised standards to ensure secure, seamless, and innovation-friendly data flows between cloud and edge services. These standards support service compatibility, data portability, and functional equivalence, while addressing multiple layers of interoperability—from syntax and semantics to behaviour and policy. Specifications listed in the Cloud Interoperability Repository will support switching and compliance under Article 30(3).

[Explore Article 35 →]

Last update

02 April 2025

Print as PDF

Shaping Europe's digital future

This site is managed by: Directorate-General for Communications Networks, Content and Technology

Accessibility

Contact us

Contact DG CONNECT

Follow us

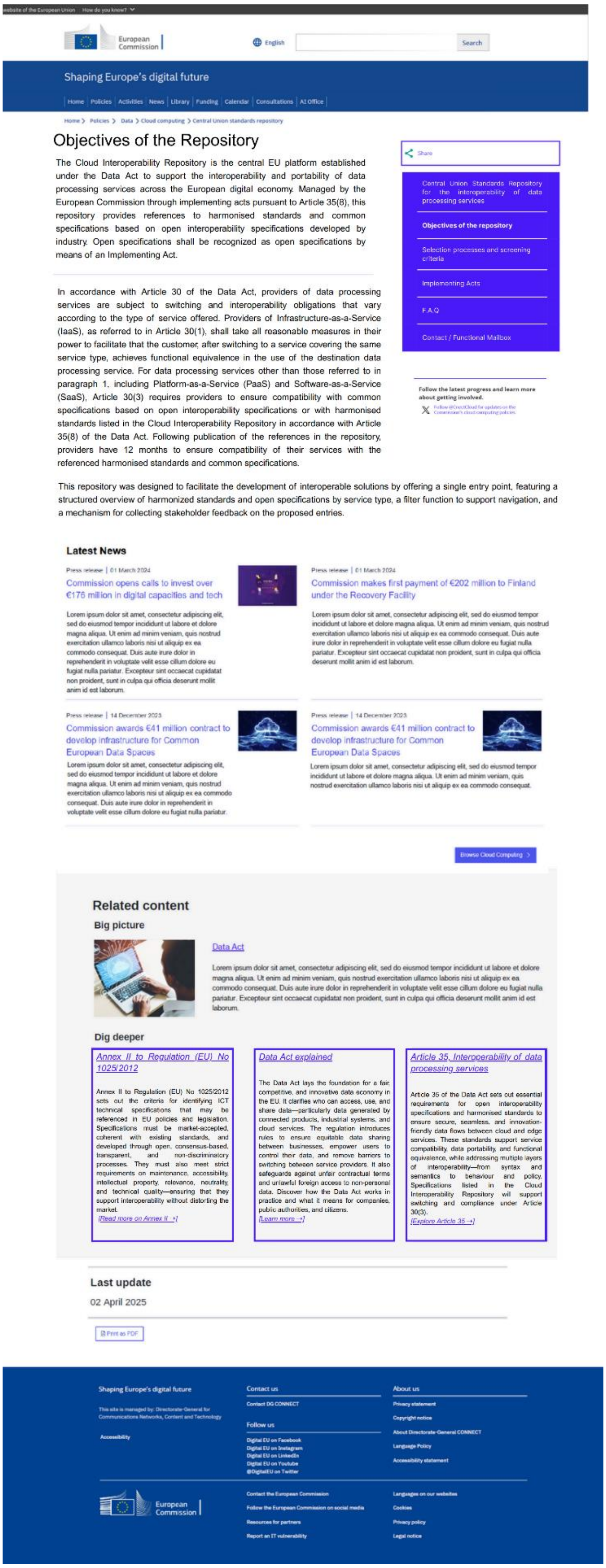
Digital EU on Facebook
Digital EU on Instagram
Digital EU on LinkedIn
Digital EU on Youtube
@DigitalEU on Twitter

About us

Privacy statement
Copyright notice
About Directorate-General CONNECT
Language Policy
Accessibility statement

Contact the European Commission
Follow the European Commission on social media
Resources for partners
Report an IT vulnerability

Languages on our websites
Cookies
Privacy policy
Legal notice



website of the European Union How do you know?
European Commission
English
Search
Shaping Europe's digital future
Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office
Home > Policies > Data > Cloud computing > Central Union standards repository

Objectives of the Repository

Share
Central Union Standards Repository for the interoperability of data processing services
Objectives of the repository
Selection processes and screening criteria
Implementing Acts
F.A.Q
Contact / Functional Mailbox

The Cloud Interoperability Repository is the central EU platform established under the Data Act to support the interoperability and portability of data processing services across the European digital economy. Managed by the European Commission through implementing acts pursuant to Article 35(8), this repository provides references to harmonised standards and common specifications based on open interoperability specifications developed by industry. Open specifications shall be recognized as open specifications by means of an Implementing Act.

