CERTAIN

Certification for Ethical and Regulatory Transparency in Artificial Intelligence

D3.4: GUIDELINES FOR ENTERING AI DATA MARKETS

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

Work package	WP3
Task	T3.4
Due date	30/06/2026
Submission date	30/06/2026
Deliverable lead	UT
Version	1.0
Authors	Olena Denysenko (UT), Janika Bachmann (UT), Martin Hayford (UT), Yasaman Yousefi (DEX), Fenia Giannakopoulou (ANAD), Irina Urumova (INCO)
Reviewers	Konstantinos Amplianitis (UCD), Zouhair Haddi (NVIS)
Abstract	This deliverable (D3.4) presents practical compliance guidelines for organisations operating in the EU data economy, synthesising the legal, ethical, and social analyses of the preceding Work Package 3 deliverables into a single, actionable instrument. Drawing on a Design Science Research framework, the deliverable systematically extracts and harmonises requirements from the four principal EU data governance instruments (the Data Act, the Data Governance Act, the GDPR, and Article 10 of the AI Act) and integrates ethical and social best practices. The central output is the Logical Decision Tree Model, a compliance-by-design tool that guides data holders, data space operators, and other actors through a structured question sequence to identify their specific legal obligations and responsible compliance best practices. The model produces a two-tier output distinguishing minimum legal requirements from ethical and social best practices, and is designed to be updatable as the regulatory landscape evolves.
Keywords	Data Act, Data Governance Act, GDPR, EU AI Act, AI data governance, EU data law, data holders, data spaces, data intermediaries, data altruism, EU compliance, regulatory compliance, legal requirements, responsible compliance, compliance-by-design, Digital Omnibus

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	04/05/2026	1st edit (UT Internal)	Martin Hayford (UT)
V0.2	27/05/2026	2nd edit (WP3 Internal)	Yasaman Yousefi (DEX)
V0.3	22/06/2026	3rd edit (Official Review)	Konstantinos Amplianitis (UCD) Zouhair Haddi (NVIS) Claude Bauzou (IPS)
V1.0	29/06/2026	Final version	Olena Denysenko (UT) Martin Hayford (UT) Janika Bachmann (UT)

Grant Agreement No: 101189650 | **Topic:** HORIZON-CL4-2024-DATA-01-01
Call: HORIZON-CL4-2024-DATA-01. | **Type of action:** HORIZON-IA

REVIEWERS' COMMENTS

Name: Konstantinos Amplianitis	Organization: UCD	Date of review: 12/06/2026

The deliverable is a well-structured and comprehensive report that successfully translates the legal, ethical, and social analyses developed in previous WP3 deliverables into a practical compliance framework for organisations entering AI data markets. The methodology is clearly presented, the document follows a logical progression from regulatory analysis to implementation, and the proposed Logical Decision Tree Model constitutes a valuable and innovative contribution towards operationalising complex regulatory requirements. The inclusion of supporting databases and accompanying materials further strengthens the usefulness and reusability of the deliverable.

Nevertheless, several editorial and consistency improvements are recommended before final submission:

- **Improving terminology and abbreviations:** The document refers to the proposed model as the Logical Decision Tree Model (LTM), while it should be LDTM.
- **Abbreviations list:** The abbreviation list should be carefully revised to ensure that entries follow a consistent alphabetical order. For example, FRAND currently appears after SME, despite alphabetically belonging earlier in the list. A systematic editorial review of this section would be required.
- **Avoid unnecessary redefinitions:** Certain concepts and abbreviations are redefined after they have already been introduced earlier in the document. For instance, the acronym FRAND (Fair, Reasonable and Non-Discriminatory) is explained multiple times. Once introduced, subsequent references can simply use the abbreviation unless additional clarification is required. Reducing such repetition would improve readability and conciseness.
- **Regulatory timeline descriptions:** The report generally presents the regulatory landscape accurately; however, descriptions regarding the applicability of certain legislative provisions should be phrased carefully to avoid implying that all obligations are already fully applicable. Where phased implementation exists (e.g., specific provisions of the Data Act or Article 10 of the AI Act), the wording should consistently reflect their respective application timelines or avoid unnecessary emphasis on dates in high-level sections such as the Executive Summary.
- **Executive Summary:** The Executive Summary effectively captures the objectives and contributions of the deliverable, but some statements regarding the immediacy of compliance obligations could be moderated to reflect the phased implementation of the relevant legislative instruments. A more nuanced formulation would ensure legal precision while maintaining readability.
- **Editorial consistency:** A final proofreading pass is recommended to ensure consistency in terminology, abbreviations, cross-references, and drafting style throughout the report. Given the highly technical nature of the deliverable, maintaining uniform language and presentation will significantly enhance its clarity for readers and future users of the proposed framework.

Overall, the deliverable represents a significant piece of work and provides a valuable compliance-oriented framework that integrates legal, ethical, and social dimensions into a practical decision-support model. The comments above are primarily editorial and presentation-related and can be addressed through a final quality assurance review, which would further strengthen the overall quality and consistency of the document.

Name: Zouhair Haddi	Organization: NVIS	Date of review: 22/06/2026

The deliverable was particularly valuable to read and reflected a high level of quality in both its methodological framework and overall synthesis. It presents a well-structured and practical compliance framework for data holders, data space operators, research organisations, and other actors navigating EU data law, supported in particular by a consolidated requirements database and a Logical Decision Tree

Model. A key strength of the deliverable lies in its clear effort to bridge the gap between regulatory text and operational practice. This is particularly valuable in a context where the EU data law landscape remains substantively complex, with the Data Act, the Data Governance Act, the GDPR, and the AI Act interacting through overlapping obligations, multiple categories of addressees, and provisions whose practical implications are not always immediately clear. D3.4 provides a timely and useful response to a genuine implementation challenge. This is especially relevant from an SME and private-sector perspective, where organisations entering AI data markets, operating data spaces, or seeking to re-use public sector data may not always have access to dedicated legal expertise. The deliverable therefore offers a meaningful and much-needed instrument for translating legal complexity into practical and actionable compliance guidance. However, a few minor recommendations may help to further strengthen the clarity of the deliverable before submission: • Complete the Abstract, Keywords and Document Revision History. • It is always valuable to link the current deliverable to previously completed activities, including earlier deliverables and outcomes, and this has been appropriately done here. However, as this deliverable is intended for public dissemination, a general reader may not be aware of the objectives of the previous deliverables and may therefore find it difficult to fully understand the rationale and relationship between the current and preceding activities. For this reason, I would suggest rephrasing the following statements: “This deliverable is part of Work Package 3 (WP3) of the CERTAIN project and synthesises the legal analysis of D3.1, the ethical requirements of D3.2, and the social requirements of D3.3.” “The methodology employed in D3.4 follows a Design Science Research (DSR) framework, specifically conceived to bridge the gap between high-level normative requirements and practical market implementation. Given that the objective of D3.4 is to transform the theoretical findings of D3.1, D3.2, and D3.3 into an actionable guidance tool for practitioners, a three-stage deductive thematic synthesis was employed” • It is recommended to clarify in Section 2.2.2 how the case of an (micro)SME exempt under the Data Act should be interpreted in relation to both the Data Act and the DGA. • I am not sure the reader is yet sufficiently equipped to fully grasp the importance of Section 2.2.4, “Regulatory Friction and Cross-Instrument Tensions,” given that several relevant aspects have not yet been introduced, including the methodology stages (notably Stage 2 of D3.4), the consolidated database (REQ-006/70/125/126), and the thematic clusters (Clusters 1 and 5). It may therefore be advisable to move this section to a later stage, once these elements have been clarified. • Section 5 does not currently explain the two-tier output structure. While Figures 1 and 5 refer to the compliance outputs, the text does not clarify their meaning. I would therefore recommend briefly introducing the compliance outputs here and directing the reader to Section 6, where they are explained more thoroughly. • Section 6 indicates that the rationale for moving from a three-tier to a two-tier structure will be explained; however, this explanation is currently not provided.
Author’s note: To address the reviewer’s final point, originally the structure of the LDTM output was envisioned in a three-tier structure. It was later revised to a two-tier structure. This left-over reference was removed, as there was no need to elaborate on the change for any theoretical reason.

DISCLAIMER

Co-funded by the European Union

Project funded by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Federal Department of Economic Affairs, Education and Research EAER
State Secretariat for Education, Research and Innovation SERI

The CERTAIN project received funding from the European Union's Horizon Europe Research and Innovation Programme under Grant Agreement No 101189650. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

COPYRIGHT NOTICE.

Project funded by the European Commission in the Horizon Europe Programme		
Nature of the deliverable:	Report (R)	
Dissemination Level		
PU	Public, fully open, e.g. web (Deliverables flagged as public will be automatically published in CORDIS project's page)	x
SEN	Sensitive, limited under the conditions of the Grant Agreement	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc.
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This deliverable is a part of Work Package 3 (WP3) of the CERTAIN project. To ensure the final outcomes are both compliant and socially grounded, this report synthesises three preceding pillars of WP3 research: the comprehensive legal analysis of EU regulations on AI and data (D3.1), the operational ethical considerations for AI compliance (D3.2), and the social acceptance of AI (D3.3). This synthesis translates complex research into a practical, layered compliance instrument for data holders, data space operators, research organisations, and other actors navigating EU data law. For any organisation that generates, holds, shares, or processes data in the EU data ecosystem, compliance is no longer prospective – most of the core framework is now applicable or imminently applicable.

The central methodological contribution of D3.4 is the application of a Design Science Research framework to regulatory compliance. The deliverable proceeds through three stages: a systematic extraction of 198 requirements from the four instruments (Data Act, Data Governance Act, GDPR and Article 10 of the AI Act); a transdisciplinary harmonisation that consolidates those requirements into 128 unified rows across ten thematic clusters, resolves cross-instrument regulatory friction, and integrates ethical and social best practices from D3.2 and D3.3; and the crystallisation of this synthesis into a Logical Decision Tree Model (LDTM) – a compliance-by-design artefact that guides different actors through a structured question sequence to determine their specific regulatory obligations and best practices.

The LDTM is the principal output of D3.4. It comprises 28 questions organised across four sections: identifying the actor's role; characterising the data held; establishing the actor's intended activities; and capturing additional cross-cutting context including international transfers, high-risk AI classification, research purpose, and third-country governmental access requests. The model produces a two-tier output: Tier 1 setting out minimum legal obligations that must be met, and Tier 2 consolidating responsible compliance best practices drawing on ethical and social guidance from the ethical and social partners.

D3.4 is delivered at a moment of regulatory flux. The European Commission's Digital Omnibus proposal of November 2025, which would significantly restructure the data governance framework, is noted throughout this report as a material development. However, as the proposal has not been adopted and existing law remains in force, D3.4 is grounded entirely in the current legal framework, relevant as of June 2026. The Digital Omnibus is assessed in Section 2.3 and discussed as a future challenge in Section 7.

ABBREVIATIONS

AI	Artificial Intelligence
B2B	Business-to-Business
B2G	Business-to-Government
BCRs	Binding Corporate Rules
D3.4 (or D)	Deliverable 3.4 (or Deliverable)
DGA	Data Governance Act
DMA	Digital Markets Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSR	Design Science Research (Framework)
EEA	European Economic Area
ELSA	Ethical, Legal and Social Aspects
EU	European Union
EUR	Euro (Currency)
FRAND	Fair, Reasonable and Non-Discriminatory (Terms)
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
ID	Identifier
IoT	Internet of Things
LDTM	Logical Decision Tree Model
MiFID	Markets in Financial Instruments Directive
NIS2	Network and Information Security 2 (Directive)
Q1 (or Q)	Question 1 (or Question)
REQ(s)	Requirement(s)
SCCs	Standard Contractual Clauses
SME	Small and Medium-sized Enterprises
WP3 (or WP)	Work Package 3 (or Work Package)

LIST OF TABLES

LIST OF FIGURES

INTRODUCTION AND SCOPE

This report presents the guidelines developed under Deliverable 3.4 of the CERTAIN project: "Guidelines for entering AI Data Markets." D3.4 is the fourth and synthesising deliverable of WP3, which produces a comprehensive legal, ethical, and social compliance framework for organisations operating in the EU data economy. It builds directly on the legal analysis of D3.1 (Comprehensive Legal Analysis and Data Map), the ethical requirements framework of D3.2 (Ethical Considerations for AI Compliance), and the social requirements analysis of D3.3 (Social Analysis and AI Acceptance Modelling), transforming those foundational analyses into practical, actionable guidance.

The present deliverable is complete as a standalone research output – it documents the methodology, the consolidated requirements database, and the Logical Decision Tree Model architecture in sufficient detail that it can be read and used independently of the tool. All design decisions made in D3.4, particularly the structure of the question set, the trigger mapping in the consolidated database, and the two-tier output format, are made with the requirements of D3.5 “Multidisciplinary Guidelines for AI Stakeholders” explicitly in mind.

