RE4DY

MANUFACTURING DATA NETWORKS

Title	D2.4: Digital 4.0 continuum value network industrial agreements
Document Owners	KUL
Contributors	KUL
Dissemination	Public
Date	30/09/2025
Version	V01

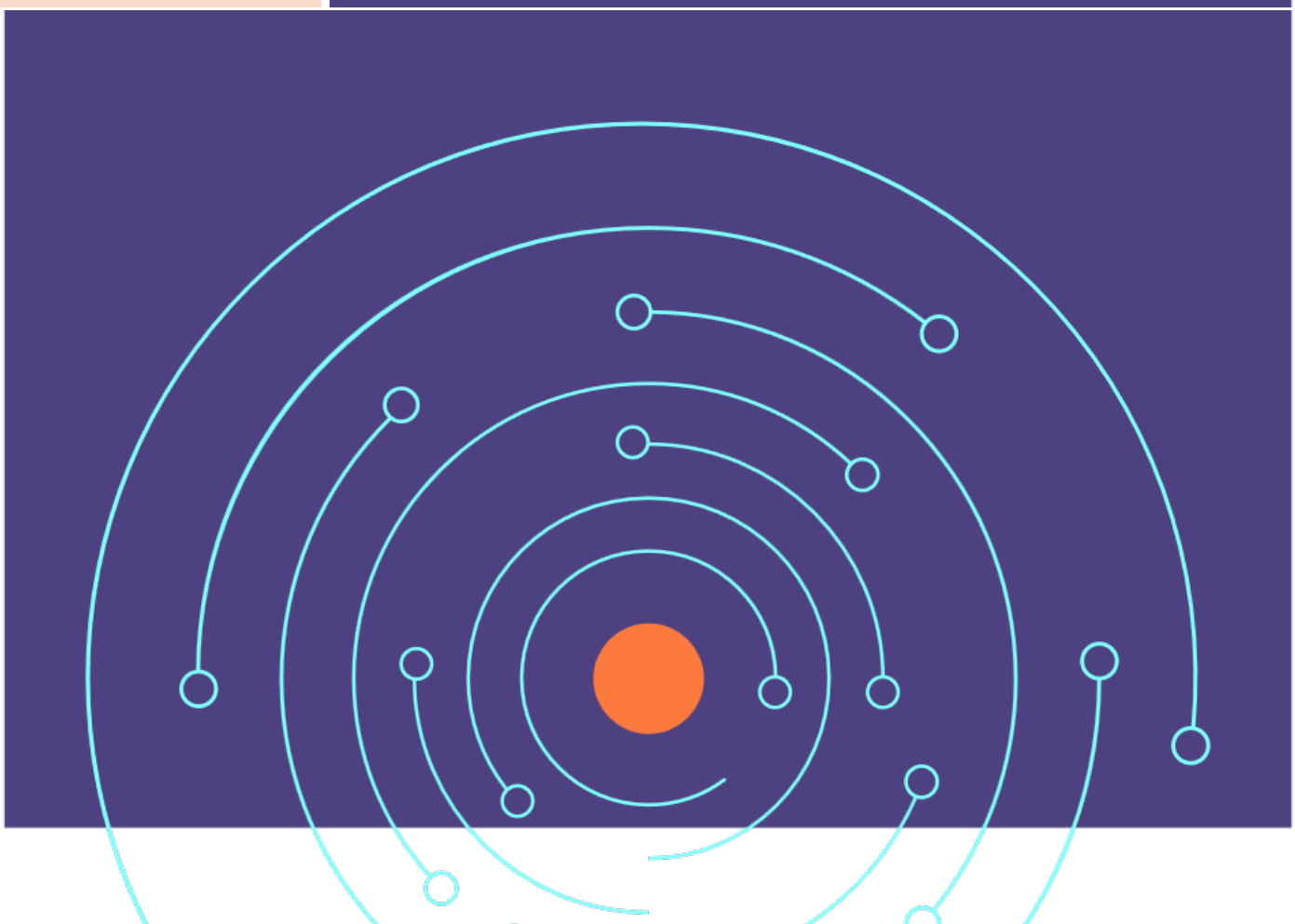

Table of Contents

Index of Figures

Index of Tables

Document Status

Leader	KUL
Internal Reviewer 1	ATOS
Internal Reviewer 2	CORE
Work Package	WP2 - Digital 4.0 Continuum Reference Architecture for Active Resiliency
Deliverable	D2.4: Digital 4.0 continuum value network industrial agreements
Due Date	M36
Delivery Date	30/09/2025
Version	V02

Version History

02/07/2025	Deliverable structure, ToC
24/09/2025	Version for peer-review
28/09/2025	Reviewer feedback
29/09/2025	Final version integrating reviewer comments

Further Information

More information about the project can be found on project website: https://re4dy.eu/

Disclaimer

Project Partners

Num	Participant organisation name	Acronym
1	ASOCIACIÓN DE EMPRESAS TECNOLÓGICAS INNOVALIA	INNO
2	CHALMERS TEKNISKA HOGSKOLA AB	Chalmers
3	INTERNATIONAL DATA SPACES EV	IDSA
4	VOLKSWAGEN AUTOEUROPA, LDA	VWAE
5	ASSECO CEIT AS	CEIT
6	UNINOVA-INSTITUTO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIAS-ASSOSIACAO	UNI
7	FILL GESELLSCHAFT MBH	FILL
8	AVL LIST GMBH	AVL
9	VISUAL COMPONENTS OY	VIS
10	UNIVERSIDAD MIGUEL HERNANDEZ DE ELCHE	UMH
11	ATLANTIS ENGINEERING AE	ATLANTIS
12	DATAPIXEL SL	DATA
13	CORE KENTRO KAINOTOMIAS AMKE	CORE
14	UNIVERSITETE I OSLO	UiO
15	GE AVIO	AVIO
16	ENGINEERING-INGENIERIA INFORMATICA SPA	ENG
17	POLITECNICO DI MILANO	POLIMI
18	ATOS IT SOLUTIONS AND SERVICES IBERIA SL	ATOS IT
18.1	ATOS SPAIN SA	ATOS ES
19	KATHOLIEKE UNIVERSITEIT LEUVEN	KU
20	NETCOMPANY-INTRASOFT SA	INTRA
21	NOVA ID FCT - ASSOCIACAO PARA A INOVACAO E DESENVOLVIMENTO DA FCT	NOVA
22	INDUSTRY COMMONS FOUNDATION (INSAMLINGSSTIFTELSE)	ICF
23	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH
24	GRUPO S 21SEC GESTION SA	S21SEC
25	UNIVERSITAT POLITECNICA DE VALENCIA	UPV
26	CONSIGLIO NAZIONALE DELLE RICERCHE	CNR
27	SOCIEDAD ANDALUZA PARA EL DESARROLLO DE LAS TELECOMUNICACIONES SA	SANDETEL
28	SWITZERLAND INNOVATION PARK BIEL/BIENNE AG	SSF
29	GF MACHINING SOLUTIONS AG	GFMS ADVMAN
30	FRAISA SA	Fraisa SA
31	SIEMENS SCHWEIZ AG	SIE

List of Abbreviations

Acronym/Abbreviation	Description
AI / AIA	Artificial Intelligence / Artificial Intelligence Act
AIaaS	Artificial Intelligence as a Service
B2B	Business to Business
CC0 / CC-BY	Creative Commons Zero / Creative Commons By Attribution
CDT	Cognitive Digital Twin
CJEU	Court of Justice of the European Union
CRA	Cyber Resilience Act
CVS	Common Vocabulary Standard
DA	Data Act
DGA	Data Governance Act
DaaP	Data as a Product
DaaS	Data as a Service
DT	Digital Twin
EC	European Commission
ECJ	European Court of Justice
EPO	European Patent Office
ESO	European Standardization Organization
EU	European Union
FDI	Federated Digital Infrastructure
FRAND	Fair, Reasonable, and Non-Discriminatory
GDPR	General Data Protection Regulation
GPAI	General-Purpose Artificial Intelligence
GUI	Graphical User Interface
HDT	Human Digital Twin
IP	Intellectual Property
IPR	Intellectual Property Right
MCT	Model Contractual Term
NIS	Network and Information Systems
PET	Privacy Enhancing Technology

RCA	Relational Contractual Agreement
SaaS	Software as a Service
SLA	Service Level Agreement
SMEs	Small and Medium-sized Enterprises
TDM	Text and Data Mining
UML	Unified Modeling Language
URL	Uniform Resource Locator

Executive Summary

This report considers the contractual, IP, and standardisation predicates to deploying a digital twin platform in the smart manufacturing sector. It complements the technical and organisational solutions previously introduced in RE4DY D2.3, as well as the regulatory framework for the sharing of non-personal data and the initial evaluation of intellectual property (IP) rights in digital twins introduced in the same deliverable.

The RE4DY project revolves around the sharing of **data as a product** in cyber-physical **digital thread** loops, all with the aim of enabling **cognitive digital twins** to assist in smart manufacturing applications that include logistics planning, E-battery design, machine tool self-optimisation, and predictive zero-defect turbine manufacturing. To enable complex data platforms such as digital twins, it is necessary to strike appropriate **industrial agreements** – multilateral agreements that span federated digital infrastructures (such as those anticipated by the RE4DY reference architecture), common vocabulary standards (such as the outlined RE4DY manufacturing resilience ontology and the legal ontology of IP rights proposed in READY D2.3), and relational contractual agreements. It is precisely this latter category that D2.4 addresses in order to round out the RE4DY project's contribution to a holistic framework for the deployment of digital twins in industrial value chains.

This report adopts Richard Kemp's eight-layer stack framework for legal reasoning over data in order to granularly analyse the contractual and IP challenges posed by digital twins as complex IP subject matter. Notably, it reveals the IP issues that may be posed by the adoption of proprietary semantic standards at the information architecture level, the interface between different configurations of data and intellectual property rights including patents, copyright, the *sui generis* database right, trade secrets, confidentiality rights, and trademarks. Attention is also paid to the applicability of text and data mining rules to digital twin use cases, underlining the importance of clearly defined rights regarding combined and derived data in the Digital 4.0 continuum, as well as revealing potential issues with data retention due to digital twin overfitting and memorisation when using deep learning models.

This report also notes the most pertinent obligations under personal data protection law for deploying a (personal) digital twin, particularly with regard to establishing appropriate data governance practices and internal privacy policies.

The importance of risk management for digital twins is highlighted both in terms of complying with cybersecurity obligations and with regard to establishing an effective data governance framework. A four-step approach to defining a data governance framework is recommended, consisting of (i) Risk management, (ii) Strategy statement, (iii) Policy statement, (iv) and Process and procedures.

The report identifies key contractual issues to be covered by digital twin data sharing agreements, including IPR assignment, post-termination data transfers, license term, joint ownership, data quality and provenance, confidentiality and security, liability, training obligations, compensation, dispute resolution, and contract termination. Using the most recent draft of the model contractual terms for data sharing from the Data Act as an example, this report illustrates the alterations that would be needed to align generic data sharing agreements with the specific needs of digital twin solutions. Anticipating the potential importance of open data in Industry 4.0, this report also flags potential issues

with data license incompatibility and offers recommendations on choosing data licenses to maximise compatibility.

Finally, this deliverable considers the interface between the RE4DY regulatory framework and harmonised standards, certification schemes, and codes of conduct. It identifies the provisions in each law that invite standardisation or compliance via soft law, aggregates all extant and approved soft law instruments for complying with each legal instrument, and collates the various European and international industrial standards and technical specifications that can facilitate the deployment of digital twin solutions. This report concludes by summarizing salient challenges (and their potential solutions) in the standardisation landscape, namely ensuring broader representation for small and medium enterprises and civil society in the standardisation process, as well as establishing sustainable financial arrangements for standardisation bodies in the face of recent Union case law on free disclosure of harmonised standards.

1. Introduction

1.1 Context and scope of this document

The main objective of this deliverable is to facilitate the deployment and adoption of the RE4DY project's Digital 4.0 Continuum by providing a legal analysis of the contractual, intellectual property, and standardisation framework of operating a Cognitive Digital Twin (CDT). The document is structured as follows:

Chapter 2 introduces the concept of industry agreements, defines the main categories of industry agreements, and presents the main Industry 4.0 paradigms that underly the RE4DY project's innovations. Subsequently, Chapter 2 motivates this report's choice to focus on contractual agreements for data sharing and IP management by identifying them as the primary organisational obstacles to deploying RE4DY CDTs.

Chapter 3 represents the main thrust of this report's analysis and focuses on the contractual an intellectual property aspects of data sharing in digital twins. Digital twins are explored as multi-party data platforms through the lens of Richard Kemp's eight-layer stack of data management which covers contractual, intellectual property and regulatory considerations. This is followed by an analysis of specific contractual terms that are essential in the procurement of data services for the purpose of creating a Digital Twin. Emphasis is laid on license compatibility in settings where datasets distributed on different licensing terms are aggregated into a single unit.

Chapter 4 switches the focus away from relational contractual agreements and analyses the role of soft law in enabling the legal compliance and technical deployment of the RE4DY CDT fabric. It identifies key technical standards, codes of conduct, and certification schemes for the project's context, then provides a general overview and policy recommendations on the current standardisation landscape in the European Union.

Chapter 5 summarises the findings of this report.

1.2 Relationship with other RE4DY deliverables

This deliverable complements the technological and organizational solutions introduced in RE4DY deliverables D2.1, D2.2, and D2.3.

To preserve this deliverable's focus on the contractual and standardisation aspects of RE4DY, the regulatory aspects of data sharing in EU law have already been introduced in RE4DY D2.3, alongside a discussion of the legal merits of data as a product and a preliminary presentation of IP rights and challenges in the context of CDTs. Thus, Section 3.6 on the Regulation of Non-Personal Data refers the reader back to Section 3.1 of RE4DY D2.3 to avoid repetition.

