D1.3 Data governance documentation

CIRCPLASTX

A DATA SPACE TO INCREASE CIRCULARITY THROUGH DATA FOR THE PLASTICS INDUSTRY

DATE: 28/02/2026

CircPlastX

Co-funded by the European Union

This project receives funding from the European Commission's Horizon Europe Research Programme under Grant Agreement Number 101195258

TECHNICAL PROJECT REFERENCES	
Project Acronym	CIRCPLASTX
Project Title	A data space to increase circularity through data for the plastics industry
Topic:	DIGITAL-2024-CLOUD-DATA-06-MANUFSPACE
Project Coordinator	IPC - CENTRE TECHNIQUE INDUSTRIEL DE LA PLASTURGIE ET DES COMPOSITES
Project Duration	36 months (March 2025 – February 2028)

DELIVERABLE REFERENCES	
Deliverable No.	D1.3
Type:	DATA / DEC / DEM /R / OTHER
Dissemination level	EUC / PU / SEN
Work Package	WP1: Digitising circularity for plastics – data space design
Leader of the deliverable	TIMELEX (Hans Graux, Paraskevi Theofanous, Ezgi Ercan)
Contributing beneficiaries	TNO (Olga Batura, Jeroen Breteler), IPC (Tjerk Timan)
Due date of deliverable	28/02/2026

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

DISCLAIMER OF WARRANTIES

This document has been prepared by CIRCPLASTX project partners as an account of work carried out within the framework of the EC-GA contract no. 101195258.

Neither Project Coordinator, nor any signatory party of CIRCPLASTX Project Consortium Agreement, nor any person acting on behalf of any of them:

(a) makes any warranty or representation whatsoever, expressed or implied,

(i) with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or

(ii) that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or

(iii) that this document is suitable to any particular user's circumstance; or

(b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the CIRCPLASTX Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Table of contents

TABLE OF CONTENTS 4

ABBREVIATIONS 7

EXECUTIVE SUMMARY 9

1. INTRODUCTION 10
1.1 PURPOSE AND SCOPE OF THE REPORT 10
1.2 CONTEXT OF THE REPORT 11
1.2.1 EUROPEAN UNION POLICY AND CONTEXT 11
1.2.2 CURRENT SITUATION, TRENDS AND CHALLENGES IN PLASTICS DATA SHARING 12
1.2.3 PROJECT CONTEXT - LINK TO OTHER DELIVERABLES 13
1.3 OVERVIEW OF CIRCPLASTX OBJECTIVES, STAKEHOLDERS, AND SERVICES 14
1.4 METHODOLOGY AND SOURCES 15
1.5 DATA SPACE GOVERNANCE AND DATA GOVERNANCE 16

2. HORIZONTAL EU LEGAL FRAMEWORK 18
2.1 EU DATA GOVERNANCE INSTRUMENTS 18
2.1.1 DATA ACT 18
2.1.1.1 Overview 18
2.1.1.2 Relevance to data spaces and data governance 21
2.1.1.3 Applicability to CircPlastX and data governance implications 25
2.1.2 DATA GOVERNANCE ACT 27
2.1.2.1 Overview 27
2.1.2.2 Relevance to data spaces and data governance 28
2.1.2.3 Applicability to CircPlastX and data governance implications 30
2.1.3 FREE FLOW OF NON-PERSONAL DATA REGULATION 32
2.1.3.1 Overview 32
2.1.3.2 Relevance to data spaces and data governance 32
2.1.3.3 Applicability to CircPlastX and governance implications 33
2.1.4 OPEN DATA DIRECTIVE 35
2.1.4.1 Overview 35
2.1.4.2 Relevance to data spaces and data governance 35
2.1.4.3 Applicability to CircPlastX and data governance implications 36
2.2 INTELLECTUAL PROPERTY AND TRADE SECRETS 38
2.2.1 COPYRIGHT DIRECTIVE 38
2.2.1.1 Overview 38
2.2.1.2 Relevance for data spaces and data governance 38
2.2.1.3 Applicability to CircPlastX and data governance implications 39
2.2.2 DATABASE DIRECTIVE 40
2.2.2.1 Overview 40
2.2.2.2 Relevance for data spaces and data governance 41
2.2.2.3 Applicability to CircPlastX and data governance implications 41
2.2.3 TRADE SECRETS DIRECTIVE 42
2.2.3.1 Overview 42
2.2.3.2 Relevance for data spaces and data governance 42
2.2.3.3 Applicability to CircPlastX and data governance implications 43
2.3 PRIVACY AND DATA PROTECTION 45

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.3.1 General Data Protection Regulation 45
2.3.1.1 Overview 45
2.3.1.2 Relevance to data spaces and data governance 46
2.3.1.3 Applicability to CircPlastX and data governance implications 48
2.3.2 E-privacy directive 51
2.3.2.1 Overview 51
2.3.2.2 Relevance to data spaces and data governance 51
2.3.2.3 Applicability to CircPlastX and data governance implications 52
2.4 Competition, platform and digital markets regulation 53
2.4.1 Article 101 TFEU 53
2.4.1.1 Overview 53
2.4.1.2 Relevance to data spaces and data governance 55
2.4.1.3 Applicability to CircPlastX and data governance implications 56
2.4.2 Article 102 TFEU 58
2.4.2.1 Overview 58
2.4.2.2 Relevance to data spaces and data governance 59
2.4.2.3 Applicability to CircPlastX and data governance implications 60
2.4.3 Digital Markets Act 61
2.4.3.1 Overview 61
2.4.3.2 Relevance for data spaces and data governance 61
2.4.3.3 Applicability to CircPlastX 62
2.5 Trust and Identity management 63
2.5.1 eIDAS / eIDAS 2.0 63
2.5.1.1 Overview 63
2.5.1.2 Relevance for data spaces and data governance 65
2.5.1.3 Applicability to CircPlastX 65

3. Sector-specific legal framework 68
3.1.1 Overview 68
3.1.2 Registering substances with the ECHA 69
3.1.2.1 Actors with obligations related to data sharing 69
3.1.2.2 Data to be shared for registration 71
3.1.3 Sharing safety data up and down the supply chain 71
3.1.3.1 Actors involved in safety data sharing 72
3.1.3.2 Data to be shared 74
3.1.4 Considerations for a compliance service 75
3.2 Regulation on Ecodesign Requirements for Sustainable Products (ESPR) 76
3.2.1 Overview 76
3.2.2 Actors in the value chain to whom the DPP is relevant, and their rights and obligations related to DPP data 77
3.2.3 Data to be shared 78
3.2.4 Quality of and access to data 80
3.3 Regulation on Packaging and Packaging Waste (PPWR) 81
3.3.1 Overview 81
3.3.2 Actors in the value chain involved in data sharing 82
3.3.3 Data to be shared 82
3.3.4 Quality of and access to data 83
3.4 Implications for CircPlastX data space and related services 84

4. Conclusion 86
4.1 The position of a data space within the regulatory landscape 86
4.2 Interoperability as a legal requirement 86

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

4.3 TRADE SECRET PROTECTION AS A FOUNDATION OF TRUST 87
4.4 NEUTRALITY AND NON-DISCRIMINATION AS CENTRAL GOVERNANCE PRINCIPLES..... 87
4.5 EIDAS AND THE EUROPEAN TRUST INFRASTRUCTURE 87
4.6 THE DYNAMIC NATURE OF THE REGULATORY ENVIRONMENT – WHAT SHOULD BE MONITORED 88
4.7 IMPLICATIONS FOR THE NEXT PROJECT PHASE 88
4.8 FINAL OBSERVATIONS 88

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Abbreviations

ABBREVIATION	MEANING
API	Application programming interface
CA	Consortium Agreement
CJEU	Court of Justice of the European Union
D	Deliverable
DA	Data Act
DoA	Description of Action
DGA	Data Governance Act
DIS	Data Intermediation Service
DMA	Digital Markets Act
DPIA	Data Protection Impact Assessment
DPP	Digital Product Passport
DSM	Digital Single Market
DSSC	Data Spaces Support Center
ECHA	European Chemicals Agency
eIDAS	Regulation on electronic identification and trust services
ENISA	European Union Agency for Cybersecurity
ESO	European Standardisation Organisation
ESPR	Ecodesign Requirements for Sustainable Products Regulation
EU	European Union
FAIR	Findable, Accessible, Interoperable, and Reusable
FFDR	Free Flow of Data Regulation
FRAND	Fair, Reasonable, and Non-Discriminatory
GDPR	General Data Protection Regulation
IoT	Internet of Things
LCA	Lifecycle Assessment
MCT	Model Contractual Term
ODD	Open Data Directive
OJ	Official Journal (of the EU)
P2B	Platform-to-Business (Regulation)
PC	Project Coordinator
PPWR	Packaging and Packaging Waste Regulation

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

REACH	(Regulation concerning) Registration, Evaluation, Authorisation and Restriction of Chemicals
SDS	Safety data sheet
TFEU	Treaty on the Functioning of the European Union
TSD	Trade Secrets Directive
WP	Work Package

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Executive summary

This deliverable provides a structured legal analysis of the European Union regulatory framework relevant to data governance in multi-actor data-sharing environments, using the CircPlastX data space as a concrete reference case. It is developed within the context of the CircPlastX project and contributes to the project's broader objective of enabling trustworthy, interoperable, and legally compliant data-sharing infrastructures that support circularity, sustainability, and innovation in the European plastics ecosystem.

The purpose of this deliverable is to identify and analyse the EU legal instruments that shape data access, data sharing, and data governance, and to assess their implications for the design, governance, and operation of the CircPlastX data space. The analysis distinguishes between horizontal EU legislation applicable to data spaces in general and sector-specific regulatory frameworks relevant to the plastics value chain, providing a comprehensive legal foundation for the development of CircPlastX as a compliance-enabling and trustworthy data-sharing environment.

The deliverable examines key horizontal regulatory instruments, including the Data Act, Data Governance Act, Free Flow of Non-Personal Data Regulation, Open Data Directive, GDPR, competition law, intellectual property law, and the trust infrastructure framework of the eIDAS. These instruments define, directly or indirectly, the legal conditions for lawful data access, sharing, interoperability, security, and governance in data spaces, and highlight that data spaces are often not direct addressees of regulatory obligations but must support participants in complying with them.

The deliverable also analyses sector-specific EU legislation relevant to the plastics value chain, notably the Regulation on Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), the Ecodesign Requirements for Sustainable Products Regulation (ESPR), and the Packaging and Packaging Waste Regulation (PPWR). These frameworks create concrete data-related obligations concerning substances, materials, sustainability performance, traceability, and lifecycle impacts, demonstrating that compliance increasingly depends on structured and interoperable data-sharing mechanisms across the value chain.

The analysis confirms that the added value services of CircPlastX - traceability and certification of recycled content, improvement of lifecycle assessment (LCA) data quality, and substances-related data services and compliance support - are directly aligned with regulatory drivers. By enabling the practical implementation of regulatory data requirements, CircPlastX is positioned as a strategic enabler of circularity, transparency, and regulatory compliance in the European plastics value chain.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

1. Introduction

1.1 Purpose and scope of the report

This report provides a structured legal analysis of European Union (EU) rules relevant to **data governance** in multi-actor data-sharing environments, with a particular focus on **data access**, **data use**, and **data sharing** in the context of a sectoral data space for the plastics value chain. It examines how EU law frames the conditions under which data can be made available, accessed, reused, and governed in collaborative data-sharing environments, taking CircPlastX as a concrete reference case.

First, the report identifies and analyses the EU legal instruments that shape data governance in CircPlastX. It distinguishes between (i) **horizontal EU legislation** that applies to data access, sharing, and governance across data spaces in general, and (ii) **sector-specific EU regulatory frameworks** for the plastics value chain that establish material and sustainability related obligations, in particular in the areas of chemicals regulation, environmental and circularity requirements, traceability, and market access, and which thereby give rise to concrete data generation and data sharing obligations across the value chain.

Second, the report supports **legal compliance, trust, and interoperability** within the CircPlastX data space by clarifying how applicable legal requirements relate to the project's governance approach, technical architecture at a conceptual level, and service-oriented design. The analysis focuses on identifying which legal obligations are relevant, how responsibilities are allocated between actors, and which aspects of data access and sharing are legally constrained or enabled in a multi-actor environment.

Third, the report contributes to the **legal groundwork for future data governance arrangements** within CircPlastX by structuring and contextualising applicable legal requirements in a way that can inform governance design choices, contractual structuring, and role allocation in later stages of implementation and post-project operation. The report does not function as a data space rulebook or code of conduct, as such an instrument presupposes concrete business decisions, operational roles, and service configurations that will only be finalised at a later stage.

The scope of the report is limited to **EU-level legal instruments and policy frameworks** relevant to data governance. It does not assess business models, economic incentives, or technical implementation choices. The report does not interpret legislation beyond its current legal status and does not anticipate future legislative outcomes, except to acknowledge ongoing policy processes where relevant. It does not constitute legal advice on individual transactions or specific data-sharing arrangements.

Furthermore, the report does not aim to provide an exhaustive analysis of all sector-specific regulatory obligations that individual participants in the plastics value chain may be subject to under EU or national law. The sector is governed by a complex and evolving regulatory landscape, including product-specific, chemicals, waste, sustainability, and market access requirements, many of which impose detailed compliance obligations at the level of individual operators. Given that the CircPlastX

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

data space is still under development - including its final participant composition, operational roles, and future service configurations - it is not feasible at this stage to assess all potential regulatory requirements that may apply to future participants. Instead, the report provides an initial structured mapping of EU-level legal instruments that generate data-related obligations across the plastics value chain, insofar as these are relevant to the design and governance of a collaborative data-sharing environment. A more granular compliance assessment may become necessary at later stages once concrete business models, role allocations, and operational scenarios are defined.

1.2 Context of the report

1.2.1 European Union policy and context

The report is set within the broader European policy context shaped by the **European Data Strategy**[1], which promotes the development of common European data spaces as a means to foster data sharing, innovation, and economic competitiveness while preserving European values such as data protection, fairness, and sovereignty. Sectoral data spaces are a central element of this strategy, particularly in industrial ecosystems where data fragmentation and trust deficits have limited cross-value-chain collaboration.

The analysis is conducted against a backdrop of regulatory evolution and policy uncertainty. In particular, the **Digital Omnibus**[2] initiative constitutes the main ongoing horizontal process relevant to EU digital regulation and data governance, aiming to review, streamline, and potentially amend key elements of the EU's digital regulatory framework. As the Digital Omnibus and related simplification measures are still under discussion at the time of writing, their final scope and legal effects remain uncertain. This report therefore assesses the applicable legal framework as currently in force, while acknowledging that CircPlastX is being developed in a dynamic regulatory

[1] European Commission, "A European strategy for data", Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2020) 66 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066.

[2] Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024, COM/2025/837 final (Digital Omnibus) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0837.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

environment.Additionally, the **European Green Deal**[3] and the **Circular Economy Action Plan**[4] form an e

ssential part of the strategic context for CircPlastX. These initiatives establish circularity, resource efficiency, and sustainability as core objectives of EU industrial policy, with direct implications for data needs related to traceability, recycled content, environmental performance, and regulatory compliance.

Finally, the **Digital Europe Programme**[5] further reinforces this context by supporting the deployment of digital infrastructures, data spaces, and advanced data services in strategic sectors, including manufacturing.

1.2.2 Current situation, trends and challenges in plastics data sharing

This section draws on Deliverable D1.1 (Needs and Gaps Analysis), which examines data practices, needs, and barriers across the plastics and composites value chain.

The current situation is characterised by strong **fragmentation** of data relevant to circularity. Information on material composition, additives and substances, recycled content, environmental performance, and regulatory compliance is generated by multiple actors at different stages of the plastics lifecycle but is rarely shared in a systematic or interoperable manner. Data is typically stored in organisation specific systems, resulting in limited traceability, loss of information between lifecycle stages, duplication of effort, and reliance on assumptions or proxy data, particularly in life cycle assessment and regulatory reporting.

Data sharing practices in the plastics sector are predominantly bilateral and ad hoc. Information is most often exchanged through static documents such as technical data sheets, certificates, safety data sheets, or audit reports, usually under confidentiality agreements and within existing contractual relationships. While these practices allow limited data exchange between known partners, they do not support automated data reuse or broader value chain collaboration.

A central challenge identified is the high sensitivity of industrial data and the resulting **reluctance** of actors to share information beyond what is strictly required by regulation or contract. Concerns relating to confidentiality, protection of commercial interests, and potential misuse of data are widespread, and are particularly acute for small and

[3] European Commission, “The European Green Deal”, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2019/640 final EUR-Lex - 52019DC0640 - EN - EUR-Lex.

[4] European Commission, “A new Circular Economy Action Plan For a cleaner and more competitive Europe”, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM/2020/98 final EUR-Lex - 52020DC0098 - EN - EUR-Lex.

[5] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 http://data.europa.eu/eli/reg/2021/694/2025-02-04.

Co-funded by the European Union

This project receives funding from the European Commission’s Digital Europe Programme under Grant Agreement Number 101195258.

medium sized enterprises that often lack dedicated legal, digital, or data governance capacities. In the absence of clear safeguards and enforceable controls on data use, voluntary data sharing is generally perceived as high risk.

At the same time, regulatory requirements increasingly rely on the availability of structured, reliable, and traceable data. EU legislation on chemicals, packaging, waste, recycled content, sustainability reporting, and product compliance creates growing demands for data collection and verification. However, current compliance practices are frequently manual, costly, and inefficient, and do not automatically lead to interoperable or reusable data flows across actors and use cases.

The analysis in D1.1 also highlights an emerging preference for purpose bound and service driven data sharing. Industry actors show greater willingness to share data when it is clearly linked to a concrete operational or regulatory use case such as recycled content certification, life cycle assessment, or substance compliance, and when the scope, recipients, and conditions of data use are clearly defined. Such approaches are seen as reducing legal and commercial uncertainty and supporting trust between participants.

Finally, the analysis points to the **absence of shared governance frameworks and interoperable infrastructures** capable of supporting controlled multi actor data exchange at scale in the plastics sector. Despite the existence of relevant standards, their application remains fragmented, and there is a lack of trusted mechanisms to ensure data sovereignty, controlled access, and accountability. This gap limits the effective circulation of data needed for circularity and hampers preparedness for emerging policy instruments such as digital product passports.

In summary, while data is increasingly recognised as essential for circularity, compliance, and competitiveness in the plastics sector, data sharing remains fragmented, cautious, and limited by technical, organisational, and governance related barriers.

1.2.3 Project context - link to other deliverables

This legal report is developed within the context of **Work Package 1 (WP1) "Digitising circularity for plastics – data space design"**, and in particular **Task 1.3 "Data governance and legal framework guiding services"**. WP1 focuses on the design of the CircPlastX data space through the development of technical, organisational, and legal frameworks, informed by regulatory requirements on circularity, and by the need to enable meaningful and trustworthy data exchange across the plastics value chain.

Within this framework, **Deliverable D1.1 (Needs and Gaps Analysis)** provides the empirical foundation for the present report. It identifies concrete data-sharing needs, barriers, and priorities from an industrial and operational perspective, including the strong reluctance of actors to share commercially sensitive data in the absence of a clearly defined regulatory obligation, certification process, or other concrete operational use case that justifies the associated risks and efforts. Building on these findings, the present report examines the legal conditions under which the use cases identified in D1.1 can be implemented, focusing on how EU law enables, constrains, or conditions data access, use, and sharing in a multi-actor data space.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

The report also builds on **Deliverable D7.1 (Data Management Plan)**, which documents how data are handled during the project, reinterprets FAIR principles for an industrial context and outlines the technical and organisational mechanisms envisaged for the data space. While D7.1 addresses mainly project-internal data management, this legal report focuses exclusively on the future operational data space, and on the EU legal framework governing data access, use, and sharing between participants once CircPlastX is deployed beyond the project phase.

The report should be read together with **Deliverable D1.2 (Architecture)**, prepared in parallel, which specifies the technical architecture of the CircPlastX data space. The legal analysis provided here is aligned with that architectural design, but remains distinct in scope, addressing legal roles, obligations, and constraints rather than technical implementation.

Finally, in combination with **Deliverable D2.2 (Code of Conduct and contractual templates)**, this report contributes to establishing a coherent legal and governance foundation for CircPlastX. While it does not constitute a data space rulebook, it prepares the legal ground for the future development of such governance instruments once post-project operational models, roles, and service configurations are defined.

1.3 Overview of CircPlastX objectives, stakeholders, and services

This section reflects the analysis of data-related needs, barriers, and priorities across the plastics and composites value chain as identified in Deliverable D1.1 (Needs and Gaps Analysis), which informs the design and positioning of CircPlastX as a sectoral data space.

CircPlastX is a project funded under the **Digital Europe Programme** that aims to support **circularity, transparency, and regulatory compliance in the plastics value chain through the establishment of a trusted and interoperable data space**. The project addresses persistent challenges related to fragmented data flows, limited traceability, regulatory complexity, and low trust between actors, which hinder effective data sharing and reuse across the lifecycle of plastic materials and products.

The CircPlastX consortium brings together industrial actors operating at different stages of the value chain, alongside digital solution providers, research and technology organisations, and legal and regulatory experts. This **multi-stakeholder composition** reflects the project's objective to align technical feasibility with legal robustness and practical industry requirements, and to address both technical and non-technical barriers to data sharing, including confidentiality concerns and uncertainty around legal responsibilities.

Data is the central enabler of CircPlastX's objectives. Access to structured, reliable, and interoperable data supports **traceability of materials and products**, **verification of recycled content**, l**ife-cycle assessment**, and **compliance with EU chemicals, product, and sustainability regulation**. At the same time, the project design recognises that many industry actors, particularly SMEs, are **reluctant to share data** in the absence of a clear purpose, legal justification, and safeguards against inappropriate disclosure or misuse.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Against this background, CircPlastX is architected as a **permission-based** and **decentralised** data-sharing infrastructure aligned with European data space principles, including data sovereignty, purpose limitation, and auditability. At an architectural level, it enables **business-to-business data exchange** by allowing participants to make data available and access data under defined contractual, technical, and governance conditions. The data space therefore provides a general capability for controlled data sharing between participants.

Data sharing is primarily designed to take place within the context of **three core value-creation services**: **(i) online testing and certification of percentage of recycled material, (ii) improving life-cycle assessment data quality, and (iii) helping SMEs improve management and compliance related to substances**. These services act as structured and purpose-bound entry points for data sharing, providing a clear justification for why specific data are shared, with whom, and for what purpose. This service-driven approach is intended to reduce legal and commercial uncertainty, support trust-building, and make data sharing acceptable for actors that would otherwise be unwilling to participate.

