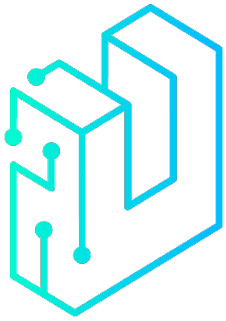

UNDERPIN

DATA SPACE FOR MANUFACTURING

Pan-European data space for holistic asset management in critical manufacturing industries

D5.2 Trust Creation Processes Design

Co-funded by the European Union

This project has received funding from the Digital Europe Programme under grant

Document information			
Project name	Pan-European data space for holistic asset management in critical manufacturing industries		
Project acronym	UNDERPIN		
Grant Agreement No	101123179		
Start / Duration	1/12/2023		
Project Coordinator	MOTOR OIL (HELLAS) DIILISTIRIA KORINTHOU AE		
Deliverable	D5.2 Trust Creation Processes Design		
Work Package	WP5		
Responsible Partner	HUA		
Dissemination level	PU - Public		
Type	Document, Report		
Due date (M)	M12	Actual delivery date	28/11/2024

Document history

Version	Date (DD/MM/YYYY)	Author(s)	Comments / Description
V0.1	1/07/2024	Elena Politi (HUA), George Dimitrakopoulos (HUA)	Initial TOC
V0.2	1/08/2024	Elena Politi (HUA), George Dimitrakopoulos (HUA), Eleni Tsaousi (HUA)	Initial Version of document
V0.3	01/10/2024	Elena Politi (HUA), Eleni Tsaousi (HUA),	Enhanced Version
V0.4	11/10/2024	Lilian Mitrou	Enhanced Version with updates on Chapter 3
V.0.5	14/10/2024	Anil Turkmayali	Enhanced Version with updates on Chapter 2
V0.6	05/11/2024	Roman Karl (AIT), Axelle Gasne	Updates on Chapter 3
V0.7	12/11/2024	Lilian Mitrou, Elena Politi (HUA)	Updates on document
V0.8	18/11/2024	Elena Politi (HUA)	Document ready for internal review
V0.9	25/12/2024	Yannis Stavrakas (ARC), Weißenfeld Axel (AIT), Gasne Axelle (AIT)	Interval review
V1.0	28/11/2024	Elena Politi (HUA)	Final version

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

List of Authors and Contributors

Name	Organisation
Elena Politi	HUA
George Dimitrakopoulos	HUA
Eleni Tsaousi	HUA
Anil Turkmayali	IDSA
Lilian Mitrou	External expert
Roman Karl	AIT
Axelle Gasne	AIT

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

UNDERPIN has received funding from the Digital European Programme under grant agreement No 101123179.

Table of Contents

Table of Contents 5

Executive summary 9

1 Introduction 11

1.1 The UNDERPIN Mission, Vision and Values 11
1.2 Purpose of this document 11
1.3 Relation to other work packages and deliverables 12
1.4 Deliverable structure 12

2 Trust creation processes 15

2.1 Introduction 15
2.2 IDS RAM and Trust Frameworks 16
2.2.1 Data Sovereignty and Usage Control 16
2.2.2 Certified IDS Connectors 17
2.2.3 Identity and Access Management (IAM) 17
2.2.4 Trust Through Transparency and Auditability 18
2.2.5 Legal Agreements and Smart Contracts 18
2.2.6 Interoperability and Alignment with Other Frameworks 19
2.3 Legal and Organizational Framework for Trust 19
2.3.1 Implementing Smart Contracts for Automating Trust 20
2.3.2 Defining Roles and Responsibilities in Data Governance 21
2.3.3 Compliance and Accountability 25

3 Legal Considerations 29

3.1 Data Protection Issues and GDPR 29
3.1.1 Personal Data and other definitions 30
3.1.2 Data Protection Principles 32
3.1.3 Legal grounds for Data Processing and Conditions for Consent 34
3.1.4 Other requirements 36
3.2 DATA GOVERNANCE ACT 38
3.2.1 Objectives, main choices and scope of DGA 38
3.2.2 Definitions 39

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.2.3 Data intermediation services and Data Intermediation Service providers 40
3.2.4 Data Altruism 43
3.2.5 Data Protection issues and the Interplay with GDPR 43
3.2.6 Competition issues 44
3.2.7 European Commission's Guidance for the Data Governance Act 44
1.1 THE DATA ACT 45
3.3 Scope of application 47
3.3.1 Data sharing under Data Act 48
3.3.2 Business-to-business and business-to-consumer data sharing in the context of the IoT market 48
3.4 Smart contracts 53
3.4.1 Concept and types of smart contracts 53
3.4.2 Smart contracts in the Data Act 54
3.4.3 Definition of Smart Contracts 54
3.4.4 Essential requirements regarding smart contracts for executing data sharing agreements 55
3.4.5 Legal requirements for smart contracts 56
3.4.6 Technical requirements for smart contracts and the "Kill switch" 56
3.4.7 Technical Considerations 57
3.5 ARTIFICIAL INTELLIGENCE AND THE ARTIFICIAL INTELLIGENCE ACT 58
3.5.1 Ethical principles and requirements 58
3.5.2 Human autonomy 59
3.5.3 Prevention of harms 59
3.5.4 Fairness 59
3.5.5 Explicability 59
3.5.6 The Artificial Intelligence Act 60
3.6 Concluding remarks and recommendations 63

4 Validation through the Data Space and Next Steps 65

4.1 Validation through Underpin Business Roles 65
4.2 Realisation through UNDERPIN 66

5 Conclusion 68

Bibliography 69

Annexes 70

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

List of Figures

Figure 1: Usage Control in IDS 17
Figure 2: Interaction between IDS Connectors and Identity Components (Source: IDS RAM) 18
Figure 3: Data sharing contract negotiation (Source: IDSA Rulebook) 21
Figure 4: Overview of Data Space entities (Source: IDSA Rulebook) 22
Figure 5: Variants for Data Space Governance Authorities 24

List of Tables

Table 1: Interlinks with other project deliverables 12
Table 2 Mapping of Business roles for UNDERPIN 65

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Acronyms and Abbreviations

AI	Artificial Intelligence
CDB	Communication and Dissemination Board
D	Deliverable
DA	Data Act
DaaS	Data-as-a-Service
DGA	Data Governance Act
DSGA	Data Space Governance Authority
ECHR	European Convention on Human Rights
EU	European Union
GA	General Assembly
GDPR	General Data Protection Regulation
HPC	High-Performance Computing
IDS	International Data Space
IDSA	International Data Spaces Association
RAM	Reference Architecture Model
SMEs	Small and Medium-sized Enterprises
WP	Work Package

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Executive summary

The deliverable D5.2 “Design of trust creation processes” (due on M12) is a public report that provides an in-depth analysis of the legal framework relevant to the UNDERPIN Data Space. Its goal is to lay the groundwork for trust by examining the legal requirements and regulations that will govern data sharing, compliance, and governance within the data space. Deliverable D5.2 is developed under Task T5.1, 'Legal Framework and Good Practices Assessment,' which focuses on evaluating relevant legislation, principles and values regarding the sharing of personal and non-personal, including industrial, data within the context of the targeted sectors throughout the deployment of the UNDERPIN Data Space.

In UNDERPIN, trust will be achieved through a combination of technical, legal, and organizational mechanisms. Data sovereignty is enforced via Usage Control Policies and Certified IDS Connectors, ensuring that data providers retain full control over their data. Smart contracts automate data-sharing agreements, with clearly defined roles, such as Data Providers, Data Users, and with the establishment of the Data Space Governance Authority (DSGA). Smart contracts will enforce data-sharing agreements between parties, ensuring secure, and transparent data transactions. These will ensure that responsibilities are transparent and aligned. Continuous compliance is maintained through audit trails, with the IDS Clearing House providing traceability for data transactions. By implementing these trust mechanisms, UNDERPIN ensures secure, compliant, and transparent data exchanges, fostering reliable collaboration between all participants in the data space.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

1 Introduction

1.1 The UNDERPIN Mission, Vision and Values

The emergent European Data Economy relies on the availability and accessibility of large amounts of data as a basis for further innovation and exponential development of technologies, regarding the European digital (data and technology) sovereignty as well as the development of trustworthy 'made in Europe' AI that reflects European values. The UNDERPIN project aims at providing a sustainable dataspace solution towards carrying out dynamic asset management and predictive/prescriptive maintenance (continuous monitoring and exchanging data on machine status, breakdowns, downtimes, service orders etc.) as an area to unlock deep industrial data for trustworthy and reliable value-added services by parties outside a production site. The UNDERPIN Data Space will thereby provide a cross-organisational data sharing and exchange solution that is secure, trusted and ensures data sovereignty, with a strong focus on the interplay of SMEs and large industry players to enable both to improve products and services. Furthermore, one of the UNDERPIN overall objectives is to incorporate the UNDERPIN outcomes within the European Standardization landscape in the area of Industrial Data Sharing. The solution will comply with EU standards and GAIA-X guidelines, providing a secure framework and tools for data sharing among partners. By facilitating data analysis, the project seeks to enhance operations for stakeholders, including machine tool manufacturers, integrators, vendors, maintenance service providers, remanufacturers, refurbishers, reuse, repair, and recycling companies, as well as governmental, public, research, and civil society entities.

1.2 Purpose of this document

The purpose of D5.2: "Design of trust creation processes" is to provide an analysis of the legal framework, pertinent to the context of the UNDERPIN Data Space. This deliverable aims to establish a foundation for trust by exploring the legal requirements and regulations that will shape data sharing, compliance, and governance within the data space. Deliverable D5.2 is developed in the context of Task T5.1" Legal framework and good practices assessment" which aims to provide the analysis of the legal and ethical (where relevant) framework and challenges relevant to the UNDERPIN Data Space. This document focuses on:

- Privacy and Data Protection: main definitions, principles, obligations and rights under the General Data Protection Regulation and the e-Privacy Directive and forthcoming Regulation, especially the legal and ethical challenges around privacy-preserving techniques, Big Data analytics and automated decision making;
- Regulation on the free flow of non-personal data, data ownership and data sovereignty;
- Financial data framework, including inter alia Anti-Money Laundering rules and Payment Service Directive;

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

- Competition law;
- Trust creation processes design and smart Contracts definitions.

1.3 Relation to other work packages and deliverables

D5.2 documents the outcomes of task "T5.1 Legal framework and good practices assessment" which is developed in the context of WP5 "Business plan and sustainability". To facilitate a clearer understanding of how this deliverable relates to the overall project ecosystem, Table 1 provides an overview of the connections between this deliverable and other project deliverables, highlighting their interdependencies.

Table 1: Interlinks with other project deliverables

Deliverable	Interdependency
D5.1 "Existing business models assessment"	The work carried out in D5.1 towards the definition of a business model for the UNDERPIN Data Space provides valuable input to the present deliverable towards developing trust mechanisms.
D5.3 "Business analysis, KVIs, Societal impact, Sustainability and Operator Model"	The work undertaken in the present document towards the identification of relevant legislation, principles and values regarding provides input to D5.3 with respect to the delivery of a comprehensive and sustainable business model for UNDERPIN.
D3.2 "UNDERPIN Data Space infrastructure, mid-term deployment and integration report"	This report receives input from the efforts undertaken in D3.2, and specifically towards establishing secure data-sharing mechanisms in the UNDERPIN ecosystem. Additionally the report draws upon the efforts developed under T3.3 "Smart contract framework establishment and integration" regarding the adoption of federated security management, self-sovereign identification schemes and smart contracts considerations in the Data Space facilities.

1.4 Deliverable structure

The structure of the deliverable is organised as follows:

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Section 1- Introduction: This section describes the mission, vision and values of the project, the next steps, the structure and the relation of the deliverable D5.2. with the other WPs of the project.

Section 2 – Trust Creation Processes: In this section the framework for the creation through technical, organizational, and legal mechanisms is defined, while the detailed methods by which trust is operationalized within the UNDERPIN data space is described. In addition, the utilization of smart contracts to facilitate and manage data-sharing agreements within UNDERPIN is detailed.

Section 3 – Legal Considerations: This section describes the legal framework including relevant provisions that realize trustworthy, secure and reliable data exchange services while ensuring "data sovereignty".

Section 4 – Validation through the Data Space and Next Steps: This section on validating the proposed concepts, frameworks, and mechanisms designed to establish trust within the UNDERPIN Data Space

Section 5- Conclusions: presents the concluding remarks of this deliverable.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

2 Trust creation processes

2.1 Introduction

Trust is the cornerstone of any data space, particularly in environments where participants span different sectors, sizes, and geographies. In the UNDERPIN project, trust is crucial to ensuring secure, sovereign, and transparent data exchanges between participants, enabling organizations to share data with confidence while maintaining control over its usage.

The International Data Spaces Association (IDSA) defines trust through a comprehensive framework that involves technical, organizational, and legal mechanisms. This framework ensures that participants in a data space can establish and maintain secure and legally safe relationships, even when exchanging sensitive industrial data. Trust within a data space is more than just securing data; it is about building reliable relationships between participants, ensuring that all entities can trust each other to act responsibly and in compliance with the law and agreed policies.

A core model for understanding trust lies in the interaction between three key roles: the Issuer, the Holder, and the Verifier. Each participant within the data space acts in one or more of these roles, where Issuers provide verifiable credentials, Holders control the credentials, and Verifiers assess these credentials to ensure trustworthiness. This model ensures that all parties can verify claims, such as membership in a data space, compliance with security standards, and certifications, before engaging in data exchanges.

Trust in data spaces, such as UNDERPIN, is built through several mechanisms:

- **Data sovereignty**: Ensuring that participants retain full control over their data, defining who can access it, under what conditions, and for what purposes. Usage Control Policies, as defined in the IDS Reference Architecture Model (RAM Version 4) [1] and Terms and Conditions for the use of joining the UNDERPIN Data Space (see Annex), enforce these rules across the data space.

- **Certified IDS connectors**: These connectors provide the necessary technical infrastructure for secure, trusted data exchanges. Each connector is certified to ensure compliance with security standards and data protection requirements.

- **Auditability and accountability**: Trust is further reinforced through **audit trails**, which provide a transparent record of data transactions, ensuring that all actions can be traced and verified by participants.

In addition, trust frameworks like those from Gaia-X [2] and iSHARE [3] also influence how trust is operationalized in UNDERPIN. While the focus remains on the IDSA framework, these complementary approaches provide additional layers of interoperability and trust, ensuring that

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

participants can seamlessly exchange data across different platforms while maintaining security, privacy, and compliance.

The Trust Creation Processes outlined in this section of the deliverable aim to describe the detailed methods by which trust is operationalized within the UNDERPIN data space. These methods are based on the principles defined in the IDS Reference Architecture Model (RAM) Version 4.