In accordance with Article 30 of the Data Act, providers of data processing services are subject to switching and interoperability obligations that vary according to the type of service offered. Providers of Infrastructure-as-a-Service (IaaS), as referred to in Article 30(1), shall take all reasonable measures in their power to facilitate that the customer, after switching to a service covering the same service type, achieves functional equivalence in the use of the destination data processing service. For data processing services other than those referred to in paragraph 1, including Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), Article 30(3) requires providers to ensure compatibility with common specifications based on open interoperability specifications or with harmonised standards listed in the Cloud Interoperability Repository in accordance with Article 35(8) of the Data Act. Following publication of the references in the repository, providers have 12 months to ensure compatibility of their services with the referenced harmonised standards and common specifications.

Follow the latest progress and learn more about getting involved.

Follow @CnectCloud for updates on the Commission's cloud computing policies

This repository was designed to facilitate the development of interoperable solutions by offering a single entry point, featuring a structured overview of harmonized standards and open specifications by service type, a filter function to support navigation, and a mechanism for collecting stakeholder feedback on the proposed entries.

Latest News

Press release | 01 March 2024

Commission opens calls to invest over €176 million in digital capacities and tech

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 01 March 2024

Commission makes first payment of €202 million to Finland under the Recovery Facility

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Related content

Big picture

Data Act

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Dig deeper

Annex II to Regulation (EU) No 1025/2012

Annex II to Regulation (EU) No 1025/2012 sets out the criteria for identifying ICT technical specifications that may be referenced in EU policies and legislation. Specifications must be market-accepted, coherent with existing standards, and developed through open, consensus-based, transparent, and non-discriminatory processes. They must also meet strict requirements on maintenance, accessibility, intellectual property, relevance, neutrality, and technical quality—ensuring that they support interoperability without distorting the market.

[Read more on Annex II →]

Data Act explained

The Data Act lays the foundation for a fair, competitive, and innovative data economy in the EU. It clarifies who can access, use, and share data—particularly data generated by connected products, industrial systems, and cloud services. The regulation introduces rules to ensure equitable data sharing between businesses, empower users to control their data, and remove barriers to switching between service providers. It also safeguards against unfair contractual terms and unlawful foreign access to non-personal data. Discover how the Data Act works in practice and what it means for companies, public authorities, and citizens.

[Learn more →]

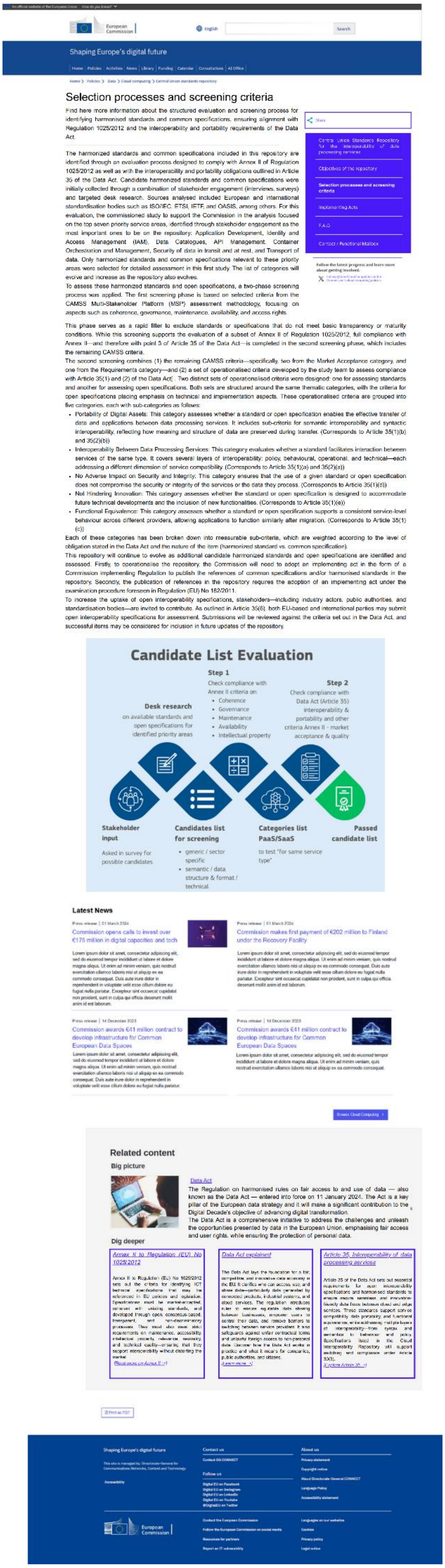
Article 35, Interoperability of data processing services

Article 35 of the Data Act sets out essential requirements for open interoperability specifications and harmonised standards to ensure secure, seamless, and innovation-friendly data flows between cloud and edge services. These standards support service compatibility, data portability, and functional equivalence, while addressing multiple layers of interoperability—from syntax and semantics to behaviour and policy. Specifications listed in the Cloud Interoperability Repository will support switching and compliance under Article 30(3).