1.1 PURPOSE AND OBJECTIVES

The primary purpose of D3.4 is to bridge the gap between regulatory text and operational practice. EU data law as it stands in 2026 is substantively complex: four instruments – the Data Act, the Data Governance Act, the General Data Protection Regulation, and the AI Act – interact in ways that are not always transparent, impose overlapping obligations on many of the same actors, and contain provisions whose practical implications are underspecified. For an organisation entering an AI data market, operating a data space, or seeking to re-use public sector data, the question of what the law actually requires is far from straightforward. D3.4 is designed to answer that question.

The deliverable pursues four specific objectives. First, to produce a complete, cross-instrument extraction of all compliance-relevant requirements from the four instruments within the defined scope, organised into a structured, reusable database. Second, to harmonise those requirements across instruments, identifying regulatory overlaps, resolving tensions, and establishing a coherent tiered compliance hierarchy. Third, to integrate the ethical and social best practices developed in D3.2 and D3.3 into a unified compliance output that goes beyond minimum legal obligations. Fourth, to crystallise this synthesis into a Logical Decision Tree Model that can be used directly by practitioners.

1.2 SCOPE AND TARGET AUDIENCE

D3.4 covers four EU legislative instruments, selected as the foundational data governance framework for data holders and data spaces:

- Regulation (EU) 2023/2854 – the Data Act – generally applicable since 12 September 2025. The Data Act establishes the right of connected product users to access data generated by those products, the B2B data sharing framework with FRAND (Fair, Reasonable and Non-Discriminatory) conditions, the business-to-government exceptional need mechanism, and interoperability requirements for data space participants. It also contains specific provisions governing smart contracts, switching between data processing service providers, and protections against third-country governmental access to non-personal data.
- Regulation (EU) 2022/868 – the Data Governance Act (DGA) – fully applicable since 24 September 2023. The DGA establishes the governance framework for re-use of protected public sector data (Chapter II), the notification and compliance conditions for data intermediation services (Chapter III), and the voluntary registration mechanism for data altruism organisations (Chapter IV).
- Regulation (EU) 2016/679 – the General Data Protection Regulation (GDPR) – applicable since 25 May 2018. D3.4 covers the GDPR selectively, focusing on provisions directly relevant to data holders sharing or processing personal data in the context of data spaces and connected product data, including

lawfulness principles, special category data restrictions, data subject rights, security obligations, and international transfer rules.

- Regulation (EU) 2024/1689 – the AI Act – specifically Article 10 on data governance for high-risk AI systems, applicable from 2 August 2026. Article 10 governs the quality, representativeness, and bias assessment requirements for training, validation, and testing datasets used in high-risk AI systems.

Other legislations, including the Cybersecurity Act, NIS2, the European Health Data Space Regulation, the Digital Markets Act (DMA), and sector-specific frameworks, may impose additional obligations on specific actor types. D3.4 acknowledges this broader landscape but focuses on the four instruments above as the core data governance framework.

The guidelines in D3.4 are addressed to a range of actors who generate, hold, share, process, or seek to access data in the EU data ecosystem. The primary audiences are:

- **Private sector data holders** – organisations that hold data generated by connected products or in the course of their activities, including manufacturers of IoT devices, health technology companies, energy providers, financial institutions, and other organisations generating data through their products or services.
- **Data space operators and data intermediaries** – organisations that facilitate data exchange between multiple parties, whether through formal data intermediation services under the DGA or through participation in sectoral or cross-sectoral data spaces.
- **Public sector bodies** – authorities and bodies holding data that is subject to the DGA Chapter II re-use framework.
- **Research and academic organisations** – universities, research institutes, and other entities that access or process data for scientific research, statistical, or public interest archiving purposes.
- **AI developers and deployers** – organisations that develop high-risk AI systems using training data subject to the AI Act Article 10 data governance framework.

1.3 STRUCTURE OF THE DELIVERABLE

Section 2 presents the regulatory landscape, including an overview of the four instruments, an analysis of how they interact, and a note on the Digital Omnibus proposal. Section 3 describes the three-stage Design Science Research methodology. Section 4 presents the consolidated requirements database, organised by thematic cluster. Section 5 presents the Logical Decision Tree Model in full. Section 6 defines the two-tier compliance output structure. Section 7 discusses challenges, limitations, and next steps. Section 8 concludes the report.

Submitted alongside this report are supporting materials, including:

1. A database file (.db) containing all of the requirements and their associated information. This includes the consolidated legal requirements, Social and Ethical best practices, and separate, more detailed requirements breakdowns for each of the four main regulations explored in the report.
2. A multi-sheet Microsoft Excel Spreadsheet (.xlsx) with the exact same information and tables as above.

These contain more information than the abridged tables included in Appendices A and B, and are intended to be used by those who wish to more deeply explore the data or even develop their own tools based on it. These will be the main materials used to further develop the compliance tools to be tested in Pilot 5 of the CERTAIN project, as well as the basis of D3.5.

1.4 HOW TO USE THESE GUIDELINES

D3.4 is designed to serve different readers in different ways. Not everyone who needs to use the guidelines needs to read the full report. This section explains how to navigate the deliverable depending on your background and purpose.

It is important to note that at this stage, working through the guidelines requires a degree of manual engagement with the question set and the requirements database. The interactive compliance tool that will

make the LDTM fully accessible to end users – guiding practitioners through the questions automatically and generating a formatted compliance output – is planned for development in D3.5, building directly on the materials produced in this deliverable. For now, the guidelines can be used manually as described below.

If you are a data holder, data space participant, or other practitioner seeking to understand your compliance obligations, you do not need to read the full report. The most direct path through the deliverable is as follows. Start with Section 5, which presents the Logical Decision Tree Model and its four sections of questions. Work through the complete question set (Appendix C) as it applies to your organisation, answering each question honestly based on your actual situation. For each question where your answer activates an output, note the requirement identifiers listed. Then turn to Section 4, which organises all requirements by thematic cluster, go directly to the clusters relevant to your answers and read the requirement descriptions for those clusters only. Section 6 explains what the Tier 1 and Tier 2 outputs mean and how to act on them. You do not need to read Sections 2, 3, or 7 to use the guidelines in practice, though Section 2.1 may be useful if you want a plain-language overview of the four regulations before working through the questions. If you wish to go deeper into the data, for instance, to explore which requirements are triggered by specific provisions, to map your obligations to specific articles, or to understand the cross-instrument relationships – the Excel spreadsheet and database file submitted alongside this report contain the full consolidated requirements database with all columns of associated information, including source articles, requirement types, related requirements across instruments, and LTM trigger mappings. These are the materials intended for practitioners who wish to conduct their own analysis or develop their own tools on top of the D3.4 foundation.

However, it is perhaps advisable for any data holder – particularly a so-called “naïve” data holder – to simply wait for release of D3.5, which will be accompanied by the user-friendly interactive tool. This tool may also be made available in the interim months on the CERTAIN website or GitHub. For the time being, use of the guidelines as presented in this report and accompanying materials is probably best left to those with a special interest in the topic or the development process.

If you are a researcher, legal expert, or policy professional interested in the methodology, the cross-instrument analysis, or the regulatory landscape, Sections 2 and 3 are most relevant. Section 2 provides the regulatory overview and cross-instrument analysis. Section 3 describes the Design Science Research framework and the three-stage extraction, harmonisation, and design methodology. Section 7 discusses the limitations of the current model, the anticipated impact of the Digital Omnibus proposal, and the planned next steps for D3.5.

If you are a developer or technical partner building on D3.4 for D3.5, the primary materials are the Excel spreadsheet and database file. The LTM trigger mapping column in the database provides the complete logic connecting each question to the requirements it activates, and is designed to be machine-readable. Appendix C provides the full question set with answer options and guidance notes. Section 6 defines the two-tier output structure that an interactive tool should implement.

In all cases, the compliance output produced by the LDTM is a starting point rather than a substitute for legal advice. The guidelines are designed to reduce the compliance burden for organisations entering the EU data economy and to help practitioners identify where to focus their attention, but complex or borderline situations will always benefit from qualified legal judgment.

2 REGULATORY LANDSCAPE

The EU data governance framework applicable to data holders and data spaces as of 2026 is constituted by four principal instruments. These instruments were developed at different points in the EU's evolving digital agenda, address overlapping subject matters from different regulatory angles, and together form a dense but not always coherent framework. This section provides an overview of each instrument (condensed overview can be found in Table 1), an analysis of how they relate to each other, and a note on the Digital Omnibus proposal, which would significantly restructure this framework if adopted.

2.1 OVERVIEW OF THE FOUR INSTRUMENTS

2.1.1 The Data Act (Regulation (EU) 2023/2854)

The Data Act entered into force on 11 January 2024 and generally applies from 12 September 2025, subject to specific phased application rules, including Article 3(1), which applies to connected products and related services placed on the market after 12 September 2026. It is the most recent of the four instruments covered by D3.4 and the most operationally demanding for private sector data holders. The Act was conceived as a response to what the Commission identified as the underutilisation of industrial data – particularly data generated by connected products and related services – and the absence of a framework governing access to and sharing of such data[1].

The Data Act operates across six main areas of relevance to D3.4. Chapter II establishes the right of users of connected products to access data generated by those products and to have it shared with third parties of their choice, subject to FRAND conditions and with specific protections for trade secrets. Chapter III sets the framework for data holders who are already obliged to make data available to data recipients, governing the conditions under which that obligation is fulfilled, including FRAND terms, compensation principles, dispute settlement mechanisms, and protections against unfair contractual terms in B2B data sharing agreements. Chapter V establishes the exceptional public interest mechanism (B2G data sharing) under which public sector bodies may request data from private holders in emergency situations. Chapter VI governs switching between data processing service providers and includes baseline interoperability requirements for data spaces. Chapter VII addresses international data transfers and third-country governmental access requests for non-personal data. Chapter VIII contains the smart contract essential requirements.

An important scope limitation applies to micro and small enterprises under Article 7(1) of the Data Act. Enterprises with fewer than 50 employees and annual turnover not exceeding EUR 10 million are exempt from the Chapter II obligations relating to connected products they manufacture or design and related services they provide, provided they are not part of a group that collectively exceeds these thresholds and do not derive more than 25% of their activities from subcontracting for larger enterprises. This exemption operates at the level of the obligation to make data available – where Chapter II is not triggered for a micro or small enterprise, the practical scope of certain Chapter III provisions governing that specific sharing scenario may also be reduced accordingly.

However, the scope of the exemption must be understood with precision across three distinct regulatory layers. First, the Chapter II access and sharing obligations (the obligation to design connected products to make data accessible by default and to make that data available to users and authorised third parties) do not apply to

[1]European Commission. (2022, February 23). Commission Staff Working Document *Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data* (SWD(2022) 34 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0034

qualifying micro and small enterprises. Second, the Chapter III framework, which sets the rules for data holders who are already obliged to make data available to data recipients, including FRAND conditions, compensation principles, dispute settlement mechanisms, and unfair contractual terms provisions, applies where a legal obligation to share data exists; where the Chapter II obligation does not arise for an exempt enterprise, the corresponding Chapter III rules for that sharing scenario have correspondingly reduced practical reach. Third, Article 13 of the Data Act, which governs unfair contractual terms in B2B data sharing agreements, has broader relevance beyond the connected product context and is not limited to situations where a Chapter II or Chapter III sharing obligation applies. Its protections against unilaterally imposed terms that are grossly unfair or deviate from good commercial practice apply to any B2B data sharing agreement, regardless of whether the sharing party is exempt from Chapter II obligations.

2.1.2 The Data Governance Act (Regulation (EU) 2022/868)

The Data Governance Act applies since 24 September 2023. It was designed to build trust in data sharing by establishing governance frameworks for three distinct contexts: the re-use of protected data held by public sector bodies; the operation of data intermediation services; and voluntary data sharing through altruism organisations. The DGA does not itself impose a general obligation to share data – it creates the governance conditions under which data sharing can happen in a trustworthy way.

DGA Chapter II governs re-use of data held by public sector bodies that is protected on grounds of commercial confidentiality, statistical confidentiality, third-party intellectual property rights, or personal data protection. The Chapter establishes non-exclusivity as a foundational principle – public sector bodies may not grant exclusive re-use rights to any single entity – and requires that conditions on re-use be non-discriminatory, transparent, proportionate, and objectively justified.

DGA Chapter III is the most operationally significant part of the Act for data space operators and data intermediaries. It establishes a mandatory notification regime for providers of data intermediation services, requiring notification to the relevant competent authority before commencing operations and compliance with a set of twelve conditions covering neutrality, non-discrimination, security, interoperability, log record-keeping, business continuity, and legal separation from other services. The transitional period for existing intermediaries expired on 24 September 2025. DGA Chapter IV establishes the voluntary framework for data altruism organisations.