2.2 IDS RAM and Trust Frameworks

In the context of the UNDERPIN project, IDS RAM provides the technical, legal, and organizational foundation necessary for building and maintaining trust between participants in the data space. This framework is designed to ensure that data sovereignty, security, and compliance are preserved throughout the data exchange process, allowing all participants to engage in trustworthy and transparent data sharing activities.

2.2.1 Data Sovereignty and Usage Control

One of the core principles of the IDS standard is the concept of data sovereignty, which ensures that data providers retain full control over their data even after it has been shared with other participants in the data space. The Usage Control mechanism defined in the IDS Reference Architecture Model (RAM Version 4) allows data providers to specify how their data can be used, who can access it, and under what conditions. These policies are enforced at the connector level, ensuring that the rules set by the data owner are followed throughout the data lifecycle.

As depicted in Figure 1, Usage Control in the IDS framework goes beyond traditional access control by continuously enforcing the data usage policies during the entire process, ensuring compliance with the law and the agreed policies and data uses even after the data has been shared. This ensures that participants in the UNDERPIN data space can share data while maintaining confidence that their data will be used according to their terms.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

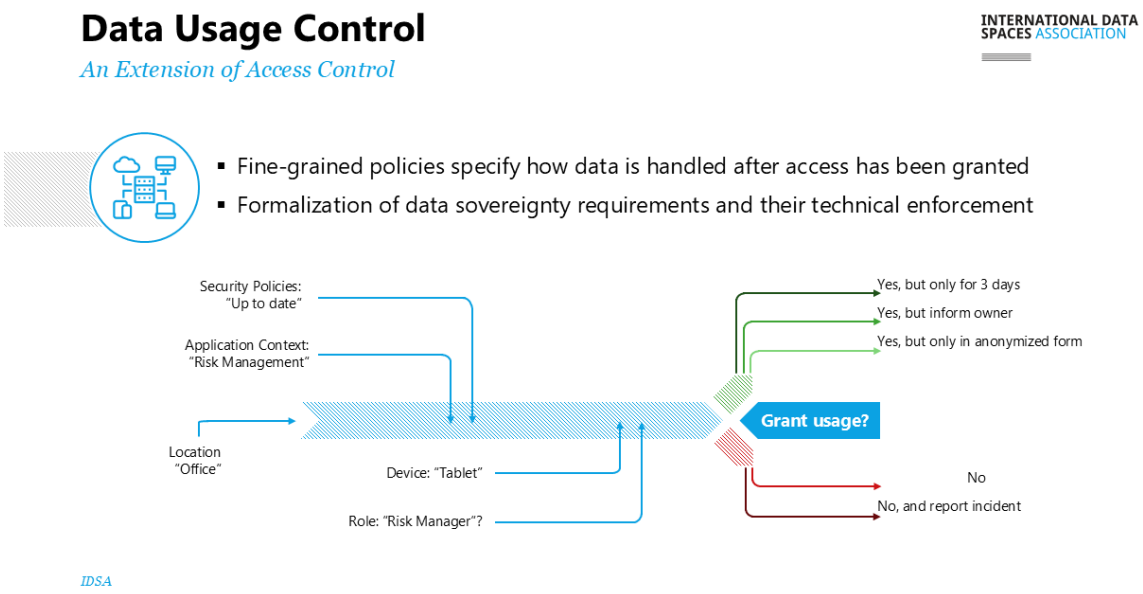

Figure 1: Usage Control in IDS

2.2.2 Certified IDS Connectors

The Certified IDS Connectors are essential to establishing secure and trustworthy communication between participants in the data space. These connectors act as the gatekeepers of data exchanges, ensuring that all data transfers are compliant with the security and trust requirements of the IDS framework.

Each connector is certified according to the IDSA Certification Scheme, which verifies that it meets strict technical and organizational requirements for security, data protection, and compliance. The certification process involves multiple trust levels (Basic, Core, and Advanced) to accommodate the varying needs of different participants in the data space. For instance, in the UNDERPIN project, certified connectors ensure that data shared between oil refineries, wind farms, and other critical manufacturing entities is protected from unauthorized access and misuse.

2.2.3 Identity and Access Management (IAM)

Identity and Access Management (IAM) plays a pivotal role in the IDS standard, as it ensures that only authorized participants can access data within the data space. The IDS Reference Architecture Model (RAM Version 4) specifies a decentralized identity management system, where participants are assigned verifiable or trusted credentials that can be used to authenticate their identity and verify their compliance with the data space's security requirements.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

In the UNDERPIN project, this decentralized IAM approach illustrated in Figure 2, allows participants, such as equipment manufacturers, service providers, and maintenance teams, to authenticate themselves using their certified credentials before accessing sensitive industrial data. The identity provider within the data space is responsible for issuing and verifying these credentials, ensuring that only trusted entities can participate in data exchanges.

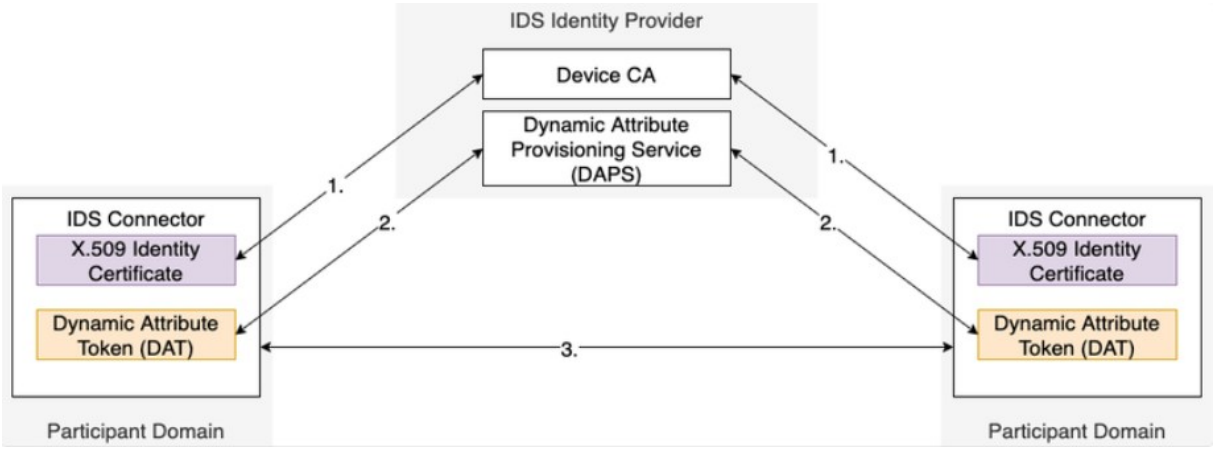

Figure 2: Interaction between IDS Connectors and Identity Components (Source: IDS RAM)

2.2.4 Trust Through Transparency and Auditability

A critical component of building trust in a data space is ensuring **transparency** in data exchanges. IDS standard achieves this by providing **audit trails** that track all data transactions between participants. These audit logs are essential for monitoring compliance with data usage policies, detecting potential security breaches, and ensuring accountability among participants.

In the UNDERPIN data space, auditability allows participants to review data exchanges and verify that all actions were compliant with predefined agreements. This transparency is crucial for fostering trust between participants, especially in sectors like oil refineries and wind farms, where the integrity and reliability of data are critical for operational efficiency.

2.2.5 Legal Agreements and Smart Contracts

Trust within the IDS framework is not limited to technical mechanisms; it also involves the issue of Terms and Conditions for joining the Data Space, the legal agreements and smart contracts (to automatically execute the terms and conditions agreed with regard to the sharing of data) that formalize/determine the relationships between participants in the data space. These agreements define the roles and responsibilities of each participant, ensuring clarity in under which terms, conditions and restrictions data is to be shared and used.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

In the context of the UNDERPIN project, smart contracts can be used to automate the enforcement of data-sharing agreements, reducing the risk of human error and increasing the efficiency of data exchanges. For instance, a smart contract could automatically enforce a data usage policy, ensuring that a service provider can only access specific machine data for maintenance purposes and cannot share it with third parties.

The use of standardized legal agreements, aligned especially with the General Data Protection Regulation (GDPR)[1], the European Data Governance Act[2] (DGA) and Data Act[3] (DA) requirements, ensures that all participants are legally accountable for their actions, further strengthening the trust within the data space.

2.2.6 Interoperability and Alignment with Other Frameworks

While the focus of the UNDERPIN project is on the IDS standard, it is important to ensure interoperability with other trust frameworks, such as Gaia-X [2] and iSHARE [3]. The IDS Reference Architecture Model (RAM Version 4) is designed to be framework-agnostic, allowing seamless integration with these and other standards.

For example, by aligning with the Gaia-X Trust Framework (or the one from iShare) the UNDERPIN data space can ensure that participants from different sectors and jurisdictions can trust each other's identity claims, data usage policies, and compliance with security standards.

2.3 Legal and Organizational Framework for Trust

A robust legal and organizational framework is critical for fostering trust in the UNDERPIN data space. This framework governs the roles, responsibilities, and legal agreements between participants, ensuring that data is shared securely and transparently. IDSA Rulebook[4] provides the foundational guidelines for establishing this trust, while practical tools and templates from the Data Spaces Support Centre (DSSC) Starter Kit[5] help streamline the implementation of governance and compliance measures. This section outlines the key legal and organizational processes that establish accountability and trustworthiness in the UNDERPIN project.

The legal agreements form the backbone of trusted data exchanges in the IDS ecosystem. These agreements define the specific terms under which data can be shared, accessed, and used, and the serially binding contracts that guarantee compliance with European laws, such as the GDPR) and the DGA.

In UNDERPIN project, these legal agreements (that will be formed) play a key role in facilitating cross-organizational data exchanges. For example, a wind farm operator and a service provider

[1] https://gdpr-info.eu/
[2] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[3] https://digital-strategy.ec.europa.eu/en/policies/data-act
[4] https://docs.internationaldataspaces.org/ids-knowledgebase/idsa-rulebook
[5] https://dssc.eu/space/SK/759234564

can formalize a contract that specifies how operational data from turbines will be shared for predictive maintenance purposes. This contract would clearly define who owns the data, who can access it, and what actions can be performed on the data, ensuring that all parties are legally protected and that the data is used in accordance with the owner's preferences.

IDSA Rulebook recommends that these agreements while being compliant with the ongoing acts, are modular and flexible, allowing participants to customize them based on their specific needs while still adhering to the broader legal frameworks governing data sovereignty and privacy. The use of these standardized agreements reduces complexity and accelerates the onboarding of new participants into the data space, ensuring a smooth and legally compliant data-sharing process.

2.3.1 Implementing Smart Contracts for Automating Trust

One of the most powerful tools for enforcing legal agreements in the IDS ecosystem is the smart contract. Smart contracts are self-executing digital contracts that automatically enforce the rules and conditions outlined in data-sharing agreements. These contracts are stored on a blockchain or a decentralized system, ensuring that they cannot be altered once deployed.

In UNDERPIN project, smart contracts provide a practical solution for automating trust. For example, a smart contract could be used to automatically grant or revoke access to a dataset based on predefined conditions. If a maintenance service provider needs to access machine data from an oil refinery, a smart contract can automatically verify that the provider has the correct credentials and that the data is being accessed for the approved purposes. If any of these conditions are not met, the smart contract can block access, ensuring that the data is protected in real-time.

Additionally, smart contracts can be used to manage payment processes for data-driven services. In a scenario where a vendor provides data-driven insights to a manufacturer, a smart contract could automatically trigger payment when the agreed-upon data is delivered. This automation not only enhances trust by ensuring compliance with the contract but also improves operational efficiency by eliminating the need for manual intervention.

Smart contracts provide a transparent and tamper-proof method for enforcing trust, reducing the risk of disputes and ensuring that all participants adhere to the terms of their agreements. As illustrated in Figure 3, the DSSC Starter Kit emphasizes the practical use of smart contracts in automating data governance, making them an essential tool for building trust in the UNDERPIN data space.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

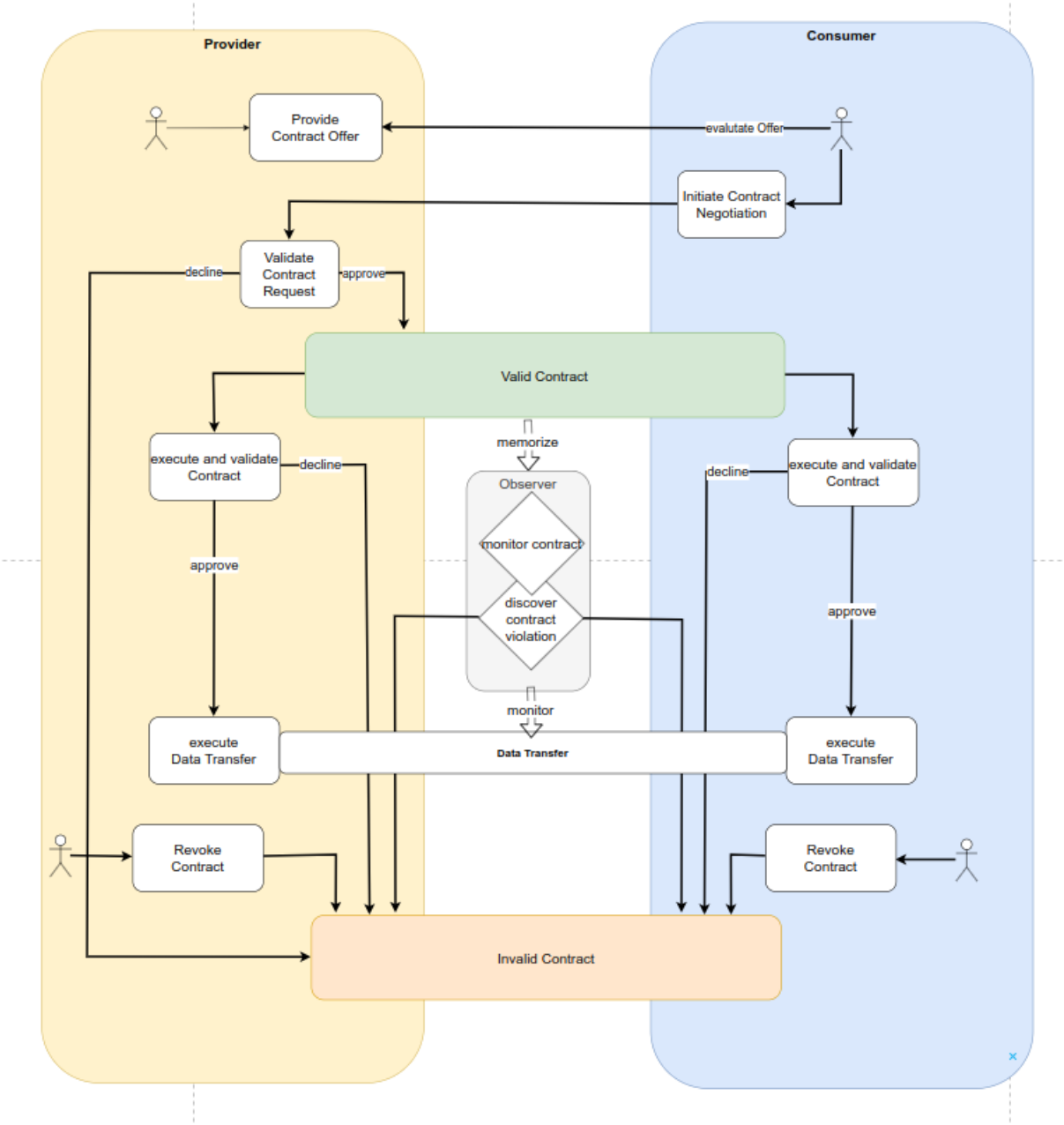

Figure 3: Data sharing contract negotiation (Source: IDSA Rulebook)

2.3.2 Defining Roles and Responsibilities in Data Governance

Establishing clear roles and responsibilities is essential for ensuring trust and accountability within a data space. IDSA Rulebook provides a structured approach for defining the roles of participants and outlining their responsibilities in terms of data sharing, governance, and compliance. These roles include Data Providers, Data Users, Identity Providers, Certification Bodies, and the overarching Data Space Governance Authority (DSGA). Together, these roles

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

form the organizational backbone of the trust framework within the UNDERPIN data space. This diagram (Fig. 4) illustrates the organizational and functional relationships within a data space ecosystem, showcasing key components and their interactions.