2. Industry Agreements & Industry 4.0 Technologies

2.1 Industry Agreements

Industry agreements (IAs) are a vital element of the European digital ecosystem, insofar as they act as enablers of (cross-)sectoral data spaces. The term IAs refers to a wide variety bilateral or multilateral agreements that may be concluded to address any building block of a data space or other collaborative data sharing ecosystem, including business, governance, legal, data interoperability, data sovereignty & trust, and data value creation enablement.[1] While IAs have not been formally defined by an EU legal or public policy body, an European Commission (EC)–sponsored study has defined IAs as "agreements on functions and interfaces between industry players that create markets and market opportunities leading to ecosystems and standards" (CARSA et al., 2021). From this definition, IAs are subsequently classified as either Federated Digital Infrastructures (FDIs), Common Vocabulary Standards (CVS'), and Relational Contractual Agreements (RCAs). It is important to note that IAs are distinct instruments from both codes of conduct and standards by virtue of always addressing, at minimum, some level of technical specification in conjunction with some level of legal and governance specification. Conversely, while standards are able to influence technical and data specifications, they lack guidance on governance and legal arrangements. Codes of conduct, in comparison, typically address behavioral norms and potentially governance mechanisms, but lack a strong interface with technical specifications and are typically excluded from the development of new specifications (CARSA et al., 2021).

In the context of the RE4DY project in particular, as well as in next-generation smart manufacturing more generally, IAs are expected to act as predicates for the core technological innovations that typify Industry 4.0, namely: data as a product (DaaP), digital threading, and digital twins (DTs).

2.2 Industry 4.0 Technologies in RE4DY

The main technologies and industrial paradigms that underly the RE4DY innovations in the manufacturing sector are closely related to each other, to the extent that they can be considered interdependent in practice.

At the most basic level – that of individual data units – the **DaaP** concept entails a transition in digital value chains away from transactions with raw data or pre-generated insights, and instead toward the sharing of data "packages" that include the data itself together with relevant metadata, code and services for data management, and the enabling infrastructure for further DaaP operations (Nizamis et al., 2025). The aim of DaaP is to render data discoverable, interoperable, trustworthy, accurate, secure, and self-describing in its semantics and syntax, which ultimately serves to align the transacted

[1] Building Block nomenclature developed by the DSSC and available at: https://dssc.eu/space/BVE2/1071252426/Building+Block+Overview

data in DaaP operations with the FAIR guiding principles for data management (Wilkinson et al., 2016).

In parallel to the adoption of the DaaP paradigm, **DTs** are another avenue by which manufacturers may significantly reduce costs, improve outcomes, and refine processes. A DT is defined by the Digital Twin Consortium as "an integrated data-driven virtual representation of real-world entities and processes, with synchronized interaction at a specified frequency and fidelity."[2] The Digital Twin Consortium (2022) further defines "cognitive" DTs as DTs which are furnished with AI functions and cognitive capabilities that allow them to learn at run-time by computing "the status, behaviours, and relevant interrelated models of the real-world elements in digital environments." DTs are notable for their capacity to *inter alia* validate designs before the underlying product is put into production, effectuate predictive maintenance at optimal time intervals, accurately evaluate the performance of assets already in use, improve resource management in complex supply chains, and enable reliable trialling of planned product and process alterations without disrupting the real-world systems already in place (Javaid et al., 2023).

The increased interoperability, accessibility, and quality of DaaP value chains, coupled with the heightened monitoring and forecasting capabilities of digital twins, directly contributes to the development of so-called "**digital threads**", which are defined as the creation of "a closed loop between the digital and physical worlds, transforming how products are engineered, manufactured and serviced" and the following of "a single set of related data as it weaves in and out of business processes and functions to enable continuity and accessibility" (CARSA et al., 2021). Margaria and Schieweck (2019) consider digital threads as information-relay frameworks that trace an asset along its entire lifecycle and clarify that these frameworks include "any data, behaviours, models, protocols, security, and their standards related to the asset as well as to the context where it is expected to operate." Digital threads are thus reliant upon DTs for establishing the closed loop between the physical and digital versions of products, and they are further enabled by the DaaP paradigm's provision of high-quality, interoperable, and secure data packets.

Digital threads are broad operational frameworks rather than specific physical or digital entities. In governance terms, the proper implementation of a digital thread is first and foremost a matter of agreeing on appropriate technical standards and, as far as IAs are implicated, establishing the necessary CVS' and FDIs to ensure that physical and digital artifacts are traceable across the value chain and between different manufacturers according to consistent schema (CARSA et al., 2021).

In contrast, a DT represents a concrete cyber-physical system, a multi-party data platform whose operation is contingent upon specific contractual, regulatory, and governance needs. Furthermore, DTs, at least in the RE4DY context, by their nature necessitate multiparty data sharing arrangements for their functioning. Thus, this deliverable focuses its analysis mainly on DTs as the composite legal subject matter that underlies the RE4DY use cases' innovations within the manufacturing sector.

[2] Digital Twin Consortium, 'What is a Digital Twin?', available at: https://www.digitaltwinconsortium.org/initiatives/the-definition-of-a-digital-twin/

3. Contractual and IP Aspects of Data Sharing in RE4DY Digital Twins

3.1 The Eight-Layer Stack of Data Management

In order to provide an ordered and systematic structure to its analysis of intellectual property, contracts, and regulation in the context of digital twins, this deliverable adopts the eight-layer stack model for a legal framework for data as developed by Richard Kemp (2025). This framework for legal analysis over data places platform infrastructure and information architecture at the bottom, followed by IP, contract, and regulatory concerns, and ending with information security and data governance & management at the top of the stack.

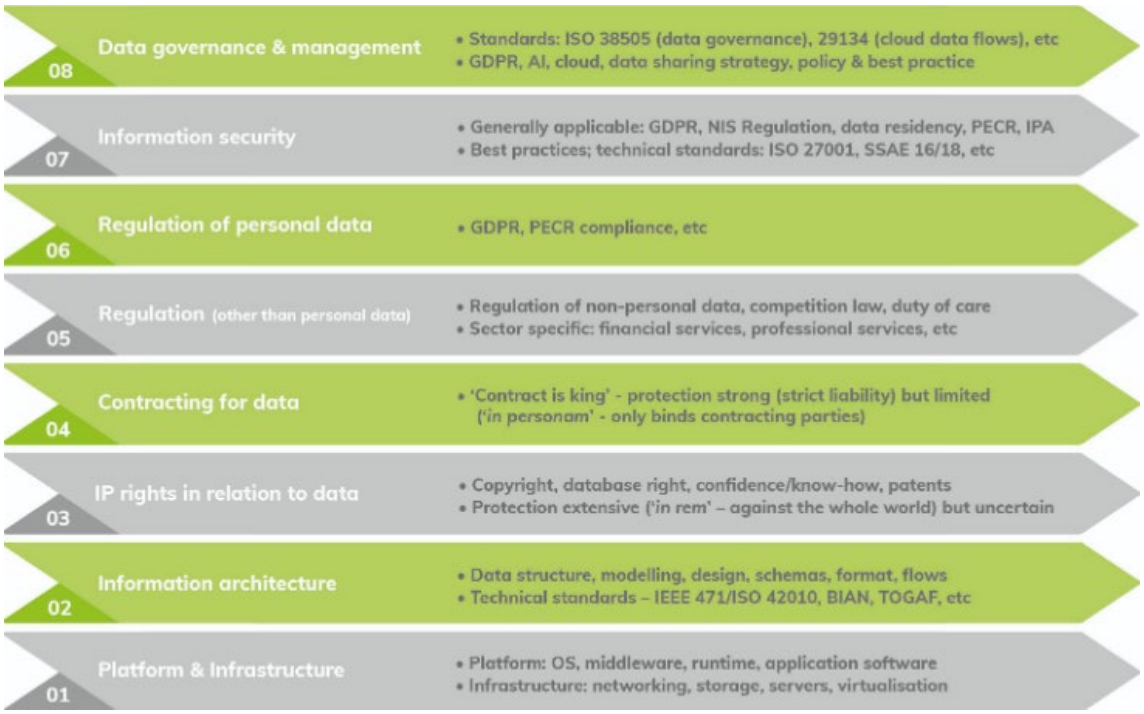

Figure 1: Kemp's eight-layer stack of a common legal framework for data.

3.2 Level 01: Platform and infrastructure

The platform and infrastructure level (level 01) comprises the physical infrastructure of the DT platform, including data centres, connectivity, routers, servers, storage, virtualization, and the software (e.g. operating system and middleware) which runs on the platform. Per Kemp, the core legal considerations in level 01 involve intellectual property and

contractual issues related to software copyright (e.g. rights in computer languages and (graphical) interfaces,), as well as the interplay between copyright and database rights in accessing and extracting the data stored in the software. It is also possible that (graphical) interfaces may be protected by (un)registered design rights or by trade marks.

3.3 Level 02: Information architecture

Between the platform and infrastructure on the one hand and the data on the other hand lies the information architecture level (level 02). This level involves designing the database schema (the formal structure and organization of the database) based on the information flow and the data model in the real world. As specified by Kemp, the data model is a representation of the data and its flow as entities, attributes, and interrelationships that can be recognized and processed by all information systems that conform to the information architecture. The information architecture also includes the data standards and API specifications that overlap from a software perspective but may differ in their functionality and coherence. The information architecture may be based on standardized models, such as ISO/IEC 42010 (a conceptual meta model of the terms and concepts for architecture description), TOGAF (an open standards based enterprise information architecture network), Lambda (an information architecture for handling very large datasets for real time and batch processing), or Kappa (a similar architecture to Lambda but with a single 'hot' or real-time path for all data flows).

Kemp highlights that information architectures are often not given sufficient attention in terms of their intellectual property status. The documents that describe and define the information architecture are usually protected by copyright as literary works. Database schema may also be eligible for copyright protection, pursuant to Directive 96/9/EC of 11 March 1996. Finally, Kemp underscores that for information architectures based on standardized models, the licensing of the IP rights is determined by the policy of the relevant standard-setting organization that manages the standard.

In the context of DTs and Industry 4.0, a key issue emerging from the information architecture level relates to the manner in which published specifications that define semantics (semantic standards) affect the design of data schemas and software. Such semantic standards can guide both data collection and interpretation, as well as code development (Morrison, 2023b). Since semantic standards establish and harmonise data semantics, technical interchange, and legal status, they are crucial for data-intensive platforms such as DTs, which rely on both data availability and the right to use and reuse information (Morrison, 2023b).

As already discussed in Section 2.1, semantic standards themselves can be considered a type of industry agreement. Morrison (2023a) proposes a taxonomic division of standards into several classes, including general controlled vocabularies and structured taxonomies on one hand, database-oriented standards such as database schemas and entity-relationship models on the other hand, or even software-oriented standards such as UML class diagrams. Finally, Morrison (2023a) identifies a category of mixed role semantic standards, which includes information exchange specifications, reference architectures, and formal ontologies.

As with any technical standard, data standards have different legal implications depending on, *inter alia*, their associated intellectual property rights and licensing arrangements. Data standards may qualify for copyright protection as databases under the EU Database Directive, and they may also independently qualify for copyright

protection as long as they can meet the prerequisite originality requirement. Various licensing frameworks may govern data standards, including Fair, Reasonable, and Non-Discriminatory (FRAND) terms, non-open public licenses, Open Definition-compliant licenses, and proprietary licensing agreements. It is therefore necessary to consider whether and how intellectual property rights attached to data standards can affect the software and datasets that conform to said standards. If works that rely on data standards for both semantics and exchange structures are seen as adaptations (i.e., derivative works) of those standards, then the use of non-open standards may create legal challenges for software or datasets distributed under otherwise suitable open licenses.

A significant issue in determining whether software and datasets complying with a semantic standards could be seen as adaptations with original contributions that warrant copyright protection is that the right to adaptation is not harmonized across the EU. As a consequence, there is no single concept of 'adaptation' across the Member States. Adaptation could therefore encompass modification of the form of expression (e.g., via transcription or translation), adaptation to customize the results (e.g., via localization of content), or enrichment of content via the addition of new elements (e.g., as in the case of combinations).

While a consideration of national provisions on copyright and related rights is outside of the scope of this deliverable, it is still relevant to consider the implications of a scenario in which the creation of conformant code and datasets is tantamount to adaptation and where, consequently, copyright protection attaches independently to the original work (in the form of a semantic standard) and to the creation of an adapted work (in the form of code or datasets).

Usually, naming conventions, entity attributes, and structural relationships would leave clear traces in conformant code or datasets. Without the original semantic standard, it would be impossible to create the adapted work. Furthermore, any changes to the underlying semantic standard would require changes to the adapted work as well, so as to maintain a wider interoperability. The adapted work would be subject to distribution, reproduction, or communication to the public, all of which are copyright-relevant acts subject to the authorization of the rightsholder. Since the copyright in the work being adapted remains intact, any proprietary terms in the underlying work may collide with any other terms applied to the complying code or dataset, whether open license terms or otherwise. Additionally, patent rights in the underlying work may present an additional obstacle to release under open terms, especially with licenses that exclude patent grants (e.g., CC0-1.0). Every attempt at separating the underlying work and the additional contributions made to create the adapted work would be practically futile. Where the objective is to maximize permissive usage on open license terms, the only real solutions seem to be licensing on CC0-1.0 or MIT terms (Morrison, 2023a).

3.4 Level 03: Intellectual property rights in data

Level 03 revolves around the IP rights in relation to data, which in turn encompass copyright, database rights, confidentiality, and trade secrets.

3.4.1 Patents and data in digital twins

While patents would apply to processes and software that manipulate data, normally there would be no patent rights in data itself. Nevertheless, data may play an important role in attaining patents over other components of an Industry 4.0 DT, such as the computer-implemented simulation itself.

In Europe, patents are granted for any inventions in all fields of technology, so long as the inventions have a technical character. Technical character is acknowledged if the claimed subject-matter requires the presence of any technical means, e.g. a computer. Consequently, at least in principle, any computer-implemented method constitutes a patentable invention.