2.1.3 The General Data Protection Regulation (Regulation (EU) 2016/679)

The GDPR is the foundational instrument for personal data protection in EU law and has been applicable since 25 May 2018. For D3.4, the GDPR operates not as a standalone subject but as the pervasive personal data layer that conditions the exercise of rights and obligations under the Data Act and the DGA whenever personal data is involved. Both the Data Act (Article 1(5)) and the DGA (Article 1(3)) contain explicit "without prejudice to GDPR" clauses, meaning that any data sharing obligation or permission under those instruments operates only within the constraints of GDPR.

D3.4 addresses GDPR provisions in four clusters: the core data processing principles (Article 5) and the lawful basis framework (Articles 6 to 10); the data subject rights framework (Articles 12 to 22); the security and breach notification obligations (Articles 32 to 34); and the international transfer rules (Articles 44 to 49). Two provisions deserve particular attention. Article 9 on the special category prohibition – is the primary legal barrier for data holders seeking to share health, genetic, or biometric data for AI training purposes. And Article 20 on the data portability right – intersects directly with the Data Act's access and sharing framework, particularly for connected product data that also qualifies as personal data under the GDPR.

2.1.4 The AI Act – Article 10 (Regulation (EU) 2024/1689)

The AI Act entered into force on 1 August 2024. D3.4 covers only Article 10[2], which applies to providers of high-risk AI systems and governs the data governance practices required for training, validation, and testing datasets. Article 10(1) establishes the basic requirement that training techniques must be applied to datasets in order to meet some quality criteria. Articles 10(2) through (4) specify the data governance practices required, including examination for biases, assessment of data gaps, and requirements for relevance, representativeness, and accuracy. Article 10(5) provides the narrow exception permitting the processing of special category data where strictly necessary for bias detection and correction, subject to stringent safeguards.

While Article 10 is addressed to AI system providers rather than data holders directly, it creates significant indirect obligations for data holders supplying training data. For the avoidance of doubt, data holders supplying training data should be treated as contractually and operationally affected by Article 10, not as direct addressees of Article 10 unless they also qualify as providers or other regulated operators under the AI Act. Any data holder entering into an arrangement to supply data for high-risk AI training must understand the quality and governance standards that the recipient is required to apply, since the data holder's practices at the point of data preparation will directly affect whether those standards can be met.

Table 1. Overview of the four legislative instruments covered by D3.4

Instrument	Timeline	Primary Objective (D3.4 scope)	Key Provisions Covered	Primary Addressees
Data Act Regulation (EU) 2023/2854	In force: 11 Jan 2024 Applies: 12 Sep 2025 Product design obligation: 12 Sep 2026	Establish rights of access to data generated by connected products and related services; enable fair B2B data sharing; support data space interoperability; protect data holders against unlawful third-country access.	Ch. II – User access rights Ch. III – B2B sharing (FRAND) Ch. V – B2G exceptional need Ch. VI – Switching / interoperability Ch. VII – Third-country access Ch. VIII – Smart contracts	Data holders (private) Connected product manufacturers Data space participants Data processing service providers Data recipients
Data Governance Act (DGA) Regulation (EU) 2022/868	In force: 23 Jun 2022 Applies: 24 Sep 2023 Ch. III transitional deadline: 24 Sep 2025	Create governance conditions for trustworthy data sharing through: a re-use framework for protected public sector data; a notification and conditions regime for data intermediation services; and a voluntary registration scheme for data altruism organisations.	Ch. II – Public sector data re-use Ch. III – Data intermediation services Ch. IV – Data altruism organisations Art. 31 – Third-country access (non-personal)	Public sector bodies Data intermediaries / data space operators Data altruism organisations Data re-users

[2] In its full capacity the AI Act will be analysed and operationalised into actionable guidelines as a part of work on D3.5.

Instrument	Timeline	Primary Objective (D3.4 scope)	Key Provisions Covered	Primary Addressees
General Data Protection Regulation (GDPR) Regulation (EU) 2016/679	In force: 25 May 2016 Applies: 25 May 2018	Protect natural persons with regard to the processing of personal data. Operates as the pervasive personal data protection layer beneath the Data Act and DGA – both instruments apply "without prejudice" to the GDPR.	Ch. II – Principles (Arts. 5–11) Ch. III – Data subject rights (Arts. 12–22) Ch. IV – Controller/processor obligations (Arts. 24–43) Ch. V – International transfers (Arts. 44–49) Art. 9 – Special category prohibition Art. 89 – Research derogations	Controllers (data holders processing personal data) Processors Data intermediaries (where personal data involved)
AI Act (Article 10 only) Regulation (EU) 2024/1689	In force: 1 Aug 2024 Art. 10 applies: 2 Aug 2026 High-risk AI (Annex III): 2 Aug 2026	Govern data governance practices for training, validation and testing datasets used in high-risk AI systems. D3.4 covers Art. 10 only – the provision most directly relevant to data holders supplying training data.	Art. 10(1) – Scope gate (quality criteria) Art. 10(2) – Data governance practices Art. 10(3–4) – Representativeness and accuracy Art. 10(5) – Special category bias exception	Providers of high-risk AI systems Data holders supplying AI training data

2.2 HOW THE FOUR INSTRUMENTS RELATE TO EACH OTHER

The four instruments covered by D3.4 do not form a single integrated regime. Understanding how they relate to each other is as important as understanding each instrument in isolation.

2.2.1 The GDPR as the Pervasive Layer

The GDPR functions as the foundational personal data layer beneath the Data Act, the DGA, and the AI Act. The practical consequence for D3.4 is that whenever a data holder's data includes personal data, the compliance analysis must proceed on two tracks simultaneously: the Data Act or DGA track (which determines what the holder can share and with whom) and the GDPR track (which determines the conditions under which personal data within that sharing can lawfully be processed). The consolidated requirements database reflects this dual-track structure through its Cluster 2 (Personal Data Protection) and Cluster 3 (Special Category and Sensitive Data) requirements, which appear alongside and condition the Cluster 1 (Data Access and Sharing) requirements.

2.2.2 Data Act and DGA: Complementary but Distinct

The Data Act and the DGA both address data sharing but from different directions. The Data Act focuses on data generated through economic activity – particularly data generated by connected products – and creates obligations on private sector data holders to make that data available. The DGA focuses on the governance structures through which data sharing takes place. The two instruments are complementary in that the data sharing created by the Data Act frequently needs the governance infrastructure that the DGA provides. The most significant point of intersection is in the data space context, where an organisation may simultaneously be subject to both instruments as a data intermediary under the DGA and as a data holder or data space participant under the Data Act.

There is also a potential tension between the two instruments around the legal separation obligation under DGA Article 12(a), which requires that data intermediation services be provided through a legally separate entity. For an organisation that simultaneously holds data and operates an intermediary service, this creates a significant structural requirement that goes beyond ordinary compliance – it requires corporate restructuring. This is one of the most operationally significant requirements in the consolidated database (REQ-080).

A further cross-instrument consideration arises in relation to the SME exemption under Data Act Article 7(1). A micro or small enterprise that qualifies for the exemption from Chapter II obligations – and that therefore has no obligation to make connected product data available to users or third parties – does not thereby escape DGA obligations. The two instruments operate on different triggers. The Data Act Chapter II exemption is triggered by the organisation's size and its role as a manufacturer or related service provider of connected products. DGA obligations, by contrast, are triggered by what the organisation does with data and how it structures its operations: if the exempt micro or small enterprise also operates a data intermediation service, registers as a data altruism organisation, or participates in a data space as an intermediary, the relevant DGA Chapter III, IV, or V obligations apply in full regardless of the organisation's size. There is no SME exemption equivalent in the DGA for these activities.

The practical implication is that size-based relief under the Data Act is narrower than it may initially appear to a practitioner who encounters both instruments together. The exemption removes the data access and sharing obligations that would otherwise arise from connected product activity – it does not remove the governance and structural obligations that arise from the organisation's role in the data ecosystem more broadly. In the LDTM, this distinction is captured through the separation of Q2 (size) from Q8, Q12, and Q13 (activities): a micro enterprise that answers Yes to Q12 or Q13 will receive the full Cluster 6 output regardless of its Q2 answer.

2.2.3 The AI Act and the Data Instruments

The relationship between Article 10 of the AI Act and the GDPR is the most legally complex cross-instrument relationship addressed in D3.4. Article 10(5) explicitly acknowledges that processing special category data for AI purposes must remain subject to the conditions in GDPR Article 9(2). Article 10(5) should not be presented as a general AI-training legal basis. It is a narrow, specific permission for bias detection and correction in high-risk AI systems, subject to strict safeguards and without displacing the GDPR's general requirements, including the need for a lawful basis under Article 6 and compliance with data protection principles. The relationship between Article 10 of the AI Act and the Data Act operates primarily through quality standards: the Data Act requires data to be made available in a machine-readable format suitable for the intended use, while the AI Act requires that training data be representative, relevant, and free of errors.

2.2.4 Regulatory Friction and Cross-Instrument Tensions

The harmonisation work in Stage 2 of D3.4's methodology (described in full in Section 3) identified several points of "regulatory friction" – situations where requirements from different instruments address the same compliance question from different normative angles. Three are worth highlighting.

First, the non-discrimination principle appears across all four instruments in slightly different formulations. The Data Act requires that data sharing obligations be applied without discriminating between similarly situated recipients. The GDPR prohibits processing that leads to discriminatory outcomes for data subjects. The DGA requires data intermediaries to operate neutrally and without favouring particular participants. The AI Act requires that training data not embed or reproduce discriminatory patterns. Each formulation addresses a different dimension of the same underlying value, and in practice an organisation subject to multiple instruments must satisfy all of them simultaneously. The consolidated database brings these overlapping formulations together and identifies where they converge on a single compliance obligation and where they genuinely diverge.

Second, the purpose limitation principle creates a specific friction in the context of AI training data. Data originally collected for the purpose of providing a connected product service – sensor readings, usage data, performance logs – was collected under a specific purpose and, where personal data is involved, under a specific legal basis. Using that same data to train an AI system involves a different purpose, and whether that secondary use is compatible with the original collection purpose is a question that neither the Data Act nor the AI Act resolves definitively. The GDPR's purpose limitation principle governs the personal data dimension, but the tension between the Data Act's sharing obligations and the GDPR's purpose limitation creates a compliance question that practitioners must actively manage rather than assume away.

Third, the anonymisation gateway creates a potentially powerful but technically demanding route out of GDPR obligations. Under GDPR Recital 26, data that has been genuinely anonymised – rendered irreversibly incapable of identifying a natural person – falls outside the GDPR altogether and can be shared without GDPR constraints. Article 11 of the GDPR addresses a related but distinct situation: where a controller does not need to identify the data subject and is not required to maintain or acquire additional identifying information solely for GDPR compliance, it is not obliged to do so. These are different concepts and should not be conflated. The practical barrier in both cases remains the same: genuine anonymisation of health, genetic, or biometric data – particularly in the context of AI training, where re-identification risks from model outputs are real – is technically difficult to achieve and even more difficult to verify. The D3.4 model treats anonymisation as a conditional gateway rather than a straightforward opt-out, and the LDTM flags it as a technical safeguard requirement rather than a simple compliance choice.

The concrete resolution of each of these tensions – how overlapping requirements are consolidated, where friction is flagged for practitioner attention, and how the LDTM navigates competing obligations – is documented in the consolidated requirements database and described cluster by cluster in Section 4.

2.3 NOTE ON THE DIGITAL OMNIBUS PROPOSAL

On 19 November 2025, the European Commission published its Digital Omnibus proposal – a legislative package designed to simplify and consolidate the EU's digital regulatory framework. The proposal would make significant changes to several of the instruments covered by D3.4, and its potential impact on the compliance landscape is a material consideration for any work in this space.

For data intermediaries and data space operators, the most significant proposed change is the transformation of the DGA Chapter III notification regime from mandatory to voluntary. Under the Digital Omnibus proposal, providers of data intermediation services would no longer be required to notify a competent authority before commencing operations. The legal separation requirement, currently one of the most operationally demanding requirements, would be replaced by a functional separation requirement with lighter conditions, and the conditions list would be significantly shortened.

For data holders and AI developers working with personal data, Digital Omnibus proposes significant amendments to the GDPR. Most notably, it would introduce a new Article 9(2)(k) exception permitting the processing of special category data as residual data in the context of AI system development and operation, where the controller implements appropriate measures to avoid collecting such data and removes it when identified. The Omnibus also proposes to clarify that the processing of personal data for AI development may be based on legitimate interest under Article 6(1)(f), and to introduce a new small mid-cap category for companies with fewer than 750 employees, extending certain protections to a broader group.