[Explore Article 35 →]

Last update

02 April 2025



An official website of the European Union | How do you know?
European Commission
English
Search
Shaping Europe's digital future
Home | Policies | Activities | News | Library | Funding | Calendar | Consultations | AI Office
Home > Policies > Data > Cloud computing > Central Union standards repository

Selection processes and screening criteria

Find here more information about the structured evaluation and screening process for identifying harmonised standards and common specifications, ensuring alignment with Regulation 1025/2012 and the interoperability and portability requirements of the Data Act.

Share
Central Union Standards Repository for the interoperability of data processing services
Objectives of the repository
Selection processes and screening criteria
Implementing Acts
F.A.Q
Contact - Functional Mailbox
Follow the latest progress and learn more about getting involved.
[illegible]

The harmonized standards and common specifications included in this repository are identified through an evaluation process designed to comply with Annex II of Regulation 1025/2012 as well as with the interoperability and portability obligations outlined in Article 35 of the Data Act. Candidate harmonized standards and common specifications were initially collected through a combination of stakeholder engagement (interviews, surveys) and targeted desk research. Sources analysed included European and international standardisation bodies such as ISO/IEC, ETSI, IETF, and OASIS, among others. For this evaluation, the commissioned study to support the Commission in the analysis focused on the top seven priority service areas, identified through stakeholder engagement as the most important ones to be on the repository: Application Development, Identity and Access Management (IAM), Data Catalogues, API Management, Container Orchestration and Management, Security of data in transit and at rest, and Transport of data. Only harmonized standards and common specifications relevant to these priority areas were selected for detailed assessment in this first study. The list of categories will evolve and increase as the repository also evolves.

To assess these harmonized standards and open specifications, a two-phase screening process was applied. The first screening phase is based on selected criteria from the CAMSS Multi-Stakeholder Platform (MSP) assessment methodology, focusing on aspects such as coherence, governance, maintenance, availability, and access rights.

This phase serves as a rapid filter to exclude standards or specifications that do not meet basic transparency or maturity conditions. While this screening supports the evaluation of a subset of Annex II of Regulation 1025/2012, full compliance with Annex II—and therefore with point 3 of Article 35 of the Data Act—is completed in the second screening phase, which includes the remaining CAMSS criteria.

The second screening combines (1) the remaining CAMSS criteria—specifically, two from the Market Acceptance category, and one from the Requirements category—and (2) a set of operationalised criteria developed by the study team to assess compliance with Article 35(1) and (2) of the Data Act[. Two distinct sets of operationalised criteria were designed: one for assessing standards and another for assessing open specifications. Both sets are structured around the same thematic categories, with the criteria for open specifications placing emphasis on technical and implementation aspects. These operationalised criteria are grouped into five categories, each with sub-categories as follows:

- Portability of Digital Assets: This category assesses whether a standard or open specification enables the effective transfer of data and applications between data processing services. It includes sub-criteria for semantic interoperability and syntactic interoperability, reflecting how meaning and structure of data are preserved during transfer. (Corresponds to Article 35(1)(b) and 35(2)(b))
- Interoperability Between Data Processing Services: This category evaluates whether a standard facilitates interaction between services of the same type. It covers several layers of interoperability: policy, behavioural, operational, and technical—each addressing a different dimension of service compatibility. (Corresponds to Article 35(1)(a) and 35(2)(a))
- No Adverse Impact on Security and Integrity: This category ensures that the use of a given standard or open specification does not compromise the security or integrity of the services or the data they process. (Corresponds to Article 35(1)(d))
- Not Hindering Innovation: This category assesses whether the standard or open specification is designed to accommodate future technical developments and the inclusion of new functionalities. (Corresponds to Article 35(1)(e))
- Functional Equivalence: This category assesses whether a standard or open specification supports a consistent service-level behaviour across different providers, allowing applications to function similarly after migration. (Corresponds to Article 35(1)(c))

Each of these categories has been broken down into measurable sub-criteria, which are weighted according to the level of obligation stated in the Data Act and the nature of the item (harmonized standard vs. common specification).

This repository will continue to evolve as additional candidate harmonized standards and open specifications are identified and assessed. Firstly, to operationalise the repository, the Commission will need to adopt an implementing act in the form of a Commission implementing Regulation to publish the references of common specifications and/or harmonised standards in the repository. Secondly, the publication of references in the repository requires the adoption of an implementing act under the examination procedure foreseen in Regulation (EU) No 182/2011.

To increase the uptake of open interoperability specifications, stakeholders—including industry actors, public authorities, and standardisation bodies—are invited to contribute. As outlined in Article 35(6), both EU-based and international parties may submit open interoperability specifications for assessment. Submissions will be reviewed against the criteria set out in the Data Act, and successful items may be considered for inclusion in future updates of the repository.

Candidate List Evaluation
Step 1
Check compliance with Annex II criteria on:
• Coherence
• Governance
• Maintenance
• Availability
• Intellectual property
Step 2
Check compliance with Data Act (Article 35) interoperability & portability and other criteria Annex II - market acceptance & quality
Desk research
on available standards and open specifications for identified priority areas
Stakeholder input
Asked in survey for possible candidates
Candidates list for screening
• generic / sector specific
• semantic / data structure & format / technical
Categories list PaaS/SaaS
to test "for same service type"
Passed candidate list

Latest News

Press release | 01 March 2024

Commission opens calls to invest over €176 million in digital capacities and tech

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 01 March 2024

Commission makes first payment of €202 million to Finland under the Recovery Facility

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Press release | 14 December 2023

Commission awards €41 million contract to develop infrastructure for Common European Data Spaces

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Related content

Big picture

Data Act

The Regulation on harmonised rules on fair access to and use of data — also known as the Data Act — entered into force on 11 January 2024. The Act is a key pillar of the European data strategy and it will make a significant contribution to the Digital Decade's objective of advancing digital transformation.

The Data Act is a comprehensive initiative to address the challenges and unleash the opportunities presented by data in the European Union, emphasising fair access and user rights, while ensuring the protection of personal data.

Dig deeper

Annex II to Regulation (EU) No 1025/2012

Annex II to Regulation (EU) No 1025/2012 sets out the criteria for identifying ICT technical specifications that may be referenced in EU policies and legislation. Specifications must be market-accepted, coherent with existing standards, and developed through open, consensus-based, transparent, and non-discriminatory processes. They must also meet strict requirements on maintenance, accessibility, intellectual property, relevance, neutrality, and technical quality—ensuring that they support interoperability without distorting the market.

(Read more on Annex II →)

Data Act explained

The Data Act lays the foundation for a fair, competitive, and innovative data economy in the EU. It clarifies who can access, use, and share data—particularly data generated by connected products, industrial systems, and cloud services. The regulation introduces rules to ensure equitable data sharing between businesses, empower users to control their data, and remove barriers to switching between service providers. It also safeguards against unfair contractual terms and unlawful foreign access to non-personal data. Discover how the Data Act works in practice and what it means for companies, public authorities, and citizens.

(Learn more →)

Article 35, Interoperability of data processing services

Article 35 of the Data Act sets out essential requirements for open interoperability specifications and harmonised standards to ensure secure, seamless, and innovation-friendly data flows between cloud and edge services. These standards support service compatibility, data portability, and functional equivalence, while addressing multiple layers of interoperability—from syntax and semantics to behaviour and policy. Specifications listed in the Cloud Interoperability Repository will support switching and compliance under Article 30(3).

(Explore Article 35 →)

Annex 10 – CAMSS MSP Reference

CAMSS MSP Reference

For reference, here is the full list of criteria in the CAMSS MSP Methodology.

On Market Acceptance (point 1 of Annex II Regulation (EU) No 1025/2012):

A1 - The technical specification or standard has been used for different implementations by different vendors/suppliers.

A2 - The implementation of the technical specification or standard does not hamper interoperability with implementations that are currently based on existing European or international standards.

A3 - There are public references (especially policies or in procurement) of the respective specification made by public authorities.

On Coherence Principle (point 2 of Annex II Regulation (EU) No 1025/2012):

A4 - Does the technical specification or standard cover areas different from areas addressed by technical specifications being under consideration to become a European standard?

A5a - Is the adoption of new European Standards which cover the same areas as the proposed specification (or standard) foreseen within a reasonable timeframe?

A5b - Are there existing European standards with market uptake which cover the same areas as the proposed specification (or standard) being assessed?

A5c - If yes, are the existing standards becoming obsolete?

On Attributes (Governance, point 3 of Annex II Regulation (EU) No 1025/2012):

A6 - Is the standards developing organisation a non-profit organisation?

A7 - Is participation in the creation process of the specification open to all interested parties (e.g. organisations, companies, and individuals)?

A8 - Are the specifications approved in a decision-making process which aims to reach consensus?

A9 - Is relevant documentation of the development and approval process of the specification archived and identified?

A10 - Is information on (new) standardisation activities widely announced through suitable and accessible means?

A11 - All relevant stakeholders can formally appeal or raise objections to the development and approval of specifications?

Requirements (point 4 of Annex II Regulation (EU) No 1025/2012):

A12 - Does the specification have a defined maintenance and support process?

A13 - Is the specification publicly available for implementation and use on reasonable terms?

A14a - Is the specification licensed on a (F)RAND basis?

A14b - Is the specification licensed on a royalty-free basis?

A15a - Does the specification address and facilitate interoperability between public administrations?

A15b - Is there evidence that the adoption of the specification positively impacts one or several of the following: organisational processes, the environment, the administrative burden, the disability support, cross-border services, public policy objectives, societal needs?

A16a - Is the specification largely independent of specific vendor products?

A16b - Is the specification largely independent of specific platforms or technologies?

A17 - Has the specification sufficient detail, consistency, and completeness for the use and development of products and services?

Annex 11 – Least Applicable Criteria in the Second Screening

Criterion Categories	Criterion Sub Categories	Criteria
Portability of digital assets	Semantic Interoperability	The specification shall define mechanisms or interfaces for automating the translation or mapping of data between heterogeneous semantic models to enable interoperability.
Portability of digital assets	Semantic Interoperability	The specification shall implement mechanisms or technologies such as widely accepted vocabularies like DCAT-AP, Dublin Core, Schema.org, ISO 11179 or domain-specific ones are mandated
Portability of digital assets	Semantic Interoperability	The specification shall make use of, or be compatible with, established vocabularies or ontologies to ensure semantic consistency across systems.
Interoperability between data processing services	Operational Interoperability	The specification shall define mechanisms, protocols, or interfaces to synchronize data and maintain consistency across systems or cloud providers.
Interoperability between data processing services	Operational Interoperability	The standard shall define principles, capabilities or frameworks to support event-driven architectures to enable real-time interoperability
No adverse impact on security and integrity	System security and integrity	The open specification shall implement or define interfaces for federated identity management to enable secure cross-cloud authentication.
No adverse impact on security and integrity	System security and integrity	The specification shall implement mechanisms or technologies such as Cross-provider authentication (e.g., Identity Federation, Single Sign-On)
Portability of digital assets	Semantic Interoperability	The specification shall implement mechanisms or technologies such as structured mappings between formats
Interoperability between data processing services	Policy Interoperability	The open specification shall define mechanisms or formats for expressing and enforcing access, consent, or data usage policies in a machine-readable and interoperable manner.
Interoperability between data processing services	Operational Interoperability	The specification shall support compatibility with open specifications that enable distributed identity management and federated access control (e.g., OAuth 2.0, OpenID Connect, DIDs).
Interoperability between data processing services	Operational Interoperability	The specification shall define interfaces, models, or deployment descriptors that enable consistent deployment of applications across different cloud providers.
Interoperability between data processing services	Technical Interoperability	The specification shall implement authentication using widely adopted and open protocols
No adverse impact on security and integrity	System security and integrity	The open specification shall implement secure and encrypted communication for all API interactions, using industry-standard protocols.
Functional Equivalence	Consistent service-level behavior	The specification shall implement mechanisms or technologies such as API compatibility tests
Functional Equivalence	Consistent service-level behavior	The specification must implement mechanisms or technologies such as rollback mechanisms in case of migration failures

The table above presents the operationalised criteria that were least frequently applicable across the nine specifications included in the second screening sample. From dark orange to light orange, the shading indicates the degree of non-applicability – ranging from criteria not applicable to any of the nine assessed specifications, to those applicable to only two.

These results should be interpreted with caution. The low applicability of certain criteria may stem from the specific composition of the sample – which consisted exclusively of open specifications from the identified priority areas – rather than from an actual gap in the standardisation landscape. Some criteria address aspects such as service-level behaviour or semantic interoperability that are not necessarily covered by specifications. As the assessment is extended to a broader range of standards and specifications, the distribution of applicability is expected to evolve accordingly.

Getting in touch with the EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
– at the following standard number: +32 22999696,
– via the following form: european-union.europa.eu/contact-eu/write-us_en.

Finding information about the EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

KK-01-25-154-EN-N

Publications Office
of the European Union