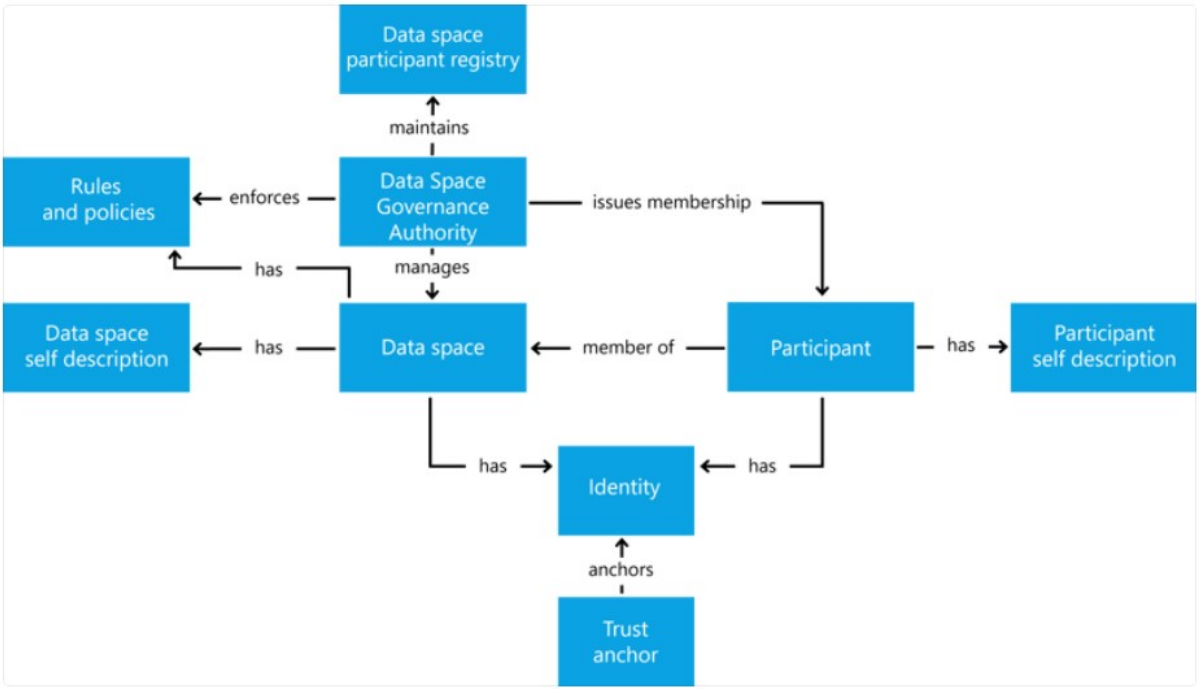

Figure 4: Overview of Data Space entities (Source: IDSA Rulebook)

Data Providers

Data Providers are the participants who own or control the data and are responsible for defining the conditions under which their data can be accessed and used by other participants. They set Usage Control Policies, which specify the rules governing how data can be processed, shared, or modified. These policies ensure that data sovereignty is preserved, even when data is shared across organizational boundaries.

In the context of UNDERPIN project, data providers could include industrial stakeholders like oil refineries or wind farm operators. These entities generate valuable operational data, such as machine performance metrics or maintenance records, and they define the conditions for sharing this data with third-party service providers or equipment manufacturers.

Data Users

Data Users are participants who access and use the data provided by others. They are obliged and responsible for complying with the usage policies set by the data providers. In UNDERPIN data space, data users could include service providers who access machine data for predictive maintenance, equipment vendors analyzing operational data for performance optimization, or third-party consultants providing data-driven insights to improve operational efficiency.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

The trust framework ensures that data users adhere to the agreed-upon conditions, safeguarding data integrity and sovereignty throughout the data-sharing process.

Identity Providers

Identity Providers are responsible for issuing verifiable credentials that authenticate participants in the data space. These credentials ensure that only authorized and certified entities can access the data and services within the data space. IDSA Rulebook outlines that identity providers play a critical role in establishing trust, as they guarantee that participants can verify each other's identity and certification status.

In UNDERPIN project, identity providers authenticate and verify participants such as equipment manufacturers, service providers, and maintenance teams. This ensures that only trusted participants can access sensitive industrial data, reducing the risk of data breaches and unauthorized access.

Certification Bodies

Certification Bodies provide the necessary certification for participants and technical components, such as IDS Connectors. The IDSA Certification Scheme ensures that all entities meet the required security and data governance standards before they can participate in the data space. Certification bodies also verify the compliance of participants with the technical and organizational requirements defined in the IDS framework.

In UNDERPIN, certification bodies ensure that all data exchanges between participants, such as wind farm operators and equipment vendors, are conducted securely and in compliance with the rules set forth by the data space governance authority. Certification not only strengthens trust between participants but also ensures that the technical infrastructure (e.g., IDS connectors) used for data exchanges is secure and compliant with industry standards.

Data Space Governance Authority (DSGA)

The Data Space Governance Authority (DSGA) plays a central role in overseeing the operational governance of the data space. As outlined in the IDSA Rulebook, DSGA is responsible for managing the governance structure and ensuring that all participants adhere to the established rules and protocols within the data space. The following figure (Fig.5) illustrates three governance models for data spaces based on the structure and distribution of the Data Space Governance Authority. Each model represents a different level of centralization and decision-making structure.

The DSGA’s core responsibilities include:

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

- **Participant onboarding**: The DSGA is responsible for managing the onboarding process of new participants, ensuring that all required certifications and credentials are in place before participants can engage in data exchanges.
- **Issuance of credentials**: DSGA collaborates with identity providers to issue and manage the verifiable credentials required for participants to access the data space. These credentials guarantee that participants meet the trust and security requirements of the data space.
- **Compliance monitoring**: DSGA oversees the compliance of participants with data governance policies and usage control agreements. This includes ensuring that data users comply with the usage policies defined by data providers and that participants adhere to the legal frameworks governing data exchanges (e.g., GDPR, Data Governance Act).
- **Dispute resolution**: In cases where conflicts arise between participants, DSGA provides mechanisms for dispute resolution. By maintaining oversight of all data transactions, DSGA can mediate and resolve disputes related to data misuse, non-compliance, or breaches of contract.

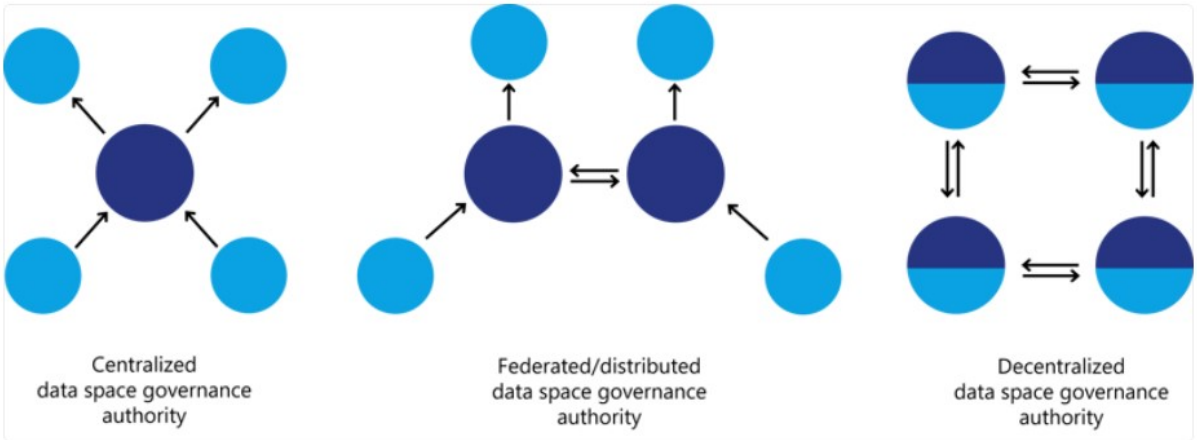

Figure 5: Variants for Data Space Governance Authorities

In the context of the UNDERPIN project, DSGA will ensure that all participants, from SMEs to large industry players, follow the necessary governance and compliance protocols when engaging in data exchanges. For example, when a wind farm operator shares predictive maintenance data with a third-party service provider, DSGA ensures that both parties adhere to the agreed-upon data usage policies and that the data consumer has the appropriate credentials and certifications to access the data.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

DSGA also plays a critical role in continuous governance and compliance monitoring, ensuring that the rules and policies governing data exchanges remain up to date and aligned with evolving regulatory standards. This ongoing oversight is essential for maintaining trust across the data space, as it ensures that participants can engage in secure and legally compliant data exchanges over the long term.

2.3.3 Compliance and Accountability

Ensuring compliance with legal, regulatory, and operational standards is essential for maintaining trust within the UNDERPIN data space. IDS RAM and the IDSA Rulebook provide comprehensive guidelines for enforcing compliance, ensuring that all participants adhere to the data usage policies, security protocols, and legal frameworks governing the data space. This section outlines how the IDS framework ensures compliance and accountability through audit trails, continuous governance, and legal enforcement mechanisms.

Ensuring Legal and Regulatory Compliance

Compliance with European regulations, such as the GDPR, the DGA and the Data Act, is a fundamental requirement for all participants in the UNDERPIN data space. The IDSA Rulebook ensures that all data transactions within the space are conducted in a manner that upholds data sovereignty, privacy, and security.

In practice, data providers and data users in the UNDERPIN data space are required to comply with legal agreements that specify how data can be used, shared, and processed. These agreements are designed to safeguard personal and sensitive data, ensuring that it is only used for authorized purposes and by trusted entities.

Audit Trails and Logging Mechanisms

Auditability is a key element of ensuring transparency and trust in the IDS framework. Audit trails and logging mechanisms provide participants with the ability to trace every data transaction within the data space, ensuring that all interactions comply with the predefined data-sharing agreements. By maintaining detailed logs of who accessed data, when it was accessed, and what actions were performed, the audit trail serves as a transparent record of activity, allowing participants to monitor compliance in real time.

In the UNDERPIN project, audit trails are particularly important for tracking data exchanges between wind farm operators, equipment vendors, and service providers. These logs provide a verifiable record of each interaction, ensuring that all data users are acting in accordance with the usage policies defined by the data provider. For instance, if a service provider accesses turbine performance data for maintenance purposes, the audit trail will capture the details of this transaction, providing visibility into whether the data was accessed correctly.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

IDS Clearing House component plays a supporting role in ensuring transparency and accountability within the data space by logging and monitoring data transactions. It provides a neutral and trusted service that records every transaction between participants, creating an immutable audit trail of data exchanges. The Clearing House does not interfere with the actual data transfer but ensures that all transactions are properly logged and can be reviewed by authorized parties. While not required for every transaction, the Clearing House can be especially useful in high-stakes data exchanges, where additional oversight and traceability are needed to verify that participants are adhering to the agreed-upon data usage policies. This logging mechanism enhances trust by ensuring that all actions within the data space are fully auditable and can be traced back if necessary.

Continuous Monitoring and Governance

Compliance within the data space is not a one-time activity; it requires ongoing monitoring and enforcement to ensure that participants continue to follow the rules. IDS standard emphasizes the need for continuous governance, which involves regular audits, security assessments, and policy updates to reflect changes in the legal landscape or operational requirements.

The Data Space Governance Authority (DSGA) plays a central role in maintaining this continuous governance. The DSGA is responsible for ensuring that participants remain compliant with the data usage policies and legal agreements that govern the data space. This includes monitoring data transactions, overseeing the issuance and renewal of certifications, and addressing any non-compliance issues that arise. The DSGA ensures that data users respect the data sovereignty rights of providers and that any violations of data-sharing agreements are dealt with swiftly.

In the UNDERPIN data space, continuous governance mechanisms will ensure that all participants, including SMEs and large industry players, maintain compliance over time. For example, if an equipment manufacturer fails to comply with data usage policies when accessing operational data from a refinery, the DSGA can intervene to revoke access and impose penalties as necessary.

Accountability Mechanisms

Accountability is a critical component of the trust framework in the IDS ecosystem. IDSA Rulebook outlines specific processes for holding participants accountable for their actions within the data space. This includes mechanisms for addressing breaches of data-sharing agreements, handling non-compliance issues, and resolving disputes between participants.

In cases of data misuse or non-compliance, participants can be held liable through dispute resolution mechanisms managed by the DSGA. For example, if a data user violates the terms of a data-sharing agreement by using data for unauthorized purposes, the DSGA can initiate a dispute resolution process, which may involve penalties such as revoking access rights, issuing fines, or suspending certifications.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

The DSSC Starter Kit further recommends the use of automated compliance tools to monitor and enforce accountability. These tools can automatically detect instances of non-compliance and trigger alerts or corrective actions, helping to prevent data breaches before they occur. In UNDERPIN, such tools can be used to continuously monitor data exchanges between refineries, wind farms, and service providers, ensuring that all participants remain accountable for their actions.