Having that in mind, the D3.4 is still built on the current legal framework. All guidelines, the consolidated requirements database, and the Logical Decision Tree Model reflect the law as it stands in June 2026. The Digital Omnibus remains at proposal stage – it has not been adopted, and the ordinary legislative procedure must be completed before any of its provisions enter into force. The Digital Omnibus is discussed in this section for orientation and transparency. Its potential impact on the compliance paths modelled in the LDTM is assessed in Section 7, and the LDTM architecture has been deliberately designed to be updatable in anticipation of legislative changes of this kind.

3 METHODOLOGY

The methodology employed in D3.4 follows a Design Science Research (DSR) framework, specifically conceived to bridge the gap between high-level normative requirements and practical market implementation. Given that the objective of D3.4 is to transform the theoretical findings of the legal analysis with the ethical and social requirements into an actionable guidance tool for practitioners, a three-stage deductive thematic synthesis was employed.

3.1 DESIGN SCIENCE RESEARCH FRAMEWORK

Design Science Research is an established research paradigm in information systems and policy research that focuses on the creation of artefacts – models, methods, frameworks, or instantiations – that address real-world problems.[3] DSR is appropriate for D3.4 because the deliverable's primary contribution is not a theoretical insight about regulatory law but a practical artefact: the Logical Decision Tree Model, designed to be used by data holders and other practitioners in real compliance contexts.

The DSR framework structures the D3.4 work into three iterative stages that move from problem identification and knowledge base construction (Stage 1), through synthesis and design (Stage 2), to the production of a validated, deployable artefact (Stage 3). Each stage produces a concrete output that feeds directly into the next, and the overall design is grounded in the empirical base of the prior WP3 deliverables rather than in abstract theoretical premises. The choice of DSR is also significant for how the deliverable positions itself: D3.4 is a regulatory engineering exercise – taking known legal requirements and designing an artefact that makes compliance with those requirements tractable for non-legal audiences.

3.2 STAGE 1 – REQUIREMENTS EXTRACTION AND FILTERING

A systematic review of the four legislative instruments was conducted to isolate all compliance-relevant requirements applicable to data holders and data spaces. Using a deductive coding approach, each provision was extracted and filtered for its relevance to the four instruments in scope, ensuring the guidelines remain focused on the operational realities of actors entering and operating within EU data ecosystems.

Each extracted requirement was classified according to a thirteen-column schema designed to serve dual purposes: as the evidence base for this written report, and as the backend data source for the compliance tool. The schema captures the full normative structure of each requirement – not merely what the law says, but who it addresses, when it activates, what exemptions apply, and what type of obligation it represents.

The Requirement Type taxonomy maps directly onto the decision tree logic of Stage 3. Requirements are classified as one of six types: Obligations (things the actor must do), Prohibitions (things the actor must not do), Permissions (things the actor is expressly permitted to do), Conditional Gates (provisions that determine whether other requirements apply), Scope Gates (provisions that define the boundaries of a regime), and Procedural requirements (administrative steps required by law). This taxonomy allows the LDTM to present requirements in their correct normative register rather than treating all provisions as equivalent obligations.

The extraction produced 198 rows across the four instruments: 95 from the Data Act, 50 from the Data Governance Act, 49 from the GDPR, and 4 from Article 10 of the AI Act. Requirement texts represent structured paraphrases of the source provisions, preserving operative legal terminology while condensing multi-paragraph articles into single actionable entries. Full source citations are provided for each row.

[3] Hevner, A., Chatterjee, S. (2010). Design Science Research Frameworks. In: Design Research in Information Systems. Integrated Series in Information Systems, vol 22. Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-5653-8_3

3.3 STAGE 2 – TRANSDISCIPLINARY HARMONISATION

The extracted requirements were mapped onto a Requirement Traceability Matrix – a consolidated cross-instrument database of 128 unified requirement rows, organised into ten thematic clusters. This stage involved identifying and resolving "regulatory friction": instances where mandatory legal obligations interact with, overlap, complement, or possibly conflict with one another across instruments.

The consolidation process involved three operations on the raw extraction data. First, deduplication: where requirements from multiple instruments address the same compliance obligation from different normative angles, they were merged into a single unified row with full cross-referencing to the source provisions. Second, cross-instrument mapping: each unified requirement carries an Overlap Flag (Yes / Partial / No), a Cross-Instrument Related IDs column referencing the original extraction entries from other instruments, and a Related Consolidated REQs column providing navigation references within the consolidated database itself. Third, LDTM trigger mapping: each unified requirement is tagged with the LDTM question or combination of questions whose answers activate it, providing the direct link between the LDTM and the requirements database.

The ten thematic clusters that organise the consolidated database reflect the substantive structure of the compliance challenge rather than the structure of any single instrument. Clusters 1 to 4 address the data asset itself: access and sharing obligations, personal data protection, special category and sensitive data, and trade secret protection. Clusters 5 and 6 address the governance and contractual framework: contractual fairness and FRAND conditions, and data space and intermediary governance. Cluster 7 addresses the international dimension. Cluster 8 addresses AI data governance specifically. Clusters 9 and 10 address enforcement and institutional framework issues: enforcement, remedies and penalties, and exemptions and compliance timelines.

3.4 STAGE 3 – COMPLIANCE-BY-DESIGN TOOL

The final synthesis is crystallised into the Logical Decision Tree Model. This artefact serves as a compliance-by-design tool, guiding stakeholders through a sequential logic flow to determine their specific regulatory obligations and best practices within the EU data ecosystem. The LDTM is the principal outcome of D3.4 and is described in full in Section 5.

The LDTM was designed according to three principles. First, **completeness**: every requirement in the consolidated database must be reachable through at least one combination of question answers. A gap analysis was conducted after the initial question set was drafted, resulting in several corrections.

Second, **precision**: the question sequence must activate the right requirements for the right actors without generating false positives. Third, **updatability**: the LDTM architecture is designed so that new requirements, questions, and exemption branches can be added without rebuilding the model. The modular structure of the question set enables this in practice: new questions can be inserted into any of the four sections without disrupting the logic of the remaining sections, and new requirements can be added to the database with a corresponding trigger mapping entry that connects them to the relevant questions. This means that when the regulatory landscape changes – as it will if the Digital Omnibus proposal is adopted – the LDTM can be updated on a per requirement and per question basis rather than rebuilt from scratch. Updatability was treated as a design constraint from the outset rather than an afterthought, precisely because the current regulatory environment is one in which significant legislative change is foreseeable and where a compliance tool that cannot adapt quickly loses its practical value.

By adopting this DSR framework, D3.4 ensures that the resulting guidelines are not merely a summary of previous work but a rigorous, validated framework that serves as the methodological and evidential foundation for the compliance tool.

3.5 ETHICAL AND SOCIAL LAYERS INTEGRATION

The ethical and social considerations of D3.4 are provided through the contributions of the D3.2 (Ethical Requirements) and D3.3 (Social Requirements) partners. Rather than treating ethical and social

considerations as an external commentary on the legal framework, D3.4 integrates them structurally into the compliance output as Tier 2 – a layer of responsible compliance best practices that any serious data holder or data space operator should aspire to meet alongside their minimum legal obligations.

These considerations were collected through a structured partner input template developed as part of Stage 2 of the D3.4 methodology. The template was designed to produce inputs that are directly usable in the compliance output, not general ethical reflections but specific, actionable best practices tied to the thematic clusters and scenarios in the consolidated database.

The partner inputs received through the template were processed, structured, and extended into the D3.4 Ethical and Social Best Practices table – a companion database of 35 rows. The table is maintained as a separate sheet within the same excel workbook as the consolidated requirements database, ensuring that both legal obligations and responsible compliance best practices are held in a single, integrated data structure.

Each row in the table carries an LDTM Trigger Mapping that connects it to the question or combination of questions in the LDTM that activates it. This mapping was validated against the full question set to ensure that every best practice is reachable through the existing framework without requiring additional questions.

4 CONSOLIDATED COMPLIANCE REQUIREMENTS

This section presents the consolidated requirements database produced in Stage 2 of the D3.4 methodology. The database brings together the 198 requirements extracted across the four legislative instruments in scope and organises them into 128 unified rows across ten thematic clusters. It is the evidential foundation for both this report and the Logical Decision Tree Model presented in Section 5. An abridged version of this table is available in Appendix A.

4.1 OVERVIEW OF THE TEN THEMATIC CLUSTERS

The ten clusters were designed to reflect the substantive structure of the compliance challenge – the types of questions that a data holder or data space operator actually needs to answer – rather than the legislative structure of any single instrument. The Table 2 below provides an overview of the clusters, their row counts, and the primary instruments and addressees involved.

Table 2. D3.4 Consolidated Requirements: Thematic Cluster Overview

#	Cluster	Rows	IDs	Sources	Primary Addressees
1	**Data Access and Sharing Obligations**	15	REQ-001–015	Data Act, DGA, GDPR	Data holders, public sector bodies
2	**Personal Data Protection**	26	REQ-016–041	GDPR, Data Act	Controllers, processors, data holders
3	**Special Category and Sensitive Data**	16	REQ-042–057	GDPR, AI Act Art. 10	Controllers, AI system providers
4	**Trade Secret and Confidentiality Protection**	8	REQ-058–065	Data Act, DGA	Data holders, re-users, public sector bodies
5	**Contractual Fairness and FRAND Conditions**	10	REQ-066–075	Data Act, DGA	Data holders, data recipients, intermediaries
6	**Data Space and Intermediary Governance**	17	REQ-076–092	DGA, Data Act	Data intermediaries, data space operators
7	**International Data Transfers**	11	REQ-093–103	GDPR, Data Act, DGA	Controllers, processors, data processing services
8	**AI Data Governance**	6	REQ-104–109	AI Act Art. 10, GDPR, DGA	AI system providers, data holders supplying training data

9	**Enforcement, Remedies and Penalties**	11	REQ-110–120	Data Act, DGA, GDPR	All actors within scope
10	**Exemptions and Compliance Timelines**	8	REQ-121–128	Data Act, DGA, GDPR	All actors – scope gates and exemptions

The following subsections describe each cluster, explaining the compliance questions it addresses, the primary cross-instrument relationships it captures, and its relationship to the LDTM question set.

4.2 CLUSTER 1: DATA ACCESS AND SHARING OBLIGATIONS

Cluster 1 contains the foundational data access and sharing obligations applicable to data holders and public sector bodies. It draws primarily from the Data Act (user access rights under Chapter II, B2B sharing and FRAND conditions under Chapter III, the B2G exceptional need mechanism under Chapter V, and data space interoperability obligations under Chapter VI) and from the DGA (public sector data re-use framework under Chapter II). The GDPR's data portability right (Article 20) is included here because it creates a parallel access entitlement for personal data that operates alongside the Data Act's connected product data access framework.

The most operationally significant requirements in this cluster are REQ-001 (connected product design obligation – products must be designed to make data accessible by default), REQ-002 and REQ-004 (data holder must make data available to users and authorised third parties without undue delay), REQ-005 (FRAND arrangement obligation), REQ-008 and REQ-009 (B2G exceptional need sharing obligations), and REQ-011 (data space interoperability compliance obligation). This cluster is conditioned by REQ-121 (SME exemption – Cluster 10) which excludes qualifying micro and small enterprises from the Chapter II obligations, and by REQ-122 and REQ-123 (compliance timelines).

4.3 CLUSTER 2: PERSONAL DATA PROTECTION

Cluster 2 is the largest cluster with 26 rows, reflecting the comprehensive nature of the GDPR's obligations on controllers. It covers the five data processing principles of Article 5 (REQ-016 to REQ-022), the lawful basis framework (REQ-023 to REQ-025), anonymisation and purpose management obligations (REQ-026, REQ-024), transparency obligations including Articles 12, 13, and 14 notices (REQ-027 to REQ-029), data subject rights (REQ-030 to REQ-032), technical and organisational security measures (REQ-033 to REQ-034), and records of processing (REQ-035).

In addition to the core GDPR obligations, this cluster includes three Data Act-specific personal data gates (REQ-036 to REQ-038) that condition data sharing under the Data Act on GDPR compliance: personal data may only be made available to users (REQ-036) or third parties (REQ-037) where there is a valid GDPR legal basis, and data holders must anonymise before sharing in the B2G exceptional need context unless personal data disclosure is strictly necessary (REQ-038). Two DGA-specific obligations are also included: the data intermediary's obligation to act in the data subject's best interest (REQ-040) and the data altruism organisation's transparency obligation to data subjects (REQ-041). This cluster is closely linked to Cluster 3 – any actor processing personal data must satisfy both clusters if special category data is involved.