At the same time, the data space infrastructure also enables participants to exchange data **outside these services**, for example through bilateral or multilateral arrangements tailored to specific downstream uses. Such data exchanges are technically supported by the same governance and access-control mechanisms, but they are not the primary focus of the platform and are not expected to occur in an open-ended or unrestricted manner. Their scope and relevance will depend on future governance and business decisions taken once the data space is operational.

On this basis, the present legal report addresses both **service-driven data sharing** and **data exchanges enabled by the data space outside the core services**.

1.4 Methodology and sources

The analysis draws on a structured review of relevant EU legal materials. Primary sources include binding **EU regulations and directives relevant to data governance**. This includes both instruments that directly regulate data access, use, and sharing, such as the Data Act, and instruments from related legal domains such as data protection, intellectual property, competition, etc., insofar **as they affect data may be access, sharing, or reuse.** In addition, the report examines a limited set of sector-specific EU regulatory instruments that are directly relevant to the plastics value chain - namely the Regulation for Registration, Evaluation, Authorisation, and Restriction of Chemicals **(REACH)**, the Ecodesign Requirements for Sustainable Products Regulation **(ESPR)**, and the Packaging and Packaging Waste Regulation **(PPWR) - to the extent that they give rise to concrete data generation, disclosure, and data-sharing obligations across the value chain**.

The analysis is further informed by conceptual frameworks and background materials developed in the context of European data space initiatives, including work undertaken

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

by the **Data Spaces Support Centre (DSSC)**[6] and by **SITRA**[7], the Finnish Innovation Fund. Additional publicly available materials from EU institutions and European standardisation bodies are considered where they help to situate the legal analysis within the broader data space policy context.

For each legal instrument examined, the report follows a consistent analytical structure aligned with the two-layer approach described above.

For horizontal instruments (Chapter 2), the analysis: (i) provides a concise overview of the legal instrument, (ii) examines its relevance to data sharing and data space governance in general, and (iii) assesses its applicability to CircPlastX in light of the project's objectives, services, and operational scope. This structure is intended to ensure analytical clarity, avoid over-generalisation, and clearly distinguish between horizontal legal considerations and their specific implications for the CircPlastX data space.

For sector-specific legal instruments (Chapter 3), the general description of the legislation is followed by a closer look at the data sharing arrangements (i.e. actors involved in data sharing, data that can or must be shared and considerations related to the quality of data and their use). This ensures that only the provisions directly relevant to the CircPlastX data space are discussed.

1.5 Data space governance and data governance

For the purposes of this report, a distinction needs to be made between **governance** and **data governance**, while recognising that the two are closely intertwined in the context of data spaces and cannot always be cleanly separated.

Data space governance framework is defined by the DSSC as "*the structured set of principles, processes, standards, protocols, rules and practices that guide and regulate the governance, management and operations within a data space to ensure effective and responsible leadership, control, and oversight. It defines the functionalities the data space provides and the associated data space roles, including the data space governance authority and participants*".[8] In the context of a data space, this includes questions such as participation criteria, allocation of roles and responsibilities, decision-making bodies, dispute resolution mechanisms, and the contractual and organisational arrangements that structure cooperation between actors.

Data governance, by contrast, can be defined by the DSSC as a "*framework of policies, processes, and standards that ensure effective management, quality,*

[6] Data Spaces Support Centre, https://dssc.eu
[7] SITRA rulebook model for a fair data economy (version 3.0) <https://www.sitra.fi/en/publication/rulebook-for-a-fair-data-economy> accessed 27/2/2026.
[8] Data Spaces Support Center Key Concept Definitions, https://dssc.eu/space/BVE2/1071251781/1+Key+Concept+Definitions, accessed 27/2/2026.

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

security, and proper use of data within an organization".[9] This includes legal and contractual conditions (policies) for making data available, allocating rights and obligations in relation to data, defining permitted purposes and recipients, ensuring compliance with applicable legal requirements, managing consent and implementing safeguards such as access controls, auditability, and accountability for data use.

Through our research we observed that, in practice, particularly in multi-actor data spaces, governance and data governance are **deeply interdependent**. Decisions that appear organisational or institutional in nature, such as who is allowed to participate in the data space, which services are offered, or how roles are defined, often have direct implications for data access and use rights. Conversely, legal requirements relating to data protection, data sharing, competition, or sector-specific regulation frequently necessitate specific governance arrangements to ensure compliance.

Accordingly, while this report focuses primarily on **data governance**, it occasionally refers to governance requirements. Such references are limited to aspects of governance that are functionally relevant to data governance and unavoidable for understanding the legal constraints and enablers applicable to CircPlastX. The report does not aim to provide a comprehensive governance framework for CircPlastX, but rather to clarify the legal foundations on which future governance and data governance arrangements can be built.

[9] Data Spaces Blueprint v2.0, Access & Usage Policies Enforcement, Glossary, Data Spaces Support Center, https://dssc.eu/space/BVE2/1071256095/Access+&+Usage+Policies+Enforcement#10.-Glossary, accessed 27/2/2026

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2. Horizontal EU legal framework

2.1 EU Data Governance Instruments

2.1.1 Data Act

2.1.1.1 Overview

Regulation (EU) 2023/2854, the Data Act,[10] is a core instrument of the European Data Strategy. Its objective is to increase availability and use of data in the Union, especially through enhancing compulsory data sharing with regard to different actors and in commercial and non-commercial data ecosystems. Simultaneously, it aims at ensuring **fair allocation of data value** between those actors. It does this by setting horizontal rules on access, use, and sharing of certain data, limiting contractual and technical barriers, and supporting interoperability. Most obligations have applied since 12 September 2025, while specific design by default requirements for connected products and related services placed on the market apply from 12 September 2026.

Data in scope

The Data Act defines 'data' as "*any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audio-visual recording*". This can include both personal data in the sense of the GDPR and non-personal data.

For the purpose of data access, the Data Act differentiates between product data and related service data:

- **Product data** are data generated by the use of a connected product and designed to be retrievable by a user, data holder or third party. *Connected products* are physical items that obtain, generate or collect data about their use or environment and can communicate such data electronically, while their primary function is not merely to store or process data.

  For instance, product data may include data collected from a single sensor or a connected group of sensors, such as temperature, pressure, flow rate, audio, pH value, liquid level, position, acceleration or speed.

- **Related service data** are data generated in connection with a related service that is necessary for a connected product to perform its functions. *Related services* are digital services linked to the product so that without them the product would not perform one or more functions.

  For example, related service data may include diagnostic outputs, predictive maintenance alerts, or optimisation parameters generated by a cloud-based monitoring or control service that supports the operation of a connected plastics

[10] 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) *OJ L, 2023/2854, 22.12.2023* http://data.europa.eu/eli/reg/2023/2854/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

manufacturing or recycling machine, where that service is required to ensure safe, compliant, or efficient functioning of the equipment.

The Data Act does not grant access rights to content protected by intellectual property rights, such as copyrighted audiovisual content. As a result, when a user watches a movie on their connected television, the movie will be out of scope but data regarding the screen's settings (e.g. brightness) can be in scope.

The Act does not create an open data regime. Access rights arise in defined circumstances and are subject to legal and technical conditions.

Allocation of roles and access/use rights

The Data Act identifies several key actors in the data ecosystem. A **user** is an individual or organisation that owns a connected product, has been granted temporary contractual rights to use it, or receives services related to that product. A **data holder** is an entity that has the legal or contractual right or obligation, under EU or national law, to access and make available data, including product or service data generated during the provision of related services. A **data recipient** is a third party acting for professional purposes, other than the user, to whom data is made available by the data holder, either at the user's request or in accordance with legal obligations. A **data processing service provider** is a digital service that offers on-demand access to scalable and configurable computing resources, such as cloud or edge infrastructure, that can be rapidly provisioned with minimal management effort.

The Data Act establishes:

- **user rights to access** and **use** in-scope data;
- **user rights to share data** with third parties;
- duties on data holders to make data available without undue delay and, where feasible, in real time;
- rules on **fair, reasonable and non discriminatory terms** and **compensation** for mandated sharing;
- protection of **trade secrets** through confidentiality and technical safeguards;
- **interoperability** requirements including for smart contracts;
- rights to **switch** between data processing services, with a phased withdrawal of switching charges; and
- safeguards against unlawful **third-party access** to non-personal data.

Under the Data Act, the new statutory data access rights are granted to two groups: (a) users of IoT products (Articles 4-6) and (b) public authorities in certain circumstances (Articles 14-17). For IoT products, these rights concern data "generated by the use" of the product and **only arise when a user requests access**, either for themselves or for a third-party recipient. The Data Act does not create any general access rights for the public or for economic operators at large.

Connected products and related services must be designed and manufactured or provided in such a manner that the data they generate can be accessed and used in practice. This means that product data and related service data – including the relevant metadata necessary to interpret and use those data – must be made available to users **by default** easily, securely, free of charge, in a structured and machine-

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

readable format that is commonly used. Where it is relevant and technically feasible, the data should also be **directly accessible to the user** without additional intermediaries. This "access by design" obligation in Article 3 of the Data Act underpins the practical effectiveness of the later access and sharing rights.

In terms of enabling data use, the Data Act advances a **contract-based approach** and stimulates contractual arrangements among nearly all actors concerned. The central provision here is article Article 4(13), according to which "*a data holder shall only use any readily available data that is non-personal data on the basis of a contract with the user"*. The Act thus does not grant data holders a free standing right to exploit non-personal data; instead, it makes their use dependent on the user's contractual consent.

At the same time, Article 4(14) restricts the ability of data holders to make non-personal data available to third parties. As a rule, they may not share such data beyond what is necessary to fulfil their contract with the user, and they must bind third parties not to share the data further, unless the user has requested or authorised such onward sharing. In this way, the Data Act positions the user as the central actor for onward data sharing.

While this provision makes a contract mandatory, the Act does not lay down any detailed regime to harmonise the content of such "central" data-use agreements. Nor does it set specific rules for data contracts involving consumers, and it remains silent on conflict-of-laws issues.

To counterbalance this contractual freedom, Chapter IV establishes a fairness regime for business-to-business data contracts. Unilaterally imposed unfair terms are not binding. The Act includes black list and grey list examples of unfairness, including unilateral changes to access conditions, disproportionate liability limitations, or termination without reasonable notice.

Article 41 mandates the Commission to develop non-binding model contractual terms (MCTs) to support negotiations and promote FRAND-compliant contracts. On 19 November 2025, the Commission published draft MCTs covering mandated sharing scenarios (data holder to user, user to third-party data recipient, and data holder to data recipient) and a fourth MCT for voluntary data sharing.[11] These model terms are designed to align contractual practice with the access, usage and sharing principles of the Data Act.

Limitations to data access and/or use

Although the Data Act establishes data access and sharing rights, these rights are subject to important limitations.

First, **competition-related constraints** apply. Access and sharing rights may be restricted where this is necessary to prevent distortions of competition, in particular in situations involving competing products or markets. Users who receive data are not allowed to use them to develop competing connected products, nor to share them with

[11] European Commission, Approval of the draft Commission Recommendation on non-binding model contractual terms on data access and use and non-binding standard contractual clauses for cloud computing contracts (with Annexes), annexed hereto, C(2025) 7750 final.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

third parties for that purpose. In addition, specific restrictions apply to the sharing of data with entities designated as gatekeepers under the Digital Markets Act (Arts. 4(10), 5(6), 6(2) Data Act).

Second, **data protection and security interests** limit access and onward use. Where personal data **or mixed datasets containing both personal and non-personal data** are involved, access and use must comply with the GDPR and, where applicable, ePrivacy rules. Article 4(12) of the Data Act clarifies that a valid legal basis under data protection law is required when the user requesting access is not the data subject. In practice, this means that the presence of personal data within a dataset triggers GDPR requirements for the entire dataset, even where non-personal data are also included.

In relation to **trade secrets**, data holders may require proportionate confidentiality and security measures as a condition for disclosure and, in exceptional cases, may refuse access where disclosure would cause serious economic damage.

Third, the Data Act introduces **rules affecting data storage and portability through data processing services**. Chapter VI grants customers rights to switch between data processing services, requires providers to ensure functional equivalence and data portability, and phases out switching charges. It also imposes safeguards against unlawful access to non-personal data by third-country authorities. While these provisions do not regulate data sharing directly, they influence how data are stored, transferred, and made available within the technical infrastructures used by actors subject to the Data Act.

2.1.1.2 Relevance to data spaces and data governance

As outlined above, the Data Act contains substantial provisions introducing and regulating data access and usage rights. However, it does not limit itself to those. It combines provisions targeted at tech regulation (e.g., with regard to interoperability, data portability, etc.), as well as provisions on enforcement structures (e.g. public enforcement and alternative dispute settlement mechanisms). In doing so, it transforms parts of the European Data Strategy into binding governance baselines. For actors who offer data or data services within European data spaces, these baselines become concrete obligations that must be reflected in rulebooks, technical specifications and operational procedures.

The Data Act expressly refers to common European data spaces as sectoral or cross sector frameworks that enable data sharing or joint processing, and it makes interoperability a legal condition for their functioning. It also places the user, not the data holder, at the centre of control over the use and onward sharing of non-personal product and service data. For data spaces that aim to orchestrate multi-party data access and reuse, this user centric allocation of rights and duties is a core constraint and design parameter.

The clearest and most immediate link is Article 33 of the Data Act, which lays down essential interoperability requirements for participants that offer data or data services in a data space. Although this report focuses on data governance rather than technical architecture as such, interoperability is a core data governance concern: the Article 33 duties determine how data must be described, accessed and exchanged in practice, and therefore set minimum conditions for how data spaces structure data access, data use and data sharing.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Interoperability requirements for data spaces (Article 33 of the Data Act)

Article 33 of the Data Act requires that datasets offered in a data space be described and made available in a manner that allows other participants to discover them, understand their legal and technical constraints, and reuse them reliably. In practice, the obligations cluster around four core categories of requirements:

- **Metadata and dataset description (Article 33.1(a)).** Participants must provide sufficiently detailed (and where relevant machine-readable) information on dataset content and context, including use restrictions, licences, collection methods, and data quality or uncertainty. Data spaces therefore need structured catalogues and rulebooks specifying mandatory metadata fields and validation processes.
- **Semantic interoperability (Article 33.1(b)).** Participants must publicly and consistently describe the data structures and formats they use, including vocabularies, taxonomies, classification schemes, and code lists. This pushes data spaces toward shared semantic assets, open documentation, version control, and mappings where different vocabularies exist.
- **Technical access interoperability (Article 33.1(c)).** Participants must document the technical means of access - particularly APIs - together with applicable terms of access and quality-of-service parameters, so that automated access and transmission (continuous, bulk, or real-time where feasible) can be supported. Data spaces must therefore standardise interfaces and ensure predictable technical conditions.
- **Interoperability of automated sharing tools (Article 33.1(d)).** Where data sharing is automated, participants must ensure interoperability of the tools used to execute agreements, including smart contracts where applicable. In practice, this means not using tools that only function inside one vendor's closed system, and instead using common standards, reusable templates, and open interfaces so that participants can connect, change tools, or link to other data spaces without major obstacles.

The aforementioned four requirements are described at a high level and leave room for several questions. These questions include the following:

- What concrete level of detail on dataset content, licences, data quality, and uncertainty is required so that other participants can genuinely find, understand, and reuse a dataset, rather than just seeing a minimal or useless description?
- In what situations must information about a dataset (both usability information and structural information) be provided in a machine-readable format, and when are human-readable documents sufficient, if the goal is real interoperability?
- How extensive and accessible semantic documentation must be so that third parties can correctly understand the meaning of shared data elements and use them consistently in their own systems and processes, including with respect to definitions, units of measurement, vocabularies, and relationships between data fields?
- What is the minimum level of openness and documentation that APIs must meet, and how far must participants go in enabling continuous, bulk, or real-

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

time access before it is considered not technically feasible or harmful to the functioning of connected products?

Taken together, these questions illustrate that while Article 33 of the Data Act establishes clear categories of interoperability obligations for data spaces, it leaves significant discretion as to their concrete operationalisation. The Regulation defines *what* must be achieved in terms of discoverability, semantic clarity, technical accessibility and interoperability of automated sharing tools, but it does not specify *how much detail*, *which formats*, or *which technical and semantic conventions* are sufficient in practice to meet these requirements. As a result, important aspects of compliance remain open. It is anticipated that these issues will be further specified through delegated acts by the European Commission, harmonised standards and detailed data space governance frameworks.

Ongoing standardisation under the European Trusted Data Framework (Mandate M/614)

The Article 33 requirements are being operationalised through the European Trusted Data Framework standardisation process. On 7 July 2025, CEN and CENELEC formally accepted the Commission's Standardisation Request under Mandate M/614[12], a milestone explicitly aimed at supporting implementation of the Data Act as from 12 September 2025.[13]

Under Mandate M/614, the European Standardisation Organisations (ESOs) CEN, CENELEC and ETSI have agreed to develop seven deliverables for the Trusted Data Framework. To meet the requirements of Article 33 specifically, they are preparing four European Standards (two intended for citation in the Official Journal) and three Technical Specifications:[14]

1. Harmonised standards on Trusted Data Transactions – Part 1: Terminology, concepts and mechanisms (deadline 1 June 2026)
2. Harmonised standards on Trusted Data Transactions – Part 2: Trustworthiness requirements (deadline 1 November 2026)
3. Harmonised standards on Trusted Data Transactions – Part 3: Interoperability requirements (deadline 1 May 2027)
4. Technical specification(s) on a data catalogue implementation framework (deadline 1 March 2026)

[12] European Commission, Implementing decision of 1.7.2025 on a 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 (Standardisation request M/614) C(2025)4135 <https://ec.europa.eu/transparency/documents-register/detail?ref=C(2025)4135&lang=en>.

[13] CENELEC, Data Act: Standardization Request Officially Accepted by CEN and CENELEC, 11.07.2025 <https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-07-11-data-act-standardization-request/> accessed 19 January 2026.

[14] European Commission, Annexes 1 to 2 to the Commission Implementing Decision on a 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, C(2025) 4135 final <https://ec.europa.eu/transparency/documents-register/api/files/C(2025)4135_1/de00000001072897?rendition=false>.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

5. Technical specification(s) on an implementation framework for semantic assets (deadline 1 September 2026)
6. European standard on a quality framework for internal data governance (deadline 1 March 2027)
7. Technical specification(s) on a maturity model for Common European Data Spaces (deadline 1 September 2026)

For data space governance, this standardisation track means that compliance will be assessed not only against the high-level legal requirements of Article 33 but also against emerging harmonised standards and specifications that concretise them. Early alignment with the Article 33 clusters - metadata, semantics, technical access, and automated enforcement - therefore functions as a risk-mitigation strategy, limiting the need for costly retrofitting once the harmonised standards stabilise. Importantly, paragraph 3 of Article 33 of the Data Act establishes a non-rebuttable presumption of conformity with the requirements of paragraph 1 if a participant offering data or data services in the data space can demonstrate compliance with the standards.

Beyond interoperability: access by design, fairness and statutory inflows

Beyond interoperability, the Data Act shapes data governance of data spaces through the **fairness control for contractual terms** governing data access and use, set out in Chapter IV. These rules apply primarily to contracts unilaterally imposed by data holders on users or third parties, but they are also relevant for the broader governance environment in which data sharing takes place. While a data space typically acts as an intermediary and does not itself conclude data sharing agreements between data holders and data users, it does establish **terms and conditions of use**, participation criteria and service-related policies that shape how actors access infrastructure, tools and services. Where such participation conditions effectively influence access to data or the ability to exercise statutory rights, they must be designed in a manner that is transparent, proportionate and non-discriminatory, and must not reinforce unfair contractual outcomes between participants.

The Data Act further affects data spaces as **facilitators of statutory data sharing flows**. Under Articles 4 and 5, users of connected products may request access to product and related service data and may instruct data holders to make those data available to a third party of their choice. A data space acts as the technical environment through which data are transmitted, but it is not itself the addressee of the access obligation. The legal responsibility to assess and comply with a data access request, including any grounds for limitation or refusal, remains with the data holder. For data spaces, the implication is that their infrastructure and procedures should be capable of accommodating data flows triggered by statutory user rights without obstructing them, while supporting lawful handling of those data once received.

In this context, data spaces may need to support **structured intake and handling mechanisms** that enable data holders and users to comply with the Data Act. This can include functionalities to document the identity and status of the requesting user, the purpose of data sharing, and the applicable safeguards for trade secrets, confidentiality and data protection. The data space does not decide on refusals, but its design should not make lawful sharing technically or organisationally impracticable.

Fair terms and compensation rules also shape data space business models. Mandated sharing with third parties at a user's request must take place on FRAND terms, and in some contexts compensation is limited to cost plus a reasonable margin.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Even outside strictly mandated flows, FRAND functions as a data governance reference point. Pricing and access differentiation in a data space should be objective, transparent and justifiable. Access tiers, subscription models or pay per use arrangements should be linked to clear criteria such as data volume, update frequency, service levels or value added functionalities, while ensuring non discriminatory treatment for comparable participants.

Trade secret protection is another essential data governance dimension. The Data Act does not require disclosure of inferred or derived data produced through substantial additional investment and permits data holders to invoke trade secret protection, but primarily through safeguards rather than refusal. Data holders asked to share in scope data must identify trade secret risks, propose proportionate confidentiality measures and only refuse where there is no feasible way to protect the secret while complying. For data spaces, this implies that trade secret handling cannot be left to ad hoc bilateral negotiation. Data governance must provide a common toolkit, including standard confidentiality undertakings, secure access environments, auditability, purpose limitation controls and technical measures such as aggregation thresholds or restricted query outputs. In this way, trade secret protection becomes a built in feature of the data space infrastructure.

Finally, the Data Act indirectly shapes data spaces through its cloud switching and non-personal data sovereignty rules. Chapter VI grants customers rights to switch between data processing services, requires providers to enable functional equivalence and portability, and phases out switching charges. In parallel, providers must implement safeguards against unlawful third country access to non-personal data. Data spaces, which are typically customers of cloud and edge services, must ensure that their technical architecture and contractual arrangements make it possible to exercise these switching rights and to uphold the sovereignty expectations of participants. This favours modular architectures, explicit portability planning and contractual clauses requiring providers to resist unlawful foreign access requests.

