

**CEN**

**CWA 18125**

**WORKSHOP**

July 2024

**AGREEMENT**

---

ICS 35.030

English version

## Trusted Data Transaction

This CEN Workshop Agreement has been drafted and approved by a Workshop of representatives of interested parties, the constitution of which is indicated in the foreword of this Workshop Agreement.

The formal process followed by the Workshop in the development of this Workshop Agreement has been endorsed by the National Members of CEN but neither the National Members of CEN nor the CEN-CENELEC Management Centre can be held accountable for the technical content of this CEN Workshop Agreement or possible conflicts with standards or legislation.

This CEN Workshop Agreement can in no way be held as being an official standard developed by CEN and its Members.

This CEN Workshop Agreement is publicly available as a reference document from the CEN Members National Standard Bodies.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



EUROPEAN COMMITTEE FOR STANDARDIZATION  
COMITÉ EUROPÉEN DE NORMALISATION  
EUROPÄISCHES KOMITEE FÜR NORMUNG

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

---

© 2024 All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CEN/CENELEC Members.  
C

Ref. No.:CWA 18125:2024 E

<b>Contents</b>	<b>Page</b>
<b>European foreword</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>4</b>
<b>1 Scope</b> .....	<b>5</b>
<b>2 Normative references</b> .....	<b>5</b>
<b>3 Terms and definitions</b> .....	<b>5</b>
<b>4 Objectives, stakeholders and concepts of trusted data transaction</b> .....	<b>8</b>
<b>4.1 Objectives</b> .....	<b>8</b>
<b>4.2 Stakeholders</b> .....	<b>8</b>
<b>4.2.1 General</b> .....	<b>8</b>
<b>4.2.2 Data provider and data user</b> .....	<b>8</b>
<b>4.2.3 Data intermediary</b> .....	<b>9</b>
<b>4.2.4 Trust service and trust anchors</b> .....	<b>9</b>
<b>4.3 Concepts</b> .....	<b>9</b>
<b>4.3.1 Data and data product</b> .....	<b>9</b>
<b>4.3.2 Data transaction</b> .....	<b>9</b>
<b>Figure1 — Scope of data transaction</b> .....	<b>10</b>
<b>4.3.3 Trusted data transaction</b> .....	<b>11</b>

## European foreword

This CEN Workshop Agreement has been developed in accordance with the CEN/CENELEC Guide 29 “CEN/CENELEC Workshop Agreements – A rapid prototyping to standardization” and with the relevant provisions of CEN/CENELEC Internal Regulations - Part 2. It was approved by a Workshop of representatives of interested parties on 2024-05-30, the constitution of which was supported by CEN following the public call for participation made on 2023-02-10. However, this CEN Workshop Agreement does not necessarily include all relevant stakeholders.

The final text of this CEN Workshop Agreement was provided to CEN for publication on 2024-06-18.

The following organizations and individuals developed and approved this CEN Workshop Agreement:

AGDATAHUB – Christophe Gervais

BIG DATA VALUE ASSOCIATION (BDVA) – Daniel Alonso and Ana Garcia

DAWEX – Fabrice Tocco

FIWARE - Andrea Battaglia and Chandra Challagonda

FRAUNHOFER ISST - Jan Jürjens and Tobias Guggenberger

GAIA-X – Giuditta Del Buono

HUB ONE – Romain Rollet

INTERNATIONAL DATA SPACES ASSOCIATION (IDSA) – Sebastian Steinbuss and Silvia Castellvi

MICROSOFT – Eric Samson

TNO – Simon Dalmolen and Matthijs Punter

Attention is drawn to the possibility that some elements of this document may be subject to patent rights. CEN policy on patent rights is described in CEN-CENELEC Guide 8 “Guidelines for Implementation of the Common IPR Policy on Patent”. CEN shall not be held responsible for identifying any or all such patent rights.

Although the Workshop parties have made every effort to ensure the reliability and accuracy of technical and non-technical descriptions, the Workshop is not able to guarantee, explicitly or implicitly, the correctness of this document. Anyone who applies this CEN Workshop Agreement shall be aware that neither the Workshop, nor CEN, can be held liable for damages or losses of any kind whatsoever. The use of this CEN Workshop Agreement does not relieve users of their responsibility for their own actions, and they apply this document at their own risk. The CEN Workshop Agreement should not be construed as legal advice authoritatively endorsed by CEN/CENELEC.

## Introduction

Data is now the backbone of the digital economy, enabling economic growth and competitiveness, fostering innovation, improving public services or advancing scientific research. Seamless and secure cross-border and cross-industry data flows, within and across data spaces or data ecosystems, have become crucial for businesses and individuals worldwide. As technologies such as artificial intelligence (AI) and internet of things (IoT) continue to evolve and spread, the importance of data exchange, data sharing and data flows will only become more significant.

In its Communication on a European strategy for data of February 29, 2020, the Commission describes its vision for the data economy, based on European values and fundamental rights and the conviction that the human being is and should remain at the centre.

Data spaces should foster an ecosystem aiming to facilitate cross-border data flow and harmonizing regulations across sectors within the EU, ensuring adherence to European rules and values such as personal data protection, consumer protection, and fair competition.

European strategy for data also seeks to establish clear, practical, and transparent rules for data access and usage, alongside robust governance mechanisms, while adopting an open yet principled approach to international data flows

The legal environment around data exchanges and data transactions plays an essential role in the development of data ecosystems, bringing a trust framework for all stakeholders involved in the exchange of data. In Europe some of the key regulations are:

- the General Data Protection Regulation (EU) 2016/679 (GDPR), a comprehensive data protection law enacted by the European Union (EU) to regulate the collection, processing, and storage of personal data. It applies both to European organisations that process personal data of individuals in the EU, and to organisations outside the EU that target people living in the EU.
- the Data Governance Act (DGA), which entered in force in the EU in June 2022 and is in application since September 24, 2023. The DGA is a cross-sectoral instrument that aims to make more data available by regulating the re-use of publicly/held, protected data, by boosting data sharing through the regulation of data intermediaries and by encouraging the sharing of data for altruistic purposes. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the General Data Protection Regulation (GDPR) applies. In addition to the GDPR, inbuilt safeguards will increase trust in data sharing and re-use, a prerequisite to making more data available on the market.
- the Data Act - which entered into force in January 2024, and will become applicable in September 2025. . While the Data Governance Act creates the processes and structures to facilitate data sharing, the Data Act clarifies who can create value from data and under which conditions and provides legal clarity for businesses as regards the use of data. The Data Act aims to facilitate the development of new services leveraging Europe's wealth of data, but also ensures fairness by regulating the rights and obligations of all the economic actors involved in sharing data, particularly from Internet of Things (IoT) devices

Along with reference architectures, trust frameworks and data regulations, the existence of standards recognized by the community represents another key pillar for developing collaborations around data, across borders and across industries, easily, effectively while facilitating interoperability.

As trust is needed for stakeholders to engage in data transactions the CEN Workshop focuses on the subject of trusted data transactions.

## 1 Scope

The scope of this document is to provide terminology, concepts and mechanisms in the field of data exchange focusing on trusted data transactions.

Those elements can be used in the development of standards in support of trusted data transactions. These terminology, concepts and mechanisms constitute the basis to identify key dimensions and criteria that contribute to the trust in a data transaction between interested parties.

Therefore, those elements may constitute a foundational understanding on which trusted data transactions can be based, independently of any architectural choices or technical implementation.

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

### 3.1

#### **data**

re-interpretable representation of information in a formalised manner suitable for communication, interpretation, or processing

[SOURCE: ISO/IEC 20546:2019 (Big data – Overview and vocabulary)]

### 3.2

#### **data user**

person or organization authorized to exploit data

Note 1 to entry: Data are in the form of data products.

Note 2 to entry: Data consumer is considered as a synonym of data user.

[SOURCE: ISO 5127:2017 with Note 1 and Note 2 to entry added]

### 3.3

#### **data exchange**

#### **data sharing**

process by which a data provider grants a data user access to a data product, subject to applicable technical, financial, legal, or organisational use requirements

Note 1 to entry: The process refers to a full spectrum of practices related to sharing or exchanging any kind of data, including but not limited to open data and the many forms of non-open data.

Note 2 to entry: The process may or may not require transfer of data.

Note 3 to entry: In the context of this document “data exchange” and “data sharing” are used in an interchangeable way.

### 3.4

#### **data licence terms**

terms and conditions of use of a data product as defined by the data provider

Note 1 to entry: Terms and conditions include notions such as, without being limited to, duration, territory, sub-licensing rights or commercial terms.

### 3.5

#### **data product**

data sharing unit, packaging data and metadata, and any associated licence terms

Note 1 to entry: Data product does not necessarily imply commercial aspects.

Note 2 to entry: Data product can be published in a data product catalogue that is searchable by data users.

Note 3 to entry: In the context of trusted data transactions, a data product will be associated with data licence terms.

### 3.6

#### **data producer**

natural person, legal person, device or any software that generates data

### 3.7

#### **data provider**

legal person that has the right or duty to make data available to data users through data products

Note 1 to entry: Data provider carries out several activities, ie.:

- non-technical, on behalf of a data rights holder, including the description of the data products, data licence terms, the publishing of data products in a data product catalogue, the negotiation with the data users, and the conclusion of contracts,
- technical, with the provision of the data products to the data users.

### 3.8

#### **data rights holder**

natural or legal person that has legal rights or obligations to use, grant access to or share certain data, or transfer such rights to others

Note 1 to entry: Data rights holder and data provider represent different roles, that can be carried out by the same entity or by different entities.

### 3.9

#### **data space** (preferred option)

#### **dataspace**

interoperable framework, based on common governance principles, standards, practices and enabling services, that enables trusted data transactions between participants Note 1 to entry: Data space enabling services are implemented by one or more infrastructures

Note 2 to entry: Data spaces enable one or more use cases.

**3.10****data transaction**

result of an agreement between a data provider and a data user with the purpose of exchanging, accessing and using data, in return for monetary or non-monetary compensation

Note 1 to entry: “Data exchange“ and “data access“ terms are used in order to describe different mechanisms, like actual transfer of data or situations where data does not move but where access is provided to different stakeholders.

Note 2 to entry: Data transactions do not necessarily imply a commercial relationship.

Note 3 to entry: Each data transaction is unique and must be treated independently of other data transactions.

**3.11****metadata**

data about data or data elements, possibly including their data descriptions, and data about data ownership, access paths, access rights and data volatility

[SOURCE: ISO/IEC 20546:2019 (Big data – Overview and vocabulary)]

**3.12****data usage contract**

agreement between a data provider and a data user specifying the terms and conditions of a data usage, including the data rights holder’s permission

**3.13****trust service**

enabling service that offers assurances within a data transaction

**3.14****trust anchor**

well-defined, shared authority that creates assurances

Note 1 to entry: Trust anchors can be used for example, but not limited to, for guaranteeing identities of natural or legal persons.

**3.15****data intermediary**

legal person that provides data intermediation services to data providers and data users

**3.16****data intermediation service**

one of the optional services which aims to support data transactions between data providers and data users

Note 1 to entry: Some data intermediation services fall under the rules defined in the Data Governance Act.

Note 2 to entry: In some regulated industries, the use of data intermediation services can be mandatory.

**3.17****data catalogue**

organized inventory of data products published by one or more data providers that can be searched by data users

### 3.18

#### **data usage consent**

legal basis for the usage of personal data

### 3.19

#### **data usage permission**

legal basis for the access and usage of non-personal data

## **4 Objectives, stakeholders and concepts of trusted data transaction**

### **4.1 Objectives**

In digital ecosystems, interoperability and trust are key to enable data exchanges between stakeholders. Therefore, the objective of a trusted data transaction is to make sure that the stakeholders involved in a data transaction can conduct it in a trusted way, with a clear and shared understanding of the conditions of the exchange, from a technical, business, legal and regulatory perspective. The goal of trusted data transactions is to increase findability, accessibility, interoperability and reusability of data, and to accelerate the flow of data.

A key goal of the Workshop is to identify and define the trust characteristics in a data transaction, that will be identified during part 2 of the workshop agreement, and could include, without being limited to, elements such as authentication, authorization, encryption, integrity, consistency, auditability, observability, security, reliability and compliance. The preliminary work done in Part 1 is structured in a way to support this goal:

- The identification and definition of key concepts and terminology that are needed in support of Part 2 of the trusted data transaction workshop
- It is not the intention of the Workshop to list and describe all the terms and concepts related to data exchange and data sharing in general, but instead to start from the definition and concept of a data transaction, and ensure that all related concepts and terms are well defined.

### **4.2 Stakeholders**

#### **4.2.1 General**

Key stakeholders that are involved in a data transaction are the data provider and the data user.

Data transactions can be supported, for example, by:

- data intermediaries,
- trust services,
- trust anchors.

#### **4.2.2 Data provider and data user**

The data provider, along with the data user are the key stakeholders that are directly engaged in a data transaction.

On the data provider side, multiple roles can be distinguished. Stakeholders can play several roles simultaneously, or these roles can be split between:

- data producer role,
- data rights holder role,



- data provider role.

The data provider is ultimately the entity that provides a data product to a data user, and co-signs with this data user a data usage contract specifying the terms and conditions for the usage of this data product.

#### **4.2.3 Data intermediary**

The data intermediary, also known as data intermediation service provider, facilitates data transactions between data providers and data users, through the provision of data intermediation services. The scope of the services offered by the data intermediation service provider can vary, depending on the operational model defined.

Data intermediaries that provide data intermediation services which fall under the definition provided by the Data Governance Act must comply with certain requirements, including but not limited to, not using the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users.

#### **4.2.4 Trust service and trust anchors**

Trust service and trust anchors are third-party service providers that provide assurance services, for example regarding claims about the identity of a participant.

### **4.3 Concepts**

#### **4.3.1 Data and data product**

Data and data products are two distinct notions that relate to each other:

Data, which is generated by a person, organization, device or software is transacted between data providers and data users through data products that include, without being limited to, metadata describing the data product and, in the context of trusted data transactions, data licence terms as defined by the data provider.

Descriptive information included in and/or associated to the data product, such as the

- specific purposes the data product is intended for,
- terms of usage,
- legal terms,
- commercial terms,
- price, if any,
- consent and authorizations

facilitate discoverability, understandability and ability to transact the data product.

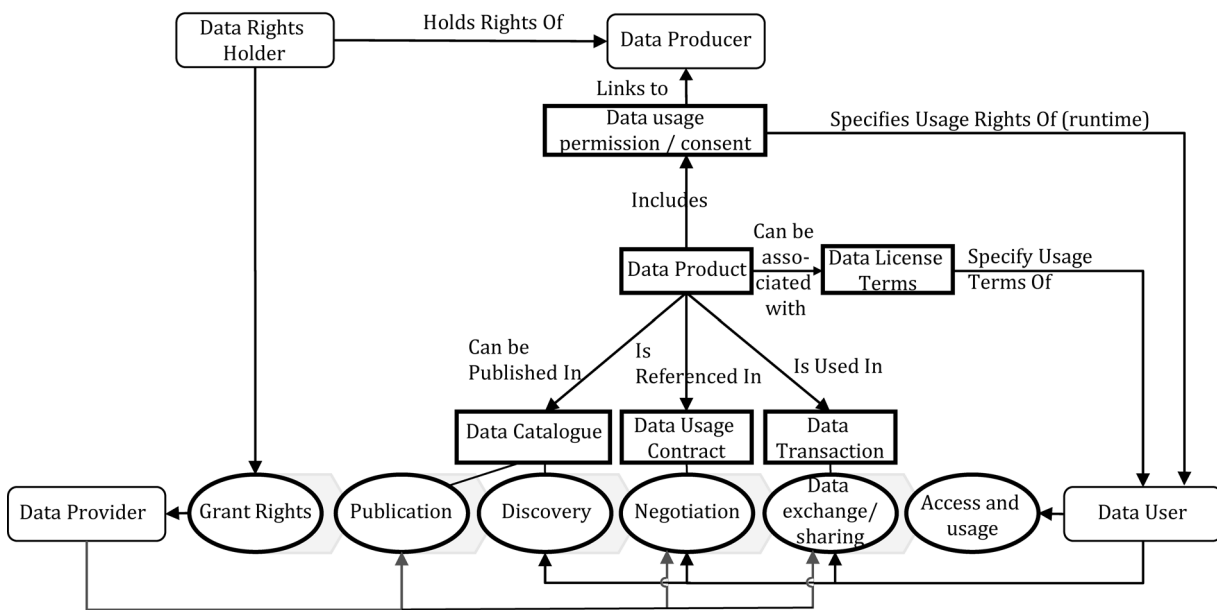
#### **4.3.2 Data transaction**

The concept of a data transaction can be understood under the general remarks below:

- A data transaction can be related to a broad set of scenarios, including but not limited to: one-time data exchanges, data subscriptions, API-based data exchanges (pull or push), data streaming, “code2data”, “data2code”, among other scenarios.

- A data transaction, in order to materialize, requires a data provider, a data user and the data product being transacted.
- Traceability of the data transaction contributes to enhancing transparency, providing accountability, improving security and meeting compliance requirements.
- The technical transfer of - or access to - the data, takes place as a result of the data transaction.
- In some cases, the data is transferred from the data provider to the data user. In other cases, the data does not move while access to the data is given to the data user.
- Data transactions do not necessarily imply a commercial relationship between the data provider and the data user, and does not necessarily imply the payment of a fee by the data user to the data provider in order to access and use the data.
- Each data transaction is “unique” indicating that it must be treated independently of other data transactions.
- Data transactions and data spaces are interconnected concepts. Data spaces provide a foundation for managing and facilitating trusted data transactions, enabling stakeholders to leverage data effectively while ensuring governance and compliance.

The concept of data transaction can be described with the conceptual model hereafter:



**Figure1 — Scope of data transaction**

The concept of data transaction relates to the following three phases:

- **Granting rights** and **publication** of the data product which is a provisioning phase leading to the publication of metadata and data policies.
- **Discovery** and **negotiation** which is the phase leading to an agreement (data usage contract) between a data provider and a data user regarding a data product

- The **data exchange or sharing** phase operationalizing the data usage contract through a data transaction which includes also the **access and usage** of the data product by the data user

Although the activities depicted in Figure 1 are typically executed in the order as displayed, certain data transactions may skip activities or reiterate parts of the process. This is not displayed in the figure for readability reasons.

Before using a data product, the data user accepts or negotiates - and co-signs - a data usage contract with the data provider, containing the terms of usage, including applicable data usage authorizations and data usage consents. Data usage authorizations and data usage consents need to be verified each time the data is accessed. Data usage contract is based on a data product description that may have evolved during the negotiations, if any, from the data product description initially published in the data catalogue.

After the data usage contract has been agreed upon and has been signed by both parties, the data user can start accessing and using the data. Such data usage with the associated data usage contract corresponds to a data transaction which relates to the technical and legal arrangements necessary to enable the proper use of data by the data user.

The data usage contract is a ricardian contract allowing to record the document as a contract at law, while placing the defining elements in a format that can be expressed and executed in software.

#### **4.3.3 Trusted data transaction**

A trusted data transaction is a data transaction based on a set of verifiable trust characteristics that will be identified during part 2 of the workshop, and could include, without being limited to, elements such as authentication, authorization, encryption, integrity, consistency, auditability, observability, security, reliability and compliance.

Part 2 of the workshop will focus on determining which are those characteristics that are relevant for defining trust in a data transaction, as well as a list of criteria, for each characteristic, that can objectively be used for measuring trust.