By combining legal enforcement, auditability, and continuous monitoring, IDS framework ensures that all participants in the UNDERPIN data space are held accountable for maintaining compliance with the agreed-upon policies. This system of accountability not only reinforces trust but also provides a clear path for resolving conflicts and ensuring that data exchanges remain secure and transparent.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3 Legal Considerations

As the UNDERPIN project aims at providing a sustainable dataspace solution towards carrying out dynamic asset management and predictive/prescriptive maintenance (continuous monitoring and exchanging data on machine status, breakdowns, downtimes, service orders etc.) its goals, activities and research outcomes ate strictly related to the governance of data in a way that is secure and effective and at the same time legally robust and compliant with the relevant legal framework at place/ in force.

The lawful data governance is a prerequisite to enable the provision of trustworthy, secure and reliable services while ensuring “data sovereignty”, i.e. control over data and safety with regard to its reliability, trustworthiness and legal status, so that the rights and legitimate interests of the involved parties are taken into consideration, respected and protected.

The legal framework includes a wide range of provisions. However, it refers mainly to General Data Protection Regulation (hereafter GDPR), Data Governance Act (hereafter DGA), Data Act and Artificial Intelligence Act (hereafter AIA). Our point of reference is the legal framework applicable in the EU but it has to be mentioned that some of the Acts have explicitly also “extraterritorial effect”, such as in GDPR and AIA.

3.1 Data Protection Issues and GDPR

UNDERPIN is oriented on Industrial data sharing and, in this context, on providing a cross-organisational data sharing and -exchange solution. However, activities referring to the collection, exchange and assessment of data may presuppose or result to the processing of personal data, such as personal data concerning employees or data that refer to manufacturers, integrators, vendors, maintenance service providers, remanufacturers etc., if and to the extent that these data about/ for the respective services, including informational transactions, refer also to personal data.

Furthermore, data processing activities and personal data may not always be obvious, or may be taken for granted (for example, mundane activities such as the collection of email addresses of named individuals can be considered as processing of personal information). However partners and future deployers/ providers/ users should be aware that both data processing and personal data can be widely construed. Thus, appropriate safeguards should be put in place for the handling of all personal data.

Therefore, it has been deemed necessary to provide a brief analysis of the applicable law. An international legal instrument that refers to the protection of informational privacy is the European Convention on Human Rights (ECHR), a legally - binding text for the signatory states concerning human rights. The ECHR enshrines a right to data protection, mainly through the Article 8 stating the right to respect for private and family life. Accordingly, and following the jurisprudence of the European Court of Human Rights with respect to interferences with Article 8

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

rights, where personal data is processed, the relevant principles should be respected (data minimization, accuracy, limited retention period, purpose limitation, transparency, respect for data subjects' rights). Furthermore, the Charter of Fundamental Rights of the European Union specifically enshrines both the right to private and family life (Article 7) and the right to data protection (Article 8).

The main applicable EU regulatory framework that governs the processing of personal data by controllers and processors is GDPR. In order to support the UNDERPIN project partners and future deployers/ providers/ users in identifying and appropriately managing their personal data processing activities, this subsection will discuss the principles, legal grounds, compliance requirements as well as the rights of the data subjects.

3.1.1 Personal Data and other definitions

3.1.1.1 Personal Data and identified/ identifiable data subjects

According to Article 4(1) of the GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject');

Information must 'relate to' the identifiable individual to be personal data. This means that it must concern the individual in some way. To decide whether or not data relates to an individual, the following has to be considered: a) the content of the data; b) the purpose of processing and the c) results of or effects on the person from processing the data.

A data subject is a natural person who can be identified, directly or indirectly. The GDPR provides in Article 4 (1) and in Recital 30[6] a non-exhaustive list of identifiers, including an identification number, location data, an online identifier to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Some characteristics are so unique that someone can be identified with no effort, but a combination of details on categorical level (age category, regional origin, etc.) may also be conclusive in some circumstances, particularly if one has access to additional information of some sort. A person remains identifiable, even if the data controller/ processor needs additional information to identify her/him.

Personal data is also applicable to video, images and audio[7] collected through CCTV systems, sensors or other tools that contains identifiers of individuals . Personal data can be based on both

6 As Recital 30 states natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular, when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them

7 According to Article 29 DPWP, image and sound data that relate to identified or identifiable natural persons is personal data: a) even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars, b) even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers, c) irrespective of the media used for the processing (e.g., fixed and/or mobile video systems such as portable video receivers, colour and/or BW images), the technique used (cabled or fibre optic devices), the type of equipment (stationary, rotating, mobile), the features applying

Co-funded by the European Union This project has received funding from the Digital Europe Programme under grant agreement No 101123179

identified (e.g., a named data subject) or identifiable persons (a person who can be identified with additional information. If it is possible to identify an individual directly from the information processed, then that information may be personal data. If an individual cannot be directly identified[8], it must be considered whether the individual is still identifiable[9].

The principles and in general the rules of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. The GDPR does not concern the processing of such anonymous information, including for statistical or research purposes (Recital 26 of GDPR).

As stated in Recital 26, to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs and the amount of time required for identification, the available technology at the time of the processing and future technological developments.

3.1.1.2 Processing of personal data

The GDPR defines "processing" in an apparently and consciously broad way: Article 4 (2) states that processing means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' This open definition aims at ensuring the technological neutrality of the provisions and the forms of processing they regulate.

3.1.1.3 Controller and Processor

In the UNDERPIN project, entities responsible for processing of personal data will be data controllers or processors who utilise in some cases personal data for the purposes of achieving research or communication, exploitation and dissemination objectives.

For clarity, a Data Controller, according to Article 4(7), means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are

to image acquisition (i.e. continuous as opposed to discontinuous), and the communication tools used (e.g. the connection with a "centre" and/or the circulation of images to remote terminals. See Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance

[8] Images of individuals captured by a video surveillance system can be personal data to the extent that the individuals are recognizable. Images generated by "counting cameras" that capture individuals from a distance and an angle that does not allow the identification of persons, are not likely to qualify as personal data.

[9] See Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data. Also Information Commissioners Office, Guide to the General Data Protection Regulation (version of 22 May 2019).

determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

A controller then decides how and why personal data is collected and processed. In UNDERPIN, a task leader or participant could be responsible for making these decisions. A joint controllership arises whereby multiple partners determine the means and purposes of data processing. A processor may be a partner who processes personal data under instruction of the data controller.

The data controller is obliged under Article 24(1)-(3) to implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with the GDPR, as well as implement appropriate data protection policies. Joint controllers must transparently determine their respective responsibilities and should designate a contact point.

A Data Processor, according to Article 4(8) means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. According to Article 28 GDPR, processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, as well as the obligations and rights of the controller.

3.1.2 Data Protection Principles

The GDPR is designed around seven key principles for governing data processing activities and protecting data subject rights. These principles are set out in Article 5 of the GDPR as follows.

3.1.2.1 Lawfulness, fairness, and transparency

Processing should be lawful, fair and transparent to the data subject. Data should be processed on an appropriate legal basis and processing should be made known to data subjects. Transparency entails that information and communications pertaining to the processing should be accessible, understandable and in clear and plain language.

3.1.2.2 Purpose specification and purpose limitation

Data should be processed for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. If it is necessary to re-purpose existing datasets, this should be done on the basis that the scientific research is compatible with its original intended purpose and such that no separate legal basis from that which allowed its collection in the first place is required (Rec. 50).

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.1.2.3 Data Minimisation

Data collection should be adequate, relevant, and limited to the purposes for which they are processed. Personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Personal data collection should be restricted to no more than what is strictly necessary to achieve the objectives and goals of the project, meaning only data that is adequate, relevant, and limited to what is needed for the completion of research tasks. Any personal data that is collected and which is not necessary for the completion of tasks should be destroyed as soon as possible.

3.1.2.4 Accuracy

Data should be accurate and up-to-date – reasonable steps should be taken to erase or rectify inaccurate data. Accuracy of data constitutes in any case a feature of the quality of data, regardless of whether it is personal or non -personal.

3.1.2.5 Storage Limitation

Data should not be stored in a way that allows the identification of data subjects for longer than necessary for the purposes for which the data is processed. This provision is subject to Article 89(1) exceptions and the implementation of appropriate technical and organisational measures safeguarding the rights and freedoms of data subjects. In the case that personal data are stored to achieve the goals and objectives of the project, they should in principle be deleted after the termination of the project.[10] Stored personal data could be reviewed by partners with a view to determine its ongoing relevance to current and future tasks. Some personal data may be required for a period of time after the completion of the project in order to comply with European Commission auditing requirements.

3.1.2.6 Integrity and Confidentiality

Data should be processed in a manner that ensures not only security and protection against unauthorised or unlawful access , but also against accidental loss, damage or destruction using appropriate technical and organisational means. Article 32(1)(a)-(d) specifies the security principle and refers to the security and organisational measures to be implemented by controller and processor, including a) the pseudonymisation and encryption of personal data, b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, c)the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, d)a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

[10] Article 5(1)(e) and Recital 39

3.1.2.7 Accountability

This principle sets out the responsibility of the Data Controller for complying with the preceding principles as well as being able to demonstrate compliance.

3.1.3 Legal grounds for Data Processing and Conditions for Consent

Article 6(1) sets out the legal bases for processing personal data, which are legal justifications for using personal data in particular ways. These bases, laid out in Article 6(1)(a)-(f), are:

- Consent of data subjects
- Necessity for the performance of a contract
- Compliance with a legal obligation
- Protection of the vital interests of a data subject
- Performance of a task in the public interest or in the exercise of official authority
- Legitimate interest of the Data Controller or a (is a word missing here ?)

For each data processing activity, UNDERPIN, as data controller, will need to carefully consider the legal basis for each data processing operation.

3.1.3.1 Consent

Consent is a common legal basis that enables the processing of personal data and the conditions for consent are set out in Article 7. Consent must be freely given (for example, not under coercion or threat or risk of adverse consequences) and data subjects must have the ability to easily withdraw their consent at any time. Consent must be unambiguous and given by a clear affirmative act. It must also clearly specify to the data subject the identity of the data controller and the purposes of data processing.

However, consent can be hard to prove, for example in the case of a power asymmetrical relationship between an employee and his/her employer. Employees might not be able to demonstrably freely consent to data processing operations entailed by the use of some technologies in the frame of their work. Therefore consent as a demonstrably meaningful choise cannot be relied upon as a lawful basis for data processing and laternative legal bases need to be sought. In the absence of consent, legitimate interest or performance of contract should be considered as the legal basis for data processing operations involving employees' personal data.

3.1.3.2 Performance of a contract and legitimate interest

With regard to the processing of personal data of manufacturers, integrators, vendors, maintenance service providers, the appropriate legal bases could be the need to perform a

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

contract or the legitimate interest of the Data controller or of a third person to whom legitimate interest must be able to pass necessity and balancing tests. Data controllers should be able to demonstrate that the data processing operations are “a reasonable and proportionate way of achieving their purpose” and that other, less intrusive methods are not available for achieving these purposes. A balancing test requires that the data controller determine whether data subjects can reasonably expect the kind of data processing operation in question and whether they are vulnerable to unjustified harm that could override the legitimate interest.

3.1.3.3 Rights of the Data Subject

The GDPR enshrines the rights and freedoms of data subjects in relation to their personal data. The enjoyment of these rights and the adoption of procedures and measures to enable and facilitate the exercise of these rights is a main element of the data protection legislation.

3.1.3.4 The right to be informed

Article 13 of the GDPR requires data controllers to inform data subjects about the processing of their personal data at point of collection. Article 14 requires the controller to inform the data subject about the processing of their personal data where it was not obtained by the data controller. Data subjects must be informed, through informed consent forms or other means (e.g., website privacy policies) of the purpose of data processing, retention periods or criteria, and with whom the data will be shared.

3.1.3.5 The right of access

It is the right of data subjects to know if their personal data is being processed. It grants them the right of access to any such data and the right to receive a copy of the personal data undergoing processing (Article 15).

3.1.3.6 The right to rectification

Data subjects have the right to request the correction of inaccurate personal data, or the completion of incomplete data (Article 16). UNDERPIN partners should therefore provide data subjects sufficient access to identify errors and incomplete information, and correct and complete it as necessary.

3.1.3.7 The right of erasure

It states the right to erase any personal data at the request of the concerned data subject (Article 17). Thus, project partners should endeavour to comply with deletion requests, including from UNDERPIN datasets or contact lists to the extent that such deletion requests do not unreasonably compromise the successful carrying out of the project objectives and goals (Article 17 (3)).

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.1.3.8 The right to restrict processing

The data subject is entitled to ask for the processing restriction of his / her personal data. Following the requirements of Article 18(1)(a)-(d), the relevant data should be store until the contested issue (for example contested accuracy) is resolved, at which point the personal data should be destroyed or processed in a manner that the data subject can and does consent to.

3.1.3.9 The right to data portability

Article 20(1) grants the data-subject the right to receive their personal data, upon request, in a "...structured, commonly used and machine-readable format" as well as the right to "...transmit those data to another controller without hindrance from the controller to which the personal data have been provided."

3.1.3.10 The right to object

The right of a data subject to object to the processing of his/her data can be exercised in case that processing is grounded on legitimate interest. In case of a processing based on consent or on the performance of the contract, the objection to the processing may be expressed through the withdrawal of consent or the renegotiation of contractual obligations and arrangements.

3.1.3.11 Rights in relation to automated decision-making and profiling

The data subject has the right not to be subjected to automated decision-making or profiling (which could, for example, relate to the analysis and prediction of individuals at work, which creates legal or similar effects for the data subject (Article 22). Data subjects can however consent to such automated profiling or decision-making (Article 22 (2) (c)).

3.1.4 Other requirements

3.1.4.1 Data protection by design

Article 25(1)-(3) establishes duties of data protection by design and by default, which further emphasise the need for data minimisation, pseudonymisation and effective safeguards. Article 25 of the GDPR sets out the responsibility of Controllers and Processors with regard to data protection by design and default. It imposes the duty to implement appropriate technical and organisational measures, which are designed to respect data protection principles in an effective manner and to integrate the necessary safeguards into the processing, in order to meet the requirements of the GDPR and protect the rights of data subjects (Data protection by design). Data controllers should also adopt and implement technical and organisational measures to ensure that processing is, by default, limited to personal data which are necessary for each specific purpose. In utilising technologies that process personal data, UNDERPIN Consortium partners do consider how the devices and methods of data collection and processing used in the project and/ or its deployment can minimise unnecessary data collection and other forms of processing of personal data. Partners should consider how to design tools and technologies to

This project has received funding from the Digital Europe Programme under grant agreement No 101123179

minimise any unnecessary data collection or processing in order to comply with the requirements of the GDPR and facilitate compliance with the GDPR by future deployers of any technologies developed.

3.1.4.2 Data Protection Impact Assessment

Article 35(1) lays out the requirement of a Data Processing Impact Assessment (DPIA) by the controller where it is established that processing may result in a high risk of harm for data subjects. In principle, a DPIA threshold analysis has always to be conducted. The categories of data processed in the context and for the purposes of UNDERPIN do not fall under the categories of processing for which conducting a DPIA is necessary and obligatory.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.2 DATA GOVERNANCE ACT

Businesses and institutions are facing far-reaching changes and challenges in the handling of data that go far beyond data protection law. The Data Governance Act as well as the Data Act (to be analysed in the next subsection) are the cornerstones of the new data ecosystem. As part of the European digital and data strategy, they stand alongside the Digital Markets Act (competitive regulation of gatekeepers), the Digital Services Act (content regulation of platform operators), the AI Regulation and the Draft Directive on AI Liability.

3.2.1 Objectives, main choices and scope of DGA

Regulation (EU) 2022/868 ("Data Governance Act") sets out the legislative framework at Union level to facilitate, on the one hand, the re-use of public sector data and, on the other hand, the establishment of a single Union-wide market for the provision of data mediation services and data processing for altruistic purposes. The initiative aims to make more data available and facilitate data sharing across sectors and EU countries in order to leverage the potential of data for the benefit of European citizens and businesses. The vision and ambition of the EU legislator is to provide the legal environment for data management and sharing that will enable industries to develop innovative products and services and will make many sectors of the economy more efficient and sustainable. It is also essential for training AI systems.

The act has entered into force on 24 September 2023. However, the rules on Data Intermediation Services will only become applicable by 24 September 2025.

With the purpose of developing a borderless digital internal market and a human-centric, trustworthy and secure data society and economy through the sharing of or access to data across borders or across the EU, the DGA lays down, among others, a framework for voluntary registration of entities which collect and process data made available for altruistic purposes. This comprehensive legal framework affects contractual freedom[11] because it stipulates requirements for data intermediation, sets the standard of liability and also provides for public oversight and enforcement over certain economic activities of market actors. The following analysis focuses on the use of DGA framework for/ while sharing of data between entities and/or acting as an intermediary for Data Intermediations services.

The DGA is a cross-sectoral instrument that aims to regulate the reuse of publicly/held, protected data, by boosting data sharing through the regulation of novel data intermediaries and by encouraging the sharing of data for altruistic purposes[12]. Both personal and non-personal data are in scope of the DGA, and wherever personal data is concerned, the General Data Protection

[11] As regulatory intervention in private actors' relations, the DGA deliberately limits the contractual freedom with regard to data access via Data Intermediaries Services. The obligations are not alterable by mutual consent of the parties – unless the DGA states otherwise.
[12] See the Guidelines on the implementation of DGA issued by the European Commission in September 2024.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Regulation (GDPR) applies. In addition to the GDPR, inbuilt safeguards will increase trust in data sharing and reuse, a prerequisite to making more data available on the market.

3.2.2 Definitions

To enable better understanding of the relevant provisions, we provide the main definitions included in the DGA.

Consent: refers to the consent given by an individual regarding the processing of their personal data; for this concept, the DGA refers to the definition in the GDPR.

Permission: on the other hand, refers to the permission given by an individual or an entity regarding the use of non-personal data pertaining to them.

Data subject: means an individual to whom data relates and who can be identified, directly or indirectly, in particular by reference to an identifier; for this concept, the DGA refers to the definition in the GDPR.

Data holder: means an entity or an individual that is not the data subject and that has the right to grant access to or to share certain (personal or non-personal) data. For example, a company that holds data about its manufacturing yield is the data holder of that data.

Data intermediation service: this is a service aiming to establish commercial relationships for data sharing between an undetermined number of individuals or companies on the one hand and data users (individuals or entities) on the other. This can be done through technical (platforms/ apps where data can be stored), legal or other means**.** According to the EC, it means a service that connects an undetermined number of data subjects and data holders with data users to establish a commercial data-sharing relationship. Services for closed user groups in particular are outside the scope of the DGA.

Data altruism: means the voluntary sharing of data for objectives of general interest without the intention of generating profit.

Public sector body: is defined as covering authorities and bodies governed by public law. Research-performing organisations that are set up as public sector bodies or governed by public law are included in this definition. Public undertakings are outside the scope.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.2.3 Data intermediation services and Data Intermediation Service providers

3.2.3.1 Data intermediaries as neutral entities

As mentioned above, the DGA understands "*data intermediation services*" as those services aimed to establish commercial relationships for the purposes of data sharing through technical, legal, or other means between data subjects and data holders on the one hand and data users on the other. That means that services related to copyright-protected content, services that focus on one party only (e.g., curation of data for a data provider), and non-commercial data-sharing services offered by public sector bodies are excluded.

The goal of the relevant provisions is to offer a model of data-handling practices and face the fears of many companies with regard to the risks of data sharing (loss of competitive advantage, risk of misuses etc.). In this respect DGA provides for a set of rules to ensure that the so-called data intermediaries to ensure that they will function as trustworthy organisers of data sharing or pooling within the Common European Data Spaces Data intermediaries will have to comply with strict requirements to ensure this neutrality and avoid conflicts of interest.

In order to increase trust in data sharing, the DGA adopts a model based on the neutrality and transparency of data intermediaries. Data intermediaries will function as neutral third parties that connect individuals and companies with data users. Both stand-alone organisations providing data intermediation services only and companies that offer data intermediation services in addition to other services could function as trusted intermediaries. In the latter case, the data intermediation activity must be strictly separated, both legally and economically, from other data services. In practice, this means that there must be a structural separation between the data intermediation service and any other services provided (i.e. they must be legally separated)[13].

The obligations imposed by Art. 12 DGA as stated below arguably qualify as per se prohibitions because the DGA aims to strengthen the trust of market actors in data intermediaries at large (Recital 4 DGA). Due to the systemic nature of the obligations, their application is not at the disposal of the parties.

3.2.3.2 Data intermediation services and their requirements / conditions

Providing Data intermediation services results to a "key role in the data economy". The DGA promotes voluntary data sharing and aims to counter the dominance of large tech companies by facilitating data exchange through intermediation services. These services act as neutral third parties, connecting SMEs and start-ups with data users, charging for facilitating data sharing without using the data for direct financial gain. The main function of a data intermediary is to

[13] Due to the restrictions of contractual freedom introduced by DGA an agreement to deviate from the obligation of neutrality would be void. In other words, even if the data holder had equal bargaining power, she could not consent to the DIS using the data for commercial exploitation. See H. Richter, Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing, *GRUR International,* 72(5), 2023, 458–470

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

enable and/or facilitate data sharing between data holders and data users. This often involves the establishment of infrastructure for the interconnection of data holders and data users.

Article 10(a) DGA quite broadly defines that the Data Intermediary Service 'may include bilateral or multilateral exchanges of data or the creation of platforms or databases enabling the exchange or joint use of data, as well as the establishment of other specific infrastructure for the interconnection of data holders and data users'. According to Recital 28 DGA, this includes data marketplaces, orchestrators of data sharing ecosystems (for instance in the context of common European data spaces), as well as data pools that are "established jointly by several legal or natural persons with the intention to license the use of such pool to all interested parties in a manner that all participants contributing to the pool would receive a reward for their contribution to the pool".

Intermediaries must comply with strict requirements, including structural separation (see above), non-discriminatory terms, and using acquired data only to improve the service. While they may charge for facilitating the data sharing between the parties, they cannot directly use the data that they intermediate for financial profit (i.e. by selling it to another company or using it to develop their own product based on this data).

According to Art. 12(a), the Data Intermediary may not use data for which it provides its intermediation services "for other purposes than to put them at the disposal of data users" while Art. 12(c) DGA also limits the use of data which the Data Intermediary collects about the activities of holders and users of the service when performing its service.

Any data and metadata acquired can be used only to improve the data intermediation service. The Data Intermediary may use such data only for the development of that service (e.g. fraud detection or cybersecurity) and has an obligation to make this data available to data holders upon request.

To be able to capture some benefits of vertical integration, Art. 12(e) DGA clarifies that DISs (and therefore the same legal person) may offer some added-value tools and services as long as they facilitate data exchange (e.g. through "temporary storage, curation, conversion, anonymization, pseudonymization")[14]. In any case, Art. 12(e) DGA requires data holders to explicitly request or approve such tools and services.

3.2.3.3 Notification to and confirmation by the competent authority

Under the DGA, data intermediaries will be required to notify the competent authority of their intention to provide such services. The competent authority will ensure that the notification procedure is non-discriminatory and does not distort competition and will confirm that the data

[14] This clause takes into consideration that Data Intermediaries would commonly offer such tools and services to sustain their intermediation business model and that such tools and services are to the advantage of data holders and users

intermediation services provider has submitted the notification containing all required information.

Upon receipt of such a confirmation from the competent authority, the data intermediary can legally start to operate and use the label 'data intermediation services provider recognised in the Union' in its written and spoken communication, as well as the common logo. Competent authorities will also monitor compliance with the data intermediation requirements and the Commission keeps a central register of recognized data intermediaries.

3.2.3.4 Nondiscrimination, transparency and continuity requirements

The DGA contains provisions on the terms and conditions between the Data Intermediary and its data holders/users. Article 12(f) DGA includes a general obligation to the Data Intermediaries to "ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including as regards prices and terms of service". This provision aims at increasing market transparency and hinder distortions / breaches of competition.

The commercial terms (including pricing) for the provision of intermediation services should not be dependent on whether a potential data holder or data user is using other services (Art. 12(b) DGA). This provision aims to prevent Data Intermediaries from contractually bundling services (or incentivising their bundled usage), which would undermine the structural separation, so that ultimately markets are kept open, and the condition-based competition remains fostered.

Art. 12(h) DGA entails a duty to "ensure a reasonable continuity of provision of its services" and – if the Data Intermediary also stores data – to install sufficient guarantees that this data remain accessible to data holders/users in case of insolvency.

3.2.3.5 Interoperability, standards and other safeguards

The DGA legislator paid specific attention to ensure interoperability. Article 12(d) DGA states that the Data Intermediary may shift the format of received data solely for the purpose of data exchange to "enhance interoperability within and across sectors or if requested by the data user [...] to ensure harmonisation with international or European data standards". Furthermore, Article 12(i) DGA requires the Data Intermediaries to "take appropriate measures to ensure interoperability with other data intermediation services", including the use of "commonly used open standards in the sector in which the data intermediation service providers operate".

Security has also to be ensured. Article 12 includes also obligations with regard to technical, organisational and legal measures and safeguards in order to protect the interests of the data holders. According to Art. 12(g) DGA, Data Intermediaries have to install procedures to prevent fraudulent or abusive practices while Art. 12(j) DGA requires implementing measures to prevent unlawful transfer or access to non-personal data. Another measure includes the information of data holders "in case of an unauthorised transfer, access or use of the non-personal data that it

Co-funded by the European Union This project has received funding from the Digital Europe Programme under grant agreement No 101123179

has shared" (Art. 12(k) DGA). Furthermore, one of the obligations imposed on Data Intermediaries is to ensure "an appropriate level of security for the storage, processing and transmission of non-personal data", which includes ensuring "the highest level of security for the storage and transmission of competitively sensitive information" (Art. 12(l) DGA). Finally, the Data Intermediary has to maintain a log record of the intermediation activity (Art. 12(o) DGA).

3.2.4 Data Altruism

The DGA aims at enabling the sharing of data for the benefit of society, as data have enormous potential to foster research and enable developing better products and services. The DGA aims to increase data availability for economic, research, and environmental purposes. Data altruism is about individuals and companies giving their consent or permission to make available data that they generate – voluntarily and without reward – to be used for objectives of general interest. The aim of the Data Governance Act is to create trusted tools that will allow data to be shared in an easy way and at the same time create the right conditions to assure individuals and companies that when they share their data, it will be handled by trusted organizations based on EU values and principles. Trust is a prerequisite for the creation of datasets and data pools of a scale to allow their use, including use for machine learning and data analytics.

The DGA imposes transparency requirements by providing safeguards for data donors, and the need to comply with a rulebook outlining specific requirements. The European Commission has established an EU-level register of recognized data altruism organizations and a common European consent form for uniform data collection.

3.2.5 Data Protection issues and the Interplay with GDPR

The DGA does not specifically distinguish between personal and non-personal data, but if personal data are affected, the requirements of data protection laws apply in any case. Data Intermediaries are not necessarily related to personal data, but they do in fact often intermediate between data subjects and processors and support data subjects in exercising their data-related rights, e.g. for pseudonymization purposes, or mandating as agent to exercise data protection preferences. If access to and sharing of personal data is at stake, the data protection rules apply. Article 1(3) DGA states that the DGA is without prejudice to the GDPR. This means that in any case, Data Intermediaries have to comply with the GDPR, and the DGA does not alter/affect rules on data protection. This provision clarifies that the DGA "does not create a legal basis for the processing of personal data and does not alter obligations and rights set out in the GDPR and the ePrivacy-Directive"[15]. The guidance of the European Commission reiterates that the role of supervisory authorities is not touched upon in the GDPR.

[15] That means that processing has to be grounded on one of the legal bases as included in Article 6 GDPR. See above under 3.1.

This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.2.6 Competition issues

There is an interplay between the DGA provisions and competition law. Art. 1(4) DGA is clear when it states that the DGA is "without prejudice to the application of competition law". Non-discrimination requirements serve avoiding implication for competition conditions and the relevant provisions. A multitude of possibilities exist to combine different datasets with one another as well as different ways to process data, and the way that sharing, pooling or use of data is organised may matter for the legality of a data exchange under competition law. As H. Richter notes: "the risk that competitively sensitive information can be drawn from a specific dataset may differ depending on whether a dataset is transferred to a competitor, or whether the dataset remains on the server of the original 'data controller' and a competitor is given access to a dataset on the basis of queries and for specified purposes only"[16].

3.2.7 European Commission's Guidance for the Data Governance Act

One year after the entry into force of DGA, the European Commission published on 24.09.24 a guidance document on Implementing the Data Governance Act (DGA). The guidance will be subject to periodic updates as the DGA is implemented.

Among others the Guidance refer to the aim of the DGA to facilitate and boost data sharing through data intermediation services

[16] See H. Richter see above.

1.1 THE DATA ACT

The Data Governance Act creates the processes and structures to facilitate data sharing by companies, individuals and the public sector. The Data Act is in a way a complementary legal framework. It is the second pillar of the European Data Strategy, complementing the Data Governance Act. The Regulation (EU) 2023/2854 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) will apply in stages from 12 September 2025 until full scope application on 12 September 2027. A large part of the Act will already apply from 12 September 2025, including the right for business users and users to access and share data from IoT devices.

The Data Act aims to create fairness in the data economy and empower users to access and share the data they generate from using connected products and related services. It allows users to directly share their data with third parties or request data holders to do so, while protecting trade secrets and security**.** The Data Act clarifies who can create value from data and under which conditions. The Data Act removes barriers to access data, for both the private and the public sector, while preserving incentives to invest in data generation by ensuring a balanced control over the data for its creators.

The Data Act aims at:

a) strengthening data sovereignty for commercial and private users of connected devices (IoT products) through transparency obligations for data holders and data access rights;
b) opening up a data cycle through data sharing rights, in which small and medium-sized enterprises (SMEs) also participate and which increases innovation and value creation from data.
c) With regard to B2B and B2C, data sharing aims to create fairness in the data economy and empower users to access and share the data they generate from using connected products and related services. It allows users to directly share their data with third parties or request data holders to do so, while protecting trade secrets and security.

According to Article 1 the Data Act lays down harmonised rules, *inter alia*, on:

(a) the making available of product data and related service data to the user of the connected product or related service;
(b) the making available of data by data holders to data recipients;
(c) the making available of data by data holders to public sector bodies, the Commission, the European Central Bank and Union bodies, where there is an exceptional need for those data for the performance of a specific task carried out in the public interest;
(d) facilitating switching between data processing services;
(e) introducing safeguards against unlawful third-party access to non-personal data; and
(f) the development of interoperability standards for data to be accessed, transferred and used.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Definitions in the Data Act: in order to understand the provisions of the Data Act it is necessary to take into consideration at least the following definitions:

(1) 'data' means 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;

(2) 'metadata' means a structured description of the contents or the use of data facilitating the discovery or use of that data;

(3) 'personal data' means personal data as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(4) 'non-personal data' means data other than personal data;

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

(6) 'related service' means a digital service, other than an electronic communications service, including software, which is connected with the product at the time of the purchase, rent or lease in such a way that its absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the product by the manufacturer or a third party to add to, update or adapt the functions of the connected product;

(7) 'processing' means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or other means of making them available, alignment or combination, restriction, erasure or destruction;

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

(12) 'user' means a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services;

This project has received funding from the Digital Europe Programme under grant agreement No 101123179

(13) 'data holder' means a natural or legal person that has the right or obligation, in accordance with this Regulation, applicable Union law or national legislation adopted in accordance with Union law, to use and make available data, including, where contractually agreed, product data or related service data which it has retrieved or generated during the provision of a related service;

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

(21) 'making available on the market' means any supply of a connected product for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge;

(22) 'placing on the market' means the first making available of a connected product on the Union market;

(23) 'consumer' means any natural person who is acting for purposes which are outside that person's trade, business, craft or profession;

(30) 'customer' means a natural or legal person that has entered into a contractual relationship with a provider of data processing services with the objective of using one or more data processing services.

3.3 Scope of application

With regard to its scope, the Data Act applies across all sectors and explicitly lays the foundation for further sector-specific regulation. The **scope** of the Data Act allows users of connected devices, ranging from smart home appliances to smart industrial machinery, to gain access to data generated by their use which is often exclusively harvested by manufacturers and service providers.

More specifically, the Data Act Regulation applies to:

(a) manufacturers of **connected products** placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers;

(b) users in the Union of **connected products** or related services as referred to in point (a);

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

(c) data holders, irrespective of their place of establishment, that make data available to data recipients in the Union;

(d) data recipients in the Union to whom data are made available;

(e) public sector bodies, the Commission, the European Central Bank and Union bodies that request data holders to make data available where there is an exceptional need for those data for the performance of a specific task carried out in the public interest and to the data holders that provide those data in response to such request;

(f) providers of data processing services, irrespective of their place of establishment, providing such services to customers in the Union;

(g) participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement.

As in GDPR and AIA, the Data Act applies extraterritorially to manufacturers of IoT products and data holders based out-side the EU if the products and associated services are used within the EU.

3.3.1 Data sharing under Data Act

The Data Act defines three actors in relation to the use and sharing of data. To create additional value from data, the framework specifies the data to be considered, along with the conditions and procedures for three types of data sharing processes: business to consumers (B2C), business to business (B2B) and business to government (B2G).

The Data Act gives users of connected products (businesses or individuals that own, lease or rent such a product) greater control over the data they generate, while maintaining incentives for those who invest in data technologies. In addition, it lays down general conditions for situations where a business has a legal obligation to share data with another business.

3.3.2 Business-to-business and business-to-consumer data sharing in the context of the IoT market

As explained by the EC, the Data Act enables users of connected products (e.g. connected cars, medical and fitness devices, industrial or agricultural machinery) and related services (i.e. anything that would make a connected product behave in a specific manner, such as an app to adjust the brightness of lights, or to regulate the temperature of a fridge) to access the data that they co-create by using the connected products/ related services. Such data includes 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.

This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Chapter II of the Data Act applies to all raw and pre-processed data generated from the use of a connected product or a related service that is readily available to the data holder (e.g. manufacturer of a connected product/ provider of a related service). That means that data[17] can be easily accessed without disproportionate effort, going beyond a simple operation.

In the context of this kind of data sharing, the main actors are the data holder and users. The data holder is the company that makes the connected product or that provides a related service. A data holder must have a contract with the user (e.g. sales contract, rental contract, related service contract, etc.) defining the rights regarding the access, use and sharing of the data that is generated by the connected product or related service. The data holder cannot use any non-personal data generated by the product without the user's agreement.

Users (i.e. any legal or natural person who owns, rents or leases a connected product – with the exception of gatekeepers under the Digital Markets Act[18]) are allowed to access the data that they generate through their use of the connected product or related service.

If the user wishes to share this data with another entity or individual ('third party'), they can either do so directly or they can ask the data holder to share it with a third party of their choice. The Data Act incudes several mechanisms to make it easier for users to be able to make use of these provisions: data holders must provide the user with information on the type of data that they will generate when using the connected product or related service (including the volume, collection frequency, etc.).

Users should be able to request access to the data through a simple process, and data holders must make the data available to users for free. The data obtained cannot be used to develop a competing connected product. The Data Act does not prohibit competition in related or aftermarket services.

If the data holders or user discover data misuse, they may require data recipients to delete the data and discontinue the use.

3.3.2.1 Mandatory business-to-business data sharing

The Chapter III regulates the mandatory business-to-business data sharing by introducing rules for situations where a business ('data holder') has a legal obligation under EU or national law to make data available to another business ('data recipient'), including in the context of IoT data. As an incentive to data sharing, data holders that are obliged to share data may request 'reasonable

[17] This applies to both personal and non-personal data, including relevant metadata

[18] https://digital-markets-act.ec.europa.eu/legislation_en

compensation' from the data recipient. This could include costs incurred for making the data available as well as technical costs related to dissemination and storage[19].

The data-sharing terms and conditions must be fair, reasonable and non-discriminatory.

In order to protect data holders, the Data Act includes a non-exhaustive list of measures to remedy situations where a third party or user has unlawfully accessed or used data. For example, a data holder could require that an infringing party stops producing the product in question or destroys the data that it has unlawfully obtained, or it could seek compensation.

3.3.2.2 Contract design and (un)fair contractual terms

The data holder is subject to the general obligation of non-discriminatory data sharing and may demand appropriate remuneration in the B2B area to cover costs plus a profit margin. When sharing data with other companies (B2B), the data holder must observe a catalogue of rules on inadmissible, unilaterally imposed contractual clauses, which serve to implement general fairness rules for data licensing, including questions of liability and warranty for poor data quality, as well as termination rules.

In order to protect small businesses seeking to acquire data, the Data Act introduces rules against unfair contractual terms. These rules cover all data, both personal and non-personal, held by a private entity that is accessed and used based on a contract between businesses.

The Data Act establishes a non-exhaustive list of terms that are always considered to be unfair (e.g. that would exclude or limit the liability of the party that unilaterally imposed the term for intentional acts or gross negligence) and of terms that are presumed to be unfair (e.g. that would inappropriately limit remedies in the case of non-performance of contractual obligations or liability in the case of a breach of those obligations, or extend the liability of the enterprise upon whom the term has been unilaterally imposed). If a term is considered to be unfair, it is no longer valid – where possible, it is simply severed from the contact. If it is presumed to be unfair, the entity that imposed the term can try to demonstrate that the term is not unfair[20].

3.3.2.3 Trade Secrets and security requirements

One of the fundamental challenges, but also concerns of data holders, is the balance between access and sharing rights on the one hand and the protection of the data holder's trade secrets on the other. The Data Act deprives data holders of the opportunity to easily invoke (alleged) trade secrets as a defence against data access and data sharing claims. In principle, the data holder must also disclose such data that contains trade secrets. To this end, the data holder must precisely identify the data sets subject to trade secret protection and instruct the user on the

[19] However, micro companies, SMEs and non-profit research organisations cannot be charged more than the costs incurred for making the data available

[20] See the explanatory text of European Commission under the title "Data Act explained" in https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

necessary technical measures to protect the trade secrets when handing the data over. Only if the data holder can credibly demonstrate the risk of significant economic (irreparable) damage resulting from the disclosure of a trade secret may he refuse access to and release of the data in question[21].

To protect trade secrets, the data holder and the user/ third party may agree on certain measures to preserve the confidentiality of the trade secrets. Where these measures are not respected, the data holder may withhold or suspend the data sharing.

The data holder and user may agree to limit data sharing if there is a risk that the security requirements of the connected product could be undermined, resulting in serious adverse effects to the health, safety or security of people. Such requirements must be laid down in EU or national law.

The data holder may only refuse to share data where it can demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets. If the data holder suspends, withholds or refuses to share data on the grounds of trade secrets protection or security requirements, it must notify the national competent authority. Users may challenge such a decision, either in front of the competent court or tribunal of a Member State, via a complaint with the competent authority or upon agreement with the data holder in front of a dispute settlement body.

3.3.2.4 Interoperability

The Data Act strengthens the position of the user and gives him – beyond an existing contractual relationship – the right to access and be provided with "readily available data" in a common machine-readable format. Manufacturers must design and develop their IoT products to make available such data.

In this context, the Data Act aims to ensure interoperability between data processing services which is essential if customers are to benefit from easier switching. The Data Act establishes some essential requirements with which participants in data spaces must comply and which can be further specified by the European Commission by way of delegated acts.

Data space participants should comply with several essential requirements to allow data to flow within and between data spaces. For example, a description of the data structures, data formats and vocabularies, where available, should be publicly accessible.

In addition, means to ensure the interoperability of data-sharing agreements, such as smart contracts, should be ensured. The Data Act lays out requirements for vendors of smart contracts for the automated execution of data-sharing agreements, for example to ensure that they

21 .....

correctly carry out the provisions of the data-sharing agreement and withstand manipulation by third parties[22].

3.3.2.5 Similarities and Differences between Digital Governance Act and Data Act

Both the Data Governance Act and the Data Act promote data sharing and utilisation. The Data Governance Act creates mechanisms for data sharing and the reuse of public sector information, while the Data Act regulates the use of data generated by connected devices and services. Both acts support the EU's vision and data strategy, where data flows freely across borders under a common regulatory framework. These acts will facilitate reliable and secure data access, promoting its use in vital economic sectors and public interest areas.

The Data Governance Act focuses on the governance of data sharing across sectors, including public sector data, and establishes a framework for data intermediation services to operate in a trustworthy manner. The Data Act primarily targets the economic aspects of data generated by IoT devices and services, addressing issues like who can use and access different types of data and under what conditions.

[22] See European Commission, Data Act explained

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.4 Smart contracts

3.4.1 Concept and types of smart contracts

Smart Contracts were first introduced in legal doctrine in the mid-1990s by Nick Szabo [4], a legal scholar and technologist. He presented a concept of con- tracts that can be self-performed and self-executed without, or with little, human intervention. According to Szabo, Smart contracts are the technological evolution of classic vending machines that facilitate automated contract performance and contract execution, significantly decreasing transactional costs and enhancing transactions' velocity.

Smart contracts can appear in transactions in one of the following forms:

3.4.1.1 Tool for self-performance and self- execution of an already concluded contract

In this type the contractual parties have already communicated in the real (off-chain) world, negotiated the contractual terms, and concluded the contract entirely off-chain. After having concluded and formed the contract, they choose to encode (part of) the contractual content in the blockchain platform to benefit from this technology, i.e. the automatic contract's self-performance and self-execution. To that end, the contract must be expressed in a programming language, namely be 'translated' from a natural language to a computer programming one and, subsequently, be embedded in the blockchain platform (smart code). The contractual content translated and embedded into the blockchain platform constitutes the so- called "contractware"[23]. The contractware does not have any legal binding character, i.e. it does not pose itself any legal obligations to the contractual parties. Instead, it is the off-chain contract that poses them and deals with all the pertinent legal issues[24]

3.4.1.2 Hybrid Smart Contract

With regard to the second type of Smart Contract, the hybrid contract, the contractual parties have also communicated in the real off-chain world and negotiated the contractual terms. The difference is the decision of the contractual parties to form the contract partially off- chain and partially on-chain, i.e., a part of the contract is formed in the real world in a natural language, orally or in prose, while the rest part of the contract is directly embedded in the smart code. These two parts are complementary to each other and together form the contractual content. Their main feature is that they are readable by a human and a computer program at the same time, as they are written in both a natural and a computer language.

[23] The contractware is not a contract from a legal point of view; it is rather a computer program that serves as a technical tool for facilitating theautomatic self- performance and self- execution of an already off-chain concluded and formed contract.

[24] For more see ***V.*** Papadouli and V. Papakonstantinou, A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs, Computer Law and Security Review 51 (2023)

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.4.1.3 Stand-alone Smart Contracts

This type, the stand-alone Smart Contract, exists entirely on-chain. This type is the most uncommon so far, but in fact it constitutes the most innovative one. When the parties usually select this type because they are able to capture their entire contractual agreement in the blockchain plat- form, from its beginning until its execution. Contrary to the previous types of Smart Contracts, this type of contract is concluded entirely on-chain through the blockchain platform with the use of the smart contract code as the contractual language.

3.4.2 Smart contracts in the Data Act

As mentioned above the Data Act applies also to participants in data spaces and vendors of applications using smart contracts and persons whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement (Article 1 par. 3 g).

For the first time smart contracts are regulated by the EU for data sharing agreements as provided in the Data Act. The rationale is to enable the conclusion and enforcement of data sharing agreements in an effective and cost-effective manner. According to recital 47 “long-term arrangements between data holders and data recipients, for instance via a subscription model or the use of smart contracts, may reduce the costs in regular or repetitive transactions in a business relationship”. Another goal refers to the use of smart contracts as a protection measure, to prevent unauthorised use of the data by the data recipients.

The rules for smart contracts will also be applicable for any other kind of data sharing agreements, not only where a data holder needs to share data with recipients. In other words, any other player that, acting as vendor, makes use of smart contracts to execute data sharing agreements, will also be bound by the Data Act. Furthermore, the requirements for “regulated” smart contracts only apply to agreements with the purpose of “making data available. the use of smart contracts with a purpose different from “making data available” will not be in-scope of the Data Act.

The rules on smart contracts will affect any vendor of applications making use of smart contracts in the context of executing an agreement or part of it, to make data available to third parties. In the absence of a vendor, the Data Act will apply to the person whose commercial activity involves making data available with the use of smart contracts.

3.4.3 Definition of Smart Contracts

The Data Act defines smart contract as a “*computer program used for the automated execution of an agreement or part thereof, using a sequence of electronic data records and ensuring their integrity and the accuracy of their chronological ordering*”. This means that once the parties have agreed on the use and content of the smart contract, the performance of the agreement will occur automatically (in full or in part. (Article 2 (39)).

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

This definition is intended, according to the recitals, to be technologically neutral. It can therefore include automation of execution using blockchain or distributed ledger technology or using another technique. It is also intended to apply only where the smart contract is used to execute contractual arrangements between different parties and not, for example, where smart contracts are used to automate a business's internal processes.

3.4.4 Essential requirements regarding smart contracts for executing data sharing agreements

According to Article 36 of the Data Act the vendor of an application using smart contracts or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall ensure that those smart contracts comply with the following essential requirements of:

(a) robustness and access control, to ensure that the smart contract has been designed to offer access control mechanisms and a very high degree of robustness to avoid functional errors and to withstand manipulation by third parties;

(b) safe termination and interruption, to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions;

(c) data archiving and continuity, to ensure, in circumstances in which a smart contract must be terminated or deactivated, there is a possibility to archive the transactional data, smart contract logic and code in order to keep the record of operations performed on the data in the past (auditability);

(d) access control, to ensure that a smart contract is protected through rigorous access control mechanisms at the governance and smart contract layers;

(e) consistency, to ensure consistency with the terms of the data sharing agreement that the smart contract executes.

Compliance with all of the above must be self-assessed by the smart contract vendor or the person deploying the smart contract commercially. The vendor of a smart contract or, in the absence thereof, the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall perform a conformity assessment with a view to fulfilling the essential requirements and, on the fulfilment of those requirements, issue an EU declaration of conformity (Article 36 par. 2) According to Article 36 par. 3, by drawing up the EU declaration of conformity, the vendor of an application using smart contracts or, in the absence thereof,

the person whose trade, business or profession involves the deployment of smart contracts for others in the context of executing an agreement or part of it, to make data available shall be responsible for compliance with the essential requirement.

The essential requirements should apply only to the vendors of smart contracts, although not where they develop smart contracts in-house exclusively for internal use. The essential requirement to ensure that smart contracts can be interrupted and terminated implies mutual consent by the parties to the data sharing agreement (Recital 104 of the Data Act).

3.4.5 Legal requirements for smart contracts

The use of smart contracts in the context of data sharing agreements shall not undermine the applicability of relevant rules of civil, contractual and consumer protection. Those laws will apply regardless of the technology used for the execution of agreements. As noted in Recital 104 "the applicability of the relevant rules of civil, contractual and consumer protection law to data sharing agreements remains or should remain unaffected by the use of smart contracts for the automated execution of such agreements**".**

For instance, agreements between data holders and data recipients cannot include unfair contractual terms (as regulated in Chapter IV of the Data Act). Agreements with consumers will need to comply with consumer laws and, in any case, agreements shall also comply with applicable civil and commercial laws.

3.4.6 Technical requirements for smart contracts and the "Kill switch"

A data holder may apply appropriate technical protection measures, including smart contracts and encryption, to prevent unauthorised access to data, including metadata, and to ensure compliance with the provisions of the Data Act, as well as with the agreed contractual terms for making data available.

According to Data Act (Article 11 par. 1), such technical protection measures shall not discriminate between data recipients or hinder a user's right to obtain a copy of, retrieve, use or access data, to provide data to third parties or any right of a third party under Union law or national legislation adopted in accordance with Union law. Users, third parties and data recipients shall not alter or remove such technical protection measures unless agreed by the data holder.

The use of smart contracts could be a useful tool to avoid the unauthorised use of the data by data recipients or the breach of the data sharing agreement. If the "smart contract" can automatically stop the flow of data to the data recipient upon the occurrence of one of the situations that the parties have agreed to provoke this result, the data holder would be in a better position to defend its rights. For instance, the data holder would not need to be proactively monitoring recipient compliance as, for many situations, a situation of non-compliance would result in automatic consequences

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Smart contracts must ensure that

(i) a mechanism exists to terminate the continued execution of transactions and that
(ii) it includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions[25].

The Data Act appears to assume that if the smart contract is being used to automate a data-sharing contract, then there are, by definition, two parties involved and that one of them can operate the switch.

The selection and design, development and deployment of smart contracts in the context and for the purposes of the project and its future use must take into consideration these technical and legal requirements embedded in the Data Act.

3.4.7 Technical Considerations

Already with the emergence of Bitcoin it became possible to encode some functionality within programming code and thus, to create some sort of smart contract on a blockchain-based system. Later on, most notable with Ethereum, it became possible to write smart contracts in languages that are turing-complete, thereby getting rid of a lot of restrictions in comparison to the programming capabilities with Bitcoin. While in theory turing completeness implies that arbitrary programs can be executed, there remain still a lot of technical limitations due to the fact that the connection from within blockchain-based systems to systems that are outside of it have to adhere to certain rules. Every information that becomes an input to a smart contract from outside has to be written from an authorised account which means that it is either given by a user or by a program, called “oracle”, without any user interaction. Oracles can be used to connect a blockchain-based system to external systems, but this comes with creating a trust issue. Either there have to be some guarantees that the oracle provides correct data or its potential untrustworthiness has to be taken into account. The limitation of the connection to the outside world is the most fundamental restriction of smart contracts on blockchain-based systems. A lot of clauses of legal contracts between persons or organisations refer to some data that can only be external to a blockchain-based system. Examples or this are weather data, stock markets or human interactions.

[25] This has been criticized by the industry as this requirement goes against the core tenets of decentralization and trustlessness that underpin blockchain technology. In a fully decentralised and automated system, none should be able to operate a kill switch. While a kill switch provides a means to intervene in instances of fraud, security breach or illegal activities, for example, purists argue that it undermines the core aspect of distributed ledger technology. In a fully decentralised and automated system, there would not be anyone to operate a kill switch

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Further technical limitations arise from the fact that programs that run on a blockchain-based system are intended to be short and computationally inexpensive. Furthermore, smart contract executions always have to be triggered externally, they can neither run periodically nor listen to certain events by itself. As smart contracts are not programs that are continuously running, they cannot be aborted or terminated in the usual sense. Deleting a smart contract is also not possible as an isolated action. As the code lies on the blockchain, deleting a smart contract would imply deleting all blocks of the blockchain starting from the block where the code is located. The only common way of deactivating a smart contract on a blockchain-based system is by including the functionality to prohibit every further data manipulation after a certain invocation. A smart contract that does not include this functionality can always be interacted with and thus, does not provide any way to be deactivated.

Blockchain-based systems can either be permissioned or not. While write access is always restricted by the use of accounts, read access is only restricted in permissioned systems. In non-permissioned systems the only way to restrict the read access is by restricting the access to the network, in particular to the blockchain clients. The focus of UNDERPIN lies on Ethereum, which is a non-permissioned system.

3.5 ARTIFICIAL INTELLIGENCE AND THE ARTIFICIAL INTELLIGENCE ACT

As mentioned in D.5.1 “Assessment of existing business models” with regard to the Manufacturing Sector, Data space business models in the manufacturing sector enable intelligent maintenance and dynamic asset management. Companies must use advanced technologies such as artificial intelligence (AI) and high-performance computing (HPC), which play a critical role in efficient data processing.

3.5.1 Ethical principles and requirements

When using AI both at the design and the development and deployment stages, Consortium partners are committed to respect the Artificial Intelligence (AI) ethical principles to be embedded into research activities that make use of AI systems/tools. These principles encompass the AI ethical principles established by the High-Level Expert Group on Artificial Intelligence (AI HLEG)[26].

[26] High-Level Expert Group on Artificial Intelligence , Ethics Guidelines for Trustworthy AI (2019). Additionally the principles adopted by the Institute of Electrical and Electronics Engineers (IEEE) are taken into account https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf

3.5.2 Human autonomy

The principle of human autonomy implies that AI-enabled technologies should be designed and deployed to respect, promote, and protect fundamental rights and to ensure human agency and oversight. AI-enabled technologies should preserve human dignity.

3.5.3 Prevention of harms

The principle of prevention of harms means that AI-enabled technologies should not cause harm or otherwise adversely affect human beings nor have detrimental consequences for individuals.

3.5.4 Fairness

The principle of fairness entails equality, diversity and the prevention of discrimination and stigmatisation against individuals and groups. Fairness can be achieved by i) promoting diversity, inclusion and non-discrimination; ii) fostering societal and environmental well-being while reducing potential harms; and, iii) adopting accountability measures.

3.5.5 Explicability

Processes need to be transparent, the capabilities and purpose of AI systems openly communicated, and decisions – to the extent possible – explainable to those directly and indirectly affected. Without such information, a decision cannot be duly contested. The principle of explicability requires transparency of the system which ultimately enables human oversight.

3.5.5.1 Requirements

These principles are translated into concrete requirements, that developers should implement and apply the requirements to design and development processes. The non exhaustive list of these requirements comprises:

1. **Human agency** and oversight Including fundamental rights
2. **Technical robustness and safety** Including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility
3. **Privacy and data governance** Including respect for privacy, quality and integrity of data, and access to data
4. **Transparency** Including traceability, explainability and communication
5. **Diversity, non-discrimination and fairness** Including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation
6. **Societal and environmental wellbeing** Including sustainability and environmental friendliness, social impact, society and democracy
7. **Accountability** Including auditability, minimisation and reporting of negative impact, trade-offs and redress.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

3.5.6 The Artificial Intelligence Act

3.5.6.1 Definitions

The AIA enshrines in EU law a definition of **AI systems** according to which 'An AI system is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments'. The definition is not intended to cover simpler traditional software systems or programming approaches, and the Commission has been tasked to develop guidelines on its application. This definition is intentionally broad to ensure that the legislation will be technology-independent/neutral and future-proof.

The act also contains a definition of general-purpose artificial intelligence (GPAI) models 'that are trained with a large amount of data using self-supervision at scale', that display 'significant generality' and are 'capable to competently perform a wide range of distinct tasks' and 'can be integrated into a variety of downstream systems or applications'. Furthermore, the AI act defines general-purpose AI systems as systems based on a GPAI model, which have the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems.

Other important definitions are:: Article 2 (3) 'provider' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge;

- Article 2 (4) 'deployer' means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity;
- Article 2 (8)'operator' means a provider, product manufacturer, deployer, authorised representative, importer or distributor.

3.5.6.2 Scope of application

The Artificial Intelligence Act[27] applies primarily to providers and deployers putting AI systems and GPAI models into service or placing on the EU market and who have their place of establishment or who are located in the EU, as well as to deployers or providers of AI systems that are established in a third country, when the output produced by their systems is used in the EU.

[27] REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

Concerning the ethical/legal issues that must be addressed by the UNDERPIN Consortium, the provisions of the Artificial Intelligence Act have to be taken into account.

The AIA does not apply to AI systems or AI models, including their output, specifically developed and put into service for the sole purpose of scientific research and development. However, it has to be taken into consideration that this exclusion a) does not cover testing in real world conditions, b) is without prejudice to the obligation to comply with this Regulation where an AI system falling into the scope of the AIAis placed on the market or put into service as a result of such research and development activity.

3.5.6.3 Risk-based approach

The AI systems are classified with different requirements and obligations tailored on a 'risk-based approach'. The levels of risk are not based on the underlying technological method used (machine learning, deep learning), but on the potential impact on 'fundamental rights' and the risk classification is based on the intended purpose of the AI system. The function performed by the AI system and the specific purpose and modalities for which the system is used are key to determine if an AI system is high-risk or not.

Levels of risks

- The AIA prohibits a wide range of AI practices because of their harmful impact (**unacceptable risks**), including social scoring, untargeted scraping of internet to create facial recognition databases or emotion recognition in workplace and education[28].
- The AI act identifies a number of use cases in which AI systems are to be considered **high risk** because they can potentially create an adverse impact on people's health, safety or their fundamental rights[29].

[28] As unacceptable risk are defined the following categories
- **Social scoring** for public and private purposes;
- Exploitation of vulnerabilities of persons, use of subliminal techniques;
- Real-time remote biometric identification in publicly accessible spaces by law enforcement, subject to narrow exceptions (see below);
- **Biometric categorisation** of natural persons based on biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs or sexual orientation. Filtering of datasets based on biometric data in the area of law enforcement will still be possible;
- Individual predictive policing;
- **Emotion recognition in the workplace and education institutions,** unless for medical or safety reasons (i.e. monitoring the tiredness levels of a pilot);
- **Untargeted scraping** of internet or CCTV for facial images to build-up or expand databases.

[29] As high risk systems are considered especially the following categories
- Certain critical infrastructures for instance in the fields of road traffic and the supply of water, gas, heating and electricity;
- **Education and vocational training,** e.g. to evaluate learning outcomes and steer the learning process and monitoring of cheating;
- **Employment, workers management** and access to self-employment, e.g. to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
- **Access to essential private and public services** and benefits (e.g. healthcare), **creditworthiness evaluation** of natural persons, and risk assessment and pricing in relation to life and health insurance;

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

- **Transparency risk**. Certain AI systems intended to interact with natural persons or to generate content may pose specific risks of impersonation or deception, irrespective of whether they qualify as high-risk AI systems or not. Such systems are subject to information and transparency requirements.
- **Minimal risks**. Systems presenting minimal risk for people (e.g. spam filters) will not be subject to further obligations beyond currently applicable legislation (e.g., GDPR).

3.5.6.4 High-risk systems

Attention must be paid to the potential identification of AI edge tools as 'high risk systems" as defined in the Artificial Intelligence Act. According to the classification of AI systems as high risk in Article 6, irrespective of whether an AI system is placed on the market or put into service independently of the products referred to in points (a) and (b), that AI system shall be considered as high-risk where both of the following conditions are fulfilled:

- (a) the AI system is intended to be used as a safety component of a product, or the AI system is itself a product, covered by the Union harmonization legislation listed in Annex I of Artificial Intelligence Act (such as civil aviation, vehicle security, marine equipment, toys, lifts, pressure equipment and personal protective equipment);
- (b) the product whose safety component pursuant to point (a) is the AI system, or the AI system itself as a product, is required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of that product pursuant to the Union harmonization legislation listed in Annex I of the AIA.

As high-risk systems are also considered (Annex III of the Artificial Intelligence Act) AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic, or in the supply of water, gas, heating or electricity (critical infrastructure). As regards stand-alone AI systems, namely high-risk AI systems other than those that are safety components of products, or that are themselves products, it is appropriate to classify them as high-risk if, in light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically pre-defined areas specified in this Regulation.
Both providers and users of high-risk systems have to comply with strict requirements to ensure that their AI systems are trustworthy, transparent and accountable. These include Conformity Assessments (with the rules before placing them on the market or putting them into service, and register their systems in an EU database that will be accessible to the public); Quality / Risk

- Certain systems used in the fields of **law enforcement**, **border control**, administration of **justice** and **democratic processes**;
- Evaluation and classification of emergency calls;
- Biometric identification, categorisation and emotion recognition systems (outside the prohibited categories);
- Recommender systems of very large online platforms are not included, as they are already covered in other legislation (DMA/DSA).

assessments ; Data governance (quality of data);Technical documentation ; Record/Logs keeping of their system's performance ; Information (inform users about the nature and purpose of their systems); Human oversight / intervention ; Accuracy, robustness, and cybersecurity.

3.6 Concluding remarks and recommendations

The UNDERPIN project is fundamentally oriented toward enabling secure and efficient industrial data sharing, providing a cross-organizational solution for the exchange of industrial data across various sectors. While the primary focus is on the sharing of non-personal industrial data, it is important to recognize that the activities related to data collection, exchange, and assessment may include information pertaining to employees, manufacturers, integrators, vendors, maintenance service providers, or remanufacturers, particularly when informational transactions reference identifiable individuals or services linked to personal data. Therefore, the UNDERPIN Consortium should ensure that data processing and personal data are broadly defined concepts under data protection frameworks and under applicable law.

Central to the success of UNDERPIN is its alignment with the evolving ethical, legal, and regulatory frameworks governing data sharing and artificial intelligence. In particular, the provisions of the Artificial Intelligence Act represent critical guidelines that the UNDERPIN Consortium must address in the selection, design, development, and deployment of technologies within the Data Space. These provisions emphasize the importance of transparency, accountability, and fairness in the implementation of AI-driven solutions, ensuring that the project not only meets technical requirements but also adheres to the highest ethical standards.

The implementation of smart contracts, a pivotal feature within the Data Space for automating and managing data exchange agreements, must also conform to the technical and legal requirements outlined in the Data Act. The Data Act establishes a clear framework for ensuring secure data transfers, safeguarding the rights of data providers, and promoting interoperability. Careful consideration of these legal requirements will ensure that the project maintains compliance while fostering trust and collaboration among participants.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

4 Validation through the Data Space and Next Steps

This section focuses on validating the proposed concepts, frameworks, and mechanisms for establishing trust creations processes within the UNDERPIN Data Space and assesses their contribution to the overall and success of the platform.

4.1 Validation through Underpin Business Roles

Business roles define the responsibilities and activities that participants perform within a data spaces. Each of these roles carries out specific tasks is related to specific services that uniquely contributes to the trust ecosystem. Data providers must ensure data quality and integrity, while consumers need to establish confidence in the reliability of data sources. Intermediaries facilitate data confidentiality and the integrity through governance frameworks, legal agreements, and technical standards that enhance transparency and security. Effective collaboration and communication among these roles are essential for fostering an environment where data sharing is perceived as safe and beneficial, ultimately driving innovation and enabling new business models, while to ensure sustainability, the business model must consider how these roles can contribute to the building of security and trust within the data space.

The UNDERPIN ecosystem features seven (7) distinct business roles, each contributing uniquely to the development, operation, and sustainability of the data space. These roles are designed to ensure a balanced and efficient ecosystem where every participant plays a critical part in supporting and advancing the data-sharing framework. These roles are analysed in Section 5.4 of D5.1 “Assessment of existing business models”, also outlined in the following table.

Table 2 Mapping of Business roles for UNDERPIN

Data provider	Provides data and makes it available to be shared within the data space.
Data users	Uses and processes data to solve a specific industry problem und create business value. Could include legals or natural persons or organisations.
Provider of core services	Responsible for deploying, operating, and maintaining all core services of the UNDERPIN Data Space
Provider of enabling services	Responsible for deploying, operating, and maintaining enablement services (e.g., EDC connector) according to UNDERPIN standards
Provider of on-boarding services	Responsible for deploying, operating, and maintaining onboarding services according to Catena-X standards. The onboarding services

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

	enable and support data space participants to register and onboard and offboard to UNDERPIN Data Space
Provider of business applications	Responsible for deploying, operating, and maintaining business applications to Catena-X standards. Business applications enable data providers and users to leverage different use cases and data-driven processes to solve a specific industry problem
Compliance Assessment Bodies	Ensure compliance with platform standards and regulatory requirements and play a crucial in the certification process.

4.2 Realisation through UNDERPIN

Lawful data governance is a cornerstone of creating and maintaining trustworthy, secure, and reliable services in a Data Space, while simultaneously upholding the principle of data sovereignty. Within the UNDERPIN project, trust among participants is established through an integrated approach that combines technical, legal, and organizational mechanisms. This ensures that data is not only shared securely and transparently but also that the rights and interests of all participants are upheld.

A critical aspect of validation in the Data Space lies in maintaining control over data. Participants retain sovereignty over their data, determining who can access it, under what conditions, and for what purposes. This control ensures that the data remains reliable and trustworthy, enhancing confidence among stakeholders. Additionally, validation also involves safeguarding the legal status of the data, ensuring that all exchanges and transactions comply with applicable laws and regulations, including the General Data Protection Regulation (GDPR) and the Data Act.

Finally, to enforce data-sharing agreements effectively and transparently, the project employs smart contracts. These automated tools enable the secure execution of predefined terms between parties without the need for intermediaries. By embedding contractual rules into blockchain-based smart contracts, the Data Space ensures that agreements are adhered to with minimal human intervention, reducing potential disputes and delays. This automation enhances the efficiency of data-sharing processes while ensuring transparency and accountability.

By implementing this rigorous framework, the UNDERPIN project establishes a secure and transparent ecosystem where all participants can engage in data exchanges with confidence. This approach not only enhances the functionality and trustworthiness of the Data Space but also sets a standard for ethical and lawful data governance, ensuring the long-term success and sustainability of the project.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

5 Conclusion

Deliverable D5.2, “Trust Creation Processes design” (due in M12), provided an in-depth analysis of the legal framework relevant to the UNDERPIN Data Space by addressing the legal requirements and regulations essential for governing data sharing, compliance, and governance. Deliverable D5.2 is developed under Task T5.1, 'Legal Framework and Good Practices Assessment,' which focuses on evaluating relevant legislation, principles and values regarding the sharing of personal and non-personal, including industrial, data within the context of the targeted sectors throughout the deployment of the UNDERPIN Data Space.

In this view, the deliverable evaluates key legislation, principles, and values related to the sharing of personal and non-personal, including industrial, data. Its insights and guidelines will play a pivotal role in ensuring the secure and ethical deployment of the UNDERPIN Data Space. The research outcomes are closely aligned with ensuring data governance that is secure, effective, and legally robust, adhering to the applicable legal framework in force.

Looking ahead, UNDERPIN is well-positioned to deliver significant value by addressing these legal and ethical challenges proactively. By incorporating the provisions of the Artificial Intelligence Act and the Data Act into its core design, the UNDERPIN Consortium ensures that the developed solutions frameworks are not only technologically innovative but also compliant and ethically sound. This alignment strengthens the long-term sustainability and scalability of the Data Space, promoting widespread adoption across sectors.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Bibliography

1. IDS Knowledge Base https://docs.internationaldataspaces.org/ids-knowledgebase/ids-ram-4
2. Gaia-X Trust Framework - 22.10 release. (n.d.). https://docs.gaia-x.eu/policy-rules-committee/trust-framework/22.10/
3. iSHARE Trust Framework: Advanced Solution for Data Sharing - iSHARE. (2024, July 18). iSHARE. https://ishare.eu/home/about/trust-framework/
4. Szabo, Nick. "Formalizing and securing relationships on public networks." *First monday* (1997).

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

Annexes

This section describes a preliminary version of the Terms and Conditions designed to regulate participation in the UNDERPIN Data Space

PLATFORM – TERMS

GENERAL

By using the platform [and applications] UNDERPIN-P, users indicate that they have read and understood the Terms of Use as described below and agree unconditionally to abide by them.

UNDERPIN-P shall have the right/is entitled, at any time and without notice, to amend or to supplement these Terms of Use, by posting the change/ modification to the website of UNDERPIN-P .The use of UNDERPIN-P after such posting shall constitute irrevocable acceptance [by the users] of these Terms of Use as amended. [. If the User does not agree to the amended or supplemented Terms of Use, he/she must refrain from using the Service, and he/she must close his/her Account.]

These Terms for User …… apply to Users when they are using the Service. They do not apply to Visitors……

The use of the UNDERPIN-P has to comply with the European and national law and the Terms of Use. The use of and access of UNDERPIN-P is permitted only for/ reserved only to the fulfilment of its aims, such as …….

Users should not use UNDERPIN-P in any manner that could damage, disable, or disturb the operation of UNDERPIN-P. and/or restrict or inhibit other users from using and enjoying UNDERPIN-P (and its services). The further use and/or reuse of data is subject to conditions and restrictions of the applicable regulatory framework

OWNERSHIP AND RIGHT(HOLDERS)

The ……. retains all ownership and other rights in the UNDERPIN-P

The rights with regard to the content of the website, the platform and applications of UNDERPIN-P are subject to applicable ……. intellectual and industrial property law.

Without prejudice to research and educational purposes, any modification, publication, performance, reproduction, distribution, transmission, transfer or any other use or exploitation

Co-funded by the European Union This project has received funding from the Digital Europe Programme under grant agreement No 101123179

of the content ,the platform and the applications of UNDERPIN-P, in whole or in part, is not allowed without the written permission of the rightholder.

CONTENT PROVIDED BY USERS-TERMS

The Users grant UNDERPIN-P a free, unencumbered, worldwide, non-exclusive licence for the use, reproduction, distribution and communication of the ……to….., and for making the Content available to…., to the extent that this is necessary for the Service agreed to be provided.

Before Content/ Data or Metadata …….can be contributed to the UNDERPIN-P, the User may be asked to create an Account in the manner agreed by/ described on the ……. During registration, the User must ……., which will provide access to the Account

It is the responsibility of the User to keep the Username/Password combination confidential. The User is therefore responsible for all use that is made of the Service through the Username and the Password.

Users who contribute (with) content or applications warrant and represent that they are the rightholders of intellectual property rights or that the rightholder of said rights has granted permission.

UNDERPIN-P disclaims and is not liable for the infringement of intellectual property rights on content or applications that have been contributed by users.

Users, who contribute content or applications warrant that they do not infringe rights of third persons/ parties, included the right to personal data protection

UNDERPIN-P examines requests, complaints and charges that are submitted by involved and/or affected persons and deal with them in accordance with applicable law.

In the event of breach of the law and/or any of these Terms, UNDERPIN-P. maintains the right either to remove the illegal content or to immediately delete the account of the user who is not complying with the law and/ or these Terms or to restrict the user's access.

GUARANTEES -DISCLAIMERS CONCERNING THE USE OF UNDERPIN-P

UNDERPIN-P does not guarantee that the Website/ Platform…. and/or the Service will at all times be accessible without interruptions or failures.

UNDERPIN-P does not warrant or represent that its services and applications will be uninterrupted or error-free.UNDERPIN-P is not liable for any errors, omissions or other defects in, delays or interruptions in the provision of [data] or for any action related to the exploitation of this data or derived therefrom.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

UNDERPIN-P makes every possible effort to operate in a scientifically accurate and technically seamless and safe manner. UNDERPIN-P disclaims, and it is not liable for the accuracy, adequacy, completeness and updating of ……. UNDERPIN-P disclaims all warranties with respect to the content, information, material, features/characteristics, services, goods, applications, opinions, statements that are provided or formulated by UNDERPIN-P or its users.

UNDERPIN-P makes no warranties with respect to the content and the operation of any site made available/accessible by UNDERPIN-P and/or any linked site.

For many or all the data, the data is by its nature approximate and will contain some inaccuracies. The data introduced by the data provider(s) or by the UNDERPIN-P may contain errors.

Any information created through the UNDERPIN-P should be used while taking into consideration that are products of modeling and computational procedures with assumptions, limitations that may lead to variable accuracy/precision and natural variability.

The content, features and outputs of UNDERPIN-P are provided to the visitors/users exclusively for …….use and cannot substitute ……..

PRIVACY-PERSONAL DATA PROTECTION

In connection with the Services/ use of…., the User will provide UNDERPIN-P with personal data as defined in the General Data Protection Regulation.

UNDERPIN will only process and use these personal data where necessary in connection with the Service, and it will not supply these personal data to Third Parties in any manner whatsoever, unless it is legally obliged to do so.

LIABILITY

Users must be aware of the abovementioned information and terms and consider them while using data, services and applications. UNDERPIN-P disclaims is not liable for miscalculations and/or error judgments or assessments.

UNDERPIN-P disclaims any liability for any positive damage or loss of profit**, arising out and/or in connection with the substance or the use of data, services and applications provided by UNDERPIN-P.**

It assumes no liability for damage or loss as a result of any failure in fulfilment of the provision of the Service, including but not limited to damage or loss arising from or relating to the use of the Website and/or any impossibility of using it, or as a result of any unlawful act or otherwise, unless this exclusion of liability is not allowed under mandatory provisions of law.

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179

The User indemnifies UNDERPIN-P against all Third-Party claims on any grounds whatsoever that relate to the compensation of damage, loss, costs or interest, in connection with or arising from his/her use of the Platform/ Service and/or any breach of these Terms and/or any other rights of Third Parties

CLOSE DOWN AND OR CHANGES

UNDERPIN-P is entitled, without any prior notice being required and without being liable to compensate the User, to close down or to temporarily close down the …….. and/or to limit the use of it if it considers this necessary, for instance in connection with any reasonably necessary maintenance of the ……and/or the ……...

UNDERPIN-P is entitled, without any prior announcement being required, to make procedural and technical changes and/or improvements to the Platform. Website and/or the Service

APPLICABLE LAW

These terms of UNDERPIN-P are governed by and construed in accordance with ……. Law. In the event of any dispute arising in relation to these Terms of UNDERPIN-P, to submit to the exclusive jurisdiction of the courts of ……

Co-funded by the European Union
This project has received funding from the Digital Europe Programme under grant agreement No 101123179