4.4 CLUSTER 3: SPECIAL CATEGORY AND SENSITIVE DATA

Cluster 3 addresses the heightened protection framework for sensitive personal data and the specific obligations arising from high-risk AI system development. It includes the GDPR Article 9(1) prohibition (REQ-042) and its exceptions (REQ-043), the children's consent threshold obligation (REQ-044), the criminal conviction data restriction (REQ-045), security measures for special category processing (REQ-046), breach notification obligations (REQ-047 to REQ-048), Data Protection Impact Assessment (DPIA) and prior consultation requirements (REQ-049 to REQ-050), Data Protection Officer (DPO) designation obligation (REQ-051), and the research and statistical derogation framework (REQ-052 to REQ-053).

Crucially, this cluster also includes the AI Act Article 10 requirements as they apply specifically to special category data in AI development: the Article 10(1) scope gate (REQ-054), the data governance practice obligations (REQ-055 to REQ-056), and the narrow Article 10(5) bias correction exception (REQ-057). These rows overlap with Cluster 8 – where they are presented in the AI-specific context – because they are substantively relevant both to data holders classifying their data and to AI system providers assessing their training data governance obligations.

4.5 CLUSTER 4: TRADE SECRET AND CONFIDENTIALITY PROTECTION

Cluster 4 addresses the interaction between data sharing obligations and trade secret protection. The core tension the cluster resolves is that the Data Act creates obligations to share data that may contain trade secrets, while EU trade secret law (Directive 2016/943) protects precisely that information. The cluster includes obligations to identify trade secret data and seek confidentiality agreements before sharing (REQ-058), the right to withhold data where no adequate confidentiality agreement can be reached (REQ-059), the limits of the sharing obligation where trade secrets are involved (REQ-060), and technical protection measure permissions (REQ-061).

It also covers the minimum necessary disclosure principle for B2G exceptional need requests (REQ-063) – trade secrets may only be disclosed to the extent strictly necessary for the purpose – and the confidentiality obligations placed on DGA Chapter II data re-users (REQ-064) and public sector bodies (REQ-065). This cluster is activated for any actor that answers Yes to Q5 (trade secrets) in the LDTM.

4.6 CLUSTER 5: CONTRACTUAL FAIRNESS AND FRAND CONDITIONS

Cluster 5 addresses the contractual framework for data sharing, focused on the Data Act's requirements that terms be fair, reasonable, and non-discriminatory. The cluster includes the invalidity provisions for terms that derogate from user and data recipient rights (REQ-066), the unfair terms prohibition for B2B data sharing contracts (REQ-067), the fairness assessment framework for unilaterally imposed terms (REQ-068), and the burden of proof rule (REQ-069). REQ-070 through REQ-072 address the compensation framework – any compensation must be non-discriminatory, FRAND-compliant, and transparently documented.

The cluster also includes DGA-specific pricing obligations for data intermediaries (REQ-073) and public sector bodies (REQ-074), and notes the Commission's power to develop non-binding model contractual terms (REQ-075) which, when published, will provide a safe harbour for compliant data sharing agreements. This cluster applies primarily to actors engaged in B2B data sharing (Q9=Yes) and data intermediation (Q12=Yes).

4.7 CLUSTER 6: DATA SPACE AND INTERMEDIARY GOVERNANCE

Cluster 6 is the most complex cluster for data space operators and data intermediaries. It contains the full DGA Chapter III compliance framework: the scope gate establishing which services must comply (REQ-076), the mandatory notification obligation and the procedure (REQ-077), the change notification requirement (REQ-078), the non-EU legal representative obligation (REQ-079), and the conditions for providing data intermediation services (REQ-080 to REQ-087). The most operationally demanding of these is REQ-080 (the legal separation and non-use obligation), which requires that the intermediary service be provided through a legally separate entity and that the intermediary does not use data for its own commercial purposes.

The cluster also includes the Data Act obligations for data space participants: the interoperability requirement (REQ-088), smart contract essential requirements (REQ-089, activated only if Q9a=Yes), non-hindrance of user access rights (REQ-090), the gatekeeper exclusion (REQ-091), and the DGA transitional compliance deadline (REQ-092). This cluster is activated primarily for actors answering Q12=Yes (register as data intermediary) and Q8=Yes (data space participation).

4.8 CLUSTER 7: INTERNATIONAL DATA TRANSFERS

Cluster 7 addresses the international dimension of data sharing across two legally distinct frameworks that are triggered by different facts and activate different obligations. The first is the GDPR international transfer framework, which applies whenever personal data is transferred to a recipient located outside the EU or EEA or processed by infrastructure subject to non-EU jurisdiction. The second is the Data Act and DGA third-country governmental access framework, which applies to non-personal data held in the Union and addresses the risk of unlawful access by non-EU governmental authorities, regardless of whether any active transfer to a third country is taking place.

The GDPR international transfer framework is covered through the scope gate (REQ-093), the adequacy decision route (REQ-094), the Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) (REQ-095), and the derogations of last resort (REQ-096). These requirements are activated by Q15a=Yes and apply only to actors who answered Q4=Yes (personal data).

For non-personal data, the cluster includes the obligation to take all reasonable technical, legal, and organisational measures to prevent unlawful third-country governmental access to non-personal data held in the Union (REQ-097), the conditions under which a third-country governmental access request may lawfully be complied with (REQ-098), the parallel obligation to protect any personal data component in a mixed dataset subject to such a request (REQ-099), the data minimisation obligation in third-country compliance (REQ-100), and the notification obligation to the competent supervisory authority (REQ-101). These requirements are activated by Q15b=Yes and apply to all actors regardless of their answer to Q4, since the governmental access risk attaches to non-personal data held on infrastructure subject to non-EU jurisdiction independently of whether any personal data is involved.

Two further obligations complete the cluster. REQ-102 applies to DGA re-users – the obligation to inform the public sector body before transferring re-used data to a third country. REQ-103 applies to data processing service providers – the obligation to publish information on the third-country jurisdictions to which they are subject and the governmental access requests they have received. Both are activated by Q15b=Yes in combination with the relevant actor role identified in Q1.

This cluster is activated for any actor answering Q15a=Yes (personal data international transfers), Q15b=Yes (non-personal data infrastructure subject to non-EU jurisdiction), and/or Q18=Yes (specific third-country governmental access request received or anticipated). Q15a and Q15b are independent – an actor may be in

scope for one, the other, or both, and the compliance output reflects only the sub-framework or sub-frameworks applicable to their specific situation.

4.9 CLUSTER 8: AI DATA GOVERNANCE

Cluster 8 addresses the specific data governance obligations arising from the development and use of high-risk AI systems. It includes the AI Act Article 10(1) scope gate (REQ-104), the data governance practice obligations of Articles 10(2) through 10(4) (REQ-105 to REQ-106), and the Data Act non-compete prohibition on data recipients (REQ-107). It also includes the GDPR data quality obligations as they apply specifically to AI training data (REQ-108) and the DGA re-user obligation when AI system development is the intended use (REQ-109).

REQ-104, REQ-105, and REQ-106 overlap with REQ-054, REQ-055, and REQ-056 in Cluster 3. This cross-cluster placement is intentional: in Cluster 3 those requirements appear in the context of special category data; in Cluster 8 they appear in the context of AI system development. A data holder supplying health data for AI training encounters both clusters in their LDTM output – Cluster 3 for the data type obligations and Cluster 8 for the AI-specific training data governance framework. This cluster is activated for actors answering Q11=Yes (supply data for AI development) combined with Q16=Yes (high-risk AI system).

4.10 CLUSTER 9: ENFORCEMENT, REMEDIES AND PENALTIES

Cluster 9 provides the enforcement context for all other clusters. It includes the dispute settlement body access obligation (REQ-110), the complaint right across all three instruments (REQ-111 – always relevant), the judicial remedy right (REQ-112 – always relevant), GDPR supervisory authority powers (REQ-113), Data Act competent authority information request powers (REQ-114), GDPR damage compensation (REQ-115), the Data Act and DGA penalty frameworks (REQ-116 to REQ-117), the GDPR fine tiers (REQ-118), the non-EU legal representative obligation (REQ-119), and the DGA re-use decision right of redress (REQ-120).

REQ-111 and REQ-112 are the only requirements in the database marked "Always relevant" as enforcement/remedy pathways, but they get triggered by alleged infringement, competent-authority action, or failure to act – the complaint right and judicial remedy right apply to all actors regardless of their answers to the LDTM questions. REQ-114, REQ-116, and REQ-117 are scoped to the Data Act and DGA actors, respectively. This cluster serves primarily as reference material in the compliance output, informing actors of the enforcement consequences and remedies available to them and their stakeholders.

4.11 CLUSTER 10: EXEMPTIONS AND COMPLIANCE TIMELINES

Cluster 10 functions as the scope management layer of the consolidated database. It contains the provisions that define who the obligations apply to, when they apply, and what optional pathways exist. The SME exemption (REQ-121) is the most operationally significant – it excludes qualifying micro and small enterprises from Data Act Chapter II obligations. The Data Act and DGA compliance timelines (REQ-122 to REQ-123) establish when obligations entered into force. The DGA Chapter II scope gate (REQ-124) defines which public sector data is subject to the DGA re-use framework. The data altruism registration conditions (REQ-125) define the voluntary pathway for altruism organisations.

The anonymisation gateway (REQ-126) is also placed here because it functions as a scope gate – data that is genuinely anonymised falls outside the GDPR and certain other obligations. The sui generis[4] database right exclusion (REQ-127) – which prevents companies from claiming intellectual property ownership over raw databases – ensures that data holders cannot use these database rights to block access obligations. The codes of conduct permission (REQ-128) provide the voluntary compliance tool available to all personal data processors. In the LDTM, Cluster 10 requirements function as the first filter in the output – they determine whether and to what extent other cluster requirements apply to the user's specific situation.

[4] Sui generis is a Latin legal term meaning "of its own kind" or "unique." In the context of the EU AI act, the "sui generis database right exclusion" refers to a specific, standalone property right that protects the investment put into creating a database.

5 THE LOGICAL DECISION TREE MODEL

The Logical Decision Tree Model is the principal artefact produced by D3.4. It is a compliance-by-design tool that translates the 128 consolidated requirements across ten thematic clusters into a structured question sequence, producing a tailored compliance output for different actors in the EU data ecosystem. This section describes the architecture and design rationale of the LDTM, presents each of its four sections with their question text and answer options. The complete question set for the LDTM is available in Appendix C.

5.1 ARCHITECTURE AND DESIGN RATIONALE

The LDTM is structured as a single tree with a shared trunk and role-sensitive branching. It is organised into four sequential sections, each addressing a different dimension of the compliance question, as shown in Figure 1. This four-section architecture reflects a deliberate design decision: rather than presenting a single long question list, the model groups questions by their logical function, making the navigation more intuitive for practitioners who may not have a legal background.

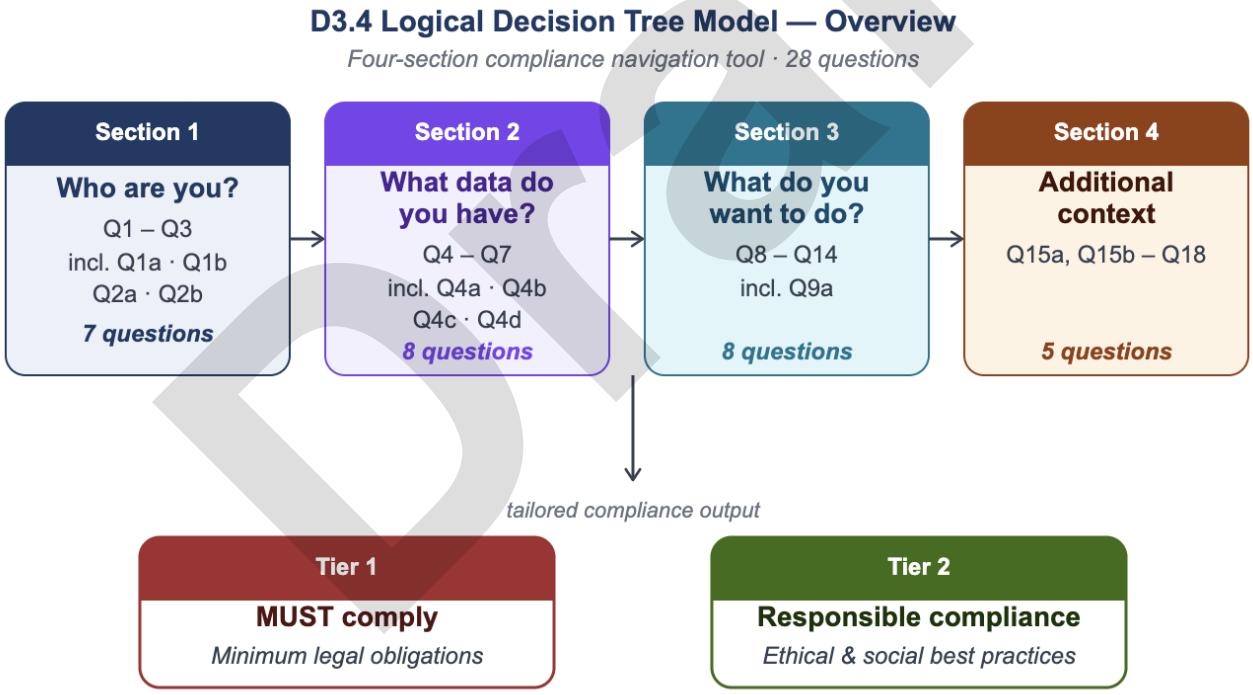

Figure 1. Overview of the Logical Decision Tree Model

The LDTM produces a two-tier compliance output tailored to the specific combination of answers provided. Tier 1 identifies the minimum legal obligations that apply to the actor, drawn from the consolidated requirements database and activated by the actor's answers across all four sections. Tier 2 presents the responsible compliance best practices that the actor should consider beyond the legal minimum. The content, rationale, and design of the two-tier output are described in full in Section 6 of this report.