The question about the technical character of an invention depends on two independent criteria, namely whether the invention is adapted to a specific technical implementation and whether it is an application to a field of technology. As a matter of principle, computer-implemented methods of simulating certain physical phenomena with the purpose of solving a technical problem can therefore be patentable. Thus, it is possible, for example, to patent a simulation of pedestrian crowd movement in an environment with the purpose of adapting the design of a building structure.[3]

Computer-implemented simulations are problematic because it is often difficult to establish a direct relationship with the physical world. The European Patent Office (EPO) has confirmed that a simulation can contribute to the technical character of the invention if, for example, it serves as the basis for: technical input (e.g., measurement from a sensor), technical output (e.g., machine control signal), or production of so-called 'functional data' to control a technical device, when adapted specifically for its technical use, adapting the simulation (software) to the computer or its operation that results in technical effects (e.g., better use of storage capacity or bandwidth), or adapting the computer or how it works to the simulation.

Identifying the technical effect in a computer-implemented simulation is not always straightforward and patent applicants may face considerable challenges in identifying, for example, whether a particular type of data qualifies as functional or not. This can become the deciding factor between an invention that has a technical character and is therefore patentable, and an invention that is devoid of any technical character and is therefore excluded as abstract subject matter.

EPO case law distinguishes between cognitive data and functional data but simultaneously rejects the notion that these two are the only kinds of data that exist.[4] The EPO illustrated the significance of the distinction between functional data and cognitive information content in relation to technical effect and character with the example of a TV signal. The board argued that a complete loss of the cognitive content resulting in a humanly meaningless picture like "snow" on a television screen has no effect on the technical working of the system, while loss of functional data will impair or even completely halt the technical operation of the system.[5] It is worth mentioning that functional data may

[3] G 0001/19 (Pedestrian simulation), No. ECLI:EP:BA:2021:G000119.20210310 (Enlarged Board of Appeal 10 March 2021).
[4] T 2049/12 (Data structure for defining transformations / MICROSOFT) 09-05-2019, reasons 5.8.
[5] T 1194/97 (Data structure product/PHILIPS) 15-03-2000, reasons 3.3.

not always be technical,[6] and that the relevant question for assessing whether a data structure has technical character is rather whether it produces a technical effect.[7]

In sum, while data *per se* does not constitute patentable subject matter, it can play a role in the assessment of the technical character of a claimed invention, particularly in the context of computer-implemented simulations running on a DT of a physical asset.

3.4.2 Trade marks and data in digital twins

Trade marks in the EU are regulated on both the Union level via Regulation (EU) 2017/1001 (the Trade Mark Regulation) and on the national (or regional) level via Directive (EU) 2015/2436 (the Trade Marks Directive). In either case, a trade mark can be claimed over "words, including personal names, or designs, letters, numerals, colours, the shape of goods or of the packaging of goods, or sounds," which are capable of distinguishing the goods or services of one undertaking from those of another undertaking and which are capable of being represented in a register in a manner that enables the clear and precise identification of the trade mark's subject matter.[8]

Under the above definition, data *per se* is not eligible for trade mark protection. However, data products as described in Section 2.2 may contain elements eligible for trade mark protection. More specifically, brands, names, symbols or other GUI elements that accompany a data product and serve to distinguish it may be subject to trade mark protection.

In consequence, the DaaP paradigm imposes a novel concern on Industry 4.0 actors to consider trade marks already at level 03 of the data management framework and engage in appropriate IP clearance practices prior to operating a DT platform.

3.4.3 Copyright, database rights, and data in digital twins

In the context of data in digital twins, copyright would normally subsist in software and documentation such as research publications, technical and user documents, information architectures, and databases. In this context, one important question of relevance to digital twins as platforms aggregating datasets from different sources in an assemblage concerns the extent of the database right to the maker of a database under the Database Directive.

3.4.4 Statutory reporting data, open data, and database rights

Even information provided under compulsory statutory reporting can obtain protection under the EU Database Directive. An illustrative example can be found in the national proceedings initiated by German journalist Michael Kreil, who took legal action against the

[6] T 2049/12 (Data structure for defining transformations / MICROSOFT) 09-05-2019, reasons 5.8.

[7] T 2049/12 (Data structure for defining transformations / MICROSOFT) 09-05-2019, reasons 5.8.

[8] Regulation 2017/1001 Art. 4; Directive 2015/2436 Art. 3

Free State of Bavaria to obtain a court ruling that the journalist be allowed to use data from an official database that contains geographical information for a journalistic publication.[9]

The Bavarian State office for Digitalisation, Broadband and Surveying filed a criminal complaint against the journalist on grounds of making a database with allegedly protected geographic data available online for downloading. The Bavarian government based its case on the database producer right.

The Kreil case was settled without an official court ruling on Kreil's claim after the Munich courts expressed support for the journalist's position in a preliminary hearing (Morrison, 2023a). As part of the settlement, Kreil was provided the geographical data free of charge and offered a cost-free license over said data.

The Kreil case illustrates, on one hand, how database producer rights may be claimed in collections of data even if the information is of public interest. On the other hand, it is also evident that a case-by-case approach is critical in identifying protected compilations of data within the scope of database producer rights, as well as in identifying permitted further uses of data protected by database rights. It is therefore critical for any digital twin solutions relying in whole or in part on open data to verify whether their database is entangled in the exclusive rights of a database producer.

3.4.5 Infringing use of databases: the criterion of significant detriment to the investment

Against this background, the Court of Justice of the EU (CJEU) has recently narrowed down the criteria that apply to investment and risk exposure on which the *sui generis* database right protection hinges. In the case of *CV-Online Latvia v Melons*[10], the Court ruled that it is not sufficient for the claimant to prove that the defendant has extracted or re-utilised all or a substantial part of the contents of the database without the permission of the database maker. The court took the view that the claimant must also demonstrate that these actions constitute a risk to the possibility of redeeming that investment through the normal operation of the database in question.[11] In other words, the claimant must be able to prove not only that extraction or re-utilisation has occurred, but also that the alleged infringer has, through his or her acts, caused significant detriment to the investment.[12]

In this context, it is also worth mentioning that it is settled case law that the resources used for the development of materials which make up the contents of a database are not protected by the *sui generis* database right of the maker of the database. The CJEU ruled in the *British Horseracing Board* case that the investment does not cover the resources used for the creation of materials which make up the contents of a database.[13] This case narrowed down the scope of the database right, especially for real-time databases.

---

[9] Gesellschaft für Freiheitsrechte e.V, State Geodata: Bavaria abuses copyright to restrict freedom of the press https://freiheitsrechte.org/en/themen/demokratie/staatliche-datenbank-urheberrecht Also reported in R Morrison, 'Commodification of Public Interest Information - Open Data'. Open Energy Modelling Initiative (blog), 31 January 2023. https://forum.openmod.org/t/commodification-of-public-interest-information/3661.

[10] CJEU, Case C-762/19, CV-Online Latvia SIA v Melons SIA, ECLI:EU:C:2021:434

[11] CJEU, Case C-762/19, CV-Online Latvia SIA v Melons SIA, ECLI:EU:C:2021:434, para 47

[12] CJEU, Case C-762/19, CV-Online Latvia SIA v Melons SIA, ECLI:EU:C:2021:434, para 39.

[13] ECJ, Case C-203/02, The British Horseracing Board Ltd and Others v William Hill Organization Ltd, ECLI:EU:C:2004:695, para 42.

The Dutch case of *Euronext v TOM and BinckBank*[14] is also relevant in this regard. Euronext, the successor of the Amsterdam Stock Exchange, ran the AEX index of Dutch companies whose shares were traded on its exchange, and a series of options based on the AEX index. TOM was an options trading platform that created, issued, and offered a different options contract by almost entirely copying Euronext's AEX index and options database. The Dutch court distinguished this case from the *British Horseracing Board* case by emphasizing that the investment in compiling a football fixtures list in those cases "did not require much effort" and did not match Euronext's investment in its AEX index option series, which included about 50,000 components annually, the accuracy of each of which was vital. With this ruling, the Dutch court essentially found that financial market data may be indirectly protectible by the *sui generis* database right.

In view of this case law, both procuring entities and suppliers in Digital Twin projects must be cautious when utilising databases which consist of data whose volume and nature may require significant efforts on the part of the database maker to obtain, verify, or present. Procuring entities and suppliers must also be aware that it is immaterial whether the collection is based on a data feed not directly provided by the database. The concepts of extraction and re-utilisation are not limited to cases in which extraction and re-utilisation take place directly from the original database. Otherwise, the maker of the database would not be protected against unauthorised copying from a copy of his database.[15]

3.4.6 Confidentiality rights

Copyright and database rights do not extend to the content of information itself. Nonetheless, equitable principles of confidentiality could offer a more appropriate means of protecting against the disclosure of substantial data that is not widely known to the public. Protection might also cover compilations of information even where individual parts may be publicly available but are not considered confidential on their own. Protection can also apply to data derived from the initially confidential information.

Similarly, the trade secrets regime of the EU Trade Secrets Directive[16] may apply to data if it meets certain conditions. Participants in the operation of a digital twin must be careful to ensure that secrecy is clearly demonstrable and that it would not erode in the environment of a DT platform that may be accessible to a wide range of entities. Related issues concern the technical steps that must be taken to ensure the secrecy of data, the steps needed to prove ownership, and how to identify, document, and keep records of the trade secret in datasets that are subject to continuous changes, e.g. through enrichment and augmentation.

3.5 Level 04: Data Contracts

Level 04 (contracting for data) addresses contractual rights in relation to data. These rights should be analysed separately from intellectual property rights. Indeed, data suppliers are entitled to impose a charge for the use of their data, regardless of any intellectual property rights that may or may not subsist in that same data. As confirmed

[14] Hague District Court, Case/Registration No C/09/442420/HA ZQ 13-152, para 4.36

[15] ECJ, Case C-203/02, The British Horseracing Board Ltd and Others v William Hill Organization Ltd, ECLI:EU:C:2004:695, para 52.

[16] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

by the British court in the case of *British Horse Racing Board*, the supplier has 'in the data, a valuable commodity, for which it is entitled to charge.'[17]

It should be kept in mind, however, that the entitlement to compensation for the provision of data is not absolute. Statutory obligations can alter what is considered an acceptable contractual arrangement depending on the nature of the data, its provenance, and the identities of the parties sending and receiving the data. As already discussed in greater detail in Section 3.1.2 of RE4DY Deliverable 2.3 "Digital 4.0 Continuum Reference Framework Final Version", the Data Act (DA)[18] stipulates that raw (as opposed to inferred) data from connected products and related services must be made available free of charge by the data holder to the user of the connected product or related service. If the user demands that the data is transferred to a third-party data recipient rather than directly to the user, the data holder is entitled to impose a charge on the third-party data recipient (as opposed to the data user). Even in this circumstance, Art. 9.1 DA establishes that the imposed charge must be limited to a "compensation" that is non-discriminatory, reasonable, and potentially includes a margin. Per Article 9.2 and 9.3 DA, the compensation should take into account *inter alia* costs related to data formatting, transmission, and storage, the data's volume, format, and nature, as well as the investments in the collection and production of the data and each involved party's contribution in obtaining, generating, and collecting the data. While it is not yet clear in practice how to operationalize the notion of "reasonable compensation" and how to arrive at an acceptable margin in relation to this compensation, Art. 9.5 DA obliges the EC to adopt guidelines on calculating reasonable compensation. At the time of writing, these guidelines are still forthcoming, as is the EC's formal recommendation of model contractual terms (MCTs) and standard contractual clauses for complying with the DA's contractual fairness regime regarding B2B data sharing agreements as described in RE4DY D2.3

Contracts create rights and obligations that are legally binding and enforceable. The main challenge with data contracts is that they are only effective between the contracting parties and not against third parties (privity of contract). Even though data contracts may and often do regulate IP rights and the data and content covered by those rights, IP rights that subsist by operation of law should be distinguished from contractual IP matters.

3.5.1 Text and data mining as a contractual matter

Even though text and data mining (TDM) is an exception to copyright, it is a matter that needs to be addressed with priority in data contracts executed in Digital Twins projects.

The EU Copyright Directive[19] introduced a new exception to copyright under the heading of text and data mining. TDM is defined as any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends, and correlations.[20] The Copyright Directive provides for a specific "permitted act" exception where research organisations and cultural heritage

[17] Attheraces Ltd & Anor v British Horse Racing Board & Anor [2005] EWHC 3015 (Ch) (21 December 2005), para 285.
[18] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828
[19] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.
[20] Art 2(2) Copyright Directive 2019/790

institutions carry out TDM for the purposes of scientific research on material protected by copyright and database rights that they have lawful access to.[21] Per Art. 7(1) of the Copyright Directive, this exception may not be excluded by contract. The Copyright Directive provides an even more general exception for TDM on lawfully accessible material for commercial purposes under Art. 4(1), but this exception may be disapplied where the rightsholder has expressly reserved the right "in an appropriate manner such as machine-readable means in the case of content made publicly available online".[22]

One relevant question for Digital Twin projects is whether the TDM exception granted for commercial purposes under the Copyright Directive can be relied upon to build digital twins using materials protected by copyright and/or *sui generis* database rights. In light of the broad scope of the definition of TDM, there is nothing to prevent DT platform operators from relying on the exception to derive analytical information from materials protected by copyright and database rights where reproduction or extraction may be performed without authorisation from the rightsholder. Additionally, Recital 9 of the Copyright Directive provides that text and data mining can also be carried out in relation to mere facts or data that are not protected by copyright. Mere facts and data that would not be protected by copyright include, for example, measured data (e.g., surface roughness or object geometry), observed data (e.g., a failing production machine), metadata (e.g., time of failure) and any other kind of factual data that captures phenomena from objective reality. In such instances no authorisation is required under copyright law.

Whenever Industry 4.0 parties rely on text and data mining to develop DT solutions, incl. computer simulations, they must consider the limitations to the TDM exception. Namely, the scope of application of the TDM exception is limited to (1) direct or indirect temporary or permanent *reproduction* by any means and in any form, in whole or in part, of a *work*; (2) permanent or temporary *reproduction, translation, adaptation, arrangement*, and any other *alteration* of a *computer program*; (3) temporary or permanent *reproduction* by any means and in any form, in whole or in part, of a *database*. In addition, the works or databases must be lawfully accessible to the entity that relies on the TDM exception, e.g., on the basis of a license or another statutory exception or limitation. With regard to storage, reproductions and extractions may only be retained for as long as necessary for the purposes of TDM. In the context of DTs, Emanuilov and Margoni (2024) find that this implies a need for rigorous testing for overfitting and memorisation wherever DTs employ deep learning models. In any case, the TDM exception does not cover the right of communication to the public or any other copyright-relevant acts that are not explicitly denoted under the exception. Finally, the TDM exception only applies where rightsholders have not expressly reserved the use of works for TDM. For digital datasets, this reservation would normally be made using machine-readable means.

The related question of the rights that apply to derived data in DT projects can be complex because of the background intellectual property position of the involved parties. These complexities are best addressed through clear and express contractual provisions. Clear contractual provisions are all the more necessary in cases where EU intellectual property frameworks are not harmonized, as in the case of the right of adaptation discussed above under level 02. Where derived data is the result of TDM, the rules on TDM apply, particularly the retention periods for temporary or permanent reproductions of the covered works and other subject matter. Contractual provisions must specifically focus on whether the user

[21] Art 3(1) Copyright Directive 2019/790
[22] Article 4(3) Copyright Directive 2019/790

is entitled to create derived data and what rights the user would have to use and share the data.

Similarly, the rights in combined data, where input data from multiple sources is combined to create a new dataset, should be addressed in contracts by clear and express stipulations. Without a specific right in contract, the original provider seeking to protect their stake in the combined data may find that copyright and database rights are not helpful. Where the provided data is confidential, confidentiality law or trade secrets protection might offer a remedy.

In DT projects, metadata also holds significant interest, especially for cloud and data service providers looking to produce more metadata. Providers often aim to create this using anonymised data, whether for data analytics or other objectives. Establishing clear contractual rights and responsibilities is a necessity when managing these kinds of inquiries.

3.6 Level 05: Regulation of non-personal data

The non-personal data regulation layer (level 05) concerns the regulatory aspects relating to the data localisation requirements, open data, smart data, and other sector-specific regulation. The core elements of horizontal EU regulations on non-personal data have been examined in Section 3.1 of Deliverable 2.3 "Digital 4.0 Continuum Reference Framework Final Version", although any DT platform will necessitate a further consideration of sector-specific and national legislation that may apply to the envisioned DT context.

3.7 Level 06: Data protection

The data protection layer (level 06) addresses considerations of data protection compliance and data governance related to the collection and use of personal data.

While the RE4DY project pilots, generally, do not involve the processing of personal data, it is nevertheless possible that other Industry 4.0 implementations of DTs will necessitate regulatory compliance with personal data protection rules. This is particularly the case when one considers so-called "human digital twins" (HDTs) or "personal digital twins", Gaffinet et al. (2025) define an HDT as "a class of Digital Twin whose twinned entity is a human individual. It is a digital representation of the twinned human, emulating their state and dynamics. It automatically receives data, with optional manual entries, and provides automatic feedback directly to the twinned human." While Gaffinet et al. (2025) tie the HDT phenomenon more closely with the concept of Industry 5.0, prior studies such as that by Naudet et al. (2021) have positioned the HDT concept within Industry 4.0 as a core enabler of resilience by way of ensuring that "humans can be integrated in predictive maintenance processes […] and undesirable events caused by human behaviour can be anticipated for dynamic adaptation of the shop floor".

Regardless of their corresponding industrial generation, HDTs carry significant regulatory obligations vis-à-vis the European legal framework for personal data protection. The

General Data Protection Regulation[23] (GDPR) establishes several core principles of personal data protection under Art. 5:

- Lawfulness, fairness, and transparency: any personal data (i.e., any information relating to an identified or identifiable natural person per Art. 4(1) GDPR) must be processed lawfully, fairly, and transparently, according to a valid legal basis.
- Purpose limitation: personal data must be collected for the previously specified purposes and not further processed in a manner incompatible with those purposes.
- Data minimisation: personal data must be processed only insofar as they are adequate, relevant, and limited to the necessities of the specified purpose.
- Accuracy: personal data must be kept accurate and up to date.
- Storage limitation: personal data must only be stored for as long as necessary for the specified processing purpose.
- Integrity and confidentiality: processing operations must be secure and protected against unauthorised/unlawful processing and accidental loss, destruction, or damage.
- Accountability: the controller (i.e., the entity which determines the purposes and means of personal data processing) is responsible for demonstrating compliance with the GDPR's personal data processing principles.

The GDPR establishes concomitant rights for data subjects, which individuals may exercise in relation to processing of their personal data[24]:

- The right to be informed: information regarding personal data processing should be communicated in an accessible and easy to understand manner.
- The right of access: a general right to information regarding the parameters of personal data processing operations in relation to a data subject, as well as a right to obtain a copy of the implicated personal data.
- The right to rectification: a right to have inaccurate or incomplete data rectified or completed without undue delay.
- The right to erasure: the right to have personal data be erased without undue delay, pursuant to certain legal conditions.
- The right to restrict processing: the right to limit the processing of personal data to mere storage until certain legal conditions are met.
- The right to data portability: the right of a data subject to receive from one controller and transmit to a different controller a machine-readable and appropriately formatted copy of their personal data.
- The right to object: the right to object to processing of personal data predicated on the legal basis of public interest, exercise of official authority, or legitimate interests.
- The qualified right not to be subject to a decision based solely on automated processing.

In order to achieve compliance of HDTs or other personal data processing operations in an Industry 4.0 context, it is vital for industry actors to foresee appropriate technical and

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
[24] Arts. 12-23 GDPR

organisational measures via contractual provisions and internal policies. These measures should include, *inter alia*, the specification of:

- A robust data governance framework. Lis et al. (2023) identify the following core elements of such a framework: the identification of available and relevant data; clarifying the ownership and usage rights over relevant data; assigning responsibilities for coordinating and aligning data activities; creating transparency and lineage of data usage internally and externally; and defining conditions of data sharing.
    - These governance elements should be used to inform a privacy policy for each industry actor implicated in the DT platform.
- Privacy notices appropriate for the specific data subjects whose data is to be processed.
- Consent and data access platforms for data subjects, where relevant.
- Employee training procedures to ensure that the privacy policy is respected.
- A plan to address personal data breaches in alignment with the RE4DY resilience framework described in Section 2 of D2.3. This plan should envision steps for anticipation (via incident response training), coping (via incident identification and notification, breach containment, and threat elimination), and adaptation (via recovery and incident analysis protocols).
- Privacy-enhancing technologies (PETs) (e.g., trusted execution environments, encryption, secure multi-party computation, differential privacy) should be considered and implemented (preferably in conjunction with each other), in accordance with the required level of personal data protection necessitated by the type of data being processed and the estimated danger of personal data breaches. PETs trade utility for security, therefore it is important to strike an appropriate balance between the demand for privacy and security on one hand, and the demand for e.g. computational efficiency on the other.

Appropriate governance frameworks are discussed in further detail under level 08 below, (data management and governance).

3.8 Level 07: Information security

The information security layer (level 07) addresses concerns related to network and information security. A DT deployed in the manufacturing industry context can be considered as a networked, multi-party platform in a safety-critical sector. As such, the entities deploying and using this information system may be subject to significant cybersecurity due diligence obligations.

The manufacturing sector is identified by the EU NIS2 Directive as a critical sector,[25] and undertakings active within this sector are thus considered 'important entities' per Art. 3 NIS2. Under NIS2 Directive Art. 21, these entities must take appropriate and proportionate technical, operational, and organisational measures to manage risks posed to the security of network and information systems which those entities use for their operations or for the

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

provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

As complex data systems that integrate physical and cyber components, digital twins are also vulnerable to cyber threats. Strengthening their cyber resilience is critical to ensure the integrity and security of virtual models and other decision-support tools and services that may be offered as part of the digital twin. Depending on their position in the supply chain, suppliers of digital twin solutions may qualify as economic operators, manufacturers, importers, or distributors of products with digital elements under the Cyber Resilience Act (CRA).[26] Under CRA Art. 3(1), products with digital elements are broadly defined as software or hardware products and their remote data processing solutions, including software or hardware components being placed on the market separately. Various components of a digital twin may qualify as products with digital elements, which means suppliers would be obliged to ensure their products meet the essential requirements and the requirements for important products with digital elements, such as securing authentication and access, intrusion prevention and detection, endpoint security or network protection, as well as network management, configuration control, or virtualisation.

3.9 Level 08: Data management and governance layer

The data management and governance layer (level 08) encompasses the organisation's data activities, such as input, processing, and output operations, and the organisation's structured approach to managing data projects.

Emerging business models such as data as a service (DaaS) or AI as a service (AIaaS) change the way in which DT platform participants share and use data. These new business models enable organisations to assess where to invest and whether to source data/AI in-house or to outsource them to a third party. To do this, however, DT contracting parties must clearly understand their rights and obligations in procurement and service agreements. The following challenges must be addressed as a matter of organisation-wide policy:[27]

- Each type of right is subject to its own rules: intellectual property contracts and regulatory obligations each contain discrete sets of legal rules which must be observed simultaneously but which must be analysed and complied with through separate legal means.
- Rights are primarily national, and they may operate differently in different countries: for example, data localisation requirements may be justified on different grounds related to public security in different Member States.
- Rights and duties apply concurrently to each element of the data stack: intellectual property rights, contracts, and regulatory obligations may apply

[26] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828

[27] The following list of challenges is based on the list in R Kemp, Legal Aspects of Data – Rights and Duties (Kemp IT Law, v4.0, March 2025), available at: https://kempitlaw.com/wp-content/uploads/2025/04/Legal-Aspects-of-Data-Rights-and-Duties-KITL-v4.0-1.pdf

concurrently to the same datasets. For example, a dataset may be subject to intellectual property rights (e.g., database right, copyright, or trade secrets), contractual rights and duties (e.g., between a data supplier and the procuring entity), and data protection regulation (e.g., for personal data contained in the dataset).

- Rights and duties may be multi-layered: as data travels through multiple database systems, different rights may be conferred on different parties and each of these parties may seek to impose different contractual obligations to different actors in the supply chain based on its own regulatory duties.
- Data is created at great speed which increases the evidence burden: the evidential burden in dispute resolution may be time consuming and costly.

Contracting parties should develop a structured approach to data projects, such as digital twins. Practical, incremental management can be built into a structured approach to data governance based around four steps:

- Risk management
- Strategy statement
- Policy statement
- Process and procedures

The objective of the risk assessment is to evaluate, assess, document, and correct current data usage practices. This phase should concentrate on pinpointing data origins, conditions of data provision, and usage policies. Following the identification of these elements, there should be an evaluation to ensure these practices are in line with current contracts and licenses. The outcome of these evaluations should be a documented report offering suggestions for a rectification plan and suggesting a strategy and policy for the future.

The strategy statement outlines the organisation's overall approach, objectives, and governance policies for data management. It should be crafted by a diverse working group that includes at least senior executives, the legal department, and the chief information officer. A critical part of this effort is to involve all stakeholders, clarify their main goals concerning data, and establish success metrics. Moreover, the strategy statement must be in sync with other organizational strategies regarding data privacy, security, information architecture, data science methodologies, artificial intelligence use policies, and intellectual property management controls.

The policy statement elaborates on the execution of the strategic vision. It addresses the organisational setting, structural framework, leadership and oversight specifications, data sharing methods, and the creation of standardised project planning procedures. The intention of examining the personnel context is to finalise the specifics of the institutional structure, such as steering committee, task force, data compliance officer, and so forth. The policy needs to mandate a project planning routing for specific data initiatives that, at the very least, encompasses:

- Scope and dependencies
- Resources
- Deliverables
- Timeline
- Authority levels
- Approval processes

The working group and policy statement must also address the legal considerations around compliant data sharing and use.

The in-depth methods and procedures signify the concluding phase that prescribes the specific processes an organisation should implement within its data management routines. This encompasses standards and timings for executing data protection impact assessments, recognising and rationalising legitimate interests, compatibility and information security analyses, methodologies for anonymisation and pseudo-anonymisation, acceptable artificial intelligence usage policies, ethical guidelines, and so forth.

Entities should embrace a standards-driven method for managing data in DT initiatives. This means treating data not only as valuable business assets but also recognising its associated risks and liabilities, such as potential data breaches. Organisations should implement uniform processes for managing the life cycle of their data, ensuring adequate protection and establishing policies that lead to increased efficiency. Technical standards like ISO/IEC 38500, which deals with IT governance for organisations, along with ISO/IEC 38505 focused on governing data, and ISO/IEC 19944 can provide a solid foundation for creating a framework that addresses data accountability mapping and governance.

3.10 Contractual terms for the digital twin solutions in Industry 4.0

Implementing a DT may require contracting with a variety of industrial partners, including cloud-based hosting services, software providers and consultancy services, and even research organisations offering access to state-of-the-art methods. Each of these relationships need to be defined, designed, and documented with procurement, consultancy, and other service agreements.[28]

Acquiring DT technologies implies a transition to service contracts that span longer periods. Indeed, with the advent of data-driven services, suppliers have gradually shifted from merely selling assets like sensors, to delivering services. This transition necessitates reaching an agreement on key performance indicators for the continued performance throughout the contract's duration.[29]

Ownership and control of the Digital Twin may belong to the procuring entity or entities or to the supplier, with title to the asset potentially remaining with the supplier. In the case of collaborative manufacturing DTs, it is vital to identify background and foreground IP prior to establishing an ownership regime for the DT platform itself.

In any case, as a minimum, the entity procuring a DT solution must have access to the digital twin and its input and output data. This requires contractual terms for data flows and digital services linked to the industrial assets, e.g. the RE4DY pilots' tool machinery or logistical centres. It is recommended to conceptualise the DT as a platform offering a variety of services, including visualisation, simulation, and validation. The following table

[28] Osborne Clarke, Digital twins: enabling sale of a service, not an asset, 14th June 2022, https://www.osborneclarke.com/insights/digital-twins-enabling-sale-service-not-asset.
[29] Osborne Clarke, Digital twins: enabling sale of a service, not an asset, 14th June 2022, https://www.osborneclarke.com/insights/digital-twins-enabling-sale-service-not-asset.

outlines the components of a DT platform and the most appropriate legal regimes for protecting access and usage.

Asset	Applicable legal regime	Legal tools to impose access and usage conditions	Remarks
Software, incl. digital twin platform cloud infrastructure and visualisation/simulation software	**Copyright** (computer programs)	License agreement and/or service agreement	If the platform runs only from a cloud instance, no license agreement is required.
Original datasets	N/A	Contractual restrictions on access and usage rights	Where data sets are combined from different sources, license compatibility must be assessed on an ad-hoc basis.
Enriched datasets	***Sui generis*** **database rights**	License agreement or contractual restrictions on access and usage rights	N/A
Visualisation	**Copyright** in 2D/3D models (graphical works)	License agreement or contractual restrictions on access and usage rights	N/A
Simulation	**Patents**, where the digital twin interacts with an external physical reality at the level of input or output (e.g. calculates or predicts the physical state of an existing real object)	License agreement	The technical effect must be clearly demonstrable, e.g., by feeding the model with the input parameters and direct conversion of the simulation results into output signals for the control or optimisation of an industrial asset.
Analytical results and insights	**Trade secrets**	Non-disclosure agreement or a confidentiality clause in a service agreement.	N/A

Table 1: Legal regimes and tools for discrete DT assets.

In structuring the contractual and intellectual property management framework for the DT, the working assumption should be that, as a matter of principle, no intellectual property rights subsist in data and that access and usage restrictions should be imposed by means of contractual arrangements. This is particularly the case for dynamic data sets accessed through APIs.

Indeed, legal obligations and entitlements interact with data distinctively. When transacting with data, parties to a DT should conceptualise data not as a commodity with inherent rights, but as the subject matter of a contract around which rights and responsibilities emerge. Specifically, Graux (2021) recommends that contracting parties check whether the terms are independently created by the data provider or whether they follow a standard contractual term template. It should then be verified that the terms define usage rights that cover the anticipated usage throughout the expected lifecycle of the DT.

Parties can freely make contracts within the limits of the law, based on the principle of freedom of contract. This means that the party that controls the data can set specific conditions for its counterparty to access, use, and share the data. These conditions usually include the purpose and duration of access and use, as well as rules on confidentiality and data sharing with third parties. Data contracts are governed by general contract law with interfaces with horizontal EU digital legislation such as the Data Act. This gives the parties the most flexibility, so long as they respect certain mandatory rules, e.g., the rules of public order and the general legal principle to act in good faith when fulfilling obligations and performing contracts (Hemmer and Woltering, 2021).

The following contractual aspects for the procurement of a DT solution in the collaborative manufacturing domain should constitute essential considerations in the development of any DT platform. Where possible, each essential contractual term is accompanied by an example formulation sourced from the most recent (May 2025) draft of the Model Contractual Terms developed by the European Commission's Expert Group on B2B data sharing and cloud computing contracts. These MCTs were drafted to support the data sharing modalities anticipated under the Data Act, namely (1) obligatory data sharing between data holders and users of connected products and related services; (2) data sharing between users of connected products and related services and data recipients; (3) obligatory data sharing between data holders and data recipients at the request of users of connected products and related services; and (4) voluntary data sharing between data sharers and data recipients. The MCTs under category 4 are most relevant for the RE4DY context, wherein it is assumed that parties voluntarily enter into data sharing contracts to establish and operate digital twin platforms. Each illustrative MCT is accompanied by remarks on the alterations it might require in order to better suit the specific needs of RE4DY/Industry 4.0. Notably, the MCTs are intended to act as benchmarks for fair data sharing contracts rather than ready-to-use legal documents for every occasion. Thus, this report does not critique the MCTs so much as it suggests adaptations to underline the unique needs of RE4DY data sharing profiles.

Intellectual property rights

Licensing of intellectual property rights in data is managed contractually by most organisations, usually under the heading of 'intellectual property'. Thus, intellectual property rights clauses may need to be amended in existing contracts. Amendment can vary but usually involves at least changing the scope of permitted use, i.e., content protected by intellectual property rights may be used in the building of a digital twin. As a rule of thumb, data should be addressed both at the input and the output of a DT.

Entities that seek to retain control and exclusive rights over the input data should have these demands reflected in the contract. Questions that should be answered via contractual clauses include:

- Who owns the intellectual property rights in the input data and what licenses need to be granted and to whom?

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 6.1.2. "The Data protected as trade secrets and the identity of the Trade Secret Holder are set out in the Appendix 2." 7.1.2. "Subject to the payment of the compensation under this contract, the Data Sharer hereby grants the Data Recipient for the term of the contract a worldwide, non-exclusive, non-transferable license, to use, copy, modify, enhance and maintain the Data that would be covered by an Intellectual Property Right solely to the extent necessary under the contract. A sublicense to the Data Recipient's subcontractors is authorized only for the purposes of the subcontracting and to the extent they are not incompatible with the provisions of this Contract." c.f. ANNEX II and ANNEX IV, "If, during this contract, new data are made available to the [User/Data Recipient] that is protected as trade secrets as set forth in clause [4/11 5.1.1], at the request of the Data Holder, Appendix 4 will be amended accordingly."	Must be adapted to also foresee other rights in datasets besides trade secrets, e.g., the *sui generis* database right. In the case of data products in the DaaP context, which may contain data models and pipelines in addition to raw data, it is also possible to anticipate the existence of copyright or even trade mark within the aggregate data product. Alterations may be desired in the parameters of the provided license under 7.1.2, particularly in order to reflect the permissions that entities in a collaborative manufacturing environment may require from each other in order to carry out their roles in a Digital Twin environment. The Annex V data sharing clauses out to be bolstered by a forward-facing clause such as those identified under Annex II and Annex IV, which allow the relevant Appendix to be amended to include new IP-protected data that is made available during the course of the contract. This is important for the continuous operation of DT platforms, whose capabilities and data sources are may evolve over the course of their lifespan.

Table 2: MCTs for IP in input data.

- Who should own the intellectual property rights in the output data? This is usually the party that is best positioned to exploit the rights (e.g., the supplier) but procuring entities may want to engage in revenue sharing mechanisms.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 7.2.1 "Should the use of the Data by the Data Recipient under this contract generate tangible work products	The MCTs do not distinguish between different categories of Results generated by the

which are capable of being protected by Intellectual Property Rights ("Results"), it is hereby agreed that: (select only one option) 7.2.2 [OPTION 1] The Data Recipient shall become the sole owner of any and all Intellectual Property Rights relating to the Results. Only the Data Recipient may, at its discretion, register for or obtain any such intellectual property title. 7.2.3 [OPTION 2] The Parties will be jointly and equally entitled to the Intellectual Property Rights on the Results and shall enter into a separate contract describing the modalities of the exercise of such rights. 7.2.4 [OPTION 3] The Data Recipient agrees to assign, to the extent necessary, to the Data Sharer the full legal and beneficial ownership of, and all Intellectual Property Rights in, the Results on an exclusive basis for a consideration to be further agreed between the Parties, worldwide, for the entire duration of Intellectual Property Rights. 7.2.5 The Parties moreover agree that further licensing on the Results shall be granted as follows (select as many options as appropriate): [OPTION 1] (specify the party which does not own IPR on the results) hereby grants to the (specify the owner of the IPR on the Results), for the duration of protection of Intellectual Property Rights, a fully paid worldwide, non-exclusive, non-transferable license to use, copy, modify, enhance and maintain its Pre-Existing Elements solely to the extent necessary to perform its rights on the Results under this Clause. [OPTION 2] (specify the owner of the IPR on the Results) hereby grants to the (specify the Party which does not own IPR on the results), for the duration of protection of Intellectual Property Rights, a fully paid worldwide, non-exclusive, non-transferable license to use, copy, modify, enhance and maintain the Results solely for the following purposes: (please fill in as applicable).	use of the data being contracted for. In a DT use case, it is preferable to adopt a more granular approach and explicitly address intellectual property rights in the individual components of a DT (i.e., output data, visualisations, and simulations). Parties to a DT should consider defining expected categories of Results in an Appendix to the contractual agreement before assigning rights to the individual Results via the main body of the contract. As above, alterations may be desired in the parameters of the provided license under 7.2.5.

Table 3: MCTs for IP in output data.

- How will data be transferred to the data holder or controller upon termination of the agreement, and will there be any additional charges levied by the supplier for carrying out transfer activities?

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 9.3.2 [OPTION 1] [The Data Sharer must take appropriate exit support measures as the Data Recipient may reasonably expect.]	It is important to clarify not just the expectation that data is transferred following the termination of the agreement,

[OPTION 2] The Data Sharer must take the following exit support measures: (specify).]	but the precise modality of transfer (e.g., transfer/access medium and timing) plus the expectation (if any) regarding remuneration for the transfer.

Table 4: MCTs for data transfers following termination of the agreement.

Term of license

When using copyrighted material to create digital twins, the license should be granted for at least as long as the digital twin is planned to operate, which usually matches the lifespan of the asset, process, or system that the DT represents.

It should also be clarified what rights the original rightsholders may have, if any, over the digital twin after the license expires or is terminated.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: This contract [OPTION 1] [takes immediate effect] [OPTION 2] [takes effect from (specify date)]. 9.1.2 [OPTION] [This contract is concluded for [OPTION 1] [an indeterminate period] [OPTION 2] [a fixed period of (specify)], subject to any grounds for expiry or termination under this contract.] 9.1.3 [OPTION] [The Data Sharer must start making the Data available to the Data Recipient [OPTION 1] without undue delay after the contract has come into effect. [OPTION 2] on (insert date and, where applicable, further details as to timing).]	The MCTs do not explicitly address the question of the rights of the original rightsholders over the digital twins after the license expires or is terminated. This should be explicitly discussed to avoid ambiguity.

Table 5: MCTs for term of license.

Joint ownership

Where intellectual property rights subsist in data used to build a digital twin, the rights of individual parties who make contributions must be recognised.

Where more than one party has contributed, agreements must consider situations of joint ownership and be explicit about the allocation of these rights.

One relevant question that contracting parties should ask concerns the rights that subsist in the digital representation and whether these are rights of individual ownership (e.g., the procuring enterprise) or joint ownership of all contributors.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 7.2.3 [OPTION 2] The Parties will be jointly and equally entitled to the Intellectual Property Rights on the Results and shall enter into a separate contract describing the modalities of the exercise of such rights.	The model contractual terms ought to be adapted to better fit the DT use case by (a) providing greater granularity regarding categories of 'Results' that may be derived from the collaboration; (b) foreseeing a third modality of intellectual property right assignment beyond sole

	ownership and joint ownership of all Results, namely split ownership based on certain criteria, e.g. the technological domain or application area of a Result.

Table 6: MCTs for joint ownership of project results.

Data sharing and provenance

Barriers to data sharing may originate from legacy organisational practices, uncertainty because of lack of information and fear of loss of control, or from legitimate concerns such as national security (e.g., data localization regimes).

Data provenance, in legal terms at least, does not seem to be an issue in cases where undertakings have purchased the datasets and have had the rights in these datasets assigned. Digital twin solutions are usually built on top of existing data infrastructures where legal provenance, understood as tracing and tracking the rights that may subsist in different data, datasets, databanks, or databases, is by design built into the metadata of the data sets.

The situation could be more challenging where access to data is provided on a DaaS basis. The service provider would usually be under an obligation to update the data continuously, so service level agreement targets in terms of availability, integrity, and accuracy must be specified contractually.

In practice, the issue of legal provenance of data is typically resolved on a technical level by specifying a service level of how recent, how accurate, and how precise the data must be at any given time. Nevertheless, since issues are usually dealt with as part of the typical contract management lifecycle, these technical arrangements must be incorporated in service level agreements.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 3.1.5 [OPTION] [Each party shall ensure that all Data, files, or software transmitted to the other Party under this contract stem from data collection activities which comply with applicable (specify: professional-, ethical industry-, cybersecurity-, research- and/or AI-) standards.] 4.1 […] The Data is made available in a comprehensive, structured, commonly used and machine- readable format. The Parties consider this requirement as fulfilled by the following specifications concerning the Data: (Please specify) […] The Data Sharer shall make the following available to the Data Recipient: (Please add/remove/complete specific quality requirements)	The MCTs appropriately foresee contracting parties specifying the data quality parameters of the contractual subject matter. By necessity, the MCTs largely leave the contracting parties to establish specific technical criteria for data quality. When drafting SLAs and data sharing contracts, DT parties are encouraged to consider the data quality dimensions defined by the EDM Council, namely:[30] -Accuracy -Completeness -Conformity -Consistency

[30] https://edmcportal.org/glossary/data-quality-dimensions/

• An exhaustive dataset, meaning that Data contains all data in possession of the Data Sharer related with the scope of this contract; and/or • An up-to-date dataset, meaning the Data reflects the data in possession of the Data Sharer at the date of signature of this contract; and/or • An accurate dataset, meaning the Data has been curated by the Data Sharer and is – to the best of its knowledge – error free, correct and reliable; and/or • A dataset which is compliant with the following standards: (specify, e.g., interoperability, accessibility, security, etc.) • A dataset available in a format which is open, meaning a format which is not proprietary and can be used by anyone, namely: (specify)]. 4.2.3 The Data Sharer shall make the Data available to the Data Recipient in conformity with the following timing requirements/calendar: (Insert timing (e.g. daily, specific time, frequency, real time) and/or detailed calendar or time limit)	-Coverage -Timeliness -Uniqueness

Table 7: MCTs for data quality and provenance.

Confidentiality

Data sharing in the context of a DT involves multiple parties who are usually concerned about the confidentiality of their data, including trade secrets.

From a data sharing perspective, a DT can be seen as a data sharing and analytics platform which can expose the involved parties to risks of security breaches and data loss.

In case of confidential data, parties should normally include non-disclosure clauses in individual contracts as well as project-wide confidentiality agreements, especially in closed groups where the number of participants is determined.

Depending on the types of end users of the DT, it may be necessary to also stipulate different levels of access permissions depending on the level of confidentiality of the data to which these users may have access.

Suppliers must ensure that adequate cyber security measures are put in place. As discussed under Section 3.8, the manufacturing industry is under the scope of legal obligations flowing from the Cyber Resilience Act and the NIS2 Directive, which include requirements regarding security incidence response and handling processes requirements. To comply with these requirements, it is desirable for contracts to address responsibilities across the entire supply chain of a DT, particularly with regard to clauses on mandatory vulnerability disclosures, periodic security audits, and software bills of material.

Any interconnection with legacy proprietary systems of the legacy proprietary systems must be accompanied by contractual warranties that this will be done in a controlled and secure manner.

Sample MCT	Remarks for RE4DY / Industry 4.0

ANNEX V: 4.4 Security measures 4.4.1 Each Party will ensure the confidentiality, integrity and availability of the Data by implementing the appropriate security measures described in Appendix 4 when making the Data available under access arrangements under 4.2.1. 4.4.2 If changes in the Data or its environment may affect the security of the Data. the Data Sharer and the Data Recipient agree to evaluate the security measures (specify: regularly / upon request of the other party/ upon special events), and to negotiate in good faith upon any necessary adaptation. 4.4.3 Each Party shall provide upon request the other Party with detailed information on implementation measures taken in accordance with this clause 4.4 and Appendix 4. 4.4.4 Each Party will report to the other one any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Data within 24 hours of discovery. 4.4.5 [OPTION] [The Data Sharer reserves the right to conduct periodic audits or request documentation to verify compliance with security requirements imposed upon the Data Recipient.] […] 11.1.1 The following information must be considered confidential: (a) information referring to the trade secrets, financial situation or any other aspect regarding the operations of the other Party unless the other Party has made this information public; (b) information setting out the basis for the calculation of the reasonable compensation; (c) information referring to any third party, unless they have already made this information public;	The MCTs envision generic security and confidentiality guarantees that are to be elaborated in the Appendices to a data sharing agreement. The heightened cyber resilience obligations imposed on the manufacturing industry warrant specific and explicit responsibility assignment along the value chain for compliance with concrete cybersecurity / cyber resilience requirements. Attention may be needed for differential access permissions based on the confidentiality level of DT data.

Table 8: MCTs for confidentiality and security.

Liability

As interconnected data systems, DTs involve multiple parties which may rely on the data shared in and/or generated by the digital twins in different degrees.

This situation means that each data source may pose a liability risk, especially if it comes with guarantees of data quality. Therefore, a gatekeeping authority is needed to, first, protect the data source from unauthorized interference, and, second, set the terms of use that regulate the involvement of individual parties and the distribution of their liability.

Contracts should clearly define the purpose and function of the data in a way that instils trust in the participating parties, for example, by reference to documents such as the UK

Gemini Principles.[31] Liability for loss or corruption of data or adverse impact on the procuring entity's connected systems should be articulated clearly in the contract.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 10.2.4 The aggrieved Party can: […] (b) claim damages for economic damage caused to them by the other Party's non-performance which is not excused under clause 10.1.2. The non-performing Party is liable only for damage which it foresaw or could be reasonably expected to have foreseen at the time of conclusion of this contract as a likely result of its non-performance, unless the non-performance was intentional or grossly negligent. 10.2.5 [OPTION] [Where a Party fails to perform its obligations under this contract it shall, in any case, pay the penalties set out in detail in Appendix 5, which the Parties deem damages within the meaning of clause 10.2.4(b). The non-performing Party has the right to request that the penalty is reduced to a reasonable amount where they can prove that the penalty is grossly excessive in relation to the damage resulting from the non-performance.]	The MCTs ought to be adapted to (a) adhere to national liability rules, which differ between EU Member States and (b) more explicitly assign liability for loss and corruption of data, as well as adverse impacts on the procuring entity's connected systems, and (c) better reflect the multiparty context of DTs by clarifying that, in the case of multiple contracting parties for the DT solution, the Parties are jointly and severally liable for their contractual performance.

Table 9: MCTs for liability.

Training

Training may be mandated via contract in order to ensure that assets are used correctly in a collaborative manufacturing setting, or in order to ensure that a DT collaborator's staff is properly able to implement the necessary privacy or security policies mandated by statute or contract.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 4.4.1 Each Party will ensure the confidentiality, integrity, and availability of the Data by implementing the appropriate security measures described in Appendix 4 when making the Data available under access arrangements under 4.2.1. 6.2 Protective measures to be taken by the Data Recipient The Data Recipient shall apply the protective measures as set out in Appendix 4 (hereinafter: 'Data Recipient's Protection Measures').	Training is not explicitly discussed under the MCTs, but would logically be expected to constitute an organisational measure described in the MCTs' envisioned Appendix 4.

Table 10: MCTs for training requirements.

[31] https://www.cdbb.cam.ac.uk/DFTG/GeminiPrinciples

Revenue model

Different revenue models can apply to DT projects. As discussed, digital twins enable suppliers to switch from selling assets to selling services. This model of servitisation allows suppliers to introduce granular pricing models where the price is calculated based on actual operation of the asset as monitored by the data flows that go back to its digital twins. The customer can then be invoiced for the exact usage of the service, i.e., the pricing is based on real usage.

Revenue streams may consist of standard Software as a Service (SaaS) billing approaches, flat rate, time and materials pricing strategies, or a blend of these models. Normally, the costs will cover licensing fees, consulting fees, and any initial setup fees paid in advance.

It is up to the supplier to determine if installation fees will be charged initially or incorporated into the ongoing service charges across the lifetime of the contract. Should the supplier opt to include these costs within the service fees, it is imperative that the contractual language clearly outlines the process for recuperating any outstanding installation expenses in the event of an early contract termination. Moreover, when contracts are renewed, the pricing structure should be adjusted to reflect the elimination of initial installation charges and any variations in additional expenses.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 8. Compensation for provision of data access The Parties agree that the Data Recipient will compensate the Data Sharer as follows: (fill as appropriate) Parties should agree, at least, on the following: amount of compensation due, and the relevant currency; time when payment is due; and modalities of payment.	The MCTs regarding compensation are left open-ended by necessity. Contracts for DTs must prioritize clear contractual provisions on revenue models, taking into account the abovementioned considerations.

Table 11: MCTs for compensation.

Technology dispute resolution

Technology disputes arise when essential partnerships fail. DT contracts should specify forums for dispute resolutions and, if applicable, choice of law. Since changing technological systems can cause significant disruption and incur high costs, it is vital for DT contracting parties to establish minimum service and performance standards for handling disagreements.

Sample MCT	Remarks for RE4DY / Industry 4.0
ANNEX V: 11.6 Dispute settlement 11.6.1 The Parties agree to use their best efforts to dissolve disputes amicably and, before bringing a case before a court or tribunal, to submit their dispute to [insert name and contact details of a particular dispute settlement body]. 11.6.2 [OPTION] [For any dispute that cannot be settled according to clause 11.6.1, the courts of (specify state)	The MCTs do not envisage minimum service and performance standards that would have to be upheld throughout dispute periods. It should be considered a priority to develop appropriate language for minimum service arrangements regarding data

will, to the extent legally possible, have exclusive jurisdiction to hear the case.]	sharing and DT operation during disputes.

Table 12: MCTs for dispute resolution and minimum service.

Termination

Parties must also come to a consensus regarding the client's continued access to past data gathered by the supplier of the DT. This information may include details on the performance and yield of the manufacturing or logistics asset.

Provisions must also be in place to ensure the supplier can promptly reclaim the asset.

Refer to Table 4 in this section for MCTs on termination and data transfer.

3.11 Open data and license compatibility

Even though most data used to build proprietary digital twins would be based on proprietary operational data obtained from the asset owners or operators, open data still has a very important role to play in the Industry 4.0 context. The EC has noted the importance of open data for predictive maintenance, material tracking, and smart factories (European Data, 2025), which correlate with the use cases for RE4DY and Industry 4.0 digital twins.

As defined under Recital 16 of the Open Data Directive,[32] open data denotes data in an open format which can be freely used, reused, and shared by anyone and for any purpose. Datasets can also be referred to as open data where they have been made available for any lawful use with minimal or no legal, technical, or financial constraints. Such datasets are often distributed under various licenses which are, in essence, legal documents that define the datasets' terms of use.

At present, open data is commonly used in combination with different datasets in value-added products or services. These can include enriched or augmented datasets or digital twins that integrate various data sources. Combinations of datasets necessitate adherence to the conditions of the license under which each of the datasets is distributed. If all data is under one license, the situation is clear and users must simply follow the uniform conditions of a single license to all datasets. However, if multiple licenses applicable to different datasets, users need to assess how license terms align with each other. This challenge is known as license compatibility.

3.11.1 License compatibility

Licenses are considered compatible when their conditions can be met simultaneously. This can be as simple as ensuring that multiple attributions are provided when releasing the combined dataset, or as complicated as aligning other limitations that must be combined, e.g., prohibition of commercial use with sublicensing or prohibition of data alteration. The latter case requires making judgments about the equivalence between license limitations. For example, where one dataset only allows use for private purposes and another dataset only allows non-commercial use, a combination of these datasets distributed for private use may raise the question whether *any* commercial use is excluded, or private for-profit use may still apply (Graux, 2023).

[32] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast)

Where licenses are compatible with each other, the rule of thumb is that the strictest requirements must apply. For example, if one license requires attribution, another prohibits commercial use, and a third prohibits modifications, then the combined dataset may only be distributed under a license that meets all three conditions at the same time. Per Graux (2023), The adverse effect of such license compatibility is that it may place significant limitations on openness.

3.11.2 License Incompatibility

Licenses are incompatible where their conditions cannot be met simultaneously. For example, where a user may wish to combine two datasets distributed under strict share-alike conditions, i.e., where both licenses only allow distribution on their own terms applied to a product containing both datasets, the product cannot be lawfully distributed.

3.11.3 License (in)compatibility in practice

A recent empirical study by Graux (2023) has shown that license compatibility is a common challenge in practice for data users. The study showed that CC licenses are the only cross-border license templates in common use today, with the CC-BY 4.0 license being the most popular license on the data.europa.eu portal. In order to facilitate reuse of its documents, the EC adopted a Decision that defines two CC licenses as default licenses for Commission content: Creative Commons Attribution 4.0 International Public License (CC-BY 4.0) for all content, and Creative Commons Universal Public Domain Dedication deed (CC0 1.0) for raw data, metadata, or other documents of comparable nature.[33]

The study by Graux (2023) also showed that all common licenses on the data.europa.eu portal are essentially permissive licenses as the only two major licensing approaches are a comprehensive waiver of rights (a CC0-style approach), and an attribution requirement (a CC-BY-style approach). Limitations to non-commercial use or share-alike requirements are not present in the most commonly used licenses.

However, even though the focus is mainly on attribution when examining license compatibility, there is a wide disparity in how this requirement is worded and applied. The study by Graux (2023) showed that attribution can cover at least the following properties:

- The identity (name) of the public administration that creates and maintains the data;
- The identity (name) of the public administration that operates the portal via which the data is made available;
- The technical source (URL) where the resource can be found;
- The name of the license;
- A link to the license;
- The date of retrieval of the data;
- The date of the latest update of the data on at the source location;
- A description of any changes made by the user;
- The date of any changes made by the user;
- Mandatory inclusion of the original metadata;
- An obligation to repeat the claim that no warranties are made.

[33] Commission Decision of 22.2.2019 adopting Creative Commons as an open licence under the European Commission's reuse policy, C(2019) 1655 final.

It is of course possible to combine all these attribution properties in a single dataset, but this would require significant compliance efforts on the part of the data user. Additionally, the study has shown that while the prevalent approach is largely CC0 and CC-BY compliant, minor requirements are often introduced such as excluded use cases, data protection clauses, or references to national law. These points have to be examined by any potential user as a matter of data supply due diligence.

There are concerns regarding the wide net that some of these licenses cast in terms of scope. For example, some of their conditions attempt to regulate the use of data for criminal activities, which is clearly a matter of statutory criminal law. Furthermore, the study by Graux revealed that there was low interest on the part of the bodies using those licenses to enforce their conditions.

In practice, when combining datasets with different licenses, parties either accept the risk without formally checking for compatibility, run a compatibility check, or exceptionally relicense the dataset under a compatible license. None of these approaches are scalable. Compatibility checks can be complex, and in cases of DTs for collaborative manufacturing, the exercise may have to be performed across national or regional borders, which could potentially elicit prohibitive costs.

The only feasible approach to overcoming these challenges is to reduce license proliferation by uniformly adopting CC licenses, particularly in cross-border collaborations where CC is the only uniformly recognized license. This policy should be supplemented by guidelines on how these licenses should be used, e.g., good practices on proper attribution, appropriateness of share-alike in different scenarios, and management of commercial use.

3.11.4 Recommendations on data license compatibility

License compatibility could be a challenge for the compliant execution of multi-party data projects such as cognitive digital twins in an Industry 4.0 context. The following recommendations can be made:[34]

- Unique national or regional licenses should be avoided as they create disproportionate burdens for re-users. Instead, internationally recognized and standardized licenses should be used, such as CC.
- CC licenses, particularly CC-BY and CC0, should be the default position for most open data use cases.
- Share-alike licenses should be avoided as well as licenses that are limited to non-commercial use or within a particular sector or field of endeavour.
- Attribution requirements should be observed, and sector-specific guidance should be developed to facilitate compliance. Where the procurer of a digital twin solution is a data holder, this data should be made available with clear attribution requirements and guidance on what sort of attribution would satisfy them. Where the procurer of a digital twin solution is a data user, it should seek to procure datasets from sources which clearly stipulate how to meet their attribution requirements.

[34] Based on H Graux, Licence Compatibility in Europe: A winding road to Creative Commons, 2023, available at: https://data.europa.eu/sites/default/files/course/Licence%20compatibility%20in%20Europe%20a%20winding%20road%20to%20Creative%20Commons_EN.pdf

- Datasets that are identified as critical for the implementation of the digital twin project should be revisited and possible licensing should be considered, e.g., by changing the license on open data portals.
- Data literacy and data licensing skills should be improved by providing in-house training on data licensing and license compatibility.

4. Standardisation and Certification Schemes in the Digital 4.0 Continuum

4.1 Standardisation and Certification under the Digital 4.0 Continuum Legal Framework

A notable trend in EU data law has been the "legalisation" of soft law by imbuing it with certain implementation, accountability, and enforcement functions that render it increasingly indispensable for the functioning of the overarching European regulatory framework of 'hard law' (van Maelen, 2022).

This trend is particularly evident within the legal framework that applies to the Digital 4.0 Continuum.

Legal Instrument	Key provisions on standards and certification
GDPR (Regulation 2016/679)	Arts. 40-43 on codes of conduct and certification schemes for compliance with data protection obligations.
Free Flow of Non-Personal Data Regulation (Regulation 2018/1807)	Article 6 on codes of conduct for data porting and switching of data processing services.
Cybersecurity Act (Regulation 2019/881)	Art. 8 and Title III on cybersecurity certification.
Data Governance Act (Regulation 2022/868)	Recital 32 on codes of conduct for data intermediation services.
NIS2 Directive (Directive 2022/2555)	Arts. 21, 24, and 25 on standards, certification schemes, and technical specifications for meeting cybersecurity risk-management obligations
Machinery Regulation (Regulation 2023/1230)	Art. 20 on the presumption of conformity with essential health and safety requirements via harmonised standards and common specifications.
Data Act (Regulation 2023/2854)	Chapter VIII on harmonised standards for interoperability of data spaces and data processing services, as well as for smart contracts & Arts. 4, 5, 19, and 41 foreseeing codes of conduct and model contractual clauses for regulatory compliance.
AI Act (Regulation 2024/1689)	Section 5 on harmonised standards, common specifications, and certification for high-risk and general-purpose AI; Section 4 on Codes of Practice for high-risk and general-purpose AI; Recital 90 on model contractual terms for high-risk AI.

Cyber Resilience Act (Regulation 2024/2847)	Art. 27 on the presumption of conformity with essential cybersecurity requirements via harmonised standards, common specifications, and certification schemes.

Table 13: Overview of provisions on standards and certification in core EU digital legislation.

The following list summarizes existing standards, certification schemes, and codes that can assist RE4DY and Industry 4.0 actors in complying with the above regulatory frameworks.

- GDPR
  - EDPB-approved EU Data Protection Seals
    - Europrivacy (European Centre for Certification and Privacy (ECCP)
    - EuroPriSe European Privacy Seal (EuroPriSe Cert GmbH)
    - BC 5701:2024 (Brand Compliance B.V.)
  - EDPB-approved National Certification Criteria
    - GDPR-CARPA (LU SA)
    - EuroPriSe (EuroPriSe Cert GmbH)
    - BC5701:2023 (Brand Compliance B.V.)
    - AUDITOR conformity assessment (Competence Centre Trusted Cloud e.V.)
    - DSGVO-zt GmbH Certification criteria (DSGVO-zt GmbH)
    - Catalogue of Criteria for the Certification of IT-supported processing of personal data (Datenschutz cert GmbH)
    - BDO Austria GmbH Certification Criteria (BDO Austria GmbH)
  - EDPB-approved Codes of Conduct
    - Data Protection Code of Conduct for Cloud Infrastructure Service Providers (Cloud Infrastructure Service Providers Europe (CISPE))
    - EU Cloud Code of Conduct (Scope Europe)
    - Data Pro Code (Nederland ICT (NL Digital))
- Free-Flow of Non-Personal Data Regulation
  - N/A [35]
- Cybersecurity Act
  - EUCC Certification Scheme (ENISA)
- Data Governance Act
  - N/A
- NIS2 Directive
  - Confer with the ENISA NIS2 Technical Implementation Guide, which lists Implementing Regulations and corresponding European, international, and national standards and frameworks.
- Machinery Regulation
  - Work on harmonised standards is ongoing under CEN/CENELEC Mandate 605, with a deadline of 20 January 2026 for updating harmonised standards

[35] SWIPO Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud services & SWIPO Code of Conduct for Switching and Portability of Data related to Software as a Service (SaaS) were developed in response to Regulation 2018/1807 but were found by the EC to offer insufficient compliance guarantees. See: Manganelli and Schnurr, 2024. Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies, p. 27. Available at: https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf

adopted under the preceding Machinery Directive (Directive 2006/42/EC) and a deadline of 20 January 2034 for new, follow-up harmonised standards.

- Data Act
  - Model Contractual Terms for data sharing contracts and Standard Contractual Clauses for cloud computing and data processing service contracts. (Group E03840 - Expert Group on B2B data sharing and cloud computing contracts) Still not formally adopted via Commission recommendation, last *officially* disseminated version: April 2025.
  - Work on harmonised standards is ongoing under CEN/CENELEC Mandate 614.
    - Includes harmonised standards on Trusted Data Transactions (Part 1: Terminology, concepts and mechanisms; Part 2: Trustworthiness requirements; Part 3: Interoperability requirements), Technical specification(s) on a data catalogue implementation framework, an implementation framework for semantic assets, and a maturity model for Common European Data Spaces, as well as a European standard on a quality framework for internal data governance
- AI Act
  - Updated EU AI model contractual clauses for public procurement, including versions for high-risk AI systems and non-high-risk AI systems. While targeted at public organisations, these model contractual clauses may serve as guidelines for private procurement as well.
  - The General-Purpose AI Code of Practice for compliance with safety, transparency, and copyright obligations.
  - Work on harmonised standards is ongoing under CEN/CENELEC Mandate 593 and CEN/CENELEC Mandate 613.
    - Includes harmonised standards on risk management systems for AI systems, governance and quality of datasets used to build AI systems, record keeping through logging capabilities by AI systems, transparency and information provisions for users of AI systems, human oversight of AI systems, accuracy specifications for AI systems, robustness specifications for AI systems, cybersecurity specifications for AI systems, quality management systems for providers of AI systems, including post-market monitoring processes, conformity assessment for AI systems.
- Cyber Resilience Act
  - Work on harmonised standards is ongoing under CEN/CENELEC Mandate 606.
    - Includes multiple harmonised standards regarding security requirements relating to the properties of products with digital elements, vulnerability handling requirements, and security requirements relating to the properties of products with digital elements .

4.2 Industrial Standards for Cognitive Digital Twins

In the RE4DY context, the European standards adopted by CEN/CENELEC and the international standards adopted by ISO will be particularly relevant for the operation of Digital Continuum 4.0 CDTs.

While many industry standards are applicable to smart manufacturing and IoT in general, this analysis focuses on the industrial standards that explicitly address Digital Twins and thereby are directly relevant for RE4DY CDT scenarios. Conversely, standards such as those adopted under CEN/CLC/JTC 13: Cybersecurity and Data Protection, ISO/TC 108/SC 5: Condition monitoring and diagnostics of machine systems, or DIN EN IEC 63270:2022-09 on predictive maintenance are important for smart manufacturing and RE4DY use cases, but are not *explicitly* linked to Digital Twins.

The identification of relevant standards represents a best effort rather than a fully exhaustive exercise, as the content of most standards is only available against a fee and its reproduction is contingent upon obtaining a proper license.

The following standards have been identified as explicitly relevant for RE4DY CDT scenarios:

- CEN/CLC/WS BIOMAT - Data-driven management of production processes
  - CWA 50751:2024 - Methodology for the data-driven management of production processes
- CEN/CLC/WS LEVEL-UP - Circularity Protocols for extending the useful Life of Large Industrial Equipment
- DIN
  - DIN SAE SPEC 91487:2025-08 - Terms, definitions and characteristics for the use of Digital Twins of electric vehicle batteries
  - DIN EN 9247:2025-07 – Draft - Aerospace series - Programme management - Verification and validation of numerical models and simulations
- ETSI
  - ETSI TS 103 845 V1.1.1 (2024-02) - SmartM2M; Digital Twins Communication Requirements
  - ETSI TS 103 846 V1.1.1 (2024-08) - SmartM2M; Digital Twins: Functionalities and communication Reference Architecture
- IDTA
  - Specification of the Asset Administration Shell Part 1: Metamodel – IDTA Number: 01001
  - Specification of the Asset Administration Shell Part 2: Application Programming Interfaces – IDTA Number: 01002
  - Specification of the Asset Administration Shell Part 3a: Data Specification – IEC 61360 – IDTA Number: 01003-a
  - Specification of the Asset Administration Shell Part 4: Security – IDTA Number: 01004
  - Specification of the Asset Administration Shell Part 5: Package File Format (AASX) – IDTA Number: 01005
- IEEE
  - IEEE 3144-2025 - IEEE Standard for Digital Twin Maturity Model and Assessment Methodology in Industry

- ISO/IEC JTC 1/SC 27: Information technology - Information security, cybersecurity and privacy protection
    - [Under Development] ISO/IEC AWI TS 27568 - Security and privacy of digital twins
- ISO/IEC JTC 1/SC 41: Information technology - Internet of things and digital twin
    - ISO/IEC 20924:2024 - Internet of Things (IoT) and digital twin — Vocabulary
    - ISO/IEC TR 30172:2023 - Internet of things (IoT) — Digital twin — Use cases
    - ISO/IEC 30173:2023 - Digital twin — Concepts and terminology
    - ISO/IEC 30186:2025 - Digital twin — Maturity model and guidance for a maturity assessment
    - ISO/IEC 30194:2024 - Internet of things (IoT) and digital twin — Best practices for use case projects
    - [Under Development] ISO/IEC AWI 20924 - Internet of Things (IoT) and digital twin — Vocabulary
    - [Under Development] ISO/IEC CD TR 30138 - Digital Twin — Fidelity metric of digital twin system
    - [Under Development] ISO/IEC CD 30151 - Digital twin — Extraction and transactions of data components
    - [Under Development] ISO/IEC AWI 30152 - Guidance on the integration of IoT and digital twins in data spaces
    - [Under Development] ISO/IEC AWI 30153 - Digital twin — Guidelines for digital entity modeling
    - [Under Development] SO/IEC CD 30188 - Digital Twin — Reference architecture
- ISO/TC 184/SC4: Automation systems and integration – Industrial Data
    - ISO 23247-1:2021 - Automation systems and integration — Digital twin framework for manufacturing — Part 1: Overview and general principles
    - ISO 23247-2:2021 - Automation systems and integration — Digital twin framework for manufacturing — Part 2: Reference architecture
    - ISO 23247-3:2021 - Automation systems and integration — Digital twin framework for manufacturing — Part 3: Digital representation of manufacturing elements
    - ISO 23247-4:2021 - Automation systems and integration — Digital twin framework for manufacturing — Part 4: Information exchange
    - ISO/TR 23247-100:2025 - Automation systems and integration — Digital twin framework for manufacturing — Part 100: Use case on management of semiconductor ingot growth process
    - ISO/TR 24464:2025 - Visualization elements of digital twin — Visualization fidelity
    - [Under Development] ISO/DIS 23247-5 - Automation systems and integration — Digital twin framework for manufacturing — Part 5: Digital thread for digital twin
    - [Under Development] ISO/DIS 23247-6 - Automation systems and integration — Digital twin framework for manufacturing — Part 6: Digital twin composition
    - [Under Development] ISO/AWI TS 25271 - Automation systems and integration — Industrial digital twin interface architecture

4.3 The State of Standardisation in Industry 4.0

One of the main objectives of the RE4DY project is to democratise industrial data spaces and stimulate adoption of the RE4DY CDT framework by SMEs. It is therefore important to consider how this objective may already be pursued at the standardisation stage.

The development of harmonised standards to guide the implementation of novel EU digital legislation is a co-operative, co-regulatory exercise that involves a standardization mandate delivered by the European Commission, standard development by the ESOs, and subsequent validation and adoption of the resulting product by the Commission. As pointed out by Baron and Larouche (2023), the public-private nature of the standardisation process is a source of significant legitimacy stemming from a combination of procedural safeguards, democratic mandates, and subject matter expertise. Nevertheless, it is desirable to further enhance both the legitimacy and the eventual uptake of standards by finding new avenues for the participation of SMEs and societal stakeholders in the standardisation process. This need has already been acknowledged by the Commission in its 2022 Standardisation Strategy (European Commission, 2022), yet scholarship notes that inclusivity in practice remains lacking (Baron and Larouche, 2023; Davies and van Waeyenberge, 2025). Suggested solutions include establishing new funding mechanisms for SME participation at EU and federal levels, implementing mentorship programs for SME representatives to benefit from the knowledge of standardisation experts, and improving the accessibility of standardisation committees via user-friendly platforms and processes (Kilian et al., 2025). Davies and Van Waeyenberge (2025) suggest establishing a verification process to assess broad stakeholder engagement prior to publishing standards in the Official Journal of the European Union.

Despite the increasing importance of harmonised standards in the legal framework for Industry 4.0 and the EU digital sector in general, there is currently significant uncertainty surrounding the economic model of ESOs and, by extension, the standardisation process. In its 2024 judgment in *Malamud*,[36] the CJEU ruled that harmonised standards form part of EU law by virtue of producing legal effects and, therefore, there is an overriding public interest that justifies the disclosure of harmonised standards without charge in the name of the rule of law, transparency, openness, and good governance. Since the financial model of ESOs is largely centred around the sale of licenses for harmonized standards, the *Malamud* ruling is likely to necessitate a significant overhaul of ESO funding mechanisms.

Already, ISO and IEC have challenged the *Malamud* ruling before the ECJ in *International Electrotechnical Commission and ISO v Commission*[37], arguing that the Commission did not properly check for an overriding public interest in disclosing international standards (having only checked in the case of harmonised standards), that there is in fact no overriding public interest in disclosing international standards, that the Commission therefore (or separately) committed copyright infringement by disclosing international standards without fair compensation, and that the Commissioned failed to consult ISO and IEC as a matter of procedural obligation. As a result of the ongoing lawsuit, the publication

[36] CJEU, Case C-588/21 Public.Resource.Org and Right to Know v Commission and Others, ECLI:EU:C:2024:201

[37] ECJ, Case T-631/24 International Electrotechnical Commission and ISO v Commission, Application ELI: http://data.europa.eu/eli/C/2025/919/oj

of ISO and IEC standards in the Official Journal has reportedly been suspended (Zacek-Gebele and Windeler-Frick, 2025).

Regardless of the outcome of the ISO/IEC case, alternatives for ESO funding are already a matter of policy debate. For example, Davies and Van Waeyenberge (2025) suggest that all harmonised standards be made available free of charge online, pursuant to limitations on their alteration and commercial distribution, while the EU Commission compensates the deficit by directly fund ESO standardization activities. Whatever the chosen resolution, the *Malamud* judgment may necessitate alterations to the EU's New Legislative Framework[38] and the Regulation on Standardisation.[39]

Due to the uncertainty this legal environment elicits in the field of standardisation, it is vital for actors in the RE4DY framework to actively monitor new developments. In case the ISO/IEC lawsuit results in a gap between harmonised standards published in the Official Journal and the true state of the art (as found in, e.g., international standards not published in the Official Journal), efforts should be made to always comply with the state of the art (Zacek-Gebele and Windeler-Frick, 2025). Despite not offering an automatic presumption of compliance in the same way that published harmonised standards do, adhering to the state of the art is a legal obligation under most of the EU's digital legislation.

5. Conclusions

This deliverable has provided an overview of key contractual, IPR, and standardisation considerations when implementing the RE4DY Digital 4.0 continuum in the context of smart manufacturing processes.

While care has been taken to deliver up-to-date analysis, the RE4DY project is positioned at a critical time for the regulatory landscape. New digital legislation with horizontal scope is being introduced as part of a "regulatory tsunami" whose pace challenges enterprises to achieve compliance and whose complexity causes delays even in the publication of official guidelines such as the GPAI Code of Practice or the Model Contractual Terms for Data Sharing. As has been discussed, legal uncertainty threatens even the official publication of technical standards at a time when they are needed the most.

Nevertheless, this deliverable has highlighted that there are no barriers to the RE4DY framework that cannot be solved through appropriate contractual mechanisms. It has analysed digital twins as a composite subject matter for intellectual property rights and identified appropriate legal tools to impose access and use conditions on each component of a digital twin. Furthermore, the key contractual questions regarding data

[38] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93; Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.

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

sharing and service provision that must be answered prior to operating a DT platform have been identified and followed up with recommendations on how to answer these questions.

This deliverable concludes with a call for greater active participation by SMEs and civil society in standard- and norm-setting, in keeping with the RE4DY project's ambition to dynamise the participation of external stakeholders in the field of smart manufacturing.

6. References

6.1 Legislation

Commission Decision adopting Creative Commons as an open licence under the European Commission's reuse policy, Brussels, 22.2.2019 C(2019)1655 final.

Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast) (Text with EEA relevance). *The Official Journal of the European Union*, *336*, 1–26.

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance). *The Official Journal of the European Union*, *157*, 1–18.

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance). *The Official Journal of the European Union*, *130*, 92–125.

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). *The Official Journal of the European Union*, *172*, 56–83.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *The Official Journal of the European Union*, *333*, 80–152.

Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance). *The Official Journal of the European Union*, *218*, 30–47.

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance. *The Official Journal of the European Union*, *316*, 12–33.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). *The Official Journal of the European Union*, *119*, 1–88.

Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification) (Text with EEA relevance). *The Official Journal of the European Union*, *154*, 1–99.

Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (Text with EEA relevance). *The Official Journal of the European Union*, *169*, 1–44.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA relevance). *The Official Journal of the European Union*.

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance). *The Official Journal of the European Union*.

6.2 Case Law

6.2.1 EU Case Law

Case C-203/02 *The British Horseracing Board Ltd and Others v William Hill Organization Ltd* [2004] ECLI:EU:C:2004:695

Case C-588/21 P *Public.Resource.Org and Right to Know v Commission and Others* [2024] ECLI:EU:C:2024:201

Case C-762/19 *SIA CV-Online Latvia v SIA Melons* [2021] ECLI:EU:C:2021:434

Case T-631/24 *International Electrotechnical Commission and ISO v Commission* ELI: http://data.europa.eu/eli/C/2025/919/oj

6.2.2 EPO Case Law

T 1194/97 (Data structure product/PHILIPS) 15-03-2000. ECLI:EP:BA:2000:T119497.20000315

T 2049/12 *(Data structure for defining transformations / MICROSOFT)* 09-05-2019. ECLI:EP:BA:2019:T204912.20190509.

G 0001/19 *(Pedestrian simulation)* 10-03-2021. The Official Journal of the EPO, ECLI:EP:BA:2021:G000119.20210310.

6.2.3 National Case Law

Case No. 3015 *Attheraces Ltd & Anor v British Horse Racing Board & Anor* [2005] (England and Wales High Court

Case C-09-442420 - HA ZA 13-512 *Euronext N.V. v Tom B.V. and BinckBank N.V.* 512 [2015] The Hague District Court

6.3 Literature

Bolton, A., Butler, L., Dabson, I., Enzer, M., Evans, M., Fenemore, T., Harradence, F., Keaney, E., Kemp, A., Luck, A., Pawsey, N., Saville, S., Schooling, J., Sharp, M., Smith, T., Tennison, J., Whyte, J., Wilson, A., & Makri, C. (2018). Gemini Principles. CDBB. doi: 10.17863/CAM.32260

Data Spaces Support Centre. (2025). Building Block Overview. *Data Spaces Blueprint v2.0*. https://dssc.eu/space/BVE2/1071252426/Building+Block+Overview

Davies, Z., & Van Waeyenberge, A. (2025). Better regulation by standards? Harmonized technical standards, transparency, and the rule of law. *Common Market Law Review*, *62*(1), 147–174. doi: 10.54648/COLA2025006

Digital Twin Consortium. (n.d.). Definition of a Digital Twin. *Glossary of Digital Twins*. https://www.digitaltwinconsortium.org/initiatives/the-definition-of-a-digital-twin/

EDM Association. (n.d.). Data Quality Dimensions. *Data Management Business Glossary*. https://edmcportal.org/glossary/data-quality-dimensions/

Emanuilov, I., and Margoni, T. (2024). Forget me not: Memorisation in generative sequence models trained on open source licensed code. *SSRN Electronic Journal*. doi: 10.2139/ssrn.4720990

European Commission, Directorate-General for Communications Networks, Content and Technology, CARSA Consultores de Automatización y Robótica S.A, ECORYS, KU Leuven Katholieke Universiteit Leuven, VDI/VDE IT, Layeux, A., Savickaite, I., Pauer, A. et al. (2021). Study on technological and economic analysis of industry agreements in current and future digital value chains: final study report. *Publications Office*. doi: 10.2759/495071.

European Commission. (2022). New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_661

European Data. (2025, February 28). The importance of open data in manufacturing: Boosting efficiency and innovation. *News and Highlights*. https://data.europa.eu/en/news-events/news/importance-open-data-manufacturing-boosting-efficiency-and-innovation

Gaffinet, B., Al Haj Ali, J., Naudet, Y., and Panetto, H. (2025). Human Digital Twins: A systematic literature review and concept disambiguation for industry 5.0. *Computers in Industry*, *166*, 104230. doi: 10.1016/j.compind.2024.104230

Gesellschaft für Freiheitsrechte e.V. (n.d.). State Geodata: Bavaria abuses copyright to restrict freedom of the press. *Issues & Cases*. https://freiheitsrechte.org/en/themen/demokratie/staatliche-datenbank-urheberrecht

Graux, H. (2021). *Data sharing as a service: Will data services remove intellectual property rights from the picture, and at what cost?*. Publications Office. doi: 10.2830/815190

Graux, H. (2023). *Licence compatibility in Europe: A winding road to Creative Commons : a short exploration of legal issues, current trends and the practical reality for data providers and re users in Europe*. Publications Office. doi: 10.2830/922544

Hemmer, MHL. and Woltering, BP. (2021). 'The Netherlands', in Nordemann, J. B., & Czychowski, C. (2021). *Law of raw data*. Kluwer Law International B.V., pp. 229 – 244.

Javaid, M., Haleem, A., & Suman, R. (2023). Digital Twin applications toward Industry 4.0: A Review. *Cognitive Robotics*, *3*, 71–92. doi: 10.1016/j.cogr.2023.04.003

Justus Baron & Pierre Larouche. (2023). The European Standartisation System at a Crossroads (Tech, Media & Telecom). CERRE. https://cerre.eu/wp-content/uploads/2023/05/230502_CERRE_Standardisation-report-.pdf

Manganelli, A., Schnurr, D. (2024). Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies (Tech, Media & Telecom). CERRE. https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf

Zacek-Gebele, D. and Windeler-Frick, J. (2025). Consequences of the Malamud ruling: No more EN ISO and EN IEC standards in the EU Official Journal? *Current Developments Regarding ISO and IEC Standards in the EU Official Journal*. https://www.ibf-solutions.com/en/seminars-and-news/news/iso-and-iec-standards-in-the-eu-official-journal

Kilian, R., Jäck, L., and Ebel, D. (2025). European AI Standards – Technical Standardisation and Implementation Challenges under the EU AI Act. *European Journal of Risk Regulation*, 1–25. doi: 10.1017/err.2025.10032

Lis, D., Gelhaar, J., and Otto, B. (2023). Data Strategy and Policies: The Role of Data Governance in Data Ecosystems. In I. Caballero & M. Piattini (Eds.), *Data Governance* (pp. 27–55). Springer Nature Switzerland. doi: 10.1007/978-3-031-43773-1_2

Margaria, T., and Schieweck, A. (2019). The Digital Thread in Industry 4.0. In W. Ahrendt & S. L. Tapia Tarifa (Eds.), *Integrated Formal Methods* (Vol. 11918, pp. 3–24). Springer International Publishing. doi: 10.1007/978-3-030-34968-4_1

Morrison, R. (2023). Can non-open data standards legally taint conforming codebases and databanks? doi: 10.5281/ZENODO.7962743

Naudet, Y., Baudet, A., and Risse, M. (2021). Human Digital Twin in Industry 4.0: Concept and Preliminary Model. *Proceedings of the 2nd International Conference on Innovative Intelligent Industrial Production and Logistics*, 137–144. doi: 10.5220/0010709000003062

Nizamis, A., Julian, M., Valero, C. I., Foti, M., Drigkopoulou, I., Esbrí, M. Á., Costa, R., Yortholt, A., Ioannidis, D., Gkonis, P., Trakadas, P., Tzovaras, D., and Palau, C. E. (2025). Data-as-a-Product to enable data-driven value networks in Industries 4.0 & 5.0: The Swiss Smart Factory experiment. *Procedia Computer Science*, *257*, 793–800. doi: 10.1016/j.procs.2025.03.102

Osborne Clarke. (2022). Digital twins: Enabling sale of a service, not an asset. *Data-Driven Business Models*. https://www.osborneclarke.com/insights/digital-twins-enabling-sale-service-not-asset

Perin Ünal. (2022). Cognitive Digital Twins: Digital Twins That Learn By Themselves, Foresee the Future, and Act Accordingly. *Digital Twin Consortium Blog*. https://www.digitaltwinconsortium.org/2022/09/cognitive-digital-twins-digital-twins-that-learn-by-themselves-foresee-the-future-and-act-accordingly/

Richard Kemp. (2025). WHITE PAPER: Legal Aspects of Data – Rights and Duties. Kemp IT Law. https://kempitlaw.com/insights/white-paper-legal-aspects-of-data-rights-and-duties/

Robbie Morrison. (2023a, January). Commodification of public interest information. *Open Energy Modelling Initiative*. https://forum.openmod.org/t/commodification-of-public-interest-information/3661

Robbie Morrison. (2023b, November). Legal issues related to an energy modelling knowledge commons. *Open Energy Modelling Initiative*. https://forum.openmod.org/t/legal-issues-related-to-an-energy-modeling-knowledge-commons/4399

Vander Maelen, C. (2022). *Articles 40-41 GDPR: A New Approach to Using Codes of Conduct in EU Law?* https://hdl.handle.net/10419/265672

Wilkinson, M. D., Dumontier, M., Aalbersberg, Ij. J., Appleton, G., Axton, M., Baak, A., Blomberg, N., Boiten, J.-W., Da Silva Santos, L. B., Bourne, P. E., Bouwman, J., Brookes, A. J., Clark, T., Crosas, M., Dillo, I., Dumon, O., Edmunds, S., Evelo, C. T., Finkers, R., … Mons, B. (2016). The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data*, *3*(1), 160018. doi: 10.1038/sdata.2016.18