Taken together, these elements show that the Data Act provides data spaces with a binding legal backbone for data governance. It mandates interoperability and openness at the data, semantic and tooling layers, creates statutory access and sharing routes that data spaces must be able to accommodate, frames fair compensation approaches, requires robust trade secret, confidentiality and data protection measures and links infrastructure choices to switching and sovereignty safeguards.

2.1.1.3 Applicability to CircPlastX and data governance implications

This section sets out the concrete data governance implications that follow from the Data Act for CircPlastX, taking into account its objectives and services. It is intended to guide the legal and organisational design of the data space and should be read together with the project's technical deliverables and business model work.

CircPlastX does not act as a data holder, data recipient or data user within the meaning of the Data Act. It does not place connected products on the market, does not generate product or related service data, and does not decide on data access rights. Accordingly, data sharing decisions remain with the participating data holders and data users and any statutory access or sharing obligations under the Data Act attach to those participants, not to CircPlastX.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

The relevance of the Data Act for CircPlastX therefore lies in ensuring that its services and governance framework **do not obstruct participants' compliance** with the Data Act where it applies.

On this basis, the data space should support the following functionalities and design principles:

- **Dataset discovery and description support [Article 33(1)(a) Data Act]**
  CircPlastX must provide catalogue and metadata functionalities that allow participants, where they choose to make datasets or data services visible to others, to describe them in a way that supports discovery and informed reuse. At a minimum, the infrastructure should support documentation of dataset scope, purpose, applicable use restrictions or licences, provenance or generation context, and known limitations related to data quality or uncertainty.
- **Semantic transparency mechanisms [Article 33(1)(b) Data Act]**
  CircPlastX must support participants in making the meaning and structure of shared data intelligible to others, by enabling references to vocabularies, taxonomies, code lists, units of measurement, and data models used. This does not require CircPlastX to define or harmonise semantics itself. It requires that the infrastructure allows participants to publish semantic documentation in an accessible and reusable manner.
- **Technical access documentation [Article 33(1)(c) Data Act]**
  CircPlastX must allow participants to document the technical means through which their data or data services can be accessed, such as APIs or other interfaces, together with relevant technical conditions. CircPlastX should not impose technical solutions that would prevent participants from complying with interoperability expectations under the Data Act.
- **Interoperability of automated tools [Article 33(1)(d) Data Act]**
  Where CircPlastX supports automated processes related to data exchange (for example, contract automation), those tools must be interoperable and not restricted to a single vendor environment. The infrastructure should rely on open standards or interfaces so that participants can connect, change tools, or interoperate with other data spaces without undue technical barriers.
- **Alignment with emerging standards [Article 33(3) Data Act]**
  CircPlastX should monitor and, where feasible, align its infrastructure and internal policies with harmonised standards and technical specifications developed under the European Trusted Data Framework. Early alignment supports participants in benefiting from the presumption of conformity foreseen in Article 33(3) and reduces the need for later retrofitting.
- **Consistent use of model contractual terms where possible [Art. 41 Data Act, Commission draft MCTs]**
  Once the Commission's model contractual terms are finalised, CircPlastX should align its participation and service contracts with them to the extent compatible with the project's objectives, to reduce legal risk and support presumptively fair and compliant data access and use clauses. At the same time, the governance framework must recognise that the Commission's MCTs allow a broad margin for customisation, while CircPlastX needs highly standardised, automatable templates for real time data sharing. This tension

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

should be managed by defining a limited set of pre-approved contractual variants, derived from the MCTs, that can be parameterised and automated within the data space without reopening full contract negotiation for each data flow.

2.1.2 Data Governance Act

2.1.2.1 Overview

Regulation (EU) 2022/868 (the Data Governance Act or "DGA")[15] is a foundational instrument of the European Data Strategy. Its core objective is to improve conditions for lawful and trustworthy data sharing in the EU internal market by introducing harmonised governance mechanisms, reducing fragmentation, and increasing trust in intermediated sharing. The DGA does not create an EU-level "ownership right" in data; instead, it organises *how* data may be made available and re-used on the basis of existing rights and obligations. It entered into force in 2022 and has been applicable since 24 September 2023.

The DGA applies to both personal and non-personal data. Where personal data are involved, the DGA operates expressly without prejudice to the GDPR/ePrivacy framework and does not itself create a new legal basis for personal data processing; in case of conflict, the EU/national data protection framework prevails.

Substantively, the DGA establishes four regulatory pillars.

First, it sets out a framework for the **re-use of certain protected public-sector data that are not open data**, where access is restricted due to confidentiality, trade secrets, intellectual property rights, statistical confidentiality, or the protection of personal data. The DGA does not impose a duty on public sector bodies to make such data available, but it harmonises the safeguards and conditions that apply where re-use is permitted.

Second, the DGA introduces a regime for **data intermediation services**, designed to ensure trust and neutrality for intermediaries that facilitate data sharing between data holders or data subjects, on the one hand, and data users, on the other. This regime is explicitly linked to the development of emerging EU data sharing ecosystems, including common European data spaces.

Third, the DGA creates a framework for **data altruism**, enabling the voluntary making available of data for objectives of general interest through "recognised" data altruism organisations that are subject to specific governance, transparency, and accountability requirements.

Fourth, the DGA establishes the **European Data Innovation Board**, an EU-level coordination body tasked with supporting the consistent application of the DGA and providing guidance for the data economy, including with a view to promoting interoperability across sectors and data sharing initiatives.

[15] Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (2022) OJ L152/1. http://data.europa.eu/eli/reg/2022/868/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.1.2.2 Relevance to data spaces and data governance

The DGA is directly relevant to data spaces because it is the first horizontal EU instrument that operationalises a trust architecture for multi-actor, cross-border data sharing ecosystems. Recital 27 explicitly links data intermediation services to the establishment of "common European data spaces".

(A) Data intermediation services as a legal archetype for many data space operators

A data intermediation service (DIS) is, in essence, a service that aims to establish commercial relationships for the purposes of data sharing between an undetermined number of data subjects and data holders, on the one hand, and data users, on the other, through technical, legal or other means. Recital 28 illustrates this concept with examples such as data marketplaces, orchestrators of data sharing ecosystems that are open to all interested parties (including in the context of common European data spaces), and data pools intended to be licensed to all interested parties.

The boundaries of DIS matter for data spaces, because the DGA also clarifies what falls outside the DIS regime. This includes services that obtain data and substantially aggregate, enrich or transform it and then license the resulting dataset without establishing a commercial relationship between the original data holders and the data users; services used exclusively by one data holder; and services used within a closed group of known partners, including supplier or customer relationships or collaborations established by contract (notably where the main objective is to ensure the functionalities of IoT-connected objects and devices). In addition, the recitals clarify that certain purely technical tools (such as cloud storage or analytics tools that do not aim to establish the commercial relationship) are not, as such, DIS.

If a data space operator qualifies as a DIS provider, the DGA imposes a specific trust and governance regime that must be reflected both in the contractual governance and in the technical architecture. Key requirements include the following:

1. **Structural separation and prohibition of bundling.** The intermediation activity must be carried out through a separate legal person, and access to the intermediation service must not be made dependent on purchasing other services from the provider or related entities.
2. **Neutrality and purpose limitation.** The provider must not use the data for any purpose other than making them available to authorised data users. In addition, information gathered about the activity of parties for the purpose of providing the service must be limited to what is necessary for operating and developing the intermediation service, including fraud detection and cybersecurity.
3. **Fair access and non-discrimination.** Access procedures must be fair, transparent and non-discriminatory for data holders, data users, and where relevant data subjects, including as regards prices and terms of service.
4. **Format and transformation controls.** Data should be made available in the format received. Conversion is permitted only under limited conditions (such as improving interoperability, at user request, or where required by law), and the framework must include an opt-out for the data holder where conversion is not legally required.
5. **Ancillary tools only on request or approval.** Tools such as temporary storage, curation, conversion, anonymisation or pseudonymisation may be

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

offered only on the explicit request or approval of the data holder or data subject, and safeguards must prevent repurposing.

6. **Logging, security and incident handling.** The provider must maintain logs of intermediation activity, apply robust security measures (including heightened security for competitively sensitive data), take measures to prevent unlawful access or transfer of non-personal data, and inform data holders without delay if unauthorised access, transfer or use occurs.
7. **Abuse prevention and continuity.** The provider must have procedures to prevent fraudulent or abusive practices by parties seeking access and must plan for continuity of the service in the event of insolvency, including practical retrievability/portability where storage is provided.
8. **Interoperability orientation.** The provider must take appropriate measures to ensure interoperability with other data intermediation services, including through commonly used (ideally open) standards.

The DGA also establishes an administrative compliance architecture for DIS. DIS providers are subject to a notification regime and are supervised by competent authorities designated in each Member State. Where the provider demonstrates compliance, it may use a recognised EU label and logo.

These elements matter for data spaces because they shape regulator and market expectations: even where a platform is structured to fall outside DIS qualification, DIS rules often function as a practical benchmark for "trusted" data space governance.

(B) Data altruism as an optional trust pathway for "general interest" sharing

The DGA establishes a framework for "data altruism", meaning the voluntary making available of data for objectives of general interest, based on the consent of data subjects (for personal data) or the permissions of data holders (for non-personal data), and without seeking or receiving a reward that goes beyond cost compensation. The central governance mechanism is the status of "recognised data altruism organisation" and the related label, which is intended to support trusted, cross-border data pooling for general-interest uses.

If a data space wishes to rely on this DGA framework, the altruism activities must be organised in a way that meets the conditions applicable to recognised data altruism organisations. In practical terms, this typically means that the altruism function cannot be treated as an informal subset of a commercial data sharing operation, but must be carried out by a legal person that satisfies the DGA requirements for recognition, including operation on a not-for-profit basis, legal independence from for-profit entities, and functional separation of altruism activities from other activities. The governance and compliance measures associated with recognition include transparency and record-keeping, annual activity reporting, information duties towards data subjects and data holders (including mechanisms to withdraw consent or permissions), purpose limitation to the stated objectives of general interest, appropriate security safeguards and notifications in the event of unauthorised access or disclosure, and restrictions on misleading marketing practices.

(C) Protected public-sector data re-use and "secure processing environments" as a governance model

The DGA's framework for the re-use of protected public-sector data is relevant to data space governance insofar as it articulates a structured model for enabling access to

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

sensitive data under controlled conditions. While the legal regime in Chapter II of the DGA applies specifically to public-sector bodies and does not regulate data spaces as such, the concept of a **secure processing environment** provides a useful reference for governing access to data that cannot be shared openly due to confidentiality, trade secret protection, or data protection constraints.

In the DGA context, secure processing environments are designed to allow authorised users to access and analyse protected datasets within a controlled technical and organisational setup. Typical features include strong identity and access management, comprehensive logging and auditability, restrictions on copying or downloading data, controls on onward transfer, and mechanisms to ensure that only authorised outputs may leave the environment. These elements are intended to minimise disclosure risks while enabling lawful and verifiable data processing.

For data spaces, the relevance of this model lies in its application as a data governance pattern rather than as a legal obligation. Data spaces do not themselves use or re-use data; instead, they facilitate controlled access, processing, or sharing between participants while preserving data sovereignty. Where participants wish to make highly sensitive industrial data available for defined purposes, governance mechanisms inspired by the secure processing environment model can support such access without requiring unrestricted data disclosure.

In practice, this may involve offering controlled access modalities as part of the data space's governance framework, such as restricted access environments, purpose-bound processing, technical limitations on data extraction, logging of access and processing activities, and output controls that ensure only permitted results are made available. These mechanisms enable participants to comply with applicable confidentiality, trade secret, and data protection obligations, while maintaining trust in multi-actor data sharing arrangements.

In this way, the DGA's secure processing environment concept contributes to the development of robust data governance approaches for sensitive datasets in data spaces, without altering the intermediary role of the data space or reallocating responsibility for data use and re-use away from the participating data holders and authorised data users.

Overall, the DGA shapes data space governance along three axes: (i) a neutrality and structural-separation model for trusted intermediation, including the possibility for compliant intermediaries to use an EU-recognised label and logo, (ii) an EU-level recognised status and label for data altruism organisations to support trusted pooling for general-interest purposes, and (iii) a controlled-access governance model for protected and sensitive datasets, informed by the DGA's secure processing environment approach.

2.1.2.3 Applicability to CircPlastX and data governance implications

This section sets out the concrete data governance implications that follow from the DGA for CircPlastX, taking into account its objectives and intended scaling beyond the initial consortium. It is intended to guide the legal and organisational design of the data space and should be read together with the project's technical deliverables and business model work.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

- **Structured assessment of whether CircPlastX performs "data intermediation services" [Art. 10 DGA]**
  CircPlastX must maintain an assessment of whether the operator provides any of the regulated categories of data intermediation services:
  (a) intermediation between data holders and data users,
  (b) intermediation enabling data subjects/natural persons to make data available to users, and/or
  (c) "services of data cooperatives".

- **Clear allocation of "operator" and "provider" roles where intermediation exists [Art. 10, 11 DGA]**
  Where CircPlastX performs any activity falling under Article 10 DGA, governance documents must clearly identify the entity acting as the DIS provider and ensure that it is prepared to comply with the DGA notification framework.

- **Neutrality by design and structural separation [Art. 12(a) DGA]**
  If CircPlastX qualifies as a data intermediation services provider, the intermediation activity must be performed through a separate legal person, and the operator must not use the intermediated data for purposes other than making them available to authorised data users.

- **Non-discriminatory access conditions and pricing logic [Art. 12(b), 12(f) DGA]**
  CircPlastX must ensure that access procedures, terms and pricing are fair, transparent and non-discriminatory for data holders and data users, including in relation to prices and terms of service. The participation terms should therefore define objective onboarding/admission criteria, suspension/termination criteria, and a transparent fee model.

- **Capability to operate (or integrate) secure processing environments for sensitive/public data use case [Art. 7(4)(a), 7(4)(c) DGA]**
  Where CircPlastX aims to integrate protected public-sector datasets subject to the Data Governance Act, its governance framework and technical architecture should be capable of supporting access conditions imposed under Article 7 DGA, including access through secure processing environments and the application of privacy-preserving techniques such as anonymisation, pseudonymisation, or the deletion of commercially confidential information where required. While CircPlastX is not itself a competent body under the DGA, the safeguards set out in Article 7 provide a concrete and legally grounded reference model for implementing controlled-access tiers, such as "data room" or "clean room" patterns, which may also be adopted voluntarily for highly sensitive industrial datasets.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.1.3 Free Flow of Non-Personal Data Regulation

2.1.3.1 Overview

Regulation (EU) 2018/1807 on the free flow of non-personal data in the European Union ("FFDR")[16] is a horizontal internal-market instrument designed to remove Member State rules that require data to be stored or processed in a specific territory (data localisation requirements), thereby enabling cross-border data processing and cloud usage across the EU.

The FFDR applies to **non-personal data** and includes rules for datasets that are **mixed** (containing both personal and non-personal data) by clarifying how the FFDR interacts with the GDPR for the personal-data component. In this context, it should be recalled that where a dataset contains any personal data, the GDPR continues to apply to the personal-data elements (and may in practice affect the handling of the dataset as a whole).

Substantively, the FFDR contains three governance-relevant pillars: first, a prohibition of data localisation requirements (with a narrow public security exception), combined with transparency duties on Member States; second, a guarantee that competent authorities retain access to data for regulatory and supervisory functions regardless of where the data are stored or processed in the EU; and third, a self-regulatory portability and switching mechanism, based on EU-level codes of conduct intended to facilitate switching between cloud and other data processing service providers and porting data.

2.1.3.2 Relevance to data spaces and data governance

The FFDR is directly relevant to data spaces developed within the European Data Strategy, as common European data spaces are conceived as cross-border infrastructures enabling the sharing, access and processing of datasets across multiple organisations and Member States. In this context, the removal of unjustified data localisation requirements is a key legal condition for their effective functioning. CircPlastX is developed within this European policy framework and is conceived as a "one-stop shop" for exchanging relevant data along the plastics value chain and developing services on top of that shared data, supported by standardised formats, interoperable architectures, connectors, and strong identity/access management.

For data spaces, the FFDR's practical governance consequences are threefold:

1. **Prohibition of localisation.** The FFDR prevents Member States from requiring that non-personal data be stored or processed in a specific national territory, except under limited public security conditions. As a result, data holders and data users are, in principle, free to store and process non-personal data anywhere within the EU.

   For data spaces, this means that infrastructure and governance choices should take advantage of this freedom and should not introduce location-based restrictions or national segmentation unless required by law. In particular, data

[16] Regulation (EU) 2018/1807 on a framework for the- and public-sector free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, pp. 59–68, http://data.europa.eu/eli/reg/2018/1807/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

spaces should avoid designing technical or organisational arrangements that would recreate data localisation effects in practice where EU law seeks to remove them.

2. **Authority-access readiness without de facto localisation.** The FFDR explicitly prevents Member States (or regulated entities) from justifying localisation on the ground that authorities need access. Instead, it requires that competent authorities be able to access data for inspections/supervision even if the data are stored/processed in another Member State, and it frames cooperation channels between authorities. For data spaces, this translates into rulebook and architecture choices that preserve auditable access and production of data to competent authorities, without building "country silos" into the platform.
3. **Portability/switching as an operational governance objective.** The FFDR expects the market to deliver portability and switching solutions through codes of conduct covering, among other items, switching conditions, timelines, technical requirements, and use of standards. For a data space, this is a governance signal to avoid provider lock-in and to document/export data and metadata in ways that enable migration between infrastructure providers.

2.1.3.3 Applicability to CircPlastX and governance implications

For CircPlastX, the FFDR does not create new data access rights or data sharing obligations. Its concrete impact is limited but important: it confirms that non-personal data handled within the data space may be stored and processed anywhere in the EU, that competent authorities must retain access irrespective of data location, and that governance choices should not recreate de facto localisation or lock-in effects. Within those boundaries, the FFDR functions primarily as a prohibition on restrictive governance choices, rather than as a source of detailed positive obligations, and results in the following requirements:

- **Identification of non-personal and mixed datasets [Art. 2 FFDR]** CircPlastX governance should be able to distinguish, at least at a high level, between datasets that are non-personal, personal, or mixed. This is necessary because the FFDR applies to non-personal data, while the GDPR continues to apply to any personal data component of mixed datasets. Where datasets are mixed, the FFDR applies to the non-personal data elements alongside the GDPR for the personal data elements.
- **No platform-level data localisation constraints within the EU [Art. 4(1) FFDR]**

  CircPlastX should not, as a matter of governance or contractual design, impose requirements that non-personal data made available through the data space be stored or processed in a specific Member State. The FFDR prohibits Member State data localisation requirements for non-personal data, except where justified on public security grounds under national law. CircPlastX governance should therefore remain neutral as to the EU location of storage and processing of non-personal data.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

- **Awareness of exceptional localisation requirements imposed by law [Art. 4(3) FFDR]**

  Where CircPlastX participants are subject to national legal obligations that restrict the location of processing of specific non-personal datasets on public security grounds, such constraints should be treated as external legal constraints applicable to the relevant participant or dataset, rather than as general platform rules. CircPlastX itself is not required by the FFDR to assess or enforce such national measures, but its governance should not contradict them.

- **No reliance on data location to resist lawful authority access [Art. 5(1) FFDR]**
  CircPlastX governance should not rely on the fact that non-personal data are stored or processed in another Member State as a reason to deny or obstruct lawful access requests from competent authorities acting within their powers. The FFDR ensures that competent authorities retain access to non-personal data for regulatory control and supervision, irrespective of the data's location within the EU.

- **Support for cooperation between competent authorities [Art. 5(2) FFDR]**
  Where access to non-personal data involves cross-border situations, CircPlastX should be able to support cooperation between competent authorities, for example by enabling the identification and production of relevant datasets or logs upon request. The FFDR does not impose proactive monitoring duties on CircPlastX, but it presupposes that cross-border data availability does not undermine regulatory oversight.

- **No contractual barriers to data portability or switching [Art. 6 FFDR]**
  While the FFDR relies on voluntary codes of conduct rather than direct obligations, CircPlastX governance should avoid contractual or technical arrangements that unnecessarily prevent the portability of non-personal data or the switching of data processing service providers. This supports the Regulation's objective of reducing vendor lock-in, without imposing a direct duty on CircPlastX to guarantee portability beyond what is contractually agreed.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.1.4 Open Data Directive

2.1.4.1 Overview

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (the "Open Data Directive" or "ODD")[17] modernises and replaces the former PSI Directive (Directive 2003/98/EC, as amended by Directive 2013/37/EU). It entered into force on 16 July 2019 and has applied since 17 July 2021.

The Directive establishes a general principle that documents - defined broadly as any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording or any part of such content[18] - held by public sector bodies and certain public undertakings, as well as accessible publicly funded research data, should be reusable for commercial and non-commercial purposes. It aims to increase the availability and re-use of public-sector information across the EU, while promoting competition, transparency and innovation in the internal market.

The ODD introduces several important evolutions compared to the earlier PSI framework. In particular, it expands the range of entities and data covered, places a specific emphasis on the re-use of publicly funded research data, and introduces a strong focus on "dynamic data", defined as documents in digital form subject to frequent or real-time updates. Public sector bodies are required, where applicable, to make such dynamic data available for re-use immediately after collection, notably via suitable application programming interfaces (APIs) and, where relevant, bulk download.

The ODD also establishes a special regime for high-value datasets, defined as datasets whose re-use is associated with significant benefits for society and the economy. These datasets must be made available free of charge, in machine-readable formats, via APIs and, where relevant, as bulk downloads. In parallel, Member States are required to support the availability of publicly funded research data through national open-access policies, following an "open by default" approach and compatible with the FAIR principles (findable, accessible, interoperable and reusable).

2.1.4.2 Relevance to data spaces and data governance

Although the ODD is formally addressed to Member States, public sector bodies, public undertakings and certain research organisations, it is relevant to data spaces where such actors choose to make public-sector or publicly funded datasets available through data space infrastructures. In these situations, the data space acts as an intermediary that facilitates access to and exchange of data under the conditions set by the Directive.

[17] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast), OJ L 172, 26.6.2019, pp. 56–83 http://data.europa.eu/eli/dir/2019/1024/oj.

[18] Article 2(6) ODD.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Data spaces do not themselves re-use public-sector data within the meaning of the Open Data Directive. Rather, they may provide the technical and organisational environment through which public data holders enable re-use by third parties. The relevance of the Directive therefore lies in the governance and technical constraints that apply when public data are made available via an intermediary, rather than in the imposition of direct obligations on the data space as a re-user.

From a data governance perspective, the Open Data Directive shapes the conditions under which public data may enter a data space. In particular, it determines the expected modalities of access (such as API-based access for dynamic data), applicable licensing conditions, pricing rules (including free-of-charge availability for high-value datasets), and requirements relating to machine-readability and standardised formats. Where a data space facilitates access to such datasets, its governance framework must be compatible with these conditions.

The Directive is also relevant in relation to publicly funded research data, which are subject to open-access policies and FAIR principles. Research organisations may therefore act as data providers within data spaces under specific openness and interoperability expectations. While the Open Data Directive does not mandate the use of data spaces, it influences how data spaces that integrate public-sector or research data must structure metadata, access mechanisms and downstream sharing conditions in order to preserve compliance with the underlying legal framework.

2.1.4.3 Applicability to CircPlastX and data governance implications

CircPlastX is not a direct addressee of the ODD. Its relevance for CircPlastX is therefore indirect and limited. It concerns how CircPlastX **receives, uses and re-shares datasets** that originate from entities subject to the ODD, and how it avoids undermining the legal conditions under which those datasets are made available. It result in the following requirement:

- **Respect for source re-use conditions attached to public-sector data [Arts. 1–2 and 8 ODD]**
  Where public sector bodies make their ODD data available via CircPlastX, CircPlastX must ensure that any onward access or sharing of those datasets within the data space respects the re-use conditions or licences set by the source entity. CircPlastX should not disregard, override or contradict such conditions when enabling downstream use.

- Beyond this requirement, the ODD may have practical implications for CircPlastX's design and operations, without creating legal obligations for the data space itself. Some datasets relevant to CircPlastX use cases (for example environmental or statistical data) may fall under the high-value dataset regime, meaning they are made available free of charge and under standardised technical conditions by the source authority. CircPlastX does not have responsibilities under that regime, but it may benefit from the increased availability and standardisation of such datasets. Also, publicly funded research organisations, including universities, may act as data providers to CircPlastX under national open-access policies inspired by the ODD. CircPlastX's role remains downstream: it should reflect the access conditions chosen by the

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

research organisation, but it is not responsible for enforcing open-access policy compliance.

Overall, the Open Data Directive functions for CircPlastX primarily as a **background framework shaping the availability and characteristics of public and research data**, rather than as a source of direct governance duties. Its main effect is to set boundaries on how CircPlastX may re-use and re-share such data, not to impose proactive publication, access or interoperability obligations on the data space itself.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.2 Intellectual property and trade secrets

2.2.1 Copyright Directive

2.2.1.1 Overview

Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market (the "Copyright DSM Directive")[19] modernises EU copyright law to address digital uses of protected works. Copyright protection applies only to **original works** that are the author's own intellectual creation and does **not** extend to facts, raw data, or non-creative information as such.

For data governance purposes, the Directive is primarily relevant with regard to the boundaries it draws between protected creative content and non-protected factual data, and to the conditions under which automated analytical techniques may lawfully be applied to copyright-protected materials. Other elements of the Directive, including the regime for online content-sharing service providers, target specific categories of services that are structurally different from permission-based data-sharing infrastructures and are therefore not central to this report.

2.2.1.2 Relevance for data spaces and data governance

From a data space perspective, the Copyright DSM Directive is **structurally relevant but often practically limited**, depending on the nature of the data being shared.

First, the Directive confirms an important baseline principle for data spaces: **copyright does not protect non-creative factual data**. Most industrial, technical, environmental, or compliance-related datasets will therefore fall outside copyright protection as such, even if they are stored or exchanged in digital form. Copyright may, however, subsist in certain elements that are shared through a data space, such as technical documentation, reports, images, manuals, or other creative content.

Second, the regime for **online content-sharing service providers** under Article 17 is relevant only for services whose main purpose is to store and give the public access to large amounts of copyright-protected content uploaded by users. Permission-based, sectoral data spaces that facilitate controlled data exchange between known participants, and that do not provide public access to creative content, will typically fall outside this regime.

Overall, the Copyright DSM Directive does not impose data-sharing obligations on data spaces. Rather, it defines **boundaries and safeguards** for the reuse and analysis of protected works within broader data-sharing ecosystems.

[19] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, PE/51/2019/REV/1, OJ L 130, 17.5.2019, p. 92–125 http://data.europa.eu/eli/dir/2019/790/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.2.1.3 Applicability to CircPlastX and data governance implications

CircPlastX is designed as a permission-based, decentralised data-sharing infrastructure in which data exchange is primarily organised around three defined value-creation services linked to regulatory compliance, certification, and sustainability reporting. Although the platform can technically support broader business-to-business data sharing, it is not positioned as a generic or open content marketplace. Data sharing is therefore expected to remain purpose-bound, selective, and governed through contractual and technical controls.

Against this background, the Copyright DSM Directive has only limited and indirect relevance for CircPlastX. The core datasets exchanged through the platform are expected to consist predominantly of non-creative, factual industrial data, which are not protected by copyright as such. Moreover, CircPlastX is not designed to store and give the public access to large amounts of user-uploaded creative content, nor to organise or promote such content for profit-making purposes. It therefore does not qualify as an online content-sharing service provider within the meaning of Article 2(6) of the Copyright DSM Directive, and the specific liability and content-management obligations introduced by Article 17 are not applicable.

Limited relevance may nevertheless arise where data products shared through CircPlastX include copyright-protected materials, such as reports, manuals, images, or studies, alongside non-protected data. In such cases, the Copyright DSM Directive governs the conditions, under which those materials may be reproduced or analysed, including the availability and limits of the text and data mining exceptions. CircPlastX itself does not determine the downstream use of data by participants and does not assess whether such uses are permitted under copyright law; responsibility remains with the relevant data providers and data users.

- **Transparency regarding copyright-protected content**
  From a data governance perspective, CircPlastX may support transparency by allowing data providers to indicate, at a dataset or metadata level, whether shared data products include elements protected by copyright. This does not create new legal obligations for the data space and does not shift responsibility away from participants. Rather, it reflects the data space's trust-oriented governance approach by signalling that access to data within a given service context does not automatically imply unrestricted reuse rights. Beyond this limited transparency function, the Copyright DSM Directive does not impose direct governance requirements on CircPlastX, and copyright compliance remains primarily a participant-level matter addressed through applicable law and contractual arrangements.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.2.2 Database directive

2.2.2.1 Overview

Directive 96/9/EC on the legal protection of databases (Database Directive) [20] establishes a harmonised EU framework for the protection of databases through two distinct intellectual property regimes. First, databases may be protected by copyright where, by reason of the selection or arrangement of their contents, they constitute the author's own intellectual creation (Article 3). This form of protection follows the general principles of EU copyright law and applies only where originality is present.

Second, the Directive creates a sui generis right for databases that are not necessarily creative but whose making has required a qualitatively and/or quantitatively substantial investment in the obtaining, verification, or presentation of their contents (Article 7). This right allows the database maker to prevent the extraction or re-utilisation of the whole or of a substantial part of the database contents.

The two regimes are cumulative: a single database may be protected by copyright, by the sui generis right, or by both. Protection of a database as such is independent of any intellectual property rights that may subsist in individual works or materials contained in the database.

The Directive also defines the position of lawful users of databases. Where a database is made available to the public, lawful users are entitled to extract and re-use insubstantial parts of its contents for any purpose, provided that such acts do not conflict with the normal exploitation of the database or unreasonably prejudice the legitimate interests of the database maker (Article 8). Extraction or re-use of substantial parts remain subject to authorisation, unless a specific exception applies. Optional exceptions for private use, teaching or scientific research, and public security or judicial and administrative procedures may be provided for in national law (Article 9).

The scope of the sui generis right has been significantly clarified by the case law of the Court of Justice of the European Union, which has established that investments relating to the creation of data as such do not qualify.[21] Only investments directed at obtaining existing materials, verifying their accuracy, or presenting them in a database are relevant. As a result, many datasets generated as a by-product of a primary activity fall outside the scope of sui generis protection.

[20] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77/20, 27.3.1996, pp. 20-28 http://data.europa.eu/eli/dir/1996/9/oj.
[21] Case C-46/02, *Fixtures Marketing Oy v Veikkaus AB* (Judgment, 9 Nov 2004, ECLI:EU:C:2004:694; Case C-203/02, *The British Horseracing Board (BHB) and Others v William Hill* (Judgment, Grand Chamber, 9 Nov 2004, ECLI:EU:C:2004:695); Case C-338/02, *Fixtures Marketing Ltd v Svenska Spel AB* (Judgment, 9 Nov 2004, ECLI:EU:C:2004:696); Case C-444/02, *Fixtures Marketing Ltd v OPAP* (Judgment, 9 Nov 2004, ECLI:EU:C:2004:697).

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.2.2.2 Relevance for data spaces and data governance

The Database Directive is relevant to data spaces because it determines whether structured collections of data may be subject to exclusive rights that limit extraction or re-utilisation. Data spaces typically rely on systematic organisation of datasets, individual accessibility, and controlled reuse, all of which may bring shared datasets within the formal definition of a database under Article 1(2).

At the same time, the Directive does not regulate data sharing infrastructures as such, nor does it impose direct governance obligations on data space operators. Its effects are indirect and arise only where a database qualifies for protection and where a participant is entitled to exercise the corresponding rights as the database maker or authorised rightholder.

From a governance perspective, the Directive underscores three points that are relevant for data spaces. First, the existence of database protection cannot be assumed and must be assessed on a case-by-case basis. Second, database rights, where they exist, attach to the maker of the database and not automatically to all entities that hold or share data that are included in the database. Third, lawful users of publicly available databases retain statutory rights to extract and re-use insubstantial parts, subject to safeguards protecting the legitimate interests of the database maker.

Accordingly, the Database Directive does not mandate specific access models or contractual structures for data spaces. Instead, it defines a legal backdrop against which data sharing may take place, leaving it to data providers and data users to address database-related rights through applicable law and, where appropriate, contractual arrangements.

2.2.2.3 Applicability to CircPlastX and data governance implications

The Database Directive does not impose direct legal obligations on CircPlastX as a data space operator. Any rights or restrictions arising under the Directive attach to the data providers (as potential database makers or rightholders) and to data users (as lawful users), not to the data space itself.

From a data governance perspective, CircPlastX's role is therefore **limited to organising and supporting rights management**, without assessing or determining database protection. In practice, this entails:

- providing metadata and governance mechanisms that allow data providers to indicate whether datasets are subject to database protection and under which reuse conditions they are made available;
- ensuring that access and reuse controls implemented through CircPlastX services respect the permissions and limitations defined by data providers, including any restrictions on extraction or re-utilisation of substantial parts;

Beyond these functions, the Database Directive does not require CircPlastX to adopt specific access models, contractual structures, or technical safeguards. Database-related compliance remains a participant-level matter, while CircPlastX acts solely as a neutral facilitator that enables rights-aware data sharing.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.2.3 Trade secrets directive

2.2.3.1 Overview

Directive (EU) 2016/943 (Trade Secrets Directive or "TSD") [22] establishes a harmonised EU framework for civil law protection against the unlawful acquisition, use and disclosure of trade secrets, including by making available measures, procedures and remedies to prevent misappropriation and obtain redress.

A "trade secret" is defined as information that (i) is secret (not generally known or readily accessible within relevant circles), (ii) has commercial value because it is secret, and (iii) has been subject to reasonable steps to keep it secret by the person lawfully in control of it.

The Directive clarifies when the acquisition of trade secrets is lawful (e.g., independent discovery, or observing/studying/disassembling/testing a product lawfully possessed and free from a duty to limit acquisition, i.e., a form of "reverse engineering" as a lawful route where no contractual restriction applies). Conversely, acquisition is unlawful where it occurs through unauthorised access/appropriation/copying of materials/files containing the trade secret or other conduct contrary to honest commercial practices; and use or disclosure is unlawful where done without consent by someone who (among others) breaches a confidentiality agreement or a duty to limit use.

The Directive also contains safeguards/exceptions (e.g., freedom of expression and information; whistleblowing/public interest disclosures; certain worker disclosures; protection of a legitimate interest recognised by law).

It further provides that it does not affect rules requiring disclosure in the public interest or permitting/mandating disclosure by public authorities under Union or national law.

2.2.3.2 Relevance for data spaces and data governance

The Trade Secrets Directive is not a data-sharing instrument as such, but it has direct relevance for the governance of data spaces because it defines the legal conditions under which commercially sensitive information may be shared without losing its protected status. In a data space, where multiple independent actors exchange operational, technical, or compliance-related data across organisational boundaries, trade secret protection becomes a central trust factor rather than a purely bilateral contractual issue.

From a data governance perspective, the Directive makes clear that trade secret protection is conditional. Information retains its status as a trade secret only if it remains secret, derives commercial value from that secrecy, and is subject to

[22] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ L 157, 15.6.2016, pp. 1–18 http://data.europa.eu/eli/dir/2016/943/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

reasonable steps to preserve confidentiality. This has practical implications for data spaces: data governance frameworks must support controlled and selective access to sensitive datasets and must not facilitate indiscriminate dissemination that would render information generally known or readily accessible within the relevant industry circles. Data space governance therefore plays a supporting role in enabling participants to meet the "reasonable steps" requirement through access control, purpose limitation, and enforceable confidentiality conditions.

The Directive also shapes how access and use rights should be framed in data space governance frameworks and participation terms. Unlawful acquisition, use, or disclosure of trade secrets includes conduct such as unauthorised access to electronic files, breach of confidentiality agreements, or use of information in violation of contractual duties to limit its use. In a shared digital environment, this translates into a need for clear governance rules governing who may access which datasets, for what purposes, and under which conditions, as well as mechanisms to prevent unauthorised copying or onward disclosure. While the Directive does not impose technical obligations, it reinforces the importance of aligning contractual and organisational measures with the technical design of the data space.

At the same time, the Directive clarifies that trade secrets do not create exclusive or monopolistic rights over information. Lawful acquisition remains possible through independent discovery or, in certain circumstances, observation and analysis of lawfully accessible products or objects. Data space governance must therefore avoid overstating the scope of confidentiality protection and should reflect that trade secret protection operates alongside, and is limited by, general principles of lawful competition and innovation.

Finally, the Directive explicitly preserves transparency and disclosure obligations imposed by Union or national law and recognises safeguards such as whistleblowing and freedom of expression. For data spaces operating in regulated sectors, this means that governance frameworks cannot treat trade secret claims as absolute barriers to disclosure. Instead, they must accommodate situations in which data must be shared with public authorities or disclosed in the public interest, even where the information would otherwise qualify as a trade secret. In this sense, the Trade Secrets Directive reinforces the need for nuanced, legally informed data governance that balances confidentiality, compliance, and trust in multi-actor data sharing environments.

2.2.3.3 Applicability to CircPlastX and data governance implications

CircPlastX is conceived as an industrial data space in the circular plastics value chain, where stakeholders are often reluctant to share data because of confidentiality concerns, and where some substance-related information may be shared only in a way that does not reveal sensitive details. These are classic conditions under which trade secrets protection becomes a practical governance constraint. Below are the main requirements for CircPlastX:

- **Governance must support "reasonable steps" to preserve secrecy for trade-secret datasets [Art. 2 TSD]**
  CircPlastX governance (rulebook/participation terms) should enable participants who share commercially sensitive datasets to maintain the **"reasonable steps"** element of trade secret protection, including by allowing

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

controlled access and confidentiality constraints over datasets shared in the data space.

- **Access control rules must prevent unauthorised access/copying of trade-secret datasets [Art. 4(2) TSD]**
  CircPlastX should implement and enforce platform-level access controls and authentication/authorisation rules designed to prevent unauthorised access, appropriation, or copying of electronic files or other materials containing trade-secret information. This is particularly important in CircPlastX given the documented confidentiality/IP-related reluctance to share.

- **Participation terms must prohibit unauthorised disclosure and impose duties to limit use [Art. 4(3) TSD]**
  CircPlastX participation terms should clearly set out contractual duties to limit use to the permitted purposes/conditions agreed between the sharing parties, since breach of such duties is explicitly a basis for “unlawful” use/disclosure under the Directive.

- **Governance must accommodate legally required disclosures and avoid overbroad confidentiality claims [Art. 1(2) TSD]**
  CircPlastX governance documentation should reflect that trade secrets protection does not override Union/national rules requiring disclosure in the public interest or permitting/mandating disclosure by public authorities. Practically, this means confidentiality frameworks should include carve-outs for legally compelled disclosures and avoid promising absolute secrecy against lawful disclosure regimes.

Co-funded by the European Union

This project receives funding from the European Commission’s Digital Europe Programme under Grant Agreement Number 101195258.

2.3 Privacy and data protection

2.3.1 General Data Protection Regulation

2.3.1.1 Overview

Regulation (EU) 2016/679 (the General Data Protection Regulation, "GDPR")[23] is the EU's horizontal framework governing the processing of personal data. It applies to processing carried out in the context of the activities of an establishment in the EU, irrespective of where the processing takes place, and it may also apply to non-EU entities where their processing relates to the offering of goods or services to individuals in the EU or the monitoring of their behaviour in the EU (Art. 3 GDPR). The GDPR has applied since 25 May 2018.

The Regulation applies only where **personal data** are processed, i.e. information relating to an identified or identifiable natural person (Art. 4(1) GDPR). "Processing" is defined broadly and covers essentially any operation performed on personal data, including collection, storage, use, disclosure by transmission, dissemination, or otherwise making available (Art. 4(2) GDPR). Where personal data are processed, the GDPR requires that processing be carried out in accordance with a set of core principles, including lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability (Art. 5 GDPR), and that a lawful basis under Article 6 GDPR (and, where relevant, additional conditions for special categories of data under Article 9 GDPR) be identified.

A central structural feature of the GDPR is its allocation of responsibility through the roles of **controller** and **processor**. The controller determines the purposes and essential means of the processing, while a processor processes personal data on behalf of the controller (Art. 4(7)–(8) GDPR). Controllers must be able to demonstrate compliance through appropriate technical and organisational measures (Art. 24 GDPR), and controller–processor relationships must be governed by an agreement meeting the requirements of Article 28 GDPR.

The GDPR also establishes enforceable rights for data subjects and corresponding duties for controllers. These include transparency obligations (Arts. 12–14 GDPR) and rights such as access, rectification, erasure, restriction, portability, and objection (Arts. 15–21 GDPR). In addition, the GDPR contains operational compliance duties that are particularly relevant in environments involving systematic data sharing, including security of processing (Art. 32 GDPR) and personal data breach notification duties (Arts. 33–34 GDPR).

[23] 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 (GDPR), OJ L 119, 4.5.2016, pp. 1–88 http://data.europa.eu/eli/reg/2016/679/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.3.1.2 Relevance to data spaces and data governance

Although the GDPR is a general data protection instrument and not a data governance framework as such, it has a decisive impact on data sharing and on the governance of data spaces. This impact follows from the breadth of the concepts of "personal data" and "processing", and from the fact that data sharing, access and re-use typically constitute processing operations within the meaning of the GDPR. As a result, data space governance must be designed so that GDPR compliance remains achievable and demonstrable across multi-actor, technically intermediated environments.

Importantly, GDPR relevance for data spaces is not limited to personal data that may be exchanged or processed through data-sharing use cases/ services. Data spaces are organisations in their own right and inevitably process personal data in the course of their ordinary operation. This includes, at a minimum, personal data relating to participants and their representatives, such as onboarding, identity and access management, authentication and authorisation, governance bodies, communications, and security logging. Consequently, the GDPR applies in full to data spaces as corporate entities for their internal and organisational processing activities, independently of whether or to what extent personal data are shared between participants through the data space.

From a data sharing perspective, the GDPR is not designed to encourage the free circulation of personal data, but rather to condition sharing of such data on compliance with substantive and procedural safeguards. In practice, this means that personal data can be shared only if the GDPR's principles are respected and if responsibility for the processing is clearly allocated.

Several GDPR concepts are particularly relevant for data spaces.

First, **the principle-based structure of the GDPR** directly affects how data sharing can be organised. Purpose limitation and data minimisation (Art. 5(1)(b)–(c) GDPR) require that personal data be shared only for specified and legitimate purposes and only to the extent necessary for those purposes. This limits open-ended or unspecified reuse of personal data within a data sharing ecosystem. Transparency and accountability (Arts. 5(1)(a) and 5(2) GDPR) further require that such sharing be intelligible to data subjects and demonstrable to supervisory authorities. Second, **role allocation between controllers and processors** is a central data governance issue in multi-actor environments. Data sharing can take different legal forms under the GDPR: a controller may disclose personal data to another independent controller; a controller may entrust processing to a processor; or multiple entities may jointly determine the purposes and means of processing, giving rise to joint controllership (Arts. 4(7)–(8), 26, 28 GDPR). Each configuration entails different obligations and risks. In data spaces, where technical infrastructure is shared but purposes may differ between participants, these distinctions are particularly important.

A baseline requirement is therefore the clear allocation of GDPR responsibility between the data space operator and participating actors, depending on the specific processing activity. The operator may act as an independent controller for platform-level functions such as user and access management, authentication, authorisation, and security logging. In other cases, the operator may process personal data on behalf of a participant strictly under that participant's instructions in the context of a specific

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

service, giving rise to a processor role. Clear and documented role allocation is essential, as it determines which GDPR obligations apply in practice, including accountability under Article 24 and the requirement for controller–processor agreements under Article 28, and prevents responsibility from being obscured by intermediated technical architectures.

This role allocation challenge is amplified by what ENISA describes as "compositional" risks in data spaces, namely risks that arise from the overall configuration of actors, dependencies, and data flows, even where each individual processing operation might appear compliant when assessed in isolation. Where a data protection impact assessment is required, this means that the assessment may need to consider not only the processing carried out by a single actor, but also inter-organisational data flows, shared technical components, and the cumulative effects of the data space architecture. From a data governance perspective, this reinforces the need for explicit role definitions, transparency of responsibilities, and coordinated risk management across the data space.[24]

Third, **data subject rights and transparency obligations** introduce operational constraints on data sharing architectures. Even where personal data are exchanged between organisations, data subjects retain rights of access, rectification, erasure, restriction, portability and objection (Arts. 15–21 GDPR). Data space governance must therefore ensure that these rights remain exercisable in practice and that responsibility for responding to requests is not obscured by technical or organisational complexity.

Fourth, **security and incident management** are structurally relevant to data spaces. Even where data are not exchanged directly between participants, data spaces typically rely on centrally operated technical components such as identity and access management, authentication services, secure connectors, and logging mechanisms that are used by multiple independent actors. Where personal data are processed through such components, the GDPR's requirements on security of processing and breach notification (Arts. 32–34 GDPR) must be addressed in a coordinated manner, as risks may arise from the interaction between services, users, and technical dependencies rather than from a single actor's processing alone.

ENISA further highlights that data spaces raise privacy risks linked both to "input" (e.g. the introduction of personal data into a shared environment, with risks of unauthorised access, re-identification, or function creep) and to "output" (e.g. results or derived data that may still enable singling out or indirect identification).[25]

Against this background, ENISA frames "data protection engineering" as a practical enabler of lawful data sharing in data spaces. While the GDPR does not mandate specific technologies, privacy-enhancing techniques and architectural measures can support compliance with GDPR principles, reduce residual risks, and strengthen trust

[24] P Drogkaris and JG Prieto (Eds), Engineering Personal Data Protection in EU Data Spaces (2024) (European Union Agency for Cybersecurity (ENISA), Study). https://www.enisa.europa.eu/publications/engineering-personal-data-protection-in-eudata-spaces accessed 27/02/2026.
[25] ibid.

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

between participants.[26] The adoption of such measures does not alter the allocation of legal responsibility under the GDPR but may form part of the technical and organisational measures implemented under Articles 24 and 32.

2.3.1.3 Applicability to CircPlastX and data governance implications

CircPlastX is conceived primarily as an industrial data space for circular plastics value-chain data. As such, it is not expected to process large volumes of personal data as part of its core data sharing activities. Nevertheless, personal data arise incidentally or unavoidably in certain contexts, including participant management and mixed datasets contributed by participants.

The GDPR therefore applies to CircPlastX **only to the extent that personal data are processed**, and the resulting governance requirements should be proportionate to that limited exposure. The requirements listed below focus on those obligations that are most likely to arise and that are essential for lawful operation.

- **Identification of controller and processor roles for platform-level processing [Arts. 4(7)–(8), 24, 28 GDPR]**

  Where the CircPlastX operator determines the purposes and means of processing personal data for platform operations (such as user account management, authentication, access control and logging), it acts as a data controller and must comply with the corresponding controller obligations. Where it processes personal data on behalf of a participant that determines purposes and essential means, it acts as a processor and must be bound by a data processing agreement meeting the requirements of Article 28 GDPR.

  The CircPlastX participation terms should describe, at a high level, which platform-related processing activities are operated under the operator's responsibility and which may be performed on behalf of participants, so that role allocation is not ambiguous and responsibilities are transparent.

- **Lawful basis and purpose limitation and data minimisation [Arts. 5(1)(b)–(c), 6 GDPR]**
  Where the CircPlastX operator processes personal data for the operation of the data space itself, it must ensure that such processing is based on a lawful ground under Article 6 GDPR and complies with the principles of purpose limitation and data minimisation. This includes, in particular, personal data processed for participant onboarding, user account administration, authentication and authorisation, access management, security logging, and communication related to the provision of CircPlastX services.
  For the core CircPlastX services, participants submit data for analysis and receive the results back, without onward sharing of those data with other participants. In this configuration, the participant submitting the data determines the purpose of the processing and therefore acts as controller for that processing. CircPlastX processes the data strictly to provide the requested service and does not determine independent purposes for the use of the data.

[26] ibid.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Accordingly, CircPlastX acts as a processor within the meaning of Article 4(8) GDPR for such service-related processing, and this relationship must be governed by a data processing agreement in accordance with Article 28 GDPR. CircPlastX data governance must ensure that service workflows and technical configurations do not enable processing beyond the purpose defined by the participant or permit reuse of personal data for unrelated or unspecified purposes. Any tooling used to describe or document the intended purpose of a service request may support transparency and accountability, but it does not replace the participant's responsibility, as controller, to identify a lawful basis and assess purpose compatibility under the GDPR.

- **Privacy information for platform-level processing [Arts. 12–14 GDPR]**
  Where the CircPlastX operator acts as controller for platform-related personal data processing, it must provide data subjects with transparent and accessible information on the processing, including purposes, legal bases, retention periods and rights.

- **Operational handling of data subject rights [Arts. 15–22 GDPR]**
  CircPlastX must ensure that data subject rights can be exercised in practice. At minimum, governance arrangements must clarify which entity is responsible for responding to rights requests relating to platform-level data and how requests relating to participant datasets are routed to the appropriate controller.

- **Security of processing for personal data handled in CircPlastX operations [Art. 32 GDPR]**
  To the extent that the CircPlastX operator processes personal data for the operation of the data space it must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Article 32 GDPR. The operator must ensure that platform functions involving personal data are protected against unauthorised access and accidental loss, and that access to such personal data is limited to those who need it for platform operation and security. Security measures should be designed with both "input" and "output" risk in mind: protecting personal data when introduced into and processed within the data space environment, and avoiding the release of outputs or derived data (where the operator is involved in generating or disclosing them) in a form that unintentionally enables re-identification or singling out.

  Article 32 does not prescribe specific technologies, but it requires that security measures be selected and maintained with reference to the state of the art, implementation cost, and the nature, scope, context and purposes of processing, as well as the risks to individuals. Where appropriate for the risk profile, this includes measures such as access controls, authentication safeguards, encryption during transmission and storage, and processes to ensure ongoing confidentiality, integrity, availability and resilience of the relevant systems.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

- **Personal data breach notification chain for platform processing (and, where relevant, processor-to-controller notification) [Arts. 33–34 GDPR]**
  Where a personal data breach occurs in the context of CircPlastX operations, the entity acting as controller for the affected processing must assess and comply with the GDPR notification duties. This includes notification to the competent supervisory authority without undue delay and, where feasible, within 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Where the breach is likely to result in a high risk, communication to affected data subjects is also required unless an exception applies.

  Where the CircPlastX operator processes personal data on behalf of a participant (i.e. acts as a processor for a defined processing operation), it must notify the relevant controller without undue delay after becoming aware of a personal data breach (Art. 33(2) GDPR).

  For CircPlastX governance, the practical consequence is that it must have a workable incident escalation pathway for the personal data it handles (and, where it is a processor, a clear route to notify the controller). This is typically reflected in internal incident response procedures and in the relevant contractual clauses allocating notification responsibilities.

- **Support for DPIA-relevant information in multi-actor processing [Art. 35 GDPR]**
  Where a participant is required to carry out a data protection impact assessment for processing involving CircPlastX services, the CircPlastX should be able to provide accurate and stable information about its own technical and organisational measures, role, and data flows, to enable the controller to assess risks arising from the shared processing environment. This does not make CircPlastX responsible for conducting DPIAs on behalf of participants.

- **Records of processing activities for operator-controlled or operator-processed personal data [Art. 30 GDPR]**

  To the extent that the CircPlastX acts as a controller or processor for any personal data processing activities, it must maintain a record of processing activities as required by Article 30 GDPR, covering those processing operations. This means CircPlastX should be able to document, for its own processing, at least the basic elements required under Article 30 (as applicable to controllers and/or processors), such as the purposes of processing, categories of data subjects and personal data, categories of recipients (if any), retention parameters, and a general description of security measures. This obligation applies only to the processing operations for which CircPlastX is the controller or processor; it does not extend to personal data processing performed independently by participants as separate controllers. Such records contribute to demonstrating compliance in complex data-sharing ecosystems but remain limited to the CircPlastX operator's own processing activities and responsibilities.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.3.2 E-privacy directive

2.3.2.1 Overview

Directive 2002/58/EC on privacy and electronic communications (the "ePrivacy Directive")[27], as amended by Directive 2009/136/EC, complements the GDPR by laying down specific rules for the protection of privacy in the electronic communications sector. It applies to the processing of personal data and to the confidentiality of communications in the context of publicly available electronic communications networks and services, as defined in the EU telecommunications framework, now consolidated in the European Electronic Communications Code (Directive (EU) 2018/1972).

The Directive contains sector-specific rules on the confidentiality of communications, traffic data and location data, as well as on the use of cookies and similar technologies stored on users' terminal equipment. Unlike the GDPR, which applies horizontally across sectors, the ePrivacy Directive targets a limited category of actors and processing contexts linked to electronic communications services. Its primary objective is the protection of communications privacy rather than the facilitation of data sharing.

2.3.2.2 Relevance to data spaces and data governance

The relevance of the ePrivacy Directive to data spaces depends on whether a data space provides, or itself constitutes, a publicly available electronic communications service within the meaning of EU telecommunications law.

In principle, most data spaces do **not** fall within the scope of the ePrivacy Directive. Data spaces typically facilitate access to data through APIs, secure connectors, or application-layer services, and do not provide electronic communications services whose purpose is the conveyance of signals or interpersonal communication. Machine-to-machine communications, backend data transfers, and service-to-service interactions used to enable data access or analytics generally fall outside the scope of the ePrivacy framework and are governed, where relevant, by the GDPR.

A data space could fall within the scope of the ePrivacy Directive only in **exceptional configurations**. For example, if a data space were to offer a publicly available, number-independent interpersonal communication service embedded in its environment (such as a real-time messaging or chat function enabling direct communication between users as a core service), that specific functionality could qualify as an over-the-top electronic communications service and trigger the

[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37–47 http://data.europa.eu/eli/dir/2002/58/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

application of ePrivacy confidentiality rules for communications metadata and content. Such configurations are atypical for industrial or sectoral data spaces.

A limited but horizontal point of relevance across many data spaces concerns the use of cookies or similar tracking technologies in user-facing interfaces (such as web portals or dashboards). These aspects are regulated by Article 5(3) of the ePrivacy Directive, as implemented in national law, in conjunction with the GDPR.

2.3.2.3 Applicability to CircPlastX and data governance implications

CircPlastX is an industrial data space focused primarily on the sharing of non-personal and commercially relevant data in the circular plastics domain. It does not provide publicly available electronic communications services and does not operate electronic communications networks. Accordingly, the core provisions of the ePrivacy Directive on the confidentiality of communications, traffic data and location data are not directly applicable to CircPlastX as a data space.

The relevance of ePrivacy for CircPlastX is therefore limited. It may arise only insofar as CircPlastX operates user-facing web interfaces that rely on cookies or similar technologies for functionality, security or analytics, in which case the applicable national ePrivacy rules on terminal equipment apply alongside the GDPR.

Overall, the ePrivacy Directive does not impose specific data governance requirements on CircPlastX beyond general compliance for ancillary web-interface functionalities, and it does not shape the core rules on data access, use and sharing within the data space.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.4 Competition, platform and digital markets regulation

This section aims to provide an overview of the most relevant EU legal instruments concerning competition, platform and digital markets regulation, insofar as they are relevant to the governance and operation of data spaces. The EU legal framework for competition law includes the Treaty on the Functioning of the European Union (TFEU)[28] articles 101, 102, 103, and 107, as well as further regulations directly concern the application of such articles. In addition, the European Commission has issued various notices and guidelines, including the Horizontal Cooperation Guidelines,[29] which are particularly relevant for assessing structured collaboration between undertakings. Finally, national competition laws of member states remain applicable.

Given the structure and objectives of data spaces, this chapter focuses primarily on Articles 101 and 102 TFEU, as these provisions are most directly engaged where multiple undertakings cooperate or where market power concerns may arise. The analysis also touches upon the Digital Markets Act (EU) 2022/1925.[30]

2.4.1 Article 101 TFEU

2.4.1.1 Overview

Article 101 TFEU prohibits agreements between undertakings, decisions by associations of undertakings, and concerted practices that have as their object or effect the prevention, restriction, or distortion of competition within the internal market and which may affect trade between Member States. This includes, inter alia, practices such as price fixing, market sharing, output limitation, and the exchange of competitively sensitive information capable of reducing strategic uncertainty on the market. The term "decision" is interpretated broadly to include actions by an association that serve to coordinate the conduct of its members or those subject to its authority.[31] The case law of the Court of Justice of the EU (CJEU) has found the following to be a "decision by an association of undertakings": the constitution of a trade association,[32] regulations governing the operation of an association,[33] an

[28] Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390 http://data.europa.eu/eli/treaty/teu_2012/oj.

[29] Communication from the Commission — Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements Text with EEA relevance, OJ C 11, 14.1.2011, pp. 1–72, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011XC0114%2804%29.

[30] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *OJ L 265, 12.10.2022, pp. 1–66, http://data.europa.eu/eli/reg/2022/1925/oj*

[31] Whish, Richard, and David Bailey, Competition Law, 11th edn (Oxford University Press, 2024), p. 116.

[32] *Re ASPA* JO [1970] L 148/9; *National Sulphuric Acid Association* OJ [1980] L 260/24.

[33] *Nederlandse Federative Vereniging voor de Grootlandel op Elektrotechnisch Gebied and Technische Unie (PEG and TU)* OJ [2000] L 39/1, para 95; *Visa International* OJ [2001] L 293/24, para 53; *Visa International-Multilateral Interchange Fee* OJ [2002] L 318/17, para 55; *International Skating Union's Eligibility Rules,* Commission decision of 8 December 2017, para 152.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

agreement entered by an association[34] and the recommendation of an association, if members have tended to comply with the recommendation that would have a significant influence on competition.[35]

Furthermore, the concept of "agreement" under Article 101 TFEU is interpreted broadly and does not require a formally binding contract; a concurrence of wills is sufficient.[36] The CJEU case law makes clear that even indirect contacts between competitors may fall within the scope of Article 101 where they influence market conduct or reveal future strategic intentions.[37] In *Anheuser-Busch*, the CJEU concluded that guidelines issued by one person that are adhered to by another can amount to an agreement.[38] In *Re Nuovo,* the CJEU concluded that the constitution of a trade association qualifies as an agreement in this regard.[39]

Similarly, a "concerted practice" covers any form of coordination which knowingly substitutes practical cooperation for the risks of competition. In *'Eturas' UAB v Lietuvos Respublikos konkurencijos taryba*[40] the CJEU considered that the use of software, and knowledge of what it could do, could lead to a concerted practice. It does not require a formal plan; Art 101 prohibits any contact that may influence market conduct or reveal an undertaking's future market behaviour.[41] There is a presumption that parties to a concerted action take account of exchanged information, and it is not necessary to prove actual market effects.[42] A concerted practice involves reciprocity, which is met where a competitor discloses its intentions or conduct to another and the other requests or at least accepts that disclosure.[43] Article 101(3) TFEU provides a legal exemption where an agreement, concerted practice or a decision by an association of undertakings contribute to improving the production or distribution of goods or to promoting technical or economic progress, while allowing consumers a fair share of the resulting benefits, provided that the restrictions are indispensable and do not eliminate competition in respect of a substantial part of the products concerned. The burden of proof for this exemption lies with the undertakings invoking it.[44]

In this context, the Horizontal Block Exemption Regulations (HBERs)[45] are also relevant as these exempt certain clearly defined categories of horizontal cooperation agreements from the prohibition in Article 101(1), provided that the conditions set out therein are met. Their scope and interpretation are further elaborated in the

[34] Whish, p. 116.
[35] Cases 96/82 *IAZ International Belgium NV v Commission* EU:C:1983:310.
[36] *Commission v Volkswagen*, C-74/04 P, EU:C:2006:460, paragraph 37.
[37] *ICI v Commission (Dyestuffs)*, Case 48/69, EU:C:1972:70, para. 64.
[38] *Anheuser-Busch Incorporated/Scottish & Newcastle OJ [2000] L 49/37, para 26.*
[39] *Re Nuovo CEGAM OJ [1984] L 99/29*
[40] Case C-74/14 EU:C:2016:42.
[41] Cases 40/73 etc *Suiker Unie v Commission* EU:C:1975:174, paras 173-174.
[42] Case C-49/92 P *Commission v Anic Partecipazioni* EU:C:1999:356, para 121.
[43] Cases T-25/95 etc *Cimenteries CBR SA v Commission* EU:T:2000:77, para 1849.
[44] See Article 2 of Council Regulation (EC) No 1/2003 of 16 December 2002 on the implementation of the rules on competition laid down in Articles 81 and 82 of the Treaty (OJ L 1, 4.1.2003 p. 1).
[45] Commission Regulation (EU) 2023/1066 on research and development agreements and Commission Regulation (EU) 2023/1067 on specialisation agreements.

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Commission's 2023 Horizontal Guidelines[46], which include detailed guidance on information exchange between competitors.

Information exchange may take place directly between competitors, indirectly through a common agency or third party, or via suppliers or retailers, and such exchanges can generate efficiencies by improving transparency, reducing duplication and facilitating innovation[47]. Under the HBER framework and the Horizontal Guidelines, information exchange is generally regarded as restrictive where it involves the sharing of individualised information concerning intended future prices, output or other commercially sensitive strategic parameters. Subject to the conditions laid down in the Regulations and the Guidelines, certain narrowly defined forms of cooperation therefore benefit from a safe harbour.

2.4.1.2 Relevance to data spaces and data governance

Data spaces constitute structured environments in which multiple undertakings interact through shared infrastructure, governance rules, contractual frameworks and technical services. These characteristics may significantly reduce the practical and informational barriers between market participants and, if not properly designed, may facilitate forms of coordination that fall within the scope of Article 101 TFEU.

Importantly, competition law risk does not arise only where a data space explicitly enables the exchange of competitively sensitive information. It may also arise where the design, governance or operation of the data space makes anticompetitive conduct more likely, more efficient, or harder to detect.

Furthermore, it is possible, depending on the composition of the data space, the relationship between the provider and users, and the services in scope, that there may be a decision or agreement of an association of undertakings for which the data space would hold liability in case such decision or agreement infringe EU competition law, especially in cases where there is no legal exemption to improve a production or distribution of goods, or providing technical or economic progress.

In this regard, EU case law confirms that an entity may incur liability under Article 101 TFEU even if it is not itself active on the affected market, where it knowingly contributes to or facilitates a restriction of competition. In *AC-Treuhand*, the CJEU held that an intermediary which provided organisational and administrative support to a cartel could be held liable where it was aware of the cartel's objectives or could reasonably foresee them and accepted the associated risk.[48] In *FNCBV v Commission*, the Court followed that the trade unions and the federations that grouped

[46] Commission Notice: Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements (2023 Revised Horizontal Guidelines), available at: https://competition-policy.ec.europa.eu/system/files/2023-07/2023_revised_horizontal_guidelines_en.pdf accessed 27/02/2026.

[47] Graux, H., "Sharing Data (Anti-)Competitively, Will European data holders need to change their ways under the proposed new data legislation?", 2022, Publications Office of the EU, p. 7, https://data.europa.eu/sites/default/files/report/Sharing_data_anti_competitively_will_European_data_holders_need_to_change_their_ways_under_the_proposed_new_data_legislation.pdf

[48] *AC-Treuhand v Commission*, C-194/14 P, EU:C:2015:717,paras 30–33.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

those unions together were associations of undertakings; and the federations, rather than the individual undertakings, were fined in this case, with consideration to the members' turnover.[49] Accordingly, a data space operator cannot assume that it is insulated from Article 101 TFEU merely because it does not compete with participants or does not determine their commercial strategy.

At the same time, structured data sharing arrangements may generate significant efficiencies. Article 101(3) TFEU provides that restrictive agreements may be exempted where they contribute to improving production or distribution or promote technical or economic progress, allow consumers a fair share of the resulting benefit, impose only indispensable restrictions; and do not eliminate competition in respect of a substantial part of the products concerned.

In the context of data spaces, potential efficiencies may include reduced duplication, enhanced interoperability, improved traceability, increased innovation capacity, better regulatory compliance, and the correction of information asymmetries that hinder market functioning. However, the assessment under Article 101(3) TFEU is strictly case-by-case, is undertaken only once a restriction under Article 101(1) TFEU has been identified, and the burden of proof lies with the undertakings invoking the exemption.

Accordingly, the design of data governance mechanisms - including access rules, data segregation, aggregation thresholds, purpose limitations and oversight mechanisms - is legally decisive in determining whether a data space merely enables pro-competitive efficiencies or crosses into prohibited coordination.

Contractual clauses allocating responsibility to participants or disclaiming operator liability may be relevant for private risk allocation, but they do not neutralise potential public enforcement under Article 101. Competition law liability is objective and cannot be contractually waived vis-à-vis competition authorities. Where the infrastructure, governance model or services materially facilitate coordination, liability exposure may arise irrespective of contractual disclaimers.

2.4.1.3 Applicability to CircPlastX and data governance implications

CircPlastX must be assessed as an analytical service infrastructure that may influence market behaviour indirectly through the nature, granularity and timing of the outputs it provides. This is an ongoing assessment through the project in line with the scope of the services covered as well as the contractual arrangements concerning those, also taking into account the circularity advantages the platform would provide and the potential exemptions under Art. 101(3) TFEU such services may fall under, for the following reasons:

- Interoperable, purpose-bound data sharing can reduce fragmentation, improve traceability, cut duplication and manual verification, and enable more reliable life cycle assessment and compliance processes (including readiness for digital product passports).

[49] Cases T-217/03 and T-245/03 EU:T:2006:391.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

- Better data quality and traceability support safer, compliant products and credible sustainability claims, and may lower compliance costs and improve circularity outcomes that benefit downstream customers and end users.

- Given the sensitivity of industrial data and widespread reluctance to share, restrictions such as access controls, confidentiality safeguards, and purpose limitations may be necessary to make multi-actor sharing workable.

- If the scheme focuses on infrastructure/governance (not commercial coordination), remains open and non-discriminatory, and avoids exchanging competitively sensitive information, it should not eliminate competition in a substantial part of the market.

However, any reliance on Article 101(3) TFEU requires that such restrictions remain indispensable and that the system does not eliminate competition in respect of a substantial part of the relevant market. Efficiencies cannot justify unnecessary transparency regarding competitively sensitive parameters.

In this respect, to minimise the risk of facilitating infringements of Article 101 TFEU, CircPlastX should embed with the following governance and operational safeguards:

1. **Strict data isolation and output segregation**
   Analytical results provided to each participant should be derived solely from that participant's own data and from sufficiently aggregated and anonymised datasets that cannot be reverse engineered to infer competitors' individual strategies.

2. **Prohibition of identifiable competitor benchmarking**
   Outputs should avoid comparative rankings, peer benchmarking tools or performance indicators that allow participants to infer rivals' costs, production levels, pricing strategies or capacity utilisation.

3. **FRAND-based participation framework**
   Participation conditions should be transparent, fair, reasonable and non-discriminatory, avoiding exclusionary effects or discriminatory access that could distort competition.

4. **Clear competition-law safeguards in participation terms**
   Participation agreements should include explicit prohibitions on using CircPlastX services or outputs for the purpose of coordinating prices, output, market allocation or other competitively sensitive conduct, and rights for the operator to suspend or terminate access where there are credible indications that the services are being misused for anticompetitive purposes. While such clauses do not exclude liability per se, they are relevant in demonstrating that CircPlastX has taken active and proportionate steps to prevent the use of its infrastructure as a vehicle for anticompetitive conduct.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.4.2 Article 102 TFEU

2.4.2.1 Overview

Article 102 TFEU[50] **prohibits the abuse of a dominant position** within the internal market or a substantial part of it. **Dominance** refers to a position of economic strength that enables an undertaking to behave to an appreciable extent independently of competitors, customers, and consumers.[51] Dominance is not unlawful as such; only the abuse of such a position is prohibited.[52]

A dominant position may be held by a single undertaking or jointly by two or more undertakings (**joint or collective dominance**). Joint dominance arises where several undertakings can adopt a common policy on the market and act to a significant extent independently of competitive pressures, even in the absence of formal agreements or a single controlling entity. EU competition law recognises joint dominance where market conditions allow **tacit coordination** to be sustained over time, typically due to a combination of factors such as high market transparency, limited competitive constraints, structural links or mutual dependencies between undertakings, and the ability to monitor and retaliate against deviations from coordinated behaviour.[53]

Abusive conduct is non-exhaustively listed in Article 102 TFEU itself (e.g., unfair prices or trading conditions; limiting production/markets/technical development; discrimination; tying). The Courts and the Commission have developed these categories further and, in practice, abuses typically take either an exploitative form (e.g., unfair pricing/conditions) or an exclusionary form (e.g., foreclosure through refusal of access/supply, discriminatory access, tying/bundling).[54] In data-related contexts, competition-law analysis emphasises that differential or exclusive control over data or data-related infrastructure may contribute to durable market power and that exclusionary abuses may materialise where such control is used to restrict access to data, reinforce intermediation power, or favour vertically integrated services within a data ecosystem.[55]

Article 102 TFEU does not impose obligations on undertakings that are not dominant. Its relevance therefore depends on market power and factual circumstances.

---

[50] Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390 http://data.europa.eu/eli/treaty/teu_2012/oj.
[51] *United Brands v Commission*, Case 27/76, EU:C:1978:22, para. 65.
[52] *Michelin v Commission*, Case 322/81, EU:C:1983:313, para. 57
[53] *Airtours v Commission*, Case T-342/99, EU:T:2002:146, paras 62–63.
[54] Communication from the Commission — Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings, OJ C 45, 24.2.2009, pp. 7–20 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2009_045_R_0007_01.
[55] H. Schweitzer, J. Haucap, W. Kerber & R. Welker, *Competition Policy for the Digital Era* (Report for the European Commission, 2019), ch. 3, pp. 48–50, ch. 4, pp. 66–71, ch. 5, section B, pp. 98–101.

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Below is a comparison of articles 101 and 102 TFEU:

Issue	Article 101 TFEU	Article 102 TFEU
Focus	• Prohibits anti-competitive agreements • Exemption where agreement improves production or distribution of goods/ promotes technical or economic progress for the benefit of consumers	• Prohibits the abuse of a dominant position • Efficiencies / objective justification
Non-exhaustive list of examples	• Price fixing • Market sharing • Customer allocation • Exclusive purchasing or supply • Exchanges of sensitive information between competitors	• Predatory pricing • Excessive pricing • Refusal to supply • Denial of access to an "essential facility" • Loyalty rebates • Tying and bundling

2.4.2.2 Relevance to data spaces and data governance

Article 102 TFEU becomes relevant only where a data space operator holds a dominant position on a relevant market. In such cases, data access rules and governance decisions may be scrutinised to ensure that they are not applied in a discriminatory or exclusionary manner. However, absent dominance, Article 102 TFEU does not impose obligations on data space operators.

That said, the definition of what "relevant market" is, and the characteristics of such market (i.e., free market with no barriers to entry, oligopoly, monopoly) are of direct relevance to whether an undertaking holds dominant position or not. Given that certain sectors may ultimately be characterised by a very limited number of data spaces operating at EU level, potentially as a result of policy-driven initiatives, standardisation effects, or public funding choices, the question of dominance and joint dominance warrants particular attention in the context of emerging European sectoral data spaces.

At present, however, several factors argue against an immediate finding of dominance, whether single or joint, in respect of most European data spaces. Many data spaces are still at an early or experimental stage, are not fully operational, and do not yet exercise stable or sustained market power. Moreover, participation in data spaces is voluntary, and alternative data-processing or compliance solutions may remain available outside the data space ecosystem.

Nonetheless, (joint) dominance cannot be excluded as a forward-looking risk. As data spaces mature and become functionally indispensable for regulatory compliance, certification, or market access, their (data) governance choices may acquire competitive significance. In such circumstances, even a small number of data spaces

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

could collectively hold a position of market power if participants and users lack realistic alternatives and if competitive pressures are limited.

From a governance perspective, this implies that data spaces should be designed with safeguards against dominance in mind, even where no dominance currently exists. In particular, data space operators should ensure that access conditions, participation criteria, and service provision rules are objective, transparent and non-discriminatory, and that they do not unduly favour certain participants, categories of users, or downstream activities. This is especially relevant where the data space performs functions that are closely linked to regulatory compliance, certification, or de facto industry standards.

In summary, while Article 102 TFEU is unlikely to be immediately applicable to most sectoral data spaces, including CircPlastX, due to their current state of development, the potential for single or joint dominance should not be disregarded as data spaces scale, consolidate, or become structurally important. Ongoing monitoring of market developments and proportionate governance safeguards are therefore advisable to mitigate future Article 102 TFEU risks.

2.4.2.3 Applicability to CircPlastX and data governance implications

Based on its envisaged role, scope and mode of operation, CircPlastX is **not expected, at the time of deployment**, to hold a dominant position on any relevant market within the meaning of Article 102 TFEU, whether individually or jointly with other undertakings. CircPlastX is conceived as a sectoral data space enabling voluntary participation, purpose-bound data sharing and service-driven data use, and does not currently appear to function as an indispensable facility for market access, regulatory compliance, or certification in the plastics value chain.

Accordingly, Article 102 TFEU does **not** give rise to **immediate or direct obligations** for CircPlastX or its operator. However, given the potential for sectoral data spaces to gain strategic importance over time, particularly where they support compliance, traceability or certification functions, CircPlastX governance should remain attentive to the risk of future single or joint dominance.

A more critical assessment nevertheless requires considering structural features that could, over time, support a finding of dominance. In particular, if CircPlastX were to become closely integrated with regulatory compliance workflows (e.g. as a de facto channel for meeting traceability, reporting, or certification requirements), strong network effects and data driven lock-in could emerge. Where access to high-quality, standardised sectoral data becomes cumulatively more valuable as participation increases, late entrants or alternative infrastructures may struggle to compete effectively.

In addition, if governance bodies or key industry players exercise decisive influence over access conditions or technical standards, there is a conceivable risk of collective market power amounting to joint dominance. Conversely, the continued availability of credible alternative solutions, interoperability with other infrastructures, and the absence of exclusivity or foreclosure mechanisms would weigh against such a finding. The assessment is therefore dynamic and contingent on how CircPlastX evolves in

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

practice, particularly regarding market uptake, regulatory embedding, and control over strategically significant datasets.

From a data governance perspective, this implies that CircPlastX should be designed and operated in a manner that preserves **safeguards against dominance** including objective and transparent participation criteria, non-discriminatory access conditions, and governance rules that avoid favouring specific participants or downstream activities. Such safeguards serve as proportionate, forward-looking risk mitigation and help ensure that the data space's evolution does not give rise to competition-law concerns should its market position change over time.

2.4.3 Digital Markets Act

2.4.3.1 Overview

Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (the Digital Markets Act or "DMA")[56] introduces an ex ante regulatory framework for large digital platforms designated as "gatekeepers". It applies only to undertakings that (i) meet specific quantitative thresholds and qualitative criteria demonstrating entrenched and durable market power and (ii) are formally designated by the European Commission as gatekeepers with respect to specific *core platform services* (Articles 3-4 DMA). The European Commission maintains a public list of designated gatekeepers and the core platform services, for which they are subject to the DMA obligations.[57]

Designated gatekeepers are subject to a set of obligations and prohibitions aimed at preventing unfair practices and ensuring contestability, including restrictions on self-preferencing, obligations to enable data access or data portability, and limits on combining personal data across services.

The DMA is also relevant in the broader data governance landscape because the Data Act expressly takes gatekeeper status into account when defining the scope and limits of certain data access and data sharing rights. In particular, the Data Act restricts or conditions the sharing of data with gatekeepers in specific scenarios in order to prevent the reinforcement of entrenched market power. The DMA and the Data Act therefore operate in a complementary manner.

2.4.3.2 Relevance for data spaces and data governance

The DMA does not apply to data spaces. By design, data spaces do not provide core platform services that function as important gateways for business users to reach end users. In particular, data spaces do not facilitate direct transactions with consumers

[56] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), *OJ L 265, 12.10.2022, pp. 1–66, http://data.europa.eu/eli/reg/2022/1925/oj*.

[57] The list is available at: https://digital-markets-act.ec.europa.eu/gatekeepers_en.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

and therefore cannot qualify as online intermediation services within the meaning of the DMA.

As a result, data spaces cannot meet the cumulative criteria required for gatekeeper designation under Article 3 DMA.

From a data governance perspective, this non-applicability means that data spaces are not subject to the DMA's ex ante obligations, such as mandatory data sharing with competitors, data portability requirements vis-à-vis business users, or restrictions on combining personal data across services.

2.4.3.3 Applicability to CircPlastX

CircPlastX does not fall within the scope of the DMA, as it does not provide a core platform service that enables business users to reach end users and therefore cannot qualify as a gatekeeper.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.5 Trust and Identity management

2.5.1 eIDAS / eIDAS 2.0

2.5.1.1 Overview

Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation),[58] as amended in 2024,[59] establishes a harmonised legal framework for **electronic identification** and **trust services** with the objective of ensuring secure and trustworthy electronic transactions across the Union. As set out in Article 1, the Regulation lays down rules on electronic identification and trust services in order to ensure the proper functioning of the internal market and to enable secure electronic interactions between natural and legal persons.

With regard to **electronic identification**, Articles 6 and 7 require Member States to recognise electronic identification means that were issued under a notified electronic identification scheme of another Member State for access to online public services, provided that the notified scheme meets at least the assurance level required domestically. In other words, with respect to electronic identification, the eIDAS Regulation establishes a nondiscrimination principle between notified electronic means of identification for e-government services: where a means of identification from another Member State is at least equally reliable as the domestic one, it must be accepted by the e-government service as well.

Article 8 defines three assurance levels (low, substantial and high), reflecting the degree of confidence in the identification process from a technical, legal and governance perspective. Articles 9 to 12 regulate the notification and assessment of national electronic identification schemes. Together, these provisions establish a system of mutual recognition of electronic identification means for cross-border public services, while leaving Member States discretion as to whether and which schemes they choose to notify.

With respect to private sector services, the eIDAS Regulation does not set any binding obligations: private sector service providers (such as e.g. banks) are not required to accept means of identification that have been notified under the Regulation; nor are non-notified means of identification regulated at all.

In parallel, the Regulation establishes a comprehensive framework for **trust services**. Article 3 defines trust services as electronic services that create, verify or validate

[58] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, pp. 73–114, http://data.europa.eu/eli/reg/2014/910/oj.

[59] 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, OJ L, 2024/1183, 30.4.2024, http://data.europa.eu/eli/reg/2024/1183/oj.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

electronic data and that are used to ensure the reliability of electronic transactions. The original Regulation (prior to its 2024 amendment which is discussed below) governed, inter alia, electronic signatures (Articles 25–28), electronic seals (Articles 35–37), electronic timestamps (Articles 41–42) and electronic registered delivery services (Articles 43–44). It distinguishes between non-qualified and qualified trust services, with qualified trust services being subject to stricter requirements, including conformity assessment and supervision by national authorities (Articles 20–24). Qualified trust services benefit from specific legal effects and presumptions across the Union. By way of example, qualified electronic signatures are automatically deemed to be legally equivalent to handwritten signatures.

The 2024 amendment of the eIDAS Regulation (via Regulation (EU) 2024/1183) significantly revised and expanded this framework, in several ways. It added new categories of trust services (including electronic archiving, electronic ledgers, and electronic attestions of attributes), revised the governance of trust services, and introduced a European Digital Identity Framework, based on European Digital Identity Wallets (EUDIWs).

On the latter point, Article 5a obliges Member States to ensure the availability of at least one European Digital Identity Wallet, free of charge, enabling users to store and present person identification data, credentials and electronic attestations of attributes, and to create qualified electronic signatures. The amended Regulation emphasises user control, data minimisation and privacy-preserving authentication, including the use of pseudonyms where identification is not legally required (Article 5a(4)–(16)).

Significantly (and unlike the original eIDAS Regulation), the legal significance of EUDIWs is not limited to public sector services, as the amended eIDAS Regulation specifies that EUDIWs must also be accepted by private sector companies[60] (except microenterprises and small enterprises) if they are required by Union or national law to use strong user authentication for online identification, or where strong user authentication for online identification is required by contractual obligations (Article 5f(2). This acceptance obligation applies as of December 2027.

Overall, eIDAS and its revision establish a horizontal legal infrastructure for electronic identification and certain trust services in the Union. Rather than regulating specific sectors or business models, the Regulation provides common legal building blocks that support trustworthy digital interactions while allocating responsibility and liability for identity verification, authenticity and integrity to clearly defined actors within a harmonised framework.

[60] The obligation is not limited to specific sectors. While the Article states that it applies "*including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunication*", these are non-exhaustive examples of affected sectors, as indicated by the word "including".

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

2.5.1.2 Relevance for data spaces and data governance

eIDAS and eIDAS 2 are relevant to data spaces because they provide the EU's common legal framework for trust in digital interactions. At a basic level, data spaces bring together different organisations so that data can be used in a controlled and reliable way. For this to work, participants need to know who they are dealing with, whether digital information really comes from the stated source, whether it has been changed, and whether electronic records can be relied upon in legal or regulatory contexts. eIDAS addresses exactly these questions by setting EU-wide rules on electronic identification and on trust services such as electronic signatures, seals, timestamps and electronic attestations of attributes.

From a data governance perspective, eIDAS helps data spaces by offering standard ways to verify identity and authority. The Regulation organises how electronic identification can be recognised across borders and introduces common assurance levels. Although private platforms are generally not obliged to accept national electronic IDs, the framework provides a reference model for building access and authentication rules.

With eIDAS 2 (i.e. the 2024 revision of the eIDAS Regulation), the relevance becomes more concrete through the European Digital Identity Wallet, which allows users to prove who they are or to present trusted digital credentials and attributes under their own control. Over time, this can support data space governance by reducing the need for custom identity solutions and by making cross-border participation easier.

The reinforces this relevance by introducing the European Digital Identity Wallet and a legal framework for electronic attestations of attributes. These elements are particularly pertinent for data space governance because they support role-based and attribute-based access models, where participants may need to demonstrate specific capacities, qualifications or organisational roles rather than disclose full identity details. In governance terms, this enables more granular and privacy-preserving access control, aligned with data minimisation principles, while relying on legally recognised trust mechanisms rather than informal declarations.

Finally, eIDAS influences how responsibilities are distributed in a data space. By relying on legally recognised trust services, a data space can position itself as a neutral environment that facilitates access and processing, while the accuracy and authenticity of information remain with the participants who issue or sign it. This helps clarify roles and supports trust among participants.

2.5.1.3 Applicability to CircPlastX

The eIDAS Regulation is potentially relevant and applicable to CircPlastX, although its impact differs with respect to electronic identification and trust services; and, its applicability partially depends on future implementation choices.

Firstly, with respect to **electronic identification,** the eIDAS Regulation is a potentially relevant toolbox that can facilitate some of the functioning of the CircPlastX platform, although the Regulation doesn't apply directly. It is relevant, because any trusted data exchange platform requires reliable identification and authentication of its users, and the eIDAS Regulation provides usable building blocks that could be integrated into the

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

architecture. Both notified eID schemes and future EUDIWs could be used to identify and authenticate users of the CircPlastX platform at a high level of reliability, in a manner that is likely to be conducive to fostering trust across the EU. Even when not using such notified eIDs or EUDIWs, the requirements defined by the eIDAS Regulation to determine the trustworthiness of electronic identification solutions could provide a useful starting point for CircPlastX' own user identification approach.

However, this relevance should not be overstated either. An important constraint is that the eIDAS identification model is strongly focused on (and in practice nearly limited to) the identification of natural persons, rather than companies or systems. While this can be relevant to CircPlastX as well, the principal actors of interest are the legal entities that share data via the platform. While the eIDAS solutions are suitable for identifying individual persons, they are less inherently suitable for determining any mandate that those users might have in relation to their companies. Nor is eIDAS a particularly useful framework for enabling direct machine to machine interactions on behalf of companies (i.e. for automated exchanges of data between companies without the intervention of an individual).

Additionally, it is also important to recognise that the eIDAS Regulation doesn't apply automatically to CircPlastX: it is not an e-government service (which is a prerequisite for the applicability of the eIDAS rules on notified electronic identification schemes), nor is strong user identification a legal obligation for the data exchanges that CircPlastX aims to enable (which is a prerequisite for the applicability of the eIDAS rules on EUDIWs). While it would be possible to make the use of eIDAS identification solutions mandatory via the CircPlastX rulebook/ governance framework, this is an inherently contractual solution, for which the suitability should be evaluated at a later stage.

Secondly, with respect to **trust services,** CircPlastX is likely to incorporate several of these regulated services. Trusted data exchanges will generally require the application of electronic seals (to automatically sign datasets and thus attest to their authenticity and integrity) and electronic time stamps (to provide evidence showing when data was created, sent or received). If CircPlastX chooses to acquire these from a commercial service provider, these will be trust services within the scope of the eIDAS Regulation. If CircPlastX instead chooses to create these itself, as internal services that are not offered to third parties outside of CircPlastX, then the eIDAS Regulation will not apply, since the seals and timestamps will not be available as independent economic services.

Perhaps most importantly in the long term, however, is the legal framework for electronic attestations of attributes in the eIDAS Regulation. Essentially, these attestations are digital statements that allows certain attributes – i.e. characteristics of a person or object - to be authenticated. Attestations thus include statements in relation to companies, or substances, including characteristics of chemical substances or plastics. Any entity that issues such attestations as an economic activity is a trust service in the sense of the eIDAS Regulation. Thus, depending on future architectural choices, CircPlastX may be a platform for the receipt, storage, validation and exchange of such attestations (without becoming an issuer of them), in which case it interacts with regulated trust services under the eIDAS Regulation); or alternatively it may become a trust service provider itself if it starts offering trusted declarations (i.e. attestations in the sense of the eIDAS Regulation) in relation to users of the CircPlastX

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

platform, or in relation to substances or compounds for which CircPlastX holds trusted information. In those instances, the eIDAS Regulation will apply to CircPlastX itself, and it will need to adhere to the Regulation's requirements in relation to trust services, including with respect to security obligations and incident handling.

To complete the picture, it is also worth highlighting that the Commission published a **proposal for a Business Wallet Act** in November 2025[61]. As a complement to the eIDAS Regulation's framework for EUDIWs, the Business Wallet Act would require most companies in the EU to obtain a Business Wallet, allowing them to store and exchange attestations with other companies and public administrations, among other functionalities. This proposal will not be analysed in significant detail in the present deliverable, since it its future is still uncertain; but if adopted, it is clear that any data space targeted towards businesses (including CircPlastX) would need to be interoperable with such Business Wallets, since the proposal frames them as the central way for businesses to manage trusted data exchanges whenever this is legally mandatory.

[61] Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets. COM/2025/838 final https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025PC0838 accessed 11/02/2026.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

3. Sector-specific legal framework

The sector-specific legal framework for plastics is vast, encompassing a great number of EU-level legal acts (from regulations and directives to European Commission's implementing acts) and many national laws. In this Section, we provide an overview of only a handful of EU-level legislations that are deemed the most relevant for the CircPlastX project. The selection covers, on the one hand, the legislations that address all plastics in circulation in the EU and, on the other hand, the legislations relevant for the value-creation services that are to be developed by the project, as described in Deliverable 1.1.

In short, the CircPlastX data space aims to accelerate circularity and safety of plastics on the EU market. This acceleration should take place on different levels, ranging from administrative burden release and regulatory compliance for companies and SME to easier uptake of recycled materials for plastics manufacturers to better traceability and transparency of materials and substances in plastics towards auditors and the wider society. Besides the creation of a better digital connection and data accessibility between different parties along the value chain, we foresee three specific services to help this acceleration: traceability and certification of recycled content, qualification of lifecycle analysis datasets and the sharing of - or offering access to those datasets, and services that help enlarge datasets concerning substances and guidance for compliance and production-and well as recycling guidance.

3.1 Regulation concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)

3.1.1 Overview

EU Regulation 1907/2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)[62] is the main and most comprehensive legislation aiming to protect human health and the environment from the risks posed by chemicals. REACH applies to all chemicals manufactured and placed on the EU market, regardless of the sector and purpose of their use.

The responsibility to manage risks from chemicals and to provide safety-related information lies with the industry. The industry (e.g. manufacturers, importers) must identify and manage risks linked to chemicals, demonstrate to the European

[62] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC, OJ L 396 30.12.2006 (in the most recently amended version of 8 August 2025): https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02006R1907-20250901.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Chemicals Agency (ECHA) how they can be safely used and communicate risk management measures to users. To effectuate this, REACH places data sharing obligations on parties in the chemicals supply chain, and restricts what substances can be used in the market.

Data sharing obligations under REACH arise mainly in two situations: 1) registration of a substance[63] with the ECHA, and 2) safety and risk management up and down the supply chain. The following sections examine the dynamics of the data sharing processes and the nature of the data being shared. In addition, the final section will highlight the ways in which REACH restricts the use of chemicals.

3.1.2 Registering substances with the ECHA

Article 5 REACH requires the registration of substances with the ECHA if they are manufactured or placed on the market in the EU. The purposes of ECHA registration are manifold. On the one hand, as a precondition for placing substances on the market, registration allows to restrict or prohibit the use of certain chemicals from market access. This also enables regulatory oversight over the types and amount of chemicals on the EU market. On the other hand, data sharing related to registration incentivises collaboration within the industry, may allow for cost reduction of testing and helps to avoid unnecessary animal testing through data and information sharing.

3.1.2.1 Actors with obligations related to data sharing

The responsibility for registration lies with the party intending to place the substance on the market, which could be a **manufacturer or an importer**, and, in specific cases, **a producer or an importer** of an article containing the substance in accordance with Article 7 REACH. This means that these actors are under the obligation to disclose and share the necessary data (see Section 3.1.2.2) towards the ECHA via the ECHA CHEM database.[64]

However, manufacturers, importers and producers that are potential registrants have an obligation to actively seek information related to their substances. Prior to registration, potential registrants have a duty to inquire with the ECHA whether a registration has already been submitted for the same substance (Article 26(1) REACH). If this is the case, study summaries submitted at least 12 years previously can be re-used for the purposes of registration by another registrant (Article 25(3) REACH).

The ECHA, as the competent authority, plays a central role in data sharing related to registrations. If prior registrations for the substance exist, the ECHA will inform the relevant parties of each other's contact information, so that they may come to an

[63] REACH distinguishes substances, mixtures containing a substance, and articles containing a substance; for brevity, we will typically only mention substances, unless the distinction is relevant to the point at hand.
[64] See the web portal: https://chem.echa.europa.eu/.

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

agreement on the ways and cost sharing for sharing the relevant data. According to Article 27(6) REACH, "[t]he previous registrant(s) shall have a claim on the potential registrant for a proportionate share of the cost incurred by him" (see also Chapter 5 of the ECHA guidance on data sharing).

Figure 1 shows a flowchart diagram of how the inquiry process works and the manner in which different actors are involved.

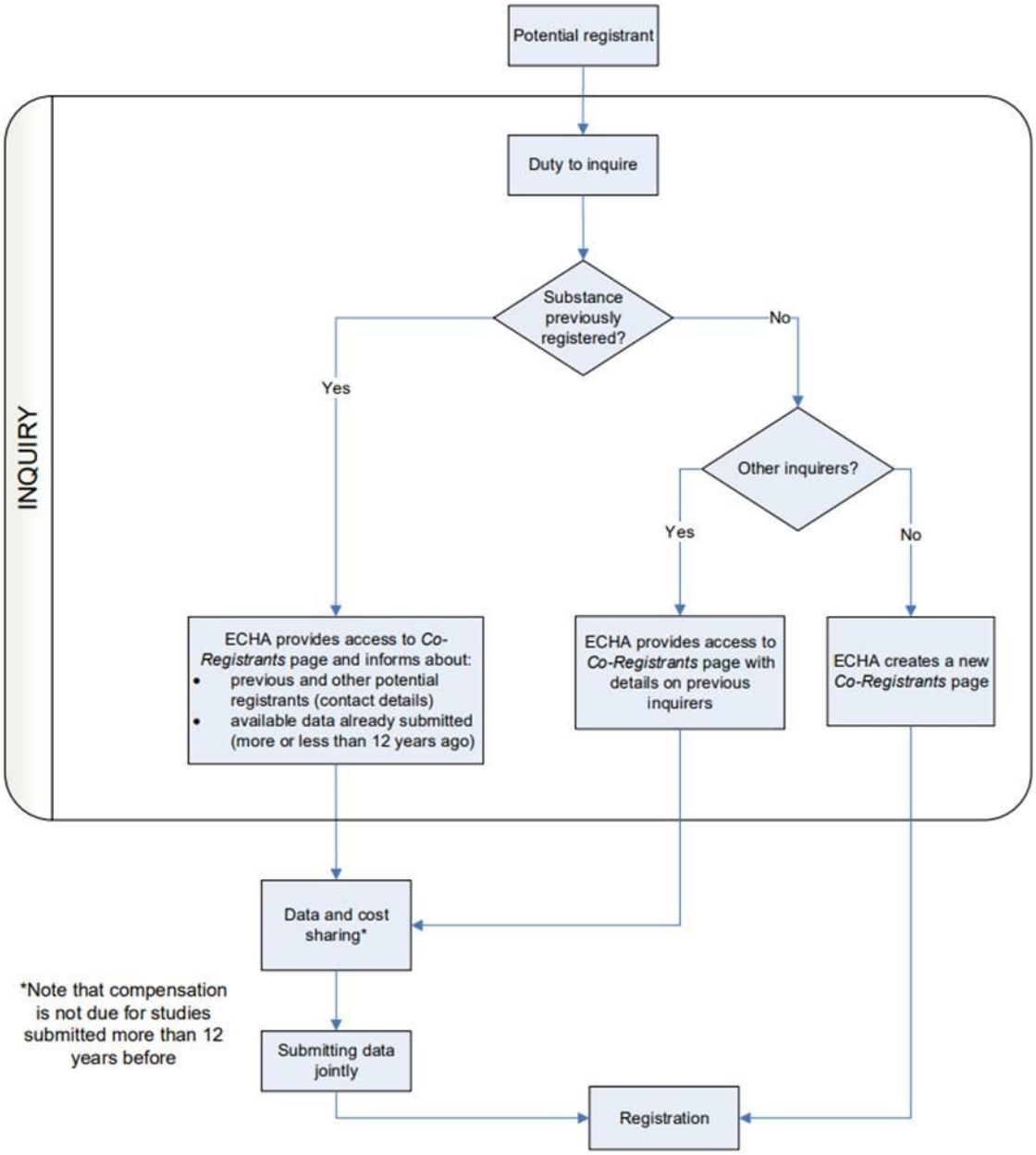

Figure 1: ECHA guidance for inquiry[65]

[65] Source: ECHA (2023). Guidance on data sharing, Version 4.1, p. 40: https://echa.europa.eu/documents/10162/2324906/guidance_on_data_sharing_en.pdf/545e4463-9e67-43f0-852f-35e70a8ead60

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

3.1.2.2 Data to be shared for registration

Article 10 REACH lists the information requirements for registrants by naming only the categories or types of data to be provided, whereas REACH Annexes detail all the data points with great specificity. The data categories are:

- Technical dossier including:
    - the identity of the manufacturer(s) or importer(s),
    - the identity of the substance to be registered,
    - information on the manufacture and use(s) of the substance, including relevant use and exposure categories,
    - the classification and labelling of the substance,
    - guidance on safe use of the substance,
    - (robust) study summaries related to testing and proposals for testing,
    - an indication as to whether the information mentioned in the previous points has been reviewed by an assessor chosen by the registrant and having appropriate experience,
    - a request for non-publication of certain information, including a justification as to why publication could be harmful to the registrant's or any other concerned party's commercial interests.
- Chemical safety report for registrations of substances in quantities exceeding 10 tonnes or more per year per registrant (Article 14 REACH), including:
    - assessments to human, physiochemical, and environmental hazards,
    - assessments of persistent, bioaccumulative and toxic (PBT) and very persistent and very bioaccumulative (vPvB) status of substances.

As mentioned above, the detailed requirements for the data and information to be included in the registration dossier are described in the REACH Annexes. Hence, the quality of information to be submitted is strictly and comprehensively regulated by the legislator.

3.1.3 Sharing safety data up and down the supply chain

The REACH provisions related to sharing of safety and risk management data are paramount for consumer protection, for ensuring the health and safety of workers handling dangerous substances and for protection of the environment. Hence, the data sharing requirements are comprehensive both in relation to the actors involved and the data shared.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

3.1.3.1 Actors involved in safety data sharing

Under Title IV REACH, parties in the supply chain have a responsibility to share data relating to safety and risk management measures. Data flows are required both up and down the supply chain.The terminology used by REACH is that of **supplier** of a substance and the **recipient** of what is being supplied. Additionally, REACH mentions the roles of **manufacturer** or **importer** for the supplier, and **downstream user** or **distributor** roles that can apply to both the supplier and the recipient. Downstream users are required under some conditions to share data also to the ECHA.

Depending on the situation, there are several kinds of data sharing requirements to be met. The most stringent requirement is when a supplier must share a safety data sheet (SDS), which reflects the outcomes of a chemical safety assessment. The detailed requirements of the SDS are codified in Annex II REACH; we will discuss them further below.

Suppliers of a substance must share an SDS with the recipients, if any of the following applies (Article 31(1) and (3) REACH):

1. a substance or mixture meets the criteria for classification as hazardous in accordance with Regulation (EC) No 1272/2008 on classification, labelling and packaging of substances and mixtures,

2. a substance meets the criteria for Annex XIII REACH on persistence, bioaccumulativeness and toxicity of substances,

3. a substance is included in the list established in accordance with Article 59(1) REACH, which lists substances under consideration for inclusion in Annex XIV REACH, which lists substances whose placement on the market or use are subject to authorisation by the ECHA, or

4. the SDS has been requested by the recipient and the substance falls under the criteria set out in Article 31(3) REACH, which entail that the substance poses human health or environmental hazards or that there are Community workplace exposure limits set for the substance.

An exception to the obligation to supply a SDS applies “where hazardous substances or mixtures offered or sold to the general public [and] are provided with sufficient information to enable users to take the necessary measures as regards the protection of human health, safety and the environment” (Article 31(4) REACH).

Conversely, any actor in the supply chain who becomes aware of new information relevant to safety or risk management considerations is obligated to communicate it to the next actor up the supply chain. Figure 2 illustrates the sharing of safety data between the supplier of a substance and the recipient.

Co-funded by the European Union

This project receives funding from the European Commission’s Digital Europe Programme under Grant Agreement Number 101195258.

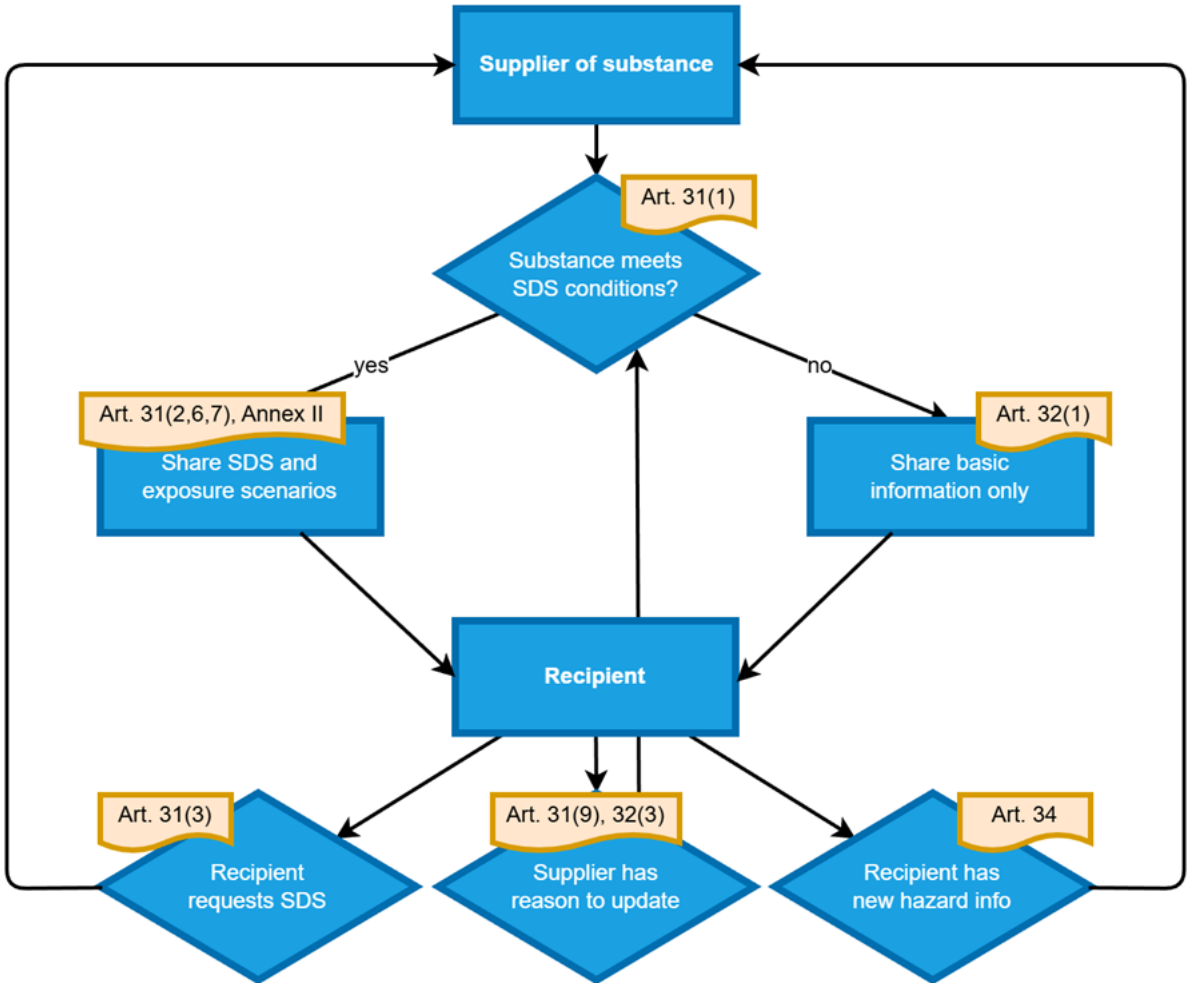

Figure 2: Flow diagram for sharing SDS downstream

In the case that a supplier is not required to share a SDS, they must nevertheless share several pieces of information about the substance. This information includes details about the registration, authorisation and restriction status of the substance. In addition, it includes any other available and relevant information about the substance that is necessary to enable appropriate risk management measures, for which Article 32(1)(d) REACH refers to Annex XI REACH, Section 3, titled “Substance-tailored exposure-driven testing”.

Title V REACH discusses rights and obligations of downstream users. Downstream users can make it known to their suppliers that they have a new use of a substance, which was not yet discussed in the supplier’s safety report or data sheet. This information is passed up the supply chain to a party that can prepare an exposure scenario or exposure category in support of a chemical safety assessment. Article 37(4) REACH requires downstream users to prepare chemical safety reports for uses falling outside the recommendations or safety information provided by their suppliers, and where certain tonnage and hazard thresholds are met. In cases where Article 37 REACH applies, Article 38 REACH states that downstream users are obligated to report to the ECHA about their identity, the substance and its uses, and the need for any additional testing to complete chemical safety assessments.

Co-funded by the European Union

This project receives funding from the European Commission’s Digital Europe Programme under Grant Agreement Number 101195258.

3.1.3.2 Data to be shared

As discussed above, a major type of data defined by REACH is the SDS, which reflects the outcomes of a chemical safety assessment. The SDS must enable users to take the necessary measures relating to protection of human health and safety at the workplace, and protection of the environment. The detailed requirements for the contents of the SDS are listed in Annex II REACH, with further guidance, including an explanation of each field in the data, provided by the ECHA.[66] To give an impression of the comprehensive information to be included in the SDS, its main sections are listed in Table 1 below. Each section contains two to seven specific information points that must be addressed.

SECTION 1: Identification of the substance/mixture and of the company/undertaking
SECTION 2: Hazards identification
SECTION 3: Composition/information on ingredients
SECTION 4: First aid measures
SECTION 5: Firefighting measures
SECTION 6: Accidental release measures
SECTION 7: Handling and storage
SECTION 8: Exposure controls/personal protection
SECTION 9: Physical and chemical properties
SECTION 10: Stability and reactivity
SECTION 11: Toxicological information
SECTION 12: Ecological information
SECTION 13: Disposal considerations
SECTION 14: Transport information
SECTION 15: Regulatory information
SECTION 16: Other information

Table 1: Sections of the Safety Data Sheet, following Annex II REACH.

Many of the requirements for the SDS listed in Annex II refer to other regulations, particularly Regulation (EC) No 1272/2008. There are also some references to other REACH Annexes. This includes Annex XIII REACH, which "lays down the criteria for the identification of persistent, bioaccumulative and toxic substances (PBT substances), and very persistent and very bioaccumulative substances (vPvB substances)." In addition, Annex II REACH states twice that "[f]or substances subject to registration, summaries of the information derived from the application of Annexes VII to XI of this Regulation shall be [included]". As discussed above in the context of registration of substances, Annexes VII to X REACH are the general information requirements for various quantity classes, and Annex XI REACH specifies the

[66] ECHA (2020). Guidance on the compilation of data safety sheets, version 4.0: https://echa.europa.eu/documents/10162/2324906/sds_en.pdf/01c29e23-2cbe-49c0-aca7-72f22e101e20?t=1608126237610. See also ECHA's general page on safety data sheets: https://echa.europa.eu/safety-data-sheets accessed 27/02/2026.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

conditions under which the standard testing regimes of Annexes VII to X REACH can be adapted.

3.1.4 Considerations for a compliance service

In support of the CircPlastX ambition of providing a substance compliance checking service, this section discusses some mechanisms in REACH to prohibit the use of chemicals, or to restrict their use to specific conditions. As discussed before, registration is one such mechanism; any manufacturer or importer should register the substance with the ECHA before placing it on the market.

Title VII REACH states that some substances can only be used if a party has received authorization from the ECHA to do so. The substances for which authorization is required are listed in Annex XIV REACH. Criteria for inclusion in this list are based on classifications by Regulation (EC) No 1272/2008 and by Annex XIII REACH (Article 57 REACH). According to Article 62 REACH, manufacturers, importers and downstream users of a substance can apply to the ECHA for an authorization for using the substance. Authorization extends to parties down the supply chain from the authorized party (Article 56(2) REACH).

Lastly, Title VIII REACH regulates the conditions under which certain dangerous substances can be used. Unlike the authorization dynamic discussed above, restrictions on the use of these substances are not dependent on a party's authorization status but apply "Community-wide". The relevant substances and their conditions of use are listed in Annex XVII REACH.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

3.2 Regulation on Ecodesign Requirements for Sustainable Products (ESPR)

3.2.1 Overview

The Ecodesign Requirements for Sustainable Products Regulation (ESPR)[67] provides a framework for setting and assessing ecodesign requirements for a wide range of products. The ecodesign requirements apply to any physical product (with some exceptions) put into service or placed on the EU market. The ecodesign requirements will be specified in the Commission's delegated acts either for a specific product group or horizontally for several product groups.

The ESPR also introduces a digital product passport (DPP), which could be described as a digital identity card for products, components and materials. The DPP must be made available for any product, put into service or placed on the EU market, and should store all relevant information regarding the product, in accordance with a delegated act adopted pursuant to Article 4 ESPR, in electronic form. The information to be included in the DPP will depend on the specific product and can range from technical performance, materials and their origins, to repair activities and recycling capabilities and to life cycle environmental impacts. The information from the DPP should be accessible for consumers, various authorities and companies along the value chain to improve the sustainability and circularity of the product and to ensure regulatory compliance.

The ESPR entered into force in July 2024. However, its application is staggered and also depends on the European Commission adopting the necessary implementing and delegated acts. For the development of ecodesign requirements, the European Commission created a working plan for 2025-2030,[68] prioritising certain product groups (e.g. textiles, tyres, mattresses). With regards to DPP, the European Commission is supposed establish and maintain a DPP registry by 19 July 2026 where at least the unique identifiers can be stored. The first group of products to get a mandatory DPP is batteries with capacity of more than 2 kWh, electric vehicles batteries and light means of transport batteries under Regulation (EU) 2023/1542, which must have the battery passport (similar to the DPP) from 18 February 2027.[69] Toys are expected to have a DPP under the Toy Safety Regulation starting from 1

[67] Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC, OJ L, 2024/1781, 28.6.2024: https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng.

[68] Communication from the Commission, Ecodesign for Sustainable Products and Energy Labelling Working Plan 2025-2030, COM(2025) 187, 16.4.2025: https://environment.ec.europa.eu/document/download/5f7ff5e2-ebe9-4bd4-a139-db881bd6398f_en?filename=FAQ-UPDATE-4th-Iteration_clean.pdf accessed 27/02/2026.

[69] Article 11 in conjection with Article 96(2) of the Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC, OJ L 191, 28.7.2023: https://eur-lex.europa.eu/eli/reg/2023/1542/oj/eng.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

August 2030.[70] Another group of products for which DPP is expressly foreseen by legislation in force is construction products.[71] The relevant Regulation applies from 8 January 2026, but the exact deadline for the DPP is not specified. The deadlines for other product groups are yet unclear.

3.2.2 Actors in the value chain to whom the DPP is relevant, and their rights and obligations related to DPP data

The fulfilment of obligations regarding the DPP requires data sharing and data-related cooperation between a great number of actors across the value chain of a specific product. Below, we describe the actors involved and indicate their direct obligations and rights in relation to data sharing. This description is relevant for the identification of stakeholders and their interests for their participation in a data space, such as CircPlastX.

- **Economic operator placing the product on the market** (i.e. manufacturer, its authorised representative, importer, see Articles 27-29 ESPR): obligation to make the DPP available for the relevant product and to store the DPP.
- **DPP service providers**: obligation to process the DPP data for the purpose of making such data available to relevant economic operators and other actors (i.e. obligation to host the DPP and/or the back-up copy of the DPP); obligation not to sell, reuse or process DPP data, in whole or in part, beyond what is necessary for the provision of the relevant storing or processing services, unless specifically agreed otherwise with the economic operator placing the product on the market.
- **Customers, manufacturers, importers, distributors, dealers, professional repairers, independent operators, refurbishers, remanufacturers, recyclers, market surveillance authorities and customs authorities, civil society organisations, trade unions and other relevant actors**: right to access the DPP data free of charge and based on their respective access rights set out in the applicable delegated act adopted pursuant to Article 4 ESPR; depending on the applicable delegated act, some of these actors may also have the right to introduce, modify or update the DPP data.
- **Consumers**: right to access the information in the DPP as per the relevant delegated act by the European Commission and free of charge. The DPP must be accessible before the customer is bound by a contract for sale, hire or hire purchase, including in the case of distance selling.
- **Public authorities** (e.g. customs authorities, market surveillance authorities): right to access the information in the DPP free of charge as necessary for the exercise of their mandate.

[70] Chapter V and Article 59 of the Regulation (EU) 2025/2509 of the European Parliament and of the Council of 26 November 2025 on the safety of toys and repealing Directive 2009/48/EC, OJ L, 2025/2509, 12.12.2025: https://eur-lex.europa.eu/eli/reg/2025/2509/oj/eng.
[71] Chapter X and Article 96 of the Regulation (EU) 2024/3110 of the European Parliament and of the Council of 27 November 2024 laying down harmonised rules for the marketing of construction products and repealing Regulation (EU) No 305/2011, OJ L, 2024/3110, 18.12.2024: https://eur-lex.europa.eu/eli/reg/2024/3110/oj/eng.

Co-funded by the European Union
This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

3.2.3 Data to be shared

This section identifies categories of data to be shared between the DPP stakeholders. The precise data items (or data points) cannot be specifically named and listed at this stage because their final list will be determined by the European Commission in delegated acts separately for different (groups of) products.

Based on Article 9 ESPR, which sets out what DPP requirements can be established via delegated acts, and Annex III ESPR, which further enumerates the types of information that may be required as per Article 9(2) ESPR, the following data categories can be identified:

1. **General product and producer information**: the unique product identifier; the Global Trade Identification Number; relevant commodity codes, such as a TARIC code; information related to the manufacturer (e.g. unique operator identifier); unique operator identifiers other than that of the manufacturer; unique facility identifiers; information related to the importer (e.g. Economic Operators Registration and Identification (EORI) number); the name, contact details and unique operator identifier of the economic operator established in the EU and responsible for obligations related to product safety and market surveillance; the reference of the DPP service provider hosting the back-up copy of the DPP.
2. **Information related to the use of the product**: user manuals, warnings or safety information applicable to the product due to legal requirements; digital instructions concerning the product in a language that can be easily understood, as determined by the Member State concerned.
3. **Compliance and conformity documentation**: compliance documentation and information required by EU law applicable to the product (e.g. the declaration of conformity, technical documentation or conformity certificates).
4. **Information on substances of concern under Article 7(5) ESPR (at a minimum)**: substance of concern are defined by the ESPR through reference to the REACH Regulation, the Classification, Labelling and Packaging Regulation and the Persistent Pollutants Regulation.[72] Generally speaking, these are chemicals with inherent hazards (e.g. carcinogens, mutagens, reprotoxins) or those hindering material reuse and recycling. The DPP must include the following information on them:

[72] Respectively: Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC, OJ L 396, 30.12.2006: https://eur-lex.europa.eu/eli/reg/2006/1907/oj/eng; Regulation (EC) No 1272/2008 of the European Parliament and of the Council of 16 December 2008 on classification, labelling and packaging of substances and mixtures, amending and repealing Directives 67/548/EEC and 1999/45/EC, and amending Regulation (EC) No 1907/2006, OJ L 353, 31.12.2008: https://eur-lex.europa.eu/eli/reg/2008/1272/oj/eng; Regulation (EU) 2019/1021 of the European Parliament and of the Council of 20 June 2019 on persistent organic pollutants, OJ L 169, 25.6.2019: https://eur-lex.europa.eu/eli/reg/2019/1021/oj/eng.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

a. the name or numerical code of the substances of concern present in the product: name in the International Union of Pure and Applied Chemistry (IUPAC) nomenclature, or another international name when IUPAC name is not available; (ii) other names, including usual name, trade name, abbreviation; (iii) European Community (EC) number, as indicated in the European Inventory of Existing Commercial Chemical Substances (EINECS), the European List of Notified Chemical Substances (ELINCS) or the No Longer Polymer (NLP) list or the number assigned by the European Chemicals Agency (ECHA), if available and appropriate; (iv) the Chemical Abstract Service (CAS) name and number, if available;
b. the location of the substances of concern within the product;
c. the concentration, maximum concentration or concentration range of the substances of concern, at the level of the product, its relevant components, or spare parts;
d. relevant instructions for the safe use of the product;
e. information relevant for disassembly, preparation for reuse, reuse, recycling and the environmentally sound management of the product at end-of-life.

5. **Information requirements under Article 7(2)(b) ESPR**:
   a. Information on the product performance in relation to parameters referred of Annex I ESPR, including a repairability score, a durability score, a carbon footprint or an environmental footprint;
   b. Information for customers and other actors on how to install, use, maintain and repair the product, how to install third-party operating systems where relevant, as well as on collection for refurbishment or remanufacture, and on how to return or handle the product at end-of-life;
   c. Information for treatment facilities on disassembly, reuse, refurbishment, recycling or disposal at end-of life; and
   d. Other information that could influence sustainable product choices for customers, and how the product is handled by parties other than the manufacturer to facilitate appropriate use, value-retaining operations and correct treatment at end-of-life.

6. **DPP System Information under Article 9(2)(b)-(i) ESPR that relate to the functioning of the DPPs**: information on the DPP system may contain role-based access control data (ensuring only authorised actors like manufacturers, recyclers, and market surveillance authorities access specific data), robust update logging (to track data changes over the product lifecycle), and reliable, long-term data availability (to maintain data throughout the product's lifespan).

7. **Requirements for disclosures under other Union law according to Annex III ESPR**: Annex III(a) allows for 'information required […] by other Union law applicable to the relevant product group' to be specified in delegated act on DPP. This means that disclosures of further information via a DPP can be required for specific (groups of) product under existing or upcoming EU law. A specific example is the information on the ecodesign requirements for particular (groups of) products that may be included in the DPP (see Article 5 (1) ESPR

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

for the list of product aspects that can be covered by ecodesign requirements; the list goes from (a) to (p)).

Some of the data categories listed above are likely to contain a large number of data points, potentially coming from different actors within the supply chain of the manufacturer and other actors across the value chain. The TNO report "Method for the definition of requirements for the inclusion of data and information in the Digital Product Passport" of 2025 contains an Annex with an indicative list of 131 data items based solely on the ESPR text.[73]

Importantly, personal data relating to customers shall not be stored in the DPP without their explicit consent according to the GDPR.

3.2.4 Quality of and access to data

The data in the DPP shall be accurate, complete and up to date. It must be maintained in this manner for the period specified in the delegated act relevant for the specific product. This period will be at least the expected lifetime of a specific product. The DPP shall remain available even after an insolvency, a liquidation or a cessation of activity in the Union of the economic operator responsible for the creation of the DPP.

All data in the DPP shall be based on open standards, developed with an interoperable format, and shall be machine-readable, structured, searchable, and transferable through an open interoperable data exchange network without vender lock-in.

Actors along the value chain of the product should be able to easily access and understand product information relevant to them. In this context, the access to data in the DPP shall be regulated in the sense that different access rights should apply to different actors and data (defined by legislation and the relevant delegated act). For instance, actors that have the right or obligation to introduce, modify or update data in the DPP must have the relevant access and relevant technical permissions. The DPP must be made available to customers before they are bound by a contract for sale, hire or hire purchase, including in the event of distance selling, and the data in the DPP must be complete before the product is placed on the EU market.

[73] See Chawla, K., Chirvasuta, T., Wolf, M.-A., Wolf, K., Rongen, S. et al., Method for the definition of requirements for the inclusion of data and in-formation in the Digital Product Passport, Publications Office of the European Union, Luxembourg, 2026, JRC145830.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

3.3 Regulation on Packaging and Packaging Waste (PPWR)

3.3.1 Overview

The main aims of the Packaging and Packaging Waste Regulation (PPWR)[74] are to prevent unnecessary packaging, to promote reuse, refill and recycling and to contribute to the circular economy and climate neutrality in the EU.

The PPWR applies to all packaging and packaging waste, regardless of its material or origin (e.g. household waste, industrial packaging and waste). It covers packaging manufactured in the EU and imported. The PPWR sets out the requirements that all packaging placed on the EU market and all operators active in the EU market must meet, such as minimum recycled materials used, single-use plastic utilisation, percentage of packaging to empty space and other.

From the perspective of data sharing across the value chain through a data space and in the context of CircPlastX, the most relevant PPWR provisions relate to:

1. The recyclability and labelling of packaging. Generally speaking, all packaging must become recyclable in the future, meaning that it must be designed for material recycling and can be collected, sorted and recycled at scale. The relevant data and information must be shared with consumers, end users and sorting and recycling facilities. The responsibility for the proper labelling and documentation in relation to packaging and packaging waste lies with the manufacturers and importers, who might need relevant data from suppliers.
2. The share of recycled material in the packaging. This data is necessary for manufacturers and recycling facilities to design for recyclability and to determine, to which recyclability performance grade the packaging belongs. The economic operators are also under obligation to record the shared of recycled materials in their technical documentation and submit this information to the competent authorities as required.

The PPWR will apply from 12 August 2026. However, many details necessary for the economic operators to become compliant with the PPWR will be adopted slightly later. For example, only by 31 December 2026, the European Commission will adopt the implementing acts establishing the methodology for the calculation and verification of the percentage of recycled content recovered from post-consumer plastic waste recycled and collected within the EU and the format for the necessary technical documentation. Standardisation work for the detailed technical specifications of the requirements on compostable packaging will only begin in February 2026. By 1 January 2028, the European Commission will adopt delegated acts establishing design for recycling criteria and recyclability performance grades, how to perform

[74] Regulation (EU) 2025/40 of the European Parliament and of the Council of 19 December 2024 on packaging and packaging waste, amending Regulation (EU) 2019/1020 and Directive (EU) 2019/904, and repealing Directive 94/62/EC, OJ L, 2025/40, 22.1.2025: https://eur-lex.europa.eu/eli/reg/2025/40/oj/eng.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

recyclability performance assessment, and a description of the conditions for compliance with their respective recyclability performance grades for different packaging categories. Many more other relevant implementing and delegated acts by the Commission are scheduled for 2026-2030.

3.3.2 Actors in the value chain involved in data sharing

While most PPWR obligations relate to the manufacturing, use/reuse and disposal of packaging, data sharing across the supply chain and value chain may play an important role in these activities.

- **Manufacturers**:[75] obligation to provide different categories of data/ information to other actors in relation to the material composition of packaging, disposal and reuse of packaging, amount of packaging and packaging waste, and other technical documentation regarding conformity assessment; right to obtain data from the downstream operators necessary to ensure that packaging is recycled at scale.
- **Suppliers** (i.e. economic operators that supply packaging materials to manufacturers): obligation to provide data/ information to manufacturers on material composition of packaging, disposal and reuse of packaging, and any other information and documentation (including technical) that are necessary for the manufacturer to demonstrate the conformity of packaging and packaging materials with the PPWR.
- **Consumers and end-users**: right to access to data/ information related to sorting of packaging waste; compostability of packaging waste; presence of substances of concern; reusability of packaging and the location of collection points.
- **Sorting facilities/ recycling facilities/ waste management facilities**: obligation to provide data to manufacturers as necessary to demonstrate sorting/ recycling at scale; need data on sorting and recyclability to conduct their respective operations effectively.
- **Competent authorities** (e.g. customs, market surveillance): right to access data/ information on packaging and packaging waste according to their mandate.

3.3.3 Data to be shared

The data that need to be shared across the value chain refer mainly to the material composition of packaging and instructions related to its reuse/ recycling and disposal and are to be provided by the manufacturer (although some data items may need to initially come from the supplier to the manufacturer):

- Material composition of packaging with the aim to facilitate sorting, in particular
  - Share of biobased plastic,

[75] We use manufacturers as a stand-in for all economic operators that may place products on the EU market (e.g. importers, distributors, authorized representatives). This is because manufacturers have the widest scope of obligations, including information and data-related obligations.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

    - Share of recycled content,
    - Presence of substances of concern,
- Compostability of the packaging (material) and related instructions (e.g. suitability for home composting, prohibition to discard in nature),
- Whether the packaging is subject to a deposit and return system,
- Destination of each packaging component with the aim to facilitate sorting,
- Reusability of the packaging,
- Information on the local, national or EU-wide reuse system and information on collection points,
- Data on trips and rotations of reuse for reusable packaging,
- Information on the manufacturer (i.e. name, registered trade name or registered trademark, postal address at which, electronic means of communication by which they can be contacted),
- Type, batch or serial number or other element of packaging allowing its identification,
- Compliance and conformity documentation (e.g. the declaration of conformity, technical documentation or conformity certificates).

The list above does not include reporting obligations of economic operators towards various competent authorities.

The exact data to be provided is likely to be influenced by the Commission's implementing acts that will establish a harmonised label and labelling requirements for packaging and the methodology for identifying the material composition (issued by 12 Augus 2026), as well as the methodology for identifying substances of concern (issued by 1 January 2030). In addition, to achieve the overall objectives of the PPWR, Member States may adopt measures related to packaging and packaging waste that could result in more data sharing (requirements).

3.3.4 Quality of and access to data

The PPWR does not contain requirements to the quality of data, but only to the quality of the information provided to the consumers/ end-users of packaging. All information provided shall be easily understandable and clear, including for people with disabilities. These information requirements may have implications for the quality of the underlying data as, for manufacturers and suppliers, it is easier to fulfil them if also the underlying data is standardised and high-quality (e.g. accurate, up-to-date, has sufficient degree of granularity as necessary for reporting, etc.).

The information about the packaging and its disposal, reflecting or based on the data specified above, shall be presented on the packaging through a label. In addition, a QR code or other type of standardised, open, digital carrier can/ shall be placed on the packaging. If the label, QR code or other standard digital marker cannot be affixed to the product due to its size or nature or because of the product's relevance for certain vulnerable groups (e.g. visually impaired), an electronically readable code or similar technology should be used. The general requirements to any type of digital or digital-marking technologies by which access to packaging and packaging waste data is provided are the same, namely that they are standardised and open.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Of a particular importance for importance is the requirement that the information on packaging and packaging waste shall be available to end-users before the purchase of the product online.

A single data carrier must be used for the data on the product and on the product packaging. However, it must be clearly distinguished, whether the data applies to the product or its packaging.

Information on packaging and packaging waste shall be separate from other information intended to sales or marketing purposes. When information is provided by digital means, personal data collection should be limited to the purpose of giving the user access to such information and subject to the GDPR.

3.4 Implications for CircPlastX data space and related services

The sector-specific regulations as mentioned above are a first exposé of a wider range of regulations that will affect – or are already affecting the plastics sector. The focus of the data space is on data sharing on the level of materials, with clear links to relevant data for example digital product passports and the wider efforts on improving and accelerating circularity of materials and products in the European market. While regulation such as the ones highlighted above shape the market on plastics and recycling, they also (often indirectly) shape digital-and data markets. The need for increased transparency and traceability of products and their materials and substances, as well as their journey to end of use and /or end of life demands a digital infrastructure and digital services. Information needs and interests vary in such a circularity-and traceability-chain, where B2B information access and sharing needs to be made ready and accessible for B2C applications.

Sector-specific- and horizontal data regulation are interconnected in the context of circularity and in the development of the *CircPlastX* data space and services. The sector-specific regulation demands companies and organisations to organise and make accessible their internal data and/or to connect and share their data with other entities. For the moment, very little is in place in terms of digital architectures or digital services to help companies and organisations with complying to these regulatory demands. At the same time, a broad set of horizontal regulations exists that defines how such data access and data sharing architectures can be designed.

Within this context, the CircPlastX data space is not a direct addressee of regulatory duties but functions as a **compliance-enabling infrastructure**, supporting participants in meeting their legal obligations through structured, secure, and interoperable data exchange.

We foresee a set of services that help especially SMEs with:

- increasing the uptake of recycled materials by providing certification and traceability data;

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

- alleviating administrative burdens on substances-compliance and potentially monetizing or at least pooling relevant data on substances that can serve a multitude of purposes and ‘data markets’;
- Increasing the data quality and data traceability for Lifecycle analysis (LCA), with a strong connection to the development of Digital Material Passports (DMPs) that will feed into Digital Product Passports (DPPs);

Through these services, CircPlastX enables the practical implementation of regulatory data requirements and supports actors in complying with obligations related to circularity, sustainability, and substances management.

The data space architecture and contractual framework to be developed will underpin the role of intermediary for services and datasets that help accelerate circularity in the plastics-sector.

Co-funded by the European Union

This project receives funding from the European Commission’s Digital Europe Programme under Grant Agreement Number 101195258.

4. Conclusion

This report has examined the European legal framework relevant to the data governance of the CircPlastX data space. It has mapped the interaction between horizontal EU data governance instruments, intellectual property and trade secret protection, data protection rules, competition law, trust infrastructure, and selected sector-specific legislation in the plastics value chain.

As such, it constitutes a first exploration of the implications of the evolving European legislative framework for a sectoral data space in the circular plastics ecosystem. The analysis has led to a set of interim conclusions that reflect the current state of the project and of EU law. As CircPlastX further develops its services, governance model and technical architecture in greater detail, certain legal considerations identified in this report may prove to be less central than anticipated, while additional issues may surface. The conclusions below should therefore be understood as structured guidance for the next phase of the CircPlastX's development rather than as a definitive legal qualification of the final operational model.

4.1 The position of a data space within the regulatory landscape

A recurring finding of this analysis is that a data space such as CircPlastX is often not the direct addressee of regulatory obligations concerning data access or data sharing. At the same time, even where statutory obligations attach to participants rather than to the data space itself, the architecture and governance of the data space must be capable of supporting participants' compliance. This includes enabling lawful data access flows under the Data Act, preserving the conditions under which trade secrets remain protected, accommodating the GDPR role allocation and transparency duties, and ensuring that sector-specific reporting or disclosure requirements can be fulfilled through structured data exchange. In this sense, the data space functions as a **compliance-enabling environment**.

4.2 Interoperability as a legal requirement

The analysis of the Data Act, and in particular Article 33, demonstrates that **interoperability has acquired a normative dimension in EU data governance**. The obligation to ensure discoverability of datasets, semantic clarity, technical accessibility and interoperability of automated sharing tools is anchored in binding law and further concretised through European standardisation processes under the Trusted Data Framework.

For CircPlastX, interoperability therefore forms part of the legal baseline. Metadata structures, semantic assets, access documentation and automated execution mechanisms must be designed with reference to these requirements and in anticipation of emerging harmonised standards. Early alignment reduces the risk of costly architectural adjustments at a later stage and strengthens the credibility of the data space as a trusted European infrastructure.

Interoperability in this context is not merely a technical design preference. It is a condition for lawful and scalable participation in the European data space ecosystem.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

4.3 Trade secret protection as a foundation of trust

The plastics value chain is characterised by **high sensitivity of industrial data** and a strong **reluctance** to share commercially valuable information. The Trade Secrets Directive clarifies that protection depends on secrecy, commercial value and the taking of reasonable steps to preserve confidentiality.

For CircPlastX, this translates into a core governance imperative. Participation terms, access controls, purpose limitation mechanisms, logging and auditability features, and contractual duties to limit use must collectively support the ability of participants to demonstrate that reasonable steps have been taken. Without such safeguards, industrial actors will lack the legal certainty necessary to share data.

Trade secret protection therefore operates as a structural **precondition for trust and participation**. The credibility of the data space depends not only on compliance with formal legal rules but also on the demonstrable robustness of its confidentiality and access management framework.

4.4 Neutrality and non-discrimination as central governance principles

Both the Data Governance Act and EU competition law highlight the importance of neutrality and non-discrimination in multi-actor infrastructures. Where a data space qualifies as a **data intermediation service** within the meaning of the Data Governance Act, additional requirements may apply, including structural separation, strict purpose limitation and fair, transparent access conditions.

Even where formal qualification as a data intermediation service is not established, **neutrality** and **objective access conditions** function as a benchmark for trustworthy governance. Participation criteria, suspension and termination rules, and pricing structures should be transparent and proportionate. This reduces regulatory risk under the Data Governance Act and mitigates potential risks under Articles 101 and 102 TFEU as the data space evolves.

4.5 eIDAS and the European trust infrastructure

The eIDAS framework provides the European legal infrastructure for electronic identification and trust services. Its relevance for CircPlastX depends on architectural and governance choices. The platform may rely on electronic seals, timestamps or electronic attestations of attributes, and it may interact with European Digital Identity Wallets or other notified identification schemes.

At present, these instruments offer building blocks rather than mandatory obligations. However, future developments may increase their practical significance. In particular, the Commission proposal for a Business Wallet Act signals a potential evolution towards mandatory, wallet-based management of trusted business attestations. If adopted, data spaces targeted at businesses would need to ensure interoperability with such wallets, as they would become the central mechanism for managing trusted data exchanges where legally required.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

Trust and identity management should therefore be treated as a strategic governance dimension, closely linked to long-term architectural planning.

4.6 The dynamic nature of the regulatory environment – what should be monitored

The EU data governance framework is evolving rapidly. Horizontal reform initiatives such as the Digital Omnibus may reshape elements of the digital regulatory acquis. Standardisation processes under the Trusted Data Framework and delegated acts under the Data Act and ESPR will further concretise obligations in the coming years.

Continuous monitoring of these developments is therefore necessary. In particular, attention should be paid to:

- the **Digital Omnibus** initiative and any amendments affecting data governance instruments,
- **delegated and implementing acts** under the Data Act and ESPR,
- **standardisation** deliverables under Mandate M/614,
- further legislative progress on the **Business Wallet Act proposal**, and
- evolving guidance from supervisory authorities in the fields of **data protection** and **competition law**.

CircPlastX should integrate regulatory monitoring into its governance roadmap to ensure that its contractual and technical framework remains aligned with the evolving acquis.

4.7 Implications for the next project phase

This report provides the legal foundation for the development of the contractual framework of the CircPlastX data space in the next phase of the project. It clarifies the allocation of regulatory responsibilities and identifies the governance constraints within which participation and service agreements must be structured.

In particular, the forthcoming contractual framework should prioritise the development of clear participation terms and an onboarding framework. At the current stage of the project, this appears more central than the immediate negotiation of complex bilateral agreements. As the services mature and the extent of data intermediation becomes clearer, it will be possible to assess whether additional bilateral or multilateral contractual arrangements are necessary, and to what extent the data space performs functions that may fall within the Data Governance Act's intermediation regime.

4.8 Final observations

Overall, the European legal framework provides both constraints and enablers for the establishment of a sectoral data space in the plastics value chain. It demands structured governance, interoperability, protection of commercially sensitive information, transparency and neutrality. At the same time, it offers harmonised instruments for data access, identity management and cross-border trust.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.

This deliverable serves as an analytical starting point. It maps the legal terrain within which CircPlastX is being developed and identifies the principal axes along which governance choices must be made. As the project advances from conceptual design to operational implementation, the interim conclusions set out here will inform the contractual architecture, the participation model and the technical configuration of the data space, while remaining open to refinement in light of practical experience and regulatory evolution.

Co-funded by the European Union

This project receives funding from the European Commission's Digital Europe Programme under Grant Agreement Number 101195258.