The architecture was designed to satisfy three properties. Completeness requires that every row in the consolidated database is reachable through at least one combination of answers. Precision requires that each

question activates the right requirements without generating false positives – a non-EU actor should not see EU enforcement penalty provisions as applicable to them, and a data altruism organisation should not be presented with the full Data Act Chapter II sharing framework. Updatability requires that new questions, requirements, and exemption branches can be added when legislation changes – a critical design requirement given the current state of EU data law.

The model comprises 28 questions. Section 1 contains 7 questions addressing the actor's identity. Section 2 contains 8 questions addressing the nature of the data. Section 3 contains 8 questions addressing the actor's intended activities. Section 4 contains 5 questions addressing cross-cutting contextual factors. Each question in Sections 2, 3, and 4 is independent – a Yes answer to one question does not preclude a Yes answer to another – and the LDTM trigger mapping column in the consolidated database records the specific question or combination of questions that activates each requirement.

5.2 SECTION 1: WHO ARE YOU?

Section 1 establishes the actor's role, organisation size, processor status, and EU establishment. These answers function as the first filter in the compliance output – they determine which regulatory regime applies, whether any size-based exemptions are available, and whether additional non-EU obligations apply.

Q1 asks the actor to identify their primary role from seven options: data holder (private sector); data holder (public sector body); data intermediary or data space operator; data altruism organisation; data re-user; provider of data processing services; and data recipient or user of connected product data. Where the actor is a private sector data holder, Q1a asks them to identify their specific activity: connected product manufacturer, related service provider, or private holder in another capacity. This sub-question is relevant because the Data Act's core access and sharing framework in Chapters II and III applies specifically to manufacturers and related service providers, while other private sector data holders are primarily subject to the contractual fairness, B2G, and interoperability provisions. Q1b is asked of all actors regardless of their Q1 answer: does the organisation also act as a data processor – processing personal data strictly on behalf of and under the instructions of another controller? A Yes answer causes processor-specific GDPR obligations (the data processing agreement requirement, the obligation to process only on instructions, and the processor security liability) to be flagged in the Tier 1 output alongside the primary role obligations.

Q2 establishes organisation size – microenterprise, small enterprise, medium enterprise, large enterprise, or public sector body. Where a micro or small enterprise is identified, Q2a asks whether the organisation has linked or partner enterprises that would affect the size calculation, and Q2b asks whether more than 25% of activities are carried out as a subcontractor for larger enterprises. The SME exemption from Data Act Chapter II is only confirmed when both Q2a and Q2b are answered No, ensuring that the exemption is not improperly claimed by enterprises that are nominally small but effectively part of larger groups. Q3 asks whether the organisation is established in the EU or offers products or services within the EU, activating the legal representative designation obligation for non-EU actors falling within scope. The entire flow of Section 1 is shown in Figure 2 below.

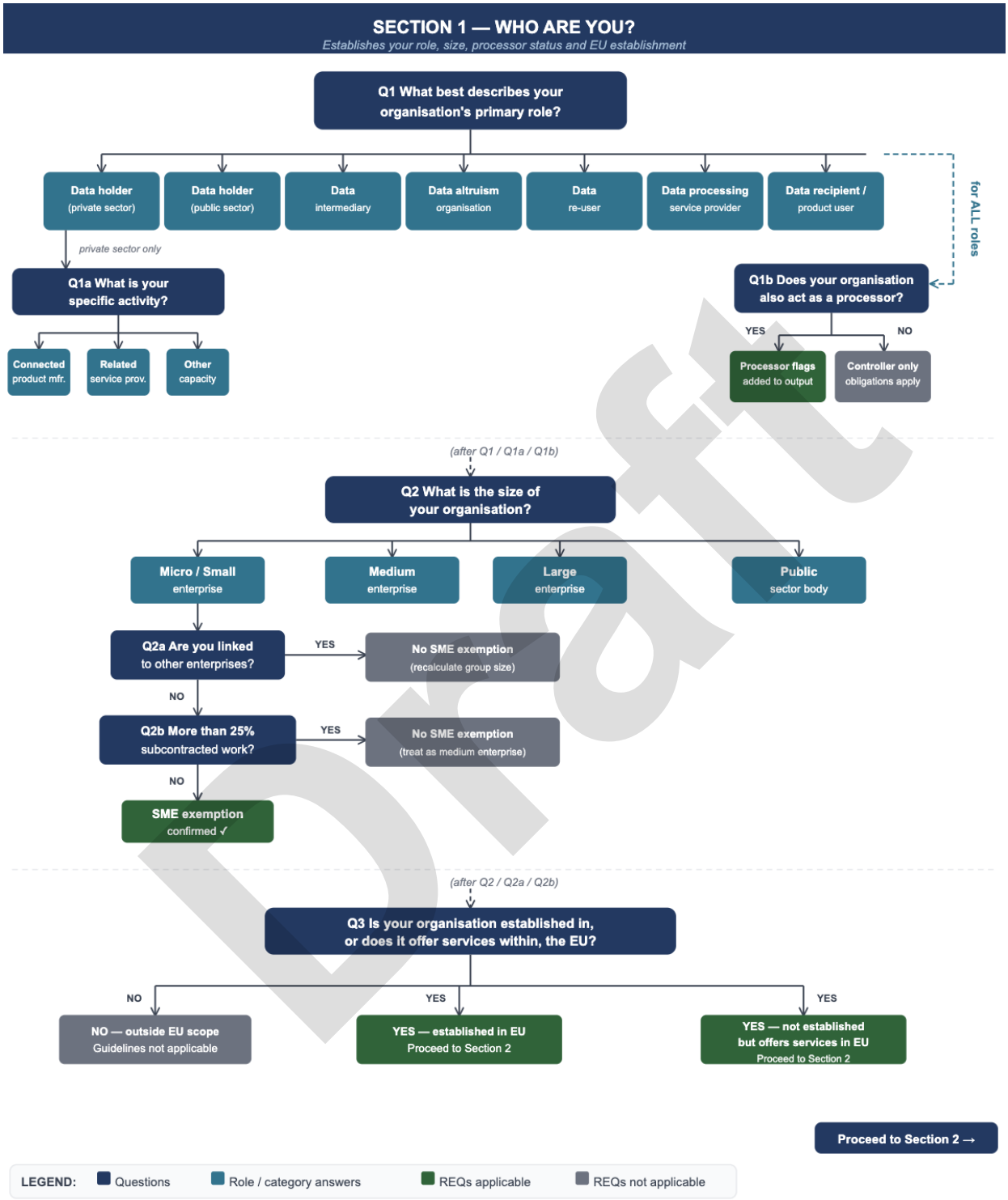

Figure 2. Section 1 of the Logical Decision Tree Model

5.3 SECTION 2: WHAT DATA DO YOU HAVE?

Section 2, shown in Figure 3, characterises the nature of the data the actor holds or intends to share. Unlike Section 1, which establishes a single primary role, the questions in Section 2 are independent – an actor may answer Yes to several questions, and each Yes answer activates a corresponding set of requirements.

Q4 is the personal data gate: does the actor process, hold, or intend to share personal data? A Yes answer activates the full Cluster 2 (Personal Data Protection) framework. It also unlocks four sub-questions. Q4a asks about health data, activating Cluster 3 special category obligations and the AI Act Article 10 pathway for health data in AI training. Q4b asks about children's data, activating the parental consent threshold and the heightened transparency obligations. Q4c asks about genetic, biometric, or other special category data within the Article 9 prohibition. Q4d asks about criminal conviction or offence data, activating the Article 10 GDPR restriction. A No answer to Q4 means GDPR does not apply to the data in question, and the actor proceeds to Q5.

Q5 asks whether any data includes trade secrets. A Yes answer activates the full Cluster 4 (Trade Secret and Confidentiality Protection) framework, including the identification, agreement, and withholding obligations. Q6 asks whether the data originates from or is held by a public sector body under DGA Chapter II conditions. A Yes answer activates the DGA Chapter II scope gate and the associated re-user and public sector body obligations in Clusters 1, 4, and 10 – both for actors actively seeking access and for actors who already hold such data under existing re-use authorisations. Q7 asks whether the data was generated by a connected product or related service. A Yes answer activates the Data Act Chapter II and III framework for connected product data, including the design-by-default obligation and the user access right.

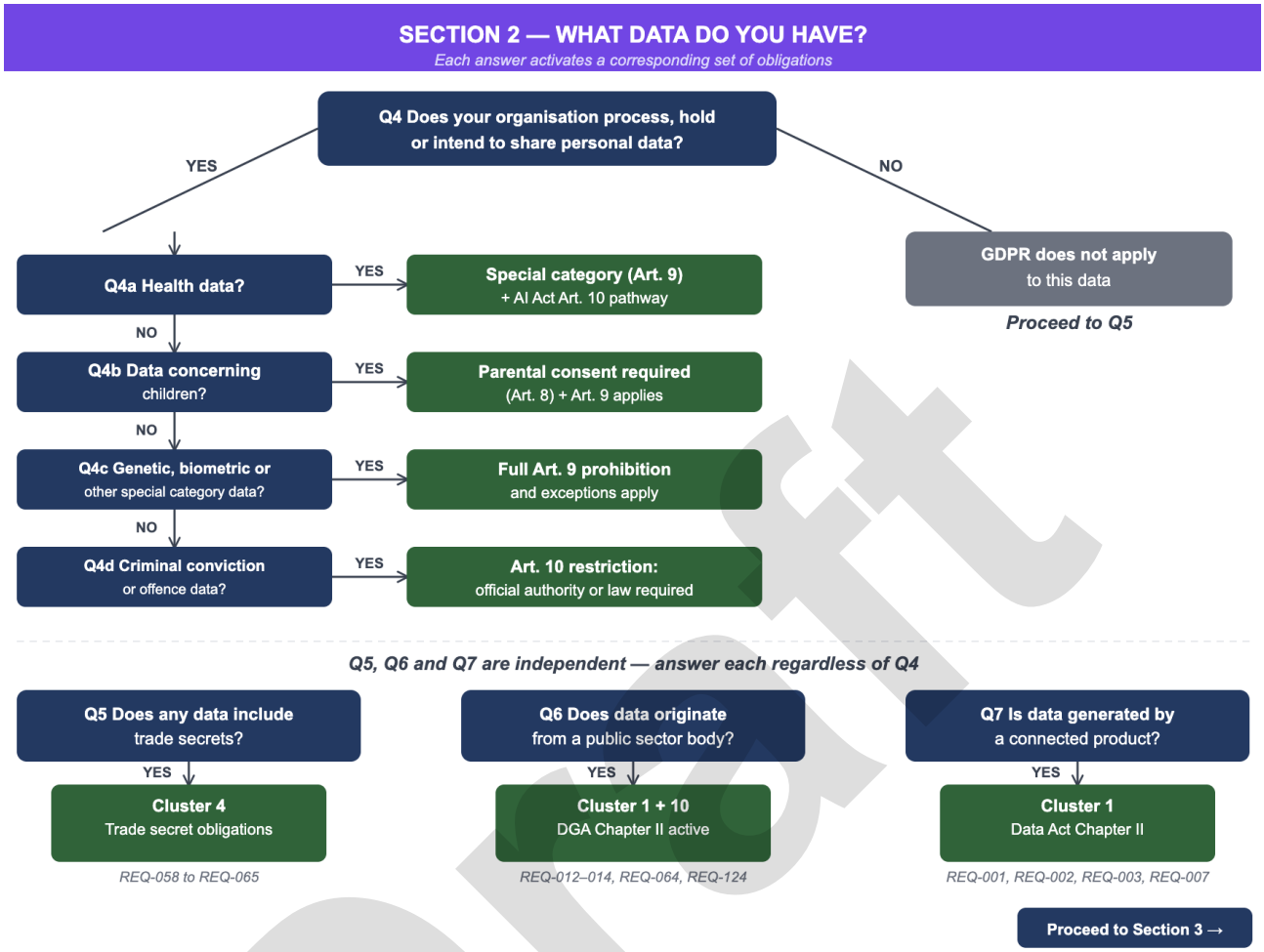

Figure 3. Section 2 of the Logical Decision Tree Model

5.4 SECTION 3: WHAT DO YOU WANT TO DO?

Section 3, presented in Figure 4, captures the actor's intended activities. Seven questions are asked, each addressing a distinct compliance context. These questions are fully independent of each other – an actor may legitimately answer Yes to multiple questions, and each Yes combination produces a cumulative compliance output.

Q8 asks whether the actor intends to enter or participate in a data space. A Yes answer activates the Data Act interoperability and data space governance obligations (REQ-011, REQ-088). Q9 asks whether the actor intends to share data commercially with third parties on a B2B basis. A Yes answer activates Clusters 1, 4, and 5 (data sharing obligations, trade secret protections, and contractual fairness). If Q9 is Yes, Q9a follows: does the actor use smart contracts to automate data sharing? A Yes to Q9a activates REQ-089 (the smart contract essential requirements of Data Act Article 36), which would otherwise not apply.

Q10 asks whether the actor intends to re-use data held by a public sector body. A Yes answer activates DGA Chapter II re-user obligations (REQ-012, REQ-013, REQ-014, and Cluster 4 re-user confidentiality obligations). Q11 asks whether the actor supplies data for AI development or develops AI systems using held data. A Yes answer activates Cluster 8 (AI Data Governance). Q11 also connects to Section 4 – if Q11=Yes, Q16 in Section 4 will ask whether the AI system is high-risk, which determines whether AI Act Article 10 applies in full. Q12 asks whether the actor operates or intends to register as a data intermediary. A Yes answer

activates the full Cluster 6 (Data Space and Intermediary Governance) framework including the DGA Chapter III notification and Article 12 conditions. Q13 asks whether the actor seeks data altruism registration, activating REQ-125 (the altruism registration conditions). Q14 asks whether the actor has received or expects a B2G exceptional need request, activating the relevant Cluster 1 and Cluster 4 obligations.

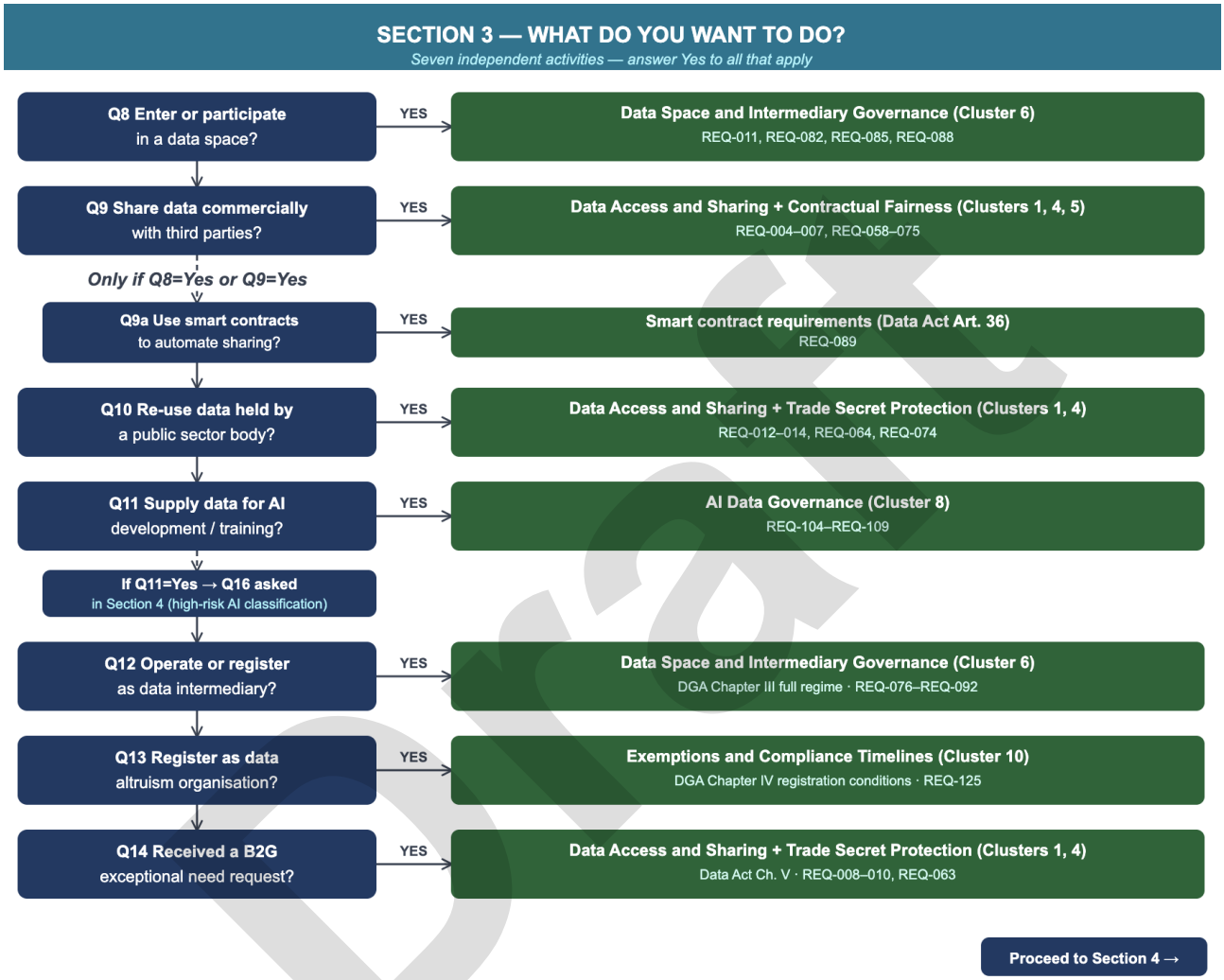

Figure 4. Section 3 of the Logical Decision Tree Model

5.5 SECTION 4: ADDITIONAL CONTEXT

Section 4, illustrated in Figure 5, captures four cross-cutting contextual factors that activate specific obligations regardless of the actor's primary role or activities. These questions are asked of all actors. Q15a asks whether the actor transfers or intends to transfer personal data to a recipient located outside the EU or EEA, or uses processors or sub-processors established outside the EU or EEA to process personal data on its behalf. This question only appears if the actor answered Yes to Q4 (personal data). A Yes answer activates the GDPR Chapter V international transfer framework – adequacy decisions, standard contractual clauses, binding corporate rules, and derogations of last resort (REQ-093 to REQ-096, REQ-099).

Q15b asks whether the actor stores, processes, or makes available non-personal data using infrastructure or service providers that are subject to the laws, regulations, or binding judicial or administrative orders of a non-EU country. This question is asked of all actors regardless of their answer to Q4, and is answered

independently of Q15a. A Yes answer activates the Data Act Articles 27 to 32 and DGA Article 31 framework – the obligation to take all reasonable technical, legal, and organisational measures to prevent unlawful third-country governmental access to non-personal data held in the Union, and the conditions and procedures for responding to any lawful access request (REQ-097 to REQ-103). Where the actor has received or anticipates a specific governmental access request, Q18 should also be answered Yes.

Q17 asks whether the purpose for which data is processed or intended to be used is scientific research, statistical, archiving in the public interest, or historical research. A Yes answer activates the GDPR Article 89 research derogations (REQ-052 to REQ-053), which permit certain departures from the data minimisation, storage limitation, and data subject rights provisions subject to appropriate safeguards. Q18 asks whether the actor has received or anticipates a request from a government authority of a non-EU country requiring access to or transfer of held data. A Yes answer activates REQ-097 to REQ-101– the prohibition on compliance with unlawful third-country access requests and the conditions and procedures for lawful compliance.

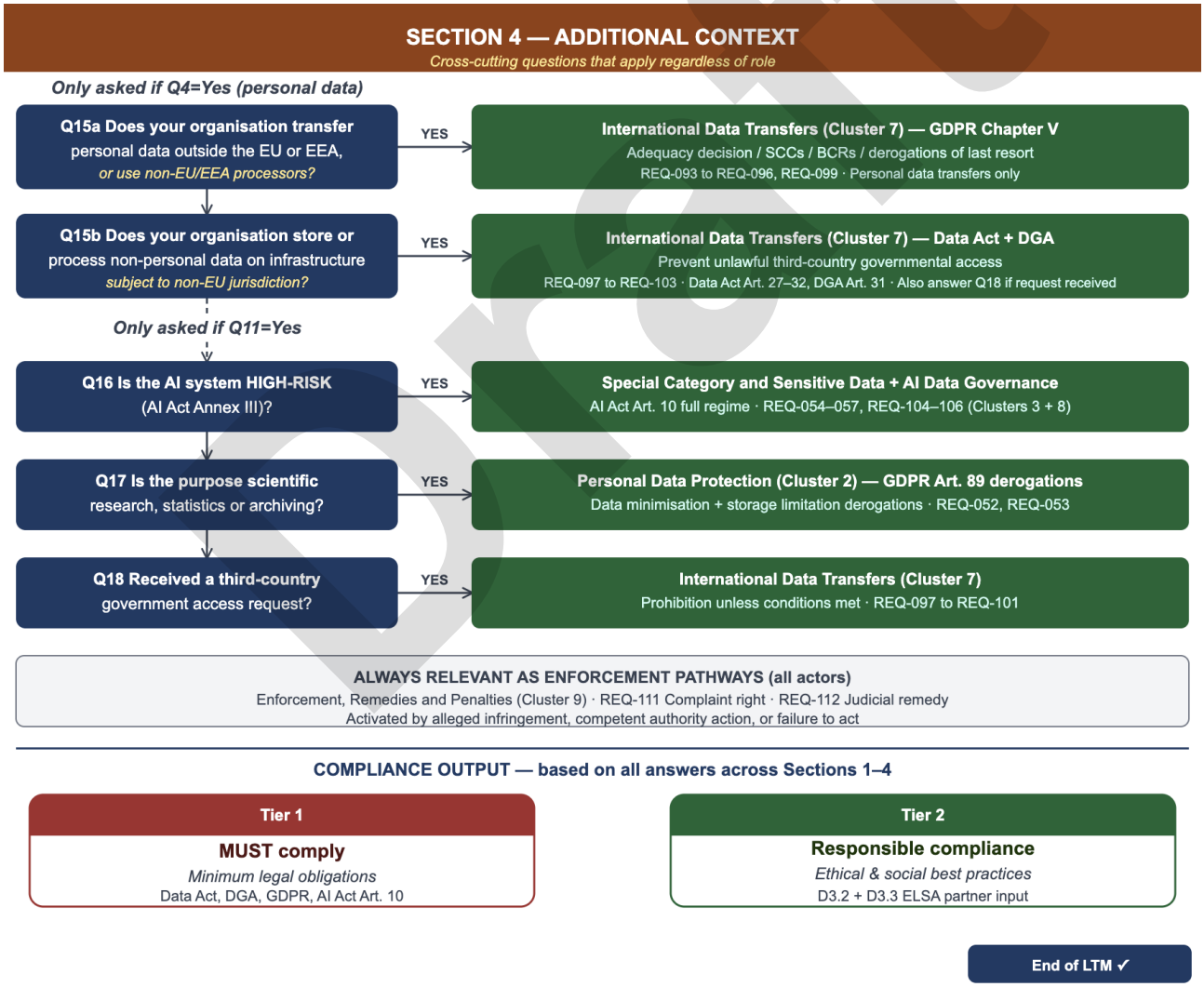

Figure 5. Section 4 of the Logical Decision Tree Model

6 COMPLIANCE TIERS

The two-tier compliance output structure, as explained in Table 3, is the mechanism through which D3.4 translates the consolidated requirements database into actionable guidance. This section describes the design and content of each tier and the ELSA partner inputs from D3.2 and D3.3.

Table 3.Compliance output tiers – structure and content

Tier	Label	Content	Basis
Tier 1	**MUST Comply (Minimum Legal Obligations)**	Minimum legal obligations derived from the four instruments. Non-compliance carries risk of penalties, enforcement action, or inability to operate within the EU data ecosystem.	Data Act, DGA, GDPR, AI Act Art. 10. Extracted from 128 unified requirements across 10 clusters.
Tier 2	**Responsible Compliance (Ethical & Social Best Practices)**	Best practices beyond the legal minimum, integrating ethical requirements from D3.2 and social requirements from D3.3. Recommended for organisations seeking to build trust, demonstrate responsible data stewardship, and position themselves as credible actors in EU data spaces.	ELSA partners input (D3.2 and D3.3). Living layer – to be enriched as additional partner inputs are received and pilot testing is completed.

6.1 TIER 1: MINIMUM LEGAL OBLIGATIONS (MUST COMPLY)

Tier 1 contains the minimum legal obligations that an actor must meet to operate lawfully within the EU data ecosystem. These requirements are derived directly from the four legislative instruments in scope and are presented in the LDTM output as mandatory obligations that carry legal consequences if breached.

The primary legal consequences for non-compliance vary by instrument and obligation type. Under the Data Act, penalties must be effective, proportionate and dissuasive (REQ-116). Under the DGA, penalties apply to infringements of the notification obligation, the international transfer prohibition, and the altruism organisation conditions (REQ-117). Under the GDPR, two administrative fine tiers apply: up to EUR 10 million or 2% of global annual turnover for infringements of Articles 8, 11, 25 to 39, and 42 to 43; and up to EUR 20 million or 4% of global annual turnover for infringements of the core principles, lawful basis requirements, data subject rights, and international transfer rules (REQ-118). In addition to administrative penalties, any person who has suffered material or non-material damage as a result of a GDPR infringement has the right to receive compensation from the controller or processor (REQ-115).

Tier 1 obligations are not uniformly applicable to all actors. The trigger mapping in the consolidated database ensures that each actor's Tier 1 output contains only the requirements that apply to their specific combination of role, data type, and intended activities. A micro or small enterprise that qualifies for the SME exemption will see Cluster 1 obligations marked as not applicable in their output (REQ-121 gate). A DGA-only actor will not see Data Act penalty provisions in their Tier 1 output. An actor not processing personal data will not see any GDPR obligations.

6.2 TIER 2: RESPONSIBLE COMPLIANCE (ETHICAL & SOCIAL BEST PRACTICES)

Tier 2 presents best practices that go beyond the legal minimum and represent responsible data stewardship. It integrates two types of content: ethical best practices derived from the D3.2 ethical requirements framework, and social best practices derived from the D3.3.

The Tier 2 content was designed to answer a specific question that Tier 1 does not address: what should a responsible actor do, as distinct from what the law requires? This distinction matters for several reasons. First, many data governance challenges, particularly in health AI, children's data, and sensitive research contexts, are not fully addressed by existing law. The GDPR sets a floor of personal data protection but does not specify the positive governance practices that build trust. Second, organisations that seek to operate in EU data spaces or to partner with public sector bodies are increasingly expected to demonstrate responsible data stewardship beyond mere legal compliance. Tier 2 provides the framework for that demonstration.

At the time of D3.4 submission (June 2026), the Tier 2 content incorporates the ELSA partner inputs received from D3.2 and D3.3. The Tier 2 layer is framed as a living component of the compliance output – it will be enriched as further partner inputs are received and as the guidelines are tested against the CERTAIN pilots. All the updates will be incorporated in the Multidisciplinary Guidelines – the planned output of D3.5 of the CERTAIN Project. The tool architecture supports this incremental enrichment: Tier 2 content is stored in dedicated columns in the consolidated database and can be added, updated, and re-weighted without affecting the Tier 1 legal output. An abridged version of this table can be found in Appendix B.

7 CHALLENGES, LIMITATIONS AND NEXT STEPS

This section reflects on the challenges encountered in developing D3.4, the limitations of the current deliverable, and the planned next steps for testing and development. It also addresses the potential impact of the Digital Omnibus proposal on the guidelines and the LDTM, and situates D3.4 within the broader research agenda of the CERTAIN project.

7.1 CHALLENGES IN THE DEVELOPMENT OF D3.4

The primary methodological challenge in developing D3.4 was the cross-instrument harmonisation work at Stage 2. The four instruments covered by D3.4 were developed at different points in the EU's digital agenda, by different Commission directorates, and with different primary objectives. The result is a regulatory landscape that is not designed to be read as a system. Provisions that are substantively equivalent appear in different structural positions across instruments. Operative legal terms – such as "effective, proportionate and dissuasive" for penalties, or "appropriate technical and organisational measures" for security – appear across all four instruments but with subtly different scopes and consequences. Resolving these instances of regulatory friction to produce a coherent, non-redundant database required judgment calls that are documented in the Overlap Notes and Overlap Flag columns of the consolidated database but remain subject to interpretive debate.

A second challenge was the scope decision to include Article 10 of the AI Act while excluding the broader AI Act framework. This decision was justified by D3.4's focus on data holders – Article 10 is the provision most directly relevant to the data holder's role in supplying or preparing training data. However, the boundary is not always clean. AI Act obligations for high-risk AI system providers include technical documentation requirements (Article 11), transparency obligations (Article 13), and conformity assessment procedures (Articles 43 to 45) that interact with data quality and governance. These provisions are not covered in D3.4, but will be fully addressed in continuous work in D3.5.

7.2 LIMITATIONS OF THE CURRENT DELIVERABLE

D3.4 is delivered as a documentation deliverable: a report, a requirements database, and a documented LDTM artefact. An interactive compliance tool that operationalises the LDTM for end users has not been built at the time of submission. This is an acknowledged limitation but not an unexpected one – the D3.4 timeline was designed to produce the design specification for the D3.5 tool, not the tool itself. Such a tool (or tools, in all likelihood) will be developed in the context of Pilot 5, which involves testing the guidelines against real-world compliance situations, evaluating whether the LDTM output accurately reflects the obligations, and providing the empirical feedback needed to refine the model before and during tool development. The interactive compliance tool, or tools, that operationalise the LDTM for end users will be developed in the context of this pilot and will also be presented and considered in the development of D3.5, though a fully functional tool is not a specific requirement for that deliverable either. Realistically, these guidelines are difficult to operationalise and demonstrate without even a simple Graphical User Interface (GUI) tool and report generator; therefore, it will be considered necessary to include for D3.5.

The consolidated requirements database represents a snapshot of the law as of mid-2026. EU data law is a living framework – the Digital Omnibus proposal would, if adopted, significantly change several clusters of requirements. The DGA transitional deadline has already passed, creating compliance obligations that some data intermediaries may not yet have met. The Data Act's product design obligation applies to products placed

on the market from September 2026. These timelines are captured in Cluster 10 but will need to be updated as they pass and as new legal developments occur.

The LDTM question set currently covers 28 questions. A gap analysis conducted during development identified and corrected six coverage issues. However, it cannot be excluded that further gaps exist – particularly for edge cases involving unusual combinations of actor types and data categories. The pilot testing planned for the guidelines is essential to validate the completeness and accuracy of the model against real-world compliance scenarios.

The scope limitation to four instruments means that sector-specific obligations are not captured. An organisation operating in the health data space is subject to the European Health Data Space Regulation in addition to the instruments covered. A financial institution is subject to sector-specific data and AI requirements under MiFID (Markets in Financial Instruments Directive), the AI-specific provisions of the Digital Finance Package, and related frameworks. D3.4 notes these additional layers where they are most salient but does not provide comprehensive coverage. Sector-specific extensions are identified as a priority for future development.

7.3 THE DIGITAL OMNIBUS AND THE UPDATABILITY OF THE LDTM

The Digital Omnibus proposal, if adopted in its current form, would require significant updates to the LDTM and the consolidated requirements database. The most operationally significant changes for D3.4 actors are the transformation of the DGA Chapter III mandatory notification regime into a voluntary label system, the replacement of the legal separation obligation with functional separation, the introduction of the Article 9(2)(k) AI training exception for special category data, and the introduction of the small mid-cap category. Each of these changes would require adding new question branches, revising requirement texts, and updating the trigger mapping column.

The LDTM architecture was deliberately designed to support these updates without rebuilding from scratch. The modular four-section structure means that new questions can be added to any section without disrupting the others. The trigger mapping column provides the link between questions and requirements in a format that can be updated requirement-by-requirement. The Related Consolidated REQs column enables new requirements to be integrated into the existing cross-reference network. The two-tier output structure means that new requirements can be classified at Tier 1 (mandatory) or Tier 2 (best practice) at the point of insertion.

Work on a Digital Omnibus impact assessment for the D3.4 guidelines began in advance of D3.4 submission and was developed in connection with CERTAIN's participation in Data Week Oslo in May 2026, where the guidelines and their interaction with the Omnibus proposal were presented to an audience of data governance practitioners and policy stakeholders. The Data Week presentation illustrated the compliance pathway for two different personas (using the developed LDTM) under the current law and the changes the Omnibus could introduce for them.

The feedback received from practitioners at the event confirmed both the practical relevance of the guidelines and the salience of the Omnibus as a concern for organisations currently planning their data governance structures. This work is documented and will continue as the Omnibus progresses through the ordinary legislative procedure. Any changes to the EU's AI and data legal landscape will continue to be monitored and incorporated in the future deliverables.

7.4 TESTING WITH CERTAIN USE CASES

The planned testing of the D3.4 guidelines against the CERTAIN use cases is a critical next step. The purpose of this testing is to move the guidelines from a theoretically complete artefact to an empirically validated compliance instrument – one that has been demonstrated to produce accurate, useful, and proportionate outputs for the real-world actors it is designed to serve.

The testing will be conducted under Pilot 5 of the CERTAIN project, which is dedicated specifically to evaluating the guidelines for data holders seeking to enter the AI data market. Pilot 5 is led by the University of Tartu in its role as guideline designer and involves three evaluation partners operating in distinct sectors and data contexts: INCOM Ltd., providing HR data including CVs and recruitment data; EMPOWER, operating in the energy sector with user consumption and behaviour data; and NVISION, working with connected device and IoT data. These three partner organisations represent meaningfully different compliance profiles, and their diversity is itself a design feature of the testing methodology. A set of guidelines that works only for one sector or one data type is not a general-purpose compliance instrument. Additionally, two data-holding stakeholders from outside the CERTAIN consortium will be recruited to pilot the guidelines as well.

The testing methodology planned for Pilot 5 involves each evaluation partner running their specific use case through the LDTM question set and evaluating whether the compliance output they receive accurately reflects their actual obligations and governance needs. For each use case, the evaluation will assess two dimensions. First, accuracy: does the Tier 1 output correctly identify the legal obligations that apply to that partner's situation, and does it exclude obligations that do not apply? Discrepancies (whether over-inclusion of irrelevant requirements or under-inclusion of applicable ones) will be used to identify gaps or inaccuracies in the trigger mapping or requirement texts in the consolidated database, and the LDTM will be updated accordingly. Second, usefulness: does the Tier 2 output provide best practices that are relevant, actionable, and proportionate to the partner's operational context? Partners will be asked to evaluate this through expert interviews and pre/post questionnaires, assessing whether the guidelines reduce their perceived compliance burden and increase their confidence in participating in EU data markets.

The value proposition that Pilot 5 is designed to validate is precisely the value proposition of D3.4 as a whole: that a well-designed compliance tool can reduce the compliance burden for organisations that would like to participate in EU data markets but currently cannot do so profitably or confidently due to the complexity of overlapping regulatory obligations.

8 CONCLUSIONS

D3.4 sets out to answer a practical question: what does EU data law actually require from an organisation that generates, holds, shares, or processes data in the EU data ecosystem, and what should a responsible actor do beyond the minimum? The answer, as this deliverable demonstrates, is neither simple nor static. Four legislative instruments in force, each with its own addressees, conditions, timelines, and exceptions, impose a compliance landscape that is genuinely complex even for legally sophisticated organisations, let alone for the data holder entering the AI market for the first time or the SME operating a connected device platform without dedicated legal counsel.

D3.4 responds to that complexity with three concrete contributions. The consolidated requirements database of 128 unified rows across ten thematic clusters translates 198 extracted legal provisions into a structured, cross-referenced, machine-readable artefact that does not currently exist in this form for the combination of instruments covered. The Logical Decision Tree Model translates that database into a navigable compliance instrument – questions that any actor can answer to receive a tailored output identifying their Tier 1 legal obligations and Tier 2 responsible compliance best practices.

Also, it is important to note that D3.4 does not aim to provide legal advice. It does not replace the judgment of a qualified practitioner in complex or borderline situations. It does not cover every instrument that may apply to a specific sector or actor type. And it does not yet exist as an interactive tool. What it provides is the methodological foundation, the validated knowledge base, and the design specification from which that tool can be built with confidence.

The deliverable is submitted at a moment of genuine regulatory uncertainty. The Digital Omnibus proposal, if adopted, would change some of the most operationally significant requirements in the model. However, it is important to clarify that adoption of the Digital Omnibus would not invalidate D3.4 or affect the CERTAIN project's activities and timeline. D3.4 documents the regulatory framework as it stands at the time of submission, which is the appropriate scope for a deliverable of this nature, and the CERTAIN pilot activities in Pilot 5 will be conducted on the basis of the law currently in force. The Omnibus remains in the ordinary legislative procedure and, