ETSI TR 104 409 V1.1.1 (2025-06)

Data Solutions (DATA);
Data Act (art. 33) requirement and references analysis

Reference
DTR/DATA-00104409

Keywords
DATA, data interoperability, oneM2M, SAREF

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Data Solutions (DATA).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

In recent years, the availability of Internet-connected products ("connected products") on the European market has increased rapidly. These products, which together form a network known as the Internet of Things (IoT), significantly increase the volume of data available for reuse in the EU. This holds enormous potential for innovation and competitiveness in the EU.

The EU Data Act [i.4] came into force in December 2023 and aims to create a new legal framework for handling data. It gives users of connected products (companies or individuals who own, lease or rent such a product) greater control over the data they generate, while maintaining incentives for those who invest in data technologies. It also sets out general conditions for situations where a company is legally obliged to share data with another company.

The EU Data Act [i.4] also includes measures to increase fairness and competition in the European cloud market and to protect companies from abusive contractual clauses related to data sharing imposed by stronger players. It also introduces a mechanism for public authorities to request data from a company when there is an exceptional need, for example in public emergency situations.

The EU Data Act [i.4] will have an impact on many companies that process data. Digitalization is progressing inexorably:

- A large proportion of society activities depend on IoT systems. They are influenced or even controlled by them.
- The users of these systems directly or indirectly generate an unprecedented amount of data.
- By storing and processing data, companies use this data to improve their services or for advertising.
- The data is often stored by providers in data silos that even users can only partially access, especially data that was generated by their activities but not directly entered by them.

The users/customers of providers are more or less tied to them. Even switching from one provider to another is difficult due to the "lock-ins". Because a lot of data is difficult to access, it is not possible to create new applications that link these data sources with each other to the desired extent and thus tap into the benefits of digitization.

Even public bodies such as administrations are unable to access the data. This makes it difficult for them to fulfil their mission. The consequences of this were demonstrated during the coronavirus pandemic. For example, it was and still is almost impossible to track the occupancy of hospital beds or the vaccination status of the population at the same time.

With the EU Data Act [i.4], the EU Commission wants to eliminate these difficulties and create the legal basis for the fair, efficient and effective use of data and thus for the digital transformation of European economic players.

Article 33 of the EU Data Act [i.4] sets out comprehensive rules on the interoperability of data, mechanisms and services for data sharing and use in shared European Data Spaces. Data Spaces include, for example, cloud environments. The EU Commission may issue implementing provisions and request standard-developing organizations (e.g. CEN, CENELEC, ETSI) to define uniform standards in this area in order to achieve this interoperability. The providers will then implement these accordingly.

Referring to article 33 of the EU Data Act [i.4], the European Commission made available the draft of the standardisation request SReq [i.3]. The SReq requests CEN, CENELEC and ETSI to draft new European standards and European standardisation deliverables as listed in the Annexes of the SReq [i.3] in support of article 33 of the EU Data Act [i.4]. For all deliverables requested by the SReq, CEN, CENELEC and ETSI are expected to co-operate in the Mode 4, which is specified in the Basic Co-operation Agreement between these three Standards Development Organizations (SDOs). According to this, one Party should take the lead of work and the other(s) may make written contributions during the progress of drafting the requested new European standards. This relation includes also full information sharing via nominated observers.

1 Scope

The present document supports the preparation of the answer to the EU standardisation request "Standardisation request to the European standardisation organisations as regards a European Trusted Data Framework in support of Regulation (EU) 2023/2854 of the European Parliament and of the Council" [i.3] further on called "SReq" in the present document. The scope of the present document is to analyse the requirements contained in the "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)" [i.4], further on called "EU Data Act" in the present document, with particular reference to its article 33, and those in the final version of the SReq [i.3] including their references (e.g. the "DSSC Blueprint V1.5" [i.5]). This analysis is conducted with reference to the existing ETSI applicable specifications and standards (e.g. oneM2M [i.6], SAREF [i.1], NGSI-LD [i.7], [i.8], etc.).

The present document provides the input for the ETSI Technical Report on "Data ACT (art. 33) standardization suggestions" ETSI TR 104 410 [i.2].

Both reports (the present document and ETSI TR 104 410 [i.2]) will prepare the normative work to satisfy the SReq.

The present document is structured as follows:

- **Clauses 1 to 3** set the scene and provide references as well as definitions of terms, symbols and abbreviations, which are used in the present document.
- **Clause 4** provides an introduction to the EU Data Act [i.4] with a focus on its structure and the technically relevant parts of it. Specifically, it establishes the reference to standardisation in the field of interoperability of data and services. Further on, it lists requirements derived from the EU Data Act [i.4] article 33 ("Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces)". The draft of the SReq [i.3] is addressing this article 33.
  Also, clause 4 provides a list of requirements derived from the EU Data Act [i.4] article 35 (Interoperability of data processing services). It addresses several items, which are related to, even if not being in the focus of, the SReq.
- **Clause 5** provides an introduction to the SReq to European Standards Organisations as regards to a European Trusted Data Framework [i.3]. The focus is on ontologies and data models as well as on approaches to manage them. It lists requirements derived from the SReq, which are additional to the published EU Data Act [i.4]. Clause 5 provides an overview of the "DSSC Blueprint, version 1.5" [i.5] and an overview of the "Data Catalog Vocabulary (DCAT) - Version 3" [i.9] within the context of potential application to SAREF [i.1].
- **Clause 6** provides an overview of which parts of the standardisation requirements derived from the documents EU Data Act [i.4] and SReq [i.3] can be satisfied by the oneM2M standards [i.6], the SAREF ecosystem [i.1] with the SAREF core and on all extensions and the NGSI-LD specifications [i.7], [i.8].
  Also it identifies the gaps which need to be filled. It also describes the relationship between oneM2M and SAREF, with special emphasis on how oneM2M standards [i.6] can be used as the means for practical SAREF deployment. Furthermore, clause 6 analyses the relation between DSSC Blueprint [i.5] and the oneM2M standards [i.6].
- **Clause 7** provides a summary of conclusions from the requirements and references analysis and gives an outlook to further potential activities.
- **Annex A** provides an overview of the EU Data Act structure.
- **Annex B** shows some highlights of articles with technical/standardisation relevance.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] ETSI SAREF portal.

[i.2] ETSI TR 104 410: "DATA; Data ACT (art. 33) standardization suggestions".

[i.3] European Commission DG GROW.H.3: "Standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards to a European Trusted Data Framework".

[i.4] 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)".

[i.5] Data Spaces Support Centre: "Data Spaces Blueprint V1.5".

[i.6] oneM2M specifications.

[i.7] ETSI GS CIM 006: "Context Information Management (CIM); NGSI-LD Information Model".

[i.8] ETSI GS CIM 009: "Context Information Management (CIM); NGSI-LD API".

[i.9] W3C®: "Data Catalog Vocabulary (DCAT) - Version 3".

[i.10] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), 03/06/2022.

[i.11] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

[i.12] ISO 19115-1:2014: "Geographic information — Metadata — Part 1: Fundamentals".

[i.13] ISO 19115-2:2019: "Geographic information — Metadata — Part 2: Extensions for acquisition and processing".

[i.14] ISO 19115-3:2023: "Geographic information — Metadata — Part 3: XML schema implementation for fundamental concepts".

[i.15] SEMIC Support Centre.

[i.16] IEC 63278-1:2023: "Asset Administration Shell for industrial applications - Part 1: Asset Administration Shell structure".

[i.17] IEC 63278-2 ED1: "Asset Administration Shell for Industrial Applications - Part 2: Information meta model".

[i.18] European Commission reference data asset countries and territories.

[i.19] European Commission: "New European Interoperability Framework", ISBN 978-92-79-63756-8, 2017.

[i.20] European Commission: "Commission Staff Working Document on Common European Data Spaces", 23.02.2022.

[i.21] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.22] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.23] CEN Workshop Agreement CWA 18125: "Trusted Data Transaction".

[i.24] EU Funding & Tenders Portal: Data Spaces Support Centre.

[i.25] EU Funding & Tenders Portal: Digital Europe Programme (DIGITAL).

[i.26] Data Spaces Support Centre (the operating portal).

[i.27] EU Funding & Tenders Portal: EU Funded projects.

[i.28] OpenAPI Specification v3.1.1.

[i.29] Linked Data Event Streams (LDES).

[i.30] SEMIC Support Centre.

[i.31] W3C®: Verifiable Credentials Overview.

[i.32] Open Digital Rights Language (ODRL) Initiative.

[i.33] eDelivery AS4 - 2.0 (2024 PR draft).

[i.34] Repository of the Asset Administration Shell Specification.

[i.35] Dataspace Protocol 2024-1.

[i.36] International Data Spaces Association (IDSA).

[i.37] Data Spaces Toolbox.

[i.38] ETSI EN 303 760: "SmartM2M; SAREF Guidelines for IoT Semantic Interoperability; Develop, apply and evolve Smart Applications ontologies".

[i.39] Next Generation Service Interfaces - Linked Data.

[i.40] Orion-LD NGSI-LD implementation.

[i.41] Scorpio NGSI-LD implementation.

[i.42] Stellio NGSI-LD implementation.

[i.43] Cassiopeia NGSI-LD implementation.

[i.44] European Union EUR-Lex: Browse by EuroVoc.

[i.45] DCMI 2025, the twenty-third International Conference.

[i.46] oneM2M Wiki.

[i.47] oneM2M Illustrative use-cases and implementation guides.

[i.48] Deploy with oneM2M.

[i.49] oneM2M developer forum and tools.

[i.50] oneM2M github.

[i.51] Ocean Developers website.

[i.52] Eclipse OM2M website.

[i.53] oneM2M device and platform software resources.

[i.54] oneM2M Apps Registry.

[i.55] oneM2M App IDs registration.

[i.56] European Commission website Interoperable Europe.

[i.57] Data.europa.eu: "Data Quality Guidelines".

[i.58] Data.europa.eu: "2023 Open Data Best Practices in Europe".

[i.59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[i.60] European Commission: "Ethics Guidelines for Trustworthy AI".

[i.61] Data Spaces Support Centre: "Data Spaces Blueprint V2.0".

[i.62] OpenID® Foundation Webpage for Verifiable Credentials.

[i.63] Homepage of OpenID® Foundation.

[i.64] EUDI Wallet Architecture and Reference Framework.

[i.65] Eclipse repository for Decentralized Claims Protocol DCP.

[i.66] Dataspace Protocol DSP.

[i.67] Homepage of AsyncAPI Initiative for event-driven APIs.

[i.68] MQTT Specifications.

[i.69] ETSI Homepage for Committees: "ETSI ISG CIM".

[i.70] Homepage of The Data Spaces Business Alliance.

[i.71] Homepage of European project Gaia-X.

[i.72] Homepage of Big Data Value Association (BDVA).

[i.73] Homepage of FIWARE Foundation.

[i.74] Homepage of Open Trip Model (OTM).

[i.75] Homepage of Smart Connected Supplier Network (SCSN).

[i.76] SETU Homepage.

[i.77] SETU documentation page: "Planning and Scheduling".

[i.78] Home page of the Smart Connected Supplier Network (SCSN) process documentation manual (Smart Connected Supplier Network API).

[i.79] ETSI TS 103 267: "SmartM2M; Smart Applications; Communication Framework".

[i.80] ETSI TS 118 111: "oneM2M; Common Terminology (oneM2M TS-0011)".

[i.81] ETSI TS 118 101: "oneM2M; Functional Architecture (oneM2M TS-0001)".

[i.82] ETSI TS 118 104: "oneM2M; Service Layer Core Protocol Specification (oneM2M TS-0004)".

[i.83] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003)".

[i.84] ETSI TS 118 116: "Secure Environment Abstraction" (oneM2M TS 0016).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

ACME CSE: open source CSE Middleware for Education

connected product: item that obtains, generates or collects data concerning its use or environment and that is able to communicate product data via an electronic communications service, physical connection or on-device access, and whose primary function is not the storing, processing or transmission of data on behalf of any party other than the user

data holder: natural or legal person that has the right or obligation, in accordance with the EU Data Act [i.4], applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service

data processing service: digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralized, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction

data recipient: natural or legal person, acting for purposes which are related to that person's trade, business, craft or profession, other than the user of a connected product or related service, to whom the data holder makes data available, including a third party following a request by the user to the data holder or in accordance with a legal obligation under Union law or national legislation adopted in accordance with Union law

EU Data Act: See Regulation (EU) 2023/2854 [i.4].

FIWARE: Open Source Platform for Our Smart Digital Future

GeoDCAT-AP: extension of DCAT-AP

OM2M: eclipse OM2M architecture

public sector body: national, regional or local authorities of the Member States and bodies governed by public law of the Member States, or associations formed by one or more such authorities or one or more such bodies

smart contract: computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering

SReq: standardisation request to the European standardisation organisations as regards a European Trusted Data Framework in support of Regulation (EU) 2023/2854 of the European Parliament and of the Council [i.3]

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AE	Application Entity
API	Application Programming Interface
ARIB	Association of Radio Industries and Business
ATIS	Alliance for Telecommunications Industry Solutions
BDVA	Big Data Value Association
CCSA	China Communications Standards Association
CEDS	Common European Data Spaces

CEF	Connecting Europe Facility
CEN	European Committee for Standardisation
CENELEC	European Committee for Electrotechnical Standardisation
DCAT	Data Catalog Vocabulary
DCAT-AP	Data Catalogue Vocabulary Application Profile
DCAT-AP-HVD	Data Catalogue Vocabulary Application High-Value Dataset Profile
DCP	Decentralized Claims Protocol
DSSC	Data Spaces Support Centre
DSP	DataSpace Protocol
EIF	European Interoperability Framework
EDIB	European Data Innovation Board
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology
IDSA	International Data Spaces Association
ISG CIM	Industry Specification Group on cross-cutting Context Information Management
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JSON	JavaScript Object Notation
LDES	Linked Data Event Streams
LoRa	Long Range
M2M	Machine-to-Machine
MQTT	Message Queuing Telemetry Transport
NB-IoT	NarrowBand IoT
NGSI	Next Generation Service Interface
NGSI-LD	Next Generation Service Interface-Linked Data
OAS	Open Api Specifications
ODRL	Open Digital Rights Language
OID4VC	Open ID for Verifiable Credentials
OMA	Open Mobile Alliance
OTM	Open Trip Model
RDF	Resource Description Framework
REST	REpresentational State Transfer
SAREF	Smart Applications REFerence ontology
SCSN	Smart Connected Supplier Network
SDO	Standards Development Organization
SEMIC	SEMantic Interoperability Community
SETU	Stichting Elektronische Transacties Uitzendbranche
SME	Small and Medium Enterprise
SReq	Standardisation Request
STF	Specialist Task Force
SW	Software
TIA	Telecommunications Industry Association, North America
TSDSI	Telecommunications Standards Development Society, India
TTA	Telecommunications Technology Association, Korea
TTC	Telecommunication Technology Committee, Japan
TR	Technical Report
TS	Technical Specification
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
W3C®	World Wide Web Consortium
Web	World Wide Web
WG	Working Group
XML	eXtensible Markup Language

4 EU Data Act requirements analysis

4.1 Introduction

On 22 December 2023 the EU Data Act [i.4] has been published in the Official Journal of the European Union. The Regulation has got into force on 11 January 2024 and, after a transition phase, will be European wide law after 12 September 2025. The EU Data Act [i.4] makes more data available for use, and sets up rules on who can use and access what data for which purposes across all economic sectors in the EU.

The EU Data Act [i.4] gives individuals and businesses entities more control over their data exchange through a reinforced data portability right, copying or transferring data easily from across different services, where the data are generated through smart objects, machines and devices. It regulates the transfer of data to and between service providers and this will encourage more actors, including SMEs, to participate in the data economy.

This Regulation applies to:

- manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;
- users in the Union of connected products or related services as referred to in the point above;
- data holders, irrespective of their place of establishment, that make data available to data recipients in the Union;
- data recipients in the Union to whom data are made available;
- public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request;
- providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;
- participants in Data Spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

Annex A of the present document provides an overview of the EU Data Act structure and Annex B shows some highlights of articles with technical/standardization relevance.

Clauses 4.2 and 4.3 of the present document identify the requirements of the EU Data Act [i.4] articles 33 and 35 in order to analyse which ETSI standards already can satisfy these requirements and to find gaps. This contributes to support the preparation of the answer to the EU standardisation request "Draft standardisation request as regards European Trusted Data Framework" [i.3].

4.2 EU Data Act Article 33

Article 33 of the EU Data Act [i.4] is titled "Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces". This article addresses participants in Data Spaces that offer data or data services to other participants. It requests them to comply with the essential requirements listed in article 33.

A dataspace is an abstraction in data management, which is defined as a set of participants, or data sources, and the relations between them. It can contain all data sources of an organization regardless of their format, physical location, or data model. The data space provides a unified interface to query data regardless of format and ways to further integrate the data when necessary.

Article 33 the EU Data Act [i.4] defines essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European Data Spaces, and per article 33 (4), request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements.

The following requirements apply to participants in Data Spaces that offer data or data services to other participants:

NOTE: Text in Italics is quoted from the EU Data Act [i.4].

- Paragraph 1 (a)
  The dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data.

- Paragraph 1 (b)
  The data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner.

- Paragraph 1 (c)
  The technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine-readable format where that is technically feasible and does not hamper the good functioning of the connected product.

- Paragraph 1 (d)
  Where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements, such as smart contracts shall be provided.

- Paragraph 3
  Offering data or data services to other participants in Data Spaces, which meet the harmonised standards (the references of which are published in the Official Journal of the European Union), needs to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such harmonised standards.

- Paragraph 8
  Offering data or data services to other participants in Data Spaces, which meet the common specifications established by implementing acts referred to in paragraph 5 needs to be in conformity with the essential requirements laid down in paragraph 1 to the extent that those requirements are covered by such common specifications.

Several essential requirements are addressing the obligations of the European Commission:

- Paragraph 2 empowers the European Commission to adopt delegated acts, to supplement this regulation by further specifying the essential requirements laid down in paragraph 1 of the article 33. This is in relation to those requirements that, by their nature, cannot produce the intended effect unless they are further specified in binding Union legal acts and in order to properly reflect technological and market developments.
  Hereby, the European Commission is obliged to take into account the advice of the European Data Innovation Board (EDIB). EDIB is a Commission expert group, which has been created by Regulation (EU) 2022/868 [i.10].

- Paragraph 4 requires the European Commission to request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of article 33.

- Paragraph 5 authorises the European Commission to adopt common specifications covering any or all of the essential requirements laid down in paragraph 1. This is bound to the following conditions:

  - The European Commission has requested one or more European standardisation organisations to draft a harmonised standard that satisfies the essential requirements laid down in paragraph 1 and the request has:

    - not been accepted; or

    - the requested harmonised standards are not delivered within the given deadline; or

    - the harmonised standards do not comply with the request.

  - No reference to harmonised standards covering the relevant essential requirements laid down in paragraph 1 of article 33 is published in the Official Journal of the European Union and no such reference is expected to be published within a reasonable time frame.

- Paragraphs 6, 7, 9 deals with processes, which accompanies paragraph 5.
- Paragraphs 10 states the right of EU Member States to inform the European Commission about a common specification that does not entirely satisfy the essential requirements laid down in paragraph 1.
- Paragraphs 11 authorises the European Commission to adopt guidelines for the functioning of common European Data Spaces considering the proposal of the EDIB.

4.3 EU Data Act Article 35

The article 35 of the EU Data Act [i.4] is titled "Interoperability of data processing services". This article addresses open interoperability specifications and harmonised standards for the interoperability of data processing services. It requests them to comply with the essential requirements listed in article 35.

Article 35 announces the creation of a central Union standards repository for the interoperability of data processing services.

The following essential requirements apply to those specifications and harmonised standards:

- For the same type of service:
  - Achieve interoperability between different data processing services.
  - Enhance portability of digital assets between different data processing services.
  - Facilitate functional equivalence between different data processing services.
- Not have an adverse impact on the security and integrity of data processing services and data.
- 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.
- Adequately addressing of:
  - Cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioural interoperability and policy interoperability.
  - Cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability.
  - Cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behaviour portability and application policy portability.

Several essential requirements are listing the obligations of the European Commission, which are similar to those of article 33 paragraphs 4, 5.

The article 33 of the EU Data Act [i.4] lists the obligations of participants in Data Spaces that offer data or data services to other participants to sufficiently describe technical characteristics of their data and data services in a publicly available and consistent manner as well as the corresponding technical means to access them to allow the recipient to find, access and use the data. In terms of being interoperable, the participants in Data Spaces that offer data or data services to other participants are supported by applying respective harmonised standards or, when missing, common specifications covering any or all of the essential requirements laid down in paragraph 1. In this context, the SReq requires European standardisation organisations to draft harmonised standards that satisfies the essential requirements laid down in paragraph 1. On the other hand, article 35 of the EU Data Act addresses open interoperability specifications and harmonised standards for the interoperability of data processing services. This term is defined by the EU Data Act [i.4] paragraph 8 as a "digital service" and with that has some direct relationship to article 33 and vice versa.

As a conclusion, also article 35 needs to be considered in clause 6 of the present document for supporting the preparation of the answer to the SReq.

5 EU standardization request as regards to a European Trusted Data Framework

5.1 Introduction

The EU Data Act [i.4] article 33 (4) requires the European Commission to "request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of article 33". Referring to this paragraph, the European Commission made available the draft of the standardisation request SReq [i.3]. The SReq requests CEN, CENELEC and ETSI to draft new European standards and European standardisation deliverables as listed in the Annexes of the SReq [i.3] in support of article 33 of the EU Data Act [i.4].

Article 1 of the SReq [i.3] addresses the three European Standardisation Organisations to draft new European standards and European standardisation deliverables listed in Table 1 Annex I and points to their requirements listed in Annex II.

Article 2 requests the preparation of a CEN, CENELEC and ETSI joint work programme indicating the European standards and European standardisation deliverables, which are referred to in the SReq [i.3] Annex I, the responsible technical bodies and a timetable for the execution of the standardisation work. Further on, the article provides a list of interrelations with some EU Regulations and the work and approaches of the DSSC and the development of sector- and domain-specific common European data spaces as well as of Interoperable Europe [i.56].

Article 3 regulates the reporting on the execution of the SReq [i.3].

Article 4 specifies the validity of the SReq [i.3].

Article 5 addresses the three European Standardisation Organisations explicitly again.

Clause 5.2 of the present document derives the main requirements of the SReq [i.3], which Annexes I and II of it contain.

NOTE: The work of drafting clause 5.2 is based on the draft SReq [i.3] of March 2025, which has been made available to the European Standardisation Organisations.

5.2 Requirements for EU standards and standardisation deliverables

Annexes I and II of the SReq [i.3] contain the main requirements for the new European standards and European standardisation deliverables to be drafted, which are expected to support the participants in Data Spaces that offer data or data services to other participants to be compliant with article 33 of the EU Data Act [i.4].

A) **General requirements for standards and European standardisation deliverables listed in Annex I** (Annex II, Part A [i.3]):

This part of Annex II requests the new harmonised standards listed as 1., 2. and 3. in the paragraph below to support the application of the essential requirements of the EU Data Act [i.4] article 33. Further on, it defines several items, which the new harmonised standards are expected to follow:

i. Provide detailed technical specifications of essential requirements, with regard to the design of data sharing system interfaces.

ii. Include a clear and precise description of the relationship between their content and the corresponding essential requirements that they aim to cover.

iii. Structure each harmonised standard such that a clear distinction can be made between its clauses and sub-clauses which are necessary for compliance with the essential requirements and those which are not.

iv. Exclusively provide provisions specific to data sharing system interfaces. These provisions include methods for the verification of compliance with such provisions including methods for the verification of compliance with such provisions.

v. No support of any other legal requirements than the EU Data Act [i.4] article 33.

vi. Not make any references to Regulation (EU) 2023/2854 [i.4] or reproduce its requirements in their normative body.

vii. When not covering all the essential requirements, indicate what are not covered.

B) **Requirements for the European standards and European standardisation deliverables referred to in Article I**
(Annex II, Part B [i.3]):

i. Be technology neutral, performance-based and objectively verifiable.

ii. May include non-binding examples of the technical implementation.

iii. In close coordination with the EDIB.

iv. Standardisation basis: Elements from DSSC Blueprint [i.5], DSSC guidelines, recommendations and specifications.

v. Consideration of solutions of the Interoperable Europe initiative [i.56].

vi. Usage of the Regulation on a framework for a European Digital Identity [i.11] for the overall strategic direction for the verification of the identity and credentials of legal and natural persons.

vii. Consideration of Standards, guidelines[i.57] and best practices [i.58] provided by the official portal for European data - data.europa.eu.

List of new European standards and European standardisation deliverables to be drafted:

1) Harmonised standards on Trusted Data Transactions
Part 1: Terminology, concepts and mechanisms

2) Harmonised standards on Trusted Data Transactions
Part 2: Trustworthiness requirements

3) Harmonised standards on Trusted Data Transactions
Part 3: Interoperability requirements

Requirements (Annex II, Part B, 2.1 [i.3]):

- Support of the automated execution of data transactions in the European single market for data.
- Enabling data space participants to presume compliance with the essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of CEDS as specified in article 33 the EU Data Act [i.4].
- Ensuring coherence with Regulation (EU) 2016/679 [i.21], Regulation (EU) 2022/868 [i.10], and Directive (EU) 2022/2555 [i.22] as regards the trust and security aspects.
- Addressing main data sharing methods, including file transfer, Application Programming Interface (API) queries, and emerging scenarios such as distributed analytics.
- Including scenarios for direct access of data residing in distributed systems and smart devices.
- Addressing tools that facilitate the automated execution of elements of a data transaction.

Defining the trustworthiness and interoperability requirements for the following key aspects of a data transaction:

- The way to make data discoverable/findable, including but not limited to metadata of data content, licences, data collection methodology, data quality and uncertainty.
- The way to record data sharing agreements, including aspects such as data usage conditions (licences), data quality conditions, service level agreements, and agreements on monetary or non-monetary compensation.

- The way to describe the technical access to the shared data, to enable automatic access and transmission of data between parties.
- The way to describe usage permissions of shared data, based on consent and licensing agreements.
- The way to describe information relevant to assess a legal basis for processing the data in question under GDPR [i.59].
- The way to document the data being shared, including but not limited to descriptions of data structures, data formats, vocabularies, classification schemes, taxonomies and code lists.
- The way to ensure observability and auditability of data transactions.

1) **Technical specification(s) on a data catalogue implementation framework**

Requirements (Annex II, Part B, 2.2 [i.3]):

a) Consideration of Interoperable Europe solutions [i.56] based on the W3C Data Catalogue Vocabulary (DCAT) standard [i.9], in particular the DCAP-AP, DCAT-AP-HVD and GeoDCAT-AP profiles.

b) Set out of the common catalogue metadata, to be applied across all Common European Data Spaces.

c) Establishment of rules on the setting out of domain-specific catalogue metadata, to be applied in selected Common European Data Spaces.

2) **Technical specification(s) on an implementation framework for semantic assets**

Requirements (Annex II, Part B, 2.3 [i.3]):

a) Provision of a framework for common, open vocabularies, classification schemes, taxonomies, code lists and ontologies, in support of the interpretation and analysis of shared data within and across Data Spaces.

b) Consideration of Core Vocabularies and the Asset Description Metadata Schema Application Profile/ADMS-AP (EC - SEMIC) [i.15], the Asset Administration Shell (IEC) [i.16], [i.17], the ISO/IEC 19115 metadata standards [i.12], [i.13], [i.14], the European Commission countries and territories reference data asset [i.18] for geospatial data, and SAREF [i.1].

c) Specification of criteria for the selection of semantic assets.

d) Specification of methods for the semantic annotation of shared data, the detailed metadata, based on the semantic assets mentioned above.

3) **European standard on a quality framework for internal data governance**

Requirements (Annex II, Part B, 2.4 [i.3]):

a) Set out of best practices for data rights management, including data for which the right owners are the data space participant, another party and personal data and for data quality management.

b) Assurance of consistent understanding of the Data Spaces concept and effective implementation across various contexts, aligned with the language and intent of the relevant legal texts on European and national level, covering horizontal and vertical legislation.

c) Addressing the way to meet domain-specific (non-regulatory) requirements.

d) Articulation in practical, non-legal language that is accessible to all stakeholders.

e) Providing simplified processes and templates for easy implementation.

4) **Technical specification(s) on a maturity model for Common European Data Spaces**

Requirements (Annex II, Part B, 2.5 [i.3]):

a) Definition of a maturity model for the self-assessment of Common European Data Spaces and related data sharing initiatives consisting of:

- key performance indicators; and
- a supporting reporting structure.

b) Enabling the evaluation of the interoperability of a data space, both internally between the data space participants as well as across Data Spaces, as per each layer of the European Interoperability Framework [i.19] (legal, organisational, semantic and technical).

c) Enabling the evaluation of the maturity of the data space in terms of the key features of Common European Data Spaces listed in section 2 of the Staff Working Document on Data Spaces [i.20] and the level of participation and the level of activity.

5.3 DSSC Blueprint

5.3.1 The DSSC

The Data Spaces Support Centre [i.24] is a European Project, fully funded under the Digital Europe Programme (DIGITAL) [i.25].

The project is coordinated by Fraunhofer Gesellschaft Zur Forderung Der Angewandten Forschung Ev (Germany).

Other participants are:

- Data Ai And Robotics Dairo (Belgium)
- Capgemini Belgium (Belgium)
- Fiware Foundation Ev (Germany)
- Gaia-X European Association For Data And Cloud (Belgium)
- International Data Spaces Ev (Germany)
- Katholieke Universiteit Leuven (Belgium)
- Mydata Global Ry (Finland)
- University Of Galway (Ireland)
- Nederlandse Organisatie Voor Toegepast Natuurwetenschappelijk Onderzoek Tno (Netherlands)
- Suomen Itsenaisyyden Juhlarahasto (Finland)
- Teknologian Tutkimuskeskus Vtt Oy (Finland)

Associated Partners not receiving EU Funding are:

- Digitaleurope Aisbl (Belgium)
- Instituto Tecnologico De Informatica (Spain)
- Asociacion De Empresas Tecnologicas Innovalia (Spain)
- Stichting Egi (Netherlands)
- Cefriel Societa Consortile A Responsabilita Limitata Societa' Benefit (Italy)
- Stichting Ishare Foundation (Netherlands)

- Deutsche Akademie Der Technikwissenschaften Ev (Germany)
- Sofia University St Kliment Ohridski (Bulgaria)
- Eigen Vermogen Van Het Instituut Voor Landbouw- En Visserijonderzoek (Belgium)
- Commissariat A L Energie Atomique Et Aux Energies Alternatives (France)
- Consorzio Meditech - Mediterranean Competence Centre 4 Innovation (Italy)
- Open & Agile Smart Cities (Belgium)
- Anewgovernance (Belgium)

The project was started on 2022-10-01 and is expected to be concluded by 2026-03-31.

Among the project objectives are:

> "set up and operate a Data Spaces Support Centre, as described in the Digital Europe Programme, to operationalize the European Strategy for Data. This Support Centre will facilitate common Data Spaces that collectively create an interoperable data sharing environment, to enable data reuse within and across sectors, fully respecting EU values, and contributing to the European economy and society" [i.24].

And

> "The Support Centre delivers the Data Spaces Blueprint, composed of common building blocks encompassing the business, legal, operational, technical and societal aspects of data spaces" [i.24].

NOTE: All the above information in the present clause are extracted from the EU Funding & Tenders Portal [i.27] at the page relevant for the DSSC Project [i.24].

5.3.2 The DSSC Blueprint

According to the provisions of the funding EU Project, the DSSC created an operational portal [i.26] from which the Blueprint [i.5] has been made available to the public.

The DSSC Blueprint [i.5] is a foundational document that outlines the vision, structure, and operational framework for establishing and supporting European Data Spaces.

It targets a wide set of stakeholders, including governments, industry players, and research institutions, aiming to provide standards and best practices.

It comes in the form of a set of guidelines to support the development of Data Spaces, with the intent of helping to speed up the development and growth of Data Spaces while, at the same time, protecting investments and facilitate collaboration among stakeholders.

It emphasizes the importance of fostering trust, interoperability, and innovation while ensuring compliance with EU regulations.

5.3.3 Data Spaces

The Blueprint [i.5] recalls that, seemingly, there currently is no formal/legal definition of a data space, so for the purpose of its scope uses a definition taken from [i.23]:

"Interoperable framework, based on common governance principles, standards, practices and enabling services, that enables trusted data transactions between participants."

NOTE: Over the various versions of the Blueprint, this key definition evolved: the adoption of this definition marks a change by version V1.5 [i.5] from previous V1.0 and V0.5 of the Blueprint.

Within this context, several concepts are presented:

1) Participants: data providers, data consumers, data space governance authorities, service providers.

2) Data Products: consisting of digital artefacts or services that are derived from or based on data, designed to provide value to users in specific use cases. These products are central to the concept of Data Spaces, as they enable the transformation of raw data into actionable insights, services, or applications.

3) Services, distinguishing them into three classes: Participant Agent Services, Federation Services, Value-Creation Services.

5.3.4 Building Blocks

The Blueprint [i.5] introduces the concept of "Building Blocks", i.e. a set of capabilities that are needed to successfully implement instances of Data Spaces, and classifies them into two categories, that are further articulated int subcategories:

1) Business and Organisational Building Blocks:

   a) Business:
   includes the business model for the data space instance, the identification of data product(s) and the role of all stakeholders.

   b) Governance:
   covers the organisational aspects of a data space initiative, including processes for governance and handling of stakeholders' management.

   c) Legal:
   considers both the contractual aspects between participants and the compliance towards legislation.

2) Technical Building Block:

   a) Data Interoperability (also referred to as Data Exchange):
   is based on the exchange of information, according to domain specific data models and semantics, usage of APIs, etc.

   b) Data Sovereignty & Trust:
   obtained by defining and enforcing rules for accessing (and possibly manipulating) data, followed by compliance verification. Includes identification of users.

   c) Data Value Creation Enablers:
   these are the entities that actually publish Data Products and provide means for finding them. The creation of a data space instance is, ultimately, done to provide a context for such entities to provide valuable, actionable information to users.

The concept of Building Block does not translate 1:1 to software implementations: for actual implementations, the Blueprint introduces the term "Services".

Building Blocks can, therefore, be considered more like a sort of high-level specification of requirements and functionalities.

At the level of the Building Blocks, the Blueprint [i.5] introduces an important distinction between a "Control Plane" and a "Data Plane" that interact with each other.

5.3.5 Building Blocks: The Control Plane

The Control Plane is responsible for identifying users and determine how the Data Plane will manage the actual data exchange, thus enforcing access and usage policies.

Typical interactions in the Control Plane are:

- Identity and Attestations:
  for this purpose, the Blueprint suggests the use of the W3C Verifiable Credentials standard [i.31].

- Catalogue Entries:
  for this purpose, the Blueprint suggests the use of the W3C DCAT standard [i.9].

- Policies and Contract Negotiation:
  here "contracts" are intended in a technical sense, not the legal one;
  for this purpose, the Blueprint suggests the ODRL standard [i.32].

- Management of the Transfer Process:
  when the data exchange eventually takes place, the Control Plane is involved to ensure the enforcement of the negotiated policies.

Other protocols are referred in the Blueprint. Some of them are considered immature, but special attention is paid to the Dataspace Protocol (DSP) [i.35], released by the International Data Spaces Association (IDSA) [i.36], notably because the IDSA has expressed the intent to submit the DSP to ISO/IEC for standardisation.

The DSP, too, takes the approach of specifying generic elements, while APIs for the actual data exchange remain data space specific.

Additional protocols are highlighted in the Blueprint 2.0 [i.61], namely:

- Open ID for Verifiable Credentials (OID4VC) [i.62]:
  Currently being standardized by the Open ID Foundation [i.63], this actually is a set of three protocols for managing credentials and their life cycle;
  it is part of EUDI Wallet Architecture and Reference Framework [i.64].

- Decentralized Claims Protocol (DCP) [i.65]:
  Currently being developed for conveying organizational identities and fostering trust while safeguarding privacy and minimizing the risk of network disruptions;
  it is defined as an interoperable overlay to the Dataspace Protocol (DSP) [i.66], also being developed under the governance of IDSA [i.36] and available at Eclipse.

Other protocols, also available at Eclipse by other organisations, may be considered for future inclusion in the DSSC Blueprint as currently they are just in their initial phase of specification.

The Blueprint remarks that the Control Plane functionalities can be highly standardised, possibly making use of the suggested standards as the foundation.

NOTE: Several organisations are working on credentials sharing, compliance assessment and trust building, this might be an indication of strong interest in these topics, and also that the search for the "right" standard is still ongoing.

5.3.6 Building Blocks: The Data Plane

While the Control Plane can be very similar between different Data Spaces, the Blueprint takes the position that, instead, the Data Plane can and will vary greatly.

For each case, appropriate semantics and APIs are requested to be selected.

The Blueprint cites some typical approaches that are adopted in some domains, e.g.:

- For e-procurement and e-invoicing, especially in the public sector, a reference is made to the CEF eDelivery specifications [i.33].

- For the exchange of asset data, in manufacturing, the Asset Administration Shell API [i.34] is mentioned.

At any rate, the Blueprint recalls that, whatever the choice made for any specific case, the EU Data Act [i.4] mandates that "data spaces should be explicit in specifying which specifications apply".

5.3.7 Reusability

The Blueprint stresses the importance of avoiding to "reinvent the wheel", by reusing existing specifications.

This approach saves valuable man time, avoiding pitfalls and, in general build on the experience of others.

For technical building blocks, it suggests to refer to specific open standards that are considered as "the basis for all data space initiatives.

5.3.8 Interoperability / Data Exchange

The Blueprint pays special attention to interoperability, making specific reference to article 33 of the EU Data Act [i.4].

It recalls the importance of interoperability, not only internally to a single data space instance but also to enable synergies with other Data Spaces (intra-data space versus cross-data space interoperability).

To achieve interoperability, the Blueprint promotes the adoption of specific building blocks:

1) Data Models:
   support capabilities define and leverage semantics (to obtain not just the transfer of raw data but useful information. Emphasis is placed on the adoption of "semantic standards" to achieve this goal.

2) Data Exchange:
   these are the capabilities that allow the actual transfer of data/information.
   the Blueprint outlines guidelines for the choice of APIs, mentioning several qualities to take into consideration, but does not endorse any specific solution.

3) Provenance and Traceability:
   the Blueprint remarks that for some domains, e.g. highly regulated or high value ones, additional care is requested to be taken to track in detail each data transaction and/or who has been involved in it.

The Blueprint provides some references for "Further Reading", i.e.:

- OpenAPI Specification (OAS) [i.28] for RESTful and HTTP APIs.
- ETSI NGSI-LD [i.7], [i.8], also mentioned as a possible solution for querying.
  It is referred as published by ETSI ISG CIM [i.69], and endorsed by the Data Space Business Alliance [i.70], itself formed by Gaia-X [i.71], Big Data Value Association (BDVA) [i.72], FIWARE Foundation [i.73] and International Data Spaces Association (IDSA) [i.36].
- Linked Data Event Streams (LDES) [i.29] by Semantic Interoperability Community Europe (SEMIC) [i.30].
- AsyncAPI [i.67], a pub/sub approach built upon MQTT [i.68].

But, as a general rule, it leaves the choice to a case-by-case basis: "The Data Space Governance Authority should identify which generic protocols and which domain-specific APIs apply for participants of the data space".

Version 2.0 of the Blueprint [i.61] adds a short list of "reference implementations", to help understand via concrete examples what is to be intended as services implementing. The list includes:

- ETSI NGSI-LD [i.7], [i.8].
- Open Trip Model (OTM) [i.74], a data model and API for real-time logistic trip data.
- SCSN [i.75] Smart Connected Supplier Network API [i.78] for order-related data between organisations.
- SETU [i.76] specifications [i.77] for planning and scheduling in the staffing industry.

5.3.9 DSSC ToolBox

As a help to choose software for the implementation of Services, the DSSC offers the ToolBox [i.37], defined as:

- "DSSC Toolbox is a catalogue of data space solutions (tools) that are aligned with the DSSC Blueprint and have passed the Toolbox validation scheme".

5.3.10 Remarks

The Blueprint offers valuable propositions and insights.

Among them, perhaps the most significant are:

1) The great care in which the non-technical part of creating and maintaining Data Spaces is described, recalling the need for governance, adherence to legislation, creation of trust (and keeping it over time), interoperability,

action ability etc.
Such aspects are often overlooked, leading to implementations that provide little value to stakeholders.

2) It is written in plain language, accessible to a large audience.
This is important, since the intended audience is vast, extremely varied and comprises many non-specialists.

The Blueprint is, as clearly stated by the DSSC and in the funding EU Project, a work in progress so it is reasonable to expect that changes and refinements will be made to it in the near future.

5.4 DCAT Vocabulary

DCAT is an RDF vocabulary designed to enhance interoperability among data catalogues published on the Web. This document outlines the schema and includes usage examples. By using a standardized model and vocabulary, DCAT allows publishers to describe datasets and data services within a catalogue, facilitating metadata aggregation and consumption across multiple catalogues. This improves dataset and data service discoverability while enabling a decentralized approach to catalogue publishing. It also supports federated searches across multiple catalogues using a common query structure. Additionally, aggregated DCAT metadata can function as a manifest file in digital preservation efforts. Effective metadata provision is essential for sharing data resources among organizations, researchers, governments, and the public.

DCAT defines RDF classes and properties to describe datasets and data services, enabling their inclusion in catalogues. By using a standardized model and vocabulary, DCAT simplifies metadata aggregation and consumption across multiple catalogues. This enhances dataset and data service discoverability and supports federated searches across catalogues on different platforms. The data within a catalogue can be available in various formats, including spreadsheets, XML, RDF, and other specialized formats. While DCAT does not impose restrictions on dataset serialization formats, it differentiates between the abstract dataset and its various manifestations or distributions.

DCAT is an RDF vocabulary for representing data catalogues. DCAT is based around the seven main classes listed below. The reader may refer to [i.9] for seeing the detailed description about the usage of such classes and the relationships between them.

`dcat:Catalog` represents a catalogue, which is a dataset in which each individual item is a metadata record describing some resource; the scope of `dcat:Catalog` is collections of metadata about datasets, data services, or other resource types.

`dcat:Resource` represents a dataset, a data service or any other resource that may be described by a metadata record in a catalogue. This class is not intended to be used directly, but is the parent class of `dcat:Dataset`, `dcat:DataService` and `dcat:Catalog`. Resources in a catalogue should be instances of one of these classes, or of a sub-class of these, or of a sub-class of `dcat:Resource` defined in a DCAT profile or other DCAT application. `dcat:Resource` is actually an extension point for defining a catalogue of any kind of resources. `dcat:Dataset` and `dcat:DataService` can be used for datasets and services which are not documented in any catalogue.

`dcat:Dataset` represents a collection of data, published or curated by a single agent or identifiable community. The notion of dataset in DCAT is broad and inclusive, with the intention of accommodating resource types arising from all communities. Data comes in many forms including numbers, text, pixels, imagery, sound and other multi-media, and potentially other types, any of which might be collected into a dataset.

`dcat:Distribution` represents an accessible form of a dataset such as a downloadable file.

`dcat:DataService` represents a collection of operations accessible through an interface (API) that provide access to one or more datasets or data processing functions.

`dcat:DatasetSeries` is a dataset that represents a collection of datasets that are published separately, but share some characteristics that group them.

`dcat:CatalogRecord` represents a metadata record in the catalogue, primarily concerning the registration information, such as who added the record and when.

A practical extension of DCAT designed to fulfil the standardization needs of European Union is the DCAT Application Profile (DCAT-AP). DCAT-AP is a specification based on DCAT for describing public sector datasets in Europe. Its basic use case is to enable cross-data portal search for data sets and make public sector data better searchable across borders and sectors. The application profile is a specification for metadata records to meet the specific application needs of data portals in Europe while providing semantic interoperability with other applications on the basis of reuse of established controlled vocabularies (e.g. EuroVoc [i.44]) and mappings to existing metadata vocabularies (e.g. Dublin Core [i.45]).

Ensuring consistency in the description metadata published by data portals across Europe is crucial, with two key scenarios in focus. First, data reusers often struggle to get a clear overview of available datasets and the public administrations responsible for them. This challenge is particularly pronounced when datasets are hosted in another Member State, where language barriers and unfamiliar government structures may create obstacles. To mitigate this issue, data publishers and portals maintain catalogues of datasets made available by public administrations on their websites. The quality of the metadata in these catalogues directly impacts how easily datasets can be discovered. Second, data providers aim to promote the reuse of their datasets by making them searchable and accessible. In some cases, publishing metadata about a dataset online is even more critical than providing direct access to the data itself. This is especially relevant when the costs of publishing datasets are high, and the actual demand is uncertain. By listing datasets on one or more data portals, providers can signal their availability at minimal cost.

The DCAT vocabulary supports the fulfilment of the requirement #2 of the SReq [i.3] reported in clause 5.2: "Technical specification(s) on a data catalogue implementation framework". Through the DCAT vocabulary it is possible to create a DCAT-AP describing each standardization resource delivered as a tangible asset, e.g. ontologies.

6 Existing applicable ETSI specifications

6.1 oneM2M specifications

6.1.1 What is oneM2M

Historically, oneM2M originates as a European standard in ETSI, which subsequently evolved into a global partnership project. Promoting its adoption helps strengthening European thought leadership.

oneM2M is a global "de jure" standard, not controlled by any single private company.

oneM2M was launched in 2012 as a global partnership initiative between eight of the world's preeminent standards development organizations: ARIB (Japan), ATIS (North America), CCSA (China), ETSI (Europe), TIA (North America), TSDSI (India), TTA (Korea), and TTC (Japan) to develop specifications that ensure the most efficient deployment of Machine-to-Machine (M2M) communications systems and the Internet of Things (IoT).

Over the years, the partners have collaborated to develop technical specifications for a universal M2M service layer. This service layer is designed to be easily integrated into a wide range of hardware and software systems, providing a reliable foundation for connecting countless devices in the field to M2M application servers across the globe.

By bringing together more than 200 players from many diverse business domains including, oneM2M ensures the global functionality of M2M and prevents the duplication of standardization effort.

Current partners are:

- CCSA (China)
- ETSI (Europe)
- TIA (North America)
- TSDSI (India)
- TTA (South Korea)

Each one of the partners transposes oneM2M specifications as their own standards, thus making them valid standards in their respective geographical area.

In the case of Europe, oneM2M specifications are transposed as ETSI TSs, which offers them to the public free of charge.

Furthermore, the ITU-T approved oneM2M specifications as ITU standard under the Y.4500 series, making the entire suite of oneM2M specifications available for use nationally by ITU-T member states.

From a technical standpoint, the oneM2M specifications define a platform that can be rather simple, e.g. a single instance, or can be articulated over many instances that are interconnected together and cooperate to form a unified system. This is a way to achieve scalability together with separation of concerns.

6.1.2 oneM2M as an Interworking Platform for General Information

oneM2M offers several features that make it suitable as a technical building block in the context of Data Spaces.

In fact, while it is common to think of oneM2M as a framework oriented to the handling of IoT data, its design allows exchanging information across different sources (platforms, Data Spaces, devices).

The framework is a comprehensive interoperability solution designed to enable seamless communication across various protocols and data models. The data, which can represent any type of information, is semantically tagged and typically exchanged in JSON format.

oneM2M is a robust standard that provides a wide range of functionalities, including dataset discovery, licensing management, flexible security levels, and advanced granular access control. These access control techniques incorporate roles, tokens, identity verification, time-based restrictions, location-based conditions, and more. Initially developed for IoT data, oneM2M has since been adapted to handle virtually any type of data.

Benefits:

- Simplifies the environment by removing unnecessary duplicated solutions, thus allowing economy of scale.
- Preserves necessary/opportune solution specialization through interworking.
- Supports developer community and accelerates IoT development.
- Transfers competition from integration/platforms to services, helping to unlock the market.
- Enables inter-technology and inter-domain data sharing, generating new services and business opportunities.
- Reduces platform development and integration costs while enlarging the market.

Key features:

- Data management, historization, and information sharing.
- Dynamic privacy and access control.
- Multiple security levels.
- Storage and exposure for historical data, data search/aggregation, context information, and dynamic/real-time data.
- Network technology independence.
- Easy database and cloud integration.
- Flexible deployment adaptable to various domain requirements.
- Scalable architecture.
- Inter-provider native support.

Interworking Framework:

- Designed to interwork also with legacy field/core server technologies, other technologies, and proprietary solutions.

- Semantic enabled for information sharing.
- Internet friendly for human interaction.

Semantic Support:

- Works well with SAREF and its extensions.
- Provides universal semantic interoperability.
- Includes a base ontology and data annotation capabilities.

Works well with devices:

- Specifies a distributed software/middleware layer between applications and underlying communication networking hardware/software.
- Integrated into devices, gateways, and servers.
- Bridges various communication technologies (fixed, NB-IoT, 3GPP 4G, 5G, LoRa, etc.).
- Manages data (communication, storage, sharing) and devices/nodes.
- Allows semantic annotation of data.
- IP-based and URL/URI-based with Internet domain-based identifiers.
- Has native device management.

Although oneM2M is often associated with IoT data, it is fundamentally designed to support general information exchange. Its architecture enables seamless information sharing across a wide range of sources, including platforms, Data Spaces, and devices.

6.1.3 Mapping of oneM2M versus EU Data Act Article 33

The paragraphs below report how oneM2M features match the standardization requirements derived from the EU Data Act [i.4] article 33 as summarized in clause 4.2.

The following requirements apply to participants in Data Spaces that offer data or data services to other participants.

oneM2M is not a participant in a Data Space, rather it is a specification of a framework that enables data participants to offer their data or data services to other participants:

- Paragraph 1 (a).
  oneM2M only partially satisfies this requirement, in that it does not provide a single master catalogue, through which participants can classify the data and/or services they offer (note: there is an ongoing work item on the integration of NGSI-LD API integration into oneM2M, thus potentially fully satisfying this requirement in the future).

  However:

  - oneM2M has good support for semantics, supporting the storage, management and discovery of ontologies, both standard and custom, and offering capabilities to discover resources based on semantic descriptions and content.
  - Everything in oneM2M is represented via resources and their contents is available to users (according to their respective access rights) in machine-readable form (e.g. JSON). This applies to data resources, but also to resources that represent, e.g. access rules or other controlling means.

Information about the data collection methodology, data quality and uncertainty are not applicable in the case of oneM2M by itself, since such a verification is demanded from the participants of the Data Space.

On the other hand, oneM2M does not specify a standardised mechanism for the participant to advertise those properties of the data/services they are providing:

- Paragraph 1 (b).
  oneM2M TSs specify the format of all type of resources, as well as the rules and mechanisms for accessing and manipulating them. The definition of actual layout of data resources is left to the participants that offer them through an oneM2M platform.

- Paragraph 1 (c).
  oneM2M specifications provide a complete documentation describing APIs, protocols and all information necessary to enable automatic access and transmission of data between participants in a controlled way.

  Such documentation is the reference according to which implementations of the oneM2M specifications are made.
  Several such implementations are available, some of them are open source (see comment on Paragraphs 3 and 8 below).
  oneM2M provides a comprehensive set of tutorials and teaching materials [i.46], [i.47], [i.48], [i.49], aiming at lowering the barrier for potential Data Space participants interested in offering their data/services on top of a oneM2M compliant platform.
  Additionally, oneM2M provides a set of specifications on standardised testing to ensure conformity of such platforms.

- Paragraph 1 (d).
  oneM2M does specify interoperability mechanisms through which data can be exchanged, both with other oneM2M instances and/or with non-oneM2M systems, all while preserving data security and access rights.
  It does not support directly the execution of specific operations, like transformative rules or smart contracts. However, it does specify standard mechanisms through which entities (called Application Entities) implementing such rules can interact with oneM2M resources in a secure and controlled way.

- Paragraph 3 and Paragraph 8.
  Currently, there are several open-source implementations of the oneM2M specifications, e.g. ACME CSE [i.50], OCEAN/Moebius [i.51], OM2M [i.52].
  These implementations, among others, are listed on the oneM2M website [i.53]. They are examples of good practices concerning the provision of data services enabling the access to actual data stored by means of the oneM2M specifications.

6.1.4 Mapping of oneM2M versus Draft SReq on Trusted Data Transactions

The paragraphs below report how oneM2M features match the standardization requirements described in clause 5.2.

1) **Harmonised standards on Trusted Data Transactions**
   Part 1: Terminology, concepts and mechanisms

oneM2M specifications consist of a set of TSs. Their quality enables independent developers to develop conformant implementations.

A list of essential oneM2M TSs (and TRs) is available as ETSI TS 103 267 [i.79].

Especially relevant in the context of point 1 are:

- ETSI TS 118 111 [i.80]: "oneM2M; Common Terminology (ETSI TS 118 111)"
- ETSI TS 118 101 [i.81]: "oneM2M; Functional Architecture (ETSI TS 118 101)"
- ETSI TS 118 104 [i.82]: "oneM2M; Service Layer Core Protocol Specification (ETSI TS 118 104)"

As part of the specifications, terminology, concepts and mechanisms used are clearly specified. These can be contributed to define the subset of the SReq that can be covered by oneM2M.

2) **Harmonised standards on Trusted Data Transactions**
   Part 2: Trustworthiness requirements

oneM2M specifications include a set of functionalities and mechanisms to create a so-called "Trust Enabling Architecture". Such architecture ensures that the various software components that form an oneM2M instance and various oneM2M instances that can be interconnected can trust each other.

In this context, "trust" is a concept that applies to digital entities, not to humans interacting with the system(s).

3) **Harmonised standards on Trusted Data Transactions**
Part 3: Interoperability requirements

The oneM2M specifications define a framework that enables the creation of Data Spaces in ways that make them compliant with the SReq:

a) oneM2M supports the execution of data transactions.

b) oneM2M is an interoperability framework by design, enabling the sharing of data, information and services, thus making oneM2M a viable technical foundation for the creation of Data Spaces.

c) Security solutions are specified in ETSI TS 118 103 [i.83] and ETSI TS 118 116 [i.84].

d) oneM2M supports data sharing by design. API queries are supported, both simple ones and semantic based, also in distributed contexts.

e) oneM2M by design supports distributed architectures. Thanks to its legacy as an IoT Platform, access to devices is native.

f) In oneM2M, the execution of custom automated procedures is accomplished by leveraging the concept of Application Entities (AEs).

g) oneM2M directly specifies several of the requirements, while offering support for the implementation of some:

- oneM2M queries (including ontology-based queries) can find data, metadata and licenses.
Other aspects, e.g. data collection methodology, data quality and uncertainty, are outside the scope of oneM2M specifications. Such information, however, can be recorded by adequately structuring the resources, thus providing the Data Producers (participants of Data Spaces) a means to convey them to Data Users/Consumers.

- License management is explicitly specified in oneM2M. Other aspects, e.g. data quality conditions, service level agreements, and agreements on monetary or non-monetary compensation can be represented via appropriate structuring of resources.

- Technical access to the shared data, to enable automatic access and transmission of data between parties are clearly specified in oneM2M TSs.

- Usage permissions of shared data, based on consent and licensing agreements are specified in oneM2M TSs. The access control policies available in oneM2M are extremely sophisticated, able to cope with the most demanding scenarios.

- Consent management support is available in oneM2M; this has been studied with explicit consideration for GDPR and similar regulations that are in force in South Korea.

- oneM2M TSs specify the structure and usage of data resources. Documentation of user data currently lies outside oneM2M specifications.

- oneM2M specifications currently support observability and auditability of data transactions in a limited way: changes to the value (so called "content instance" in oneM2M jargon) of any resource are kept available and can be accessed by users (subject to access control policies). This represents a sort of data versioning.

Therefore, using a certified conformant implementation of the oneM2M specifications enables the fulfilment of this requirement when constructing a new data space.

4) **Technical specification(s) on a data catalogue implementation framework**

The oneM2M specifications support the adoption of ontologies and a rich set of functionalities for dealing with them directly, for tagging data resources and for finding and acting upon resources using semantic query.

Creators of Data Spaces leverage such capabilities to adopt metadata catalogues that are compliant to this requirement. Notably, oneM2M explicitly supports SAREF, which is discussed in detail in clause 6.2 of the present document.

5) **Technical specification(s) on an implementation framework for semantic assets**

The oneM2M specifications satisfy the requirements:

a) The oneM2M framework provides support for the adoption of common, open vocabularies, ontologies, etc. as per point a).

b) The oneM2M framework provides the mechanisms enabling creators of Data Spaces to adopt ontologies of their choice. Multiple ontologies can coexist in a single oneM2M instance. Among those mentioned at point b), SAREF is often used.

c) The definition of the criteria as per point c) falls into the duties of the data space designer. oneM2M does not constrain the designer's process for establishing such definition.

d) The methods referred at point d) are clearly specified for oneM2M.

6) **European standard on a quality framework for internal data governance**

These requirements are partially satisfied by oneM2M specifications.

Noting that the requirement calls for responsibilities that, at least in part, pertain to the duties of data space creators, while oneM2M is a framework supporting their choices, here is a breakdown of the various points:

a) oneM2M specifications clearly describe rich ways to technically define and control data ownership and access by the interested parties, taking into consideration also data licensing aspects and mechanisms that enable compliance with regulatory requirements (there are WIs addressing these aspects).

b) oneM2M specifications are technical in nature, legal aspects are currently not addressed beyond the scope of point a) above.

c) oneM2M specifications are technical in nature and describe APIs, mechanisms for managing information etc. There are guidelines and best practices for implementation and usage of the specifications but, currently, they too are oriented towards technical users and provide little in the sense that the two points require.

d) oneM2M specifications are technical in nature and describe APIs, mechanisms for managing information etc. There are guidelines and best practices for implementation and usage of the specifications but, currently, they too are oriented towards technical users and provide little in the sense that the two points require.

e) technical guides, wikis, video tutorials, learning notebooks are available, aiming to lower the barrier for potential data space participants interested in offering their data/services on top of a oneM2M compliant platform.
Additionally, some open source platforms (most notably, ACME CSE) offer straightforward ways to quickly and easily deploy instances of oneM2M together with useful tools, that can also be used for hands-on learning purposes.

7) **Technical specification(s) on a maturity model for Common European Data Spaces**

Currently the requirements are partially satisfied by oneM2M specifications.

a) Largely not satisfied by the oneM2M specifications.

b) Partially satisfied, at least regarding technical aspects.
In fact, the specifications cover in detail the way conformance tests are to be executed, and according to which patterns and methodologies, that are formally defined (this is the scope of a dedicated WG). Building upon these specifications, certification authorities have been created.

c) Largely not satisfied by the oneM2M specifications.

6.1.5 Mapping of oneM2M versus the DSSC Blueprint

The paragraphs below report how oneM2M features match the requirements by the DSSC Blueprint as described in clause 5.3.

Data Spaces

The oneM2M specifications define an information management and interoperability framework that enables the creation of Data Spaces taking into account the concepts mentioned in clause 5.3.3.

Building Blocks

Clause 5.3.4 introduces the concepts of Building Blocks, articulating them in two categories: "Business & Organisational" and "Technical".

The oneM2M specifications cover the areas that fall into the scope of the "Technical" category (they are technical specifications after all).

They do not address the area that falls into the scope of the "Business & Organisational" category.

Operating business entities that are oneM2M based, of course cannot dispense with "Business & Organisational" aspects, but each of them implements these aspects using techniques that are beyond the scope of oneM2M specifications.

Also worth noting is the fact that the concept of Building Block does not translate 1:1 to software implementations: for actual implementations, the Blueprint introduces the term "Services".

According to this, the oneM2M specifications (TSs) are to be considered as the specification for the actual implementation of an interoperability platform, thus falling into the realm of "Services".

Control Plane and Data Plane

The oneM2M specifications do not make explicit distinction between a Control Plane and a Data Plane as described in clauses 5.3.5 and 5.3.6.

With respect to the provisions for the Control Plane, the oneM2M specifications address some of them, e.g. those referring to Catalogue Entries and Management of the Transfer Process. The way they are specified and managed, however, revolves around the same concept of resources that also is used for the Data Plane.

Other provisions, like those related to Identity and Attestations, fall outside the scope of the oneM2M specifications.

Regarding the Data Plane, the Blueprint assumes that a great variety is to be expected among different Data Spaces: appropriate semantics and APIs are selected on a case-by-case basis.

oneM2M, instead, takes the stance that, with specifications designed for a suitable degree of flexibility, it is possible within a single framework to provide support for an exceptionally wide set of use cases. Even when specific foreign ontologies and data transfer protocols are requested to be adhered to, like in the examples at clause 5.3.6, it is possible:

a) to import said foreign ontologies and use them for tagging, searching and acting on resources;

b) in order to accommodate "foreign" protocols for data transfer, specifications are available for the creation of suitable connectors (named "Application Entities" in oneM2M jargon) and to govern their interaction with the rest of the oneM2M framework in a secure and controlled way. With this approach, oneM2M aims to minimise the effort for supporting these specific cases.

Reusability and Interoperability / Data Exchange

As mentioned above, the oneM2M specifications are designed with the intent of supporting the maximum possible degree of reusability, so as not to "reinvent the wheel" as stated in clause 5.3.7.

Regarding clause 5.3.8, here is a breakdown according to the provisions mentioned:

1) Data models:
   The oneM2M specifications define the support for semantic data models, as stated many times in the present document. Both standard (e.g. SAREF) and non-standard ontologies are supported. Multiple ontologies can coexist within a single instance of oneM2M framework. The specifications cover also the use of ontologies for interoperability with foreign (i.e. non-oneM2M systems).

2) Data Exchange:
   The Blueprint outlines guidelines for the choice of APIs, mentioning several qualities to take into consideration, but does not endorse any specific solution.
   The oneM2M specifications define a comprehensive set of protocols that are suitable for a wide set of use cases. For those cases where a different protocol are requested to be used, oneM2M specifies the creation of appropriate Application Entities, that ensure the interaction with the rest of the oneM2M framework in a secure and controlled way. Application Entities are reusable across different instances of the oneM2M framework. This approach greatly reduces the need for "reinventing the wheel", while keeping all specialisations clearly identifiable and localised at the border of the framework.
   A public registry of oneM2M Application Entities is available at [i.54]. Developers wishing to submit their own Application Entity can do so at [i.55].

3) Provenance and Traceability:
   The oneM2M specifications only partially satisfy this provision.
   A functionality that can help addressing this provision is the concept of "container instances", where changes to data resources are kept in the data base. In this way, changes over time of the values of any resource can be tracked.
   This functionality, however, is generic and might not satisfy specific requirements of some highly regulated domains.

6.2 ETSI SAREF specifications

The Smart Applications REFerence (SAREF) is a methodology supporting the creation of data repositories containing series of data produced through Internet of Things (IoT) devices. The SAREF methodology is instantiated by means of a suite of ontologies [i.1] forms a shared model of consensus intended to enable semantic interoperability between solutions from different providers and among various activity sectors on the IoT, thus contributing to the development of Data Spaces. The SAREF ecosystem is composed of a suite of individually versioned ontologies that contains a core ontology, a set of reference ontology patterns that provide guidelines on how to use and extend SAREF, and different extensions for vertical domains.

The paragraphs below report how datasets produced through the SAREF methodology meets the standardization requirements derived from the EU Data Act [i.4] article 33 and summarized in clause 4:

- Paragraph 1 (a).
  Each dataset built by using the SAREF suites includes information about its content, use restrictions, and licences in a machine-readable format, to allow the recipient to find, access and use the data. Information about the data collection methodology, data quality and uncertainty are partially supported by the SAREF methodology since it does not provide specifications about how to describe such aspects. These aspects are shortcomings towards the meet of standardization requirements.

- Paragraph 1 (b).
  To satisfy this requirement, it is necessary to integrate the DCAT-AP into SAREF. This way, the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, will be described in a publicly available and consistent manner to allowing the publication of SAREF-based datasets within the Common European Data Spaces catalogue.

- Paragraph 1 (c).
  This accessibility requirement is satisfied by the current SAREF methodology that, in turn, make the produced datasets compliant as well. SAREF is published by using the RDF Turtle language, a machine-readable format recommended by the W3C. This way, it is possible to understand the structure of the datasets built by using SAREF in a clear manner. Moreover, datasets can be made available by using the same data structure adopted in the SAREF.

- Paragraph 1 (d).
  Not applicable in the context of the datasets produced by using the SAREF suite.

- Paragraph 3 and Paragraph 8.
  Currently, even SAREF is available for download through its website, it is not equipped with a facility allowing the access to the structured data produced by using SAREF. This issue is going to be addressed through the work planned for Specialist Task Force (STF) 693 on "IoT Ontology Web Server". The main outcome of the STF is, indeed, a web server supporting such a harmonised data access fulfilling this requirement.

The second part of this clause reports the considerations concerning how SAREF meets the standardization requirements described in clause 5.2. Below, the considerations for each requirement in terms of both adherence and gaps are reported.

Concerning the General Requirement A, the deliverables providing the details of the SAREF methodology already fulfil the SReq described. Hence, SAREF is compliant with it.

1) **Harmonised standards on Trusted Data Transactions - Part 1: Terminology, concepts and mechanisms**

   The SAREF methodology consists of a set of TSs. Their quality enables independent developers to develop conformant implementations. As part of the specifications, terminology, concepts and mechanisms used are clearly specified. These can be contributed to define the subset of the SReq that can be covered by SAREF.

2) **Harmonised standards on Trusted Data Transactions - Part 2: Trustworthiness requirements**

   The analysis of the SAREF methodology in the context of the trustworthiness requirements provided by the European Commission [i.60] revealed how such requirements are not correlated with the SReq except for the Requirement #3 about "Privacy and Data Governance".

   In this context, the datasets built by using the SAREF methodology are compliant with such a requirement since the adoption of the SAREF methodology grants the quality and the integrity of the data contained in the dataset, as well as the access to them. These aspects are supported by the SAREF pipeline.

3) **Harmonised standards on Trusted Data Transactions - Part 3: Interoperability requirements**

   Concerning this requirement, the SAREF methodology is affected by some gaps that can be addressed through the provision of a more structure technical solution. In particular, the gaps to fulfil are the following. The other requests by the SReq not mentioned below, are to be considered already satisfied by the SAREF ecosystem or not applicable:

   a) "Addressing main data sharing methods, including file transfer, Application Programming Interface (API) queries, and emerging scenarios such as distributed analytics."

The whole SAREF ecosystem is available for download through the dedicated portal. However, it is still missing an endpoint to query SAREF-based datasets aiming to extract knowledge about their structures and contents.

   b) "Including scenarios for direct access of data residing in distributed systems and smart devices."

The SAREF ecosystem comes with a collection of synthetic examples showing how the ontologies can be instantiated. However, the type of scenarios specified in the SReq is not addressed since, currently, the SAREF ecosystem does not include an accompanying web server enabling the mentioned type of access.

   c) "Defining the trustworthiness and interoperability requirements for the following key aspects of a data transaction."

This gap is linked with the one described in the next point. The datasets built by using the SAREF ecosystem are, on the one hand, equipped with some descriptors coming from the RDF language. But, on the other hand, each dataset is not associated with a datasheet providing all the necessary information required by the SReq (e.g. data quality descriptors).

1) **Technical specification(s) on a data catalogue implementation framework**

To fulfil this gap is necessary to equip an asset with a catalogue of metadata describing the resource. The vocabulary recommended by the EU SReq is DCAT. Through DCAT, it is possible to generate a DCAT Application Profile (DCAT-AP) for each dataset built by using one or more ontologies composing the SAREF ecosystem. An application profile allows to provide metadata describing such datasets to make them compliant with the SReq.

2) **Technical specification(s) on an implementation framework for semantic assets**

This requirement is completely satisfied by the datasets produced through the SAREF ecosystem. Indeed, SAREF is mentioned within the SReq as a virtuous example since it can be used by other data repositories to fulfil the SReq.

3) **European standard on a quality framework for internal data governance**

This requirement is satisfied by the SAREF ecosystem through the ETSI EN 303 760 [i.38] aims to bring together widely considered good practices in semantic interoperability for IoT smart applications in a set of high-level outcome-focused provisions. The objective of the document is to support all parties involved in the development and manufacturing of IoT smart applications and products with guidance on making them interoperable in compliance to the SAREF framework. The provisions give organizations and companies the flexibility to innovate and implement SAREF-compliant semantic interoperability solutions appropriate for their products and applications.

Through the content of this document, the dataset produced through the SAREF ecosystem meets this aspect of the SReq.

4) **Technical specification(s) on a maturity model for Common European Data Spaces**

Currently, this request of the SReq is not satisfied by dataset built by using SAREF since no evaluation procedures to assess their maturity and their interoperability compared to the Common European Data Space has been defined within the SAREF methodology.

6.3 ETSI NGSI-LD specifications

NGSI-LD [i.39] is information model and API for publishing, querying and subscribing to context information. It enables structured information sharing across multiple domains like smart cities, smart industries, and digital twins. Standardized by ETSI through ISG CIM, it builds on decades of context management research and evolved from the OMA's NGSI specifications via the FIWARE community.

The NGSI-LD information model represents Context Information as entities that have properties and relationships to other entities. It is derived from property graphs, with semantics formally defined on the basis of RDF and the semantic web framework.

The paragraphs below report how NGSI-LD meets the standardization requirements derived from the EU Data Act [i.4] article 33 and summarized in clause 4:

- Paragraph 1 (a).
  NGSI-LD satisfies this requirement by including information about its content, use restrictions, and licences in a machine-readable format, to allow the recipient to find, access and use the data. Information about the data collection methodology, data quality and uncertainty are not applicable in the case of NGSI-LD since it is defined as a vocabulary to annotate data that have been previously collected. Hence, such a verification is demanded to the creator of the dataset annotated with the NGSI-LD vocabulary.

- Paragraph 1 (b).
  The NGSI-LD standard is aligned with this requirement since it is classified at the same level of DCAT, i.e. a vocabulary to describe datasets.

- Paragraph 1 (c).
  This accessibility requirement is satisfied by the NGSI-LD standard. The specifications provide a complete documentation concerning the accessing mechanisms to all the data stored by using such a standard. NGSI-LD comes also with a set of open-source implementations of web service that can be used to access data collections stored by using this standard.

- Paragraph 1 (d).
  Not applicable in the context of NGSI-LD.

- Paragraph 3 and Paragraph 8.
  Currently, there are several open-source brokers implementing the NGSI-LD specifications, e.g. Orion-LD [i.40], Scorpio [i.41], Stellio [i.42], and Cassiopea [i.43]. These implementations are examples of good practices concerning the provision of data services enabling the access to actual data stored by means of the NGSI-LD specifications.

The second part of this clause reports the considerations concerning how NGSI-LD meets the standardization requirements described in clause 5.2. Below, the considerations for each requirement in terms of both adherence and gaps are reported.

Concerning the General Requirement A, the deliverables providing the details of the NGSI-LD specifications already fulfil the SReq described. Hence, SAREF is compliant with it.

1) **Harmonised standards on Trusted Data Transactions - Part 1: Terminology, concepts and mechanisms**

The NGSI-LD information model consists of a specifications. Their quality enables independent developers to develop conformant implementations. As part of the specifications, terminology, concepts and mechanisms used are clearly specified. These can be contributed to define the subset of the SReq that can be covered by NGSI-LD.

2) **Harmonised standards on Trusted Data Transactions - Part 2: Trustworthiness requirements**

The analysis of the NGSI-LD information model in the context of the trustworthiness requirements provided by the EU Commission [i.60] revealed how such requirements are not correlated with the SReq except for the Requirement #3 about "Privacy and Data Governance".

In this context, the NGSI-LD information model provides a set of APIs enabling the development of data brokers. Such data brokers support the access to the data stored by using the NGSI-LD model.

3) **Harmonised standards on Trusted Data Transactions - Part 3: Interoperability requirements**

Concerning this requirement, the NGSI-LD specifications play the role of drivers to build assets being compliant with the SReq. Hence, the appropriate adoption of NGSI-LD specifications would allow the fulfilment of all aspects mentioned by this requirement when constructing new data resources.

4) **Technical specification(s) on a data catalogue implementation framework**

The NGSI-LD specifications are aligned with this requirement since they provide a mechanism to define common catalogue metadata that can be applied across all Common European Data Spaces. Moreover, through such specifications, NGSI-LD drives the definition of domain-specific catalogue metadata. Finally, NGSI-LD is accompanied by a governance structure, i.e. ETSI, supporting the development and maintenance of the specifications.

5) **Technical specification(s) on an implementation framework for semantic assets**

This requirement is satisfied by the NGSI-LD specifications. Indeed, the provision of a framework for common, open vocabularies; the definition of criteria for the selection of semantic assets; and the definition of methods for the semantic annotation of shared data are addressed by the current version of the framework.

6) **European standard on a quality framework for internal data governance**

This requirement is partially satisfied by the NGSI-LD specifications through the documents available on the NGSI-LD portal describing the best practices about how to manage data repositories through NGSI-LD and its applicability across different domains. Then, documents providing implementation guidelines for NGSI-LD brokers are available as well.

The standardization aspect that is not addressed by the specifications is how these specifications support the meet of domain-specific requirements not linked directly with regulatory aspects.

7) **Technical specification(s) on a maturity model for Common European Data Spaces**

Currently, this SReq is not satisfied by NGSI-LD since the evaluation procedure to assess the maturity and the interoperability of the NGSI-LD specifications within the Common European Data Space is still under development.

7 Conclusions

The article 33 of the EU Data Act [i.4] addresses participants in Data Spaces that offer data or data services to other participants. It requests them to comply with the essential requirements listed in it. Following article 33 (4), which requires the European Commission to "request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of article 33". The European Commission has made available the draft of the standardisation request SReq [i.3]. The SReq requests CEN, CENELEC and ETSI to draft new European standards and European standardisation deliverables as listed in the Annexes of the SReq in support of article 33 of the EU Data Act [i.4]. These new standards to be developed are expected to support the participants in Data Spaces that offer data or data services to other participants to comply with article 33 of the EU Data Act [i.4] and apply already existing standards.

The present document has analysed the requirements of article 33 of the EU Data Act [i.4] and the SReq [i.3] with respect to the question, how existing standards of oneM2M, ETSI SAREF and ETSI NGSI-LD specifications match these standardization requirements. Further analysis regards the mapping of oneM2M versus the DSSC Blueprint which is explicitly referred to in the SReq.

oneM2M matches almost all of the requirements of the EU Data Act [i.4] article 33 listed in clause 4.2. Paragraph 1 (a) is partially satisfied. However, work on the gap has already been started based on the work item on the integration of NGSI-LD API integration into oneM2M. oneM2M matches requirements for the requested standardisation activities #1, #2 and #3 of the SReq [i.3]. In contrast, the requirements for the standardisation activities #4 and #5 are partially satisfied by oneM2M specifications which opens the door for further oneM2M standardisation activities.

SAREF matches the paragraphs 1 (a) and (c) of the EU Data Act [i.4] article 33 listed in clause 4.2. The paragraph 1 (b) is partially satisfied, while SAREF currently does not match the requirements of paragraphs 3 and 8. The latest issues have already been addressed through the work planned for Specialist Task Force (STF) 693 on "IoT Ontology Web Server". SAREF matches requirements for the requested standardisation activities #3 and #4, of the SReq [i.3], whereas the requirements for the standardisation activities #1 and #2 are partially satisfied and #5 not matched by SAREF. Respective gaps are listed in clause 6.2.

ETSI NGSI-LD specifications match all applicable paragraphs of the EU Data Act [i.4] article 33 listed in clause 4.2. They match the requirements for the requested standardisation activities #1, #2, #3, whereas the requirements for the standardisation activities #4 and #2 are partially satisfied and #5 is not matched. The respective gaps listed in clause 6.2 will provide opportunities for standardization work.

Annex A:
Structure of the EU Data Act

- **Chapter I - General Provisions**
  - Article 1 - Subject matter and scope
  - Article 2 - Definitions
- **Chapter II - Business to consumer and business to business data sharing**
  applies to data, with the exception of content, concerning the performance, use and environment of connected products and related services
  - Article 3 - Obligation to make product data and related service data accessible to user
  - Article 4 - The rights and obligations of users and data holders with regard to access, use and making available product data and related service data
  - Article 5 - Right of the user to share data with third parties
  - Article 6 - Obligations of third parties receiving data at the request of the user
  - Article 7 - Scope of business-to-consumer and business-to-business data sharing obligations
- **Chapter III - Obligations for the data holders obliged to make data available pursuant to Union law**
  applies to any private sector data that is subject to statutory data sharing obligations
  - Article 8 - Conditions under which data holders make data available to data recipients
  - Article 9 - Compensation for making data available
  - Article 10 - Dispute settlement
  - Article 11 - Technical protection measures on the unauthorised use or disclosure of data
  - Article 12 - Scope of obligations for data holders obliged pursuant to Union law to make data available
- **Chapter IV - Unfair contractual terms related to data access and use between enterprises**
  applies to any private sector data accessed and used on the basis of contract between enterprises
  - Article 13 - Unfair contractual terms unilaterally imposed on another enterprise
- **Chapter V - Making data available to public sector bodies, the Commission, The European Central Bank and Union bodies on the basis of an exceptional need**
  applies to any private sector data with a focus on non-personal data
  - Article 14 - Obligation to make data available on the basis of an exceptional need
  - Article 15 - Exceptional need to use data
  - Article 16 - Relationship with other obligations to make data available to public sector bodies, the Commission, the European Central Bank and Union bodies
  - Article 17 - Request for data to be made available
  - Article 18 - Compliance with requests for data
  - Article 19 - Obligations of public sector bodies, the Commission, the European Central Bank and Union bodies
  - Article 20 - Compensation in cases of an exceptional need
  - Article 21 - Sharing of data obtained in the context of an exceptional need with research organisations or statistical bodies

- Article 22 - Mutual assistance and cross-border cooperation

- **Chapter VI - Switching between data processing services**
  applies to any data and services processed by providers of data processing services
  - Article 23 - Removing obstacles to effective switching
  - Article 24 - Scope of the technical obligations
  - Article 25 - Contractual terms concerning switching
  - Article 26 - Information obligation of providers of data processing services
  - Article 27 - Obligation of good faith
  - Article 28 - Contractual transparency obligations on international access and transfer
  - Article 29 - Gradual withdrawal of switching charges
  - Article 30 - Technical aspects of switching
  - Article 31 - Specific regime for certain data processing services
- **Chapter VII - Unlawful** international **governmental access and transfer of non-professional data**
  applies to any non-personal data held in the Union by providers of data processing services.
  - Article 32 - International governmental access and data transfer
- **Chapter VIII - Interoperability**
  - Article 33 - Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces
  - Article 34 - Interoperability of the purposes of in-parallel use of data processing services
  - Article 35 - Interoperability of data processing services
  - Article 36 - Essential requirements regarding smart contracts for executing data sharing agreements
- **Chapter IX - Implementation of enforcement**
  - Article 37 - Competent authorities and data coordinators
  - Article 38 - Right to lodge a complaint
  - Article 39 - Right to effective judicial remedy
  - Article 40 - Penalties
  - Article 41 - Model contractual terms and standard contractual clauses
  - Article 42 - Role of the EDIB
- **Chapter X - SUI generis right under Directive 96/9/EC**
  - Article 43 - Data basis containing certain data
- **Chapter XI - Final provisions**
  - Article 44 - Other Union legal acts governing rights and obligations on data access and use
  - Article 45 - Exercise of the delegation
  - Article 46 - Committee procedure
  - Article 47 - Amendment to Regulation (EU) 2017/2394
  - Article 48 - Amendment to Directive (EU) 2020/1828

- Article 49 - Evaluation and review
- Article 50 - Entry into force and application

Annex B:
Highlights of EU Data Act articles with technical/standardisation relevance

Chapter I - General Provisions

Article 1 - Subject matter and scope

- Rules on:
  - making available of product data and related service data to the user and of data by data holders to data recipients, public sector bodies, the Commission, the European Central Bank and Union bodies;
  - facilitating switching between data processing services;
  - introducing safeguards against unlawful third-party access to non-personal data;
  - the development of interoperability standards for data to be accessed, transferred and used.
- Covers personal and non-personal data.
- Applies to:
  - *manufacturers of connected products placed on the market in the Union and providers of related services;*
  - *users in the Union of connected products or related services;*
  - *data holders that make data available to data recipients in the Union*;
  - *data recipients in the Union to whom data are made available;*
  - *public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need;*
  - *providers of data processing services providing such services to customers in the Union;*
  - *participants in Data Spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.*
- *Regulation refers to connected products or related services, such references are also understood to include virtual assistants* (SW) *insofar as they interact with them.*

Article 2 - Definitions

- *'interoperability'*
  means the ability of two or more Data Spaces or communication networks, systems, connected products, applications, data processing services or components to exchange and use data in order to perform their functions.
- *'open interoperability specification'*
  means a technical specification in the field of information and communication technologies which is performance oriented towards achieving interoperability between data processing services.

Chapter II - Business to consumer and business to business data sharing

Article 3 - Obligation to make product data and related service data accessible to user

- *Connected products shall be designed and manufactured,*
  and related services shall be designed and provided, in such a manner that
  product data and related service data,
  including the relevant metadata necessary to interpret and use those data,
  are, by default, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and,
  where relevant and technically feasible, directly accessible to the user:

  - *purchase, rent or lease of a connected product*
    Seller, rentor or lessor, which may be the manufacturer, shall provide at least the following information to the user, in a clear and comprehensible manner:

    - *the type, format and estimated volume of product data which the connected product is capable of generating;*
    - *whether the connected product is capable of generating data continuously and in real-time;*
    - *whether the connected product is capable of storing data on-device or on a remote server, including, where applicable, the intended duration of retention;*
    - *how the user may access, retrieve or, where relevant, erase the data, including the technical means to do so, as well as their terms of use and quality of service.*

- Provision of a related service
  Provider of such related service shall provide at least the following information to the user:

  - *the nature, estimated volume and collection frequency of product data that the prospective data holder is expected to obtain and*
    of related service data to be generated, and, where relevant, the arrangements for the user to access or retrieve such data;
  - *how the user can request that the data are shared with a third party and, where applicable, end the data sharing.*

Article 4 - The rights and obligations of users and data holders with regard to access, use and making available product data and related service data

- *Where data cannot be directly accessed by the user from the connected product or related service,*
  data holders shall make readily available data,
  as well as the relevant metadata necessary to interpret and use those data,
  accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.
  This shall be done on the basis of a simple request through electronic means where technically feasible.

Article 5 - Right of the user to share data with third parties

- *Upon request, the data holder shall make available readily available data,*
  as well as the relevant metadata necessary to interpret and use those data,
  to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time.

Chapter III - Obligations for the data holders obliged to make data available pursuant to Union law

Article 11 - Technical protection measures on the unauthorised use or disclosure of data

- *A data holder may apply appropriate technical protection measures,*
  including smart contracts and encryption,
  to prevent unauthorised access to data, including metadata.

Such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties pursuant to Article 5.

Chapter VI - Switching between data processing services

Article 23 - Removing obstacles to effective switching

- *Providers of data processing services shall enable customers to switch to a data processing service, covering the same service type, which is provided by a different provider of data processing services, or to on-premises ICT infrastructure, or, where relevant, to use several providers of data processing services at the same time.*

Chapter VI - Switching between data processing services

Article 30 - Technical aspects of switching

- *Providers of data processing services* (exceptions specified in paragraph 1 of this article) *shall make open interfaces available to an equal extent to all their customers and the concerned destination providers of data processing services to facilitate the switching process.*
  Those interfaces shall include sufficient information on the service concerned to enable the development of software to communicate with the services, for the purposes of data portability and interoperability.

- *Providers of data processing services* (exceptions specified in paragraph 1 of this article) *shall ensure compatibility with common specifications based on open interoperability specifications or harmonised standards for interoperability at least 12 months after the references to those common specifications or harmonised standards for interoperability of data processing services were published in the central Union standards repository for the interoperability of data processing services following the publication of the underlying implementing acts in the Official Journal of the European Union in accordance with Article 35(8).*

- If those standards for the applied service type, *have not been published in the central Union standards repository as mentioned above, the provider of data processing services shall, at the request of the customer, export all exportable data in a structured, commonly used and machine-readable format.*

Chapter VIII - Interoperability

Article 33 - Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces

- *Participants in Data Spaces that offer data or data services to other participants shall comply with the following essential requirements to facilitate the interoperability of data, of data sharing mechanisms and services, as well as of common European Data Spaces which are purpose- or sector-specific or cross-sectoral interoperable frameworks for common standards and practices to share:*

  - *the dataset content, use restrictions, licences, data collection methodology, data quality and uncertainty shall be sufficiently described, where applicable, in a machine-readable format, to allow the recipient to find, access and use the data;*

  - *the data structures, data formats, vocabularies, classification schemes, taxonomies and code lists, where available, shall be described in a publicly available and consistent manner;*

  - *the technical means to access the data, such as application programming interfaces, and their terms of use and quality of service shall be sufficiently described to enable automatic access and transmission of data between parties, including continuously, in bulk download or in real-time in a machine-readable format where that is technically feasible and does not hamper the good functioning of the connected product;*

  - *where applicable, the means to enable the interoperability of tools for automating the execution of data sharing agreements, such as smart contracts shall be provided.*

Article 33 - Essential requirements regarding interoperability of data, of data sharing mechanisms and services, as well as of common European data spaces

- *The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.*

- *Paragraph 5: The Commission may, by means of implementing acts, adopt common specifications covering any or all of the essential requirements laid down in paragraph 1. Conditions are specified in paragraphs 6, 7 and 9.*

Article 35 - Interoperability of data processing services

Open interoperability specifications and harmonised standards for the interoperability of data processing services:

- *shall (paragraph 1):*
  - *achieve, where technically feasible, interoperability between different data processing services that cover the same service type;*
  - *enhance portability of digital assets between different data processing services that cover the same service type;*
  - *facilitate, where technically feasible, functional equivalence between different data processing services referred to in Article 30(1) that cover the same service type;*
  - *not have an adverse impact on the security and integrity of data processing services and data;*
  - *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.*
- *shall adequately address (paragraph 2):*
  - *the cloud interoperability aspects of transport interoperability, syntactic interoperability, semantic data interoperability, behavioral interoperability and policy interoperability;*
  - *the cloud data portability aspects of data syntactic portability, data semantic portability and data policy portability;*
  - *the cloud application aspects of application syntactic portability, application instruction portability, application metadata portability, application behavior portability and application policy portability*.

Article 35 - Interoperability of data processing services

- *Open interoperability specifications shall comply with Annex II to Regulation (EU) No 1025/2012.*
- *After taking into account relevant international and European standards and self-regulatory initiatives, the Commission may, in accordance with Article 10(1) of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraphs 1 and 2 of this Article.*
- *The Commission may, by means of implementing acts, adopt common specifications based on open interoperability specifications covering all of the essential requirements laid down in paragraphs 1 and 2*. More conditions are specified in paragraphs 6, 7, 8 and 9.

Article 36 - Essential requirements regarding smart contracts for executing data sharing agreements

- Paragraph 1
  The vendor of an application using smart contracts shall ensure that those smart contracts comply with the following essential requirements of:
  - *robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;*
  - *safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;*
  - *data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);*

- *access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers;*
- *consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.*

- *The vendor of a smart contract shall perform a conformity assessment with a view to fulfilling the essential requirements laid down in paragraph 1 and, on the fulfilment of those requirements, issue an EU declaration of conformity.*
- *The Commission shall, pursuant to Article 10 of Regulation (EU) No 1025/2012, request one or more European standardisation organisations to draft harmonised standards that satisfy the essential requirements laid down in paragraph 1 of this Article.*
- *The Commission may, by means of implementing acts, adopt common specifications covering any or all of the essential requirements laid down in paragraph 1*. Conditions are specified in paragraphs 6, 7 and 8.

History

Document history		
V1.1.1	June 2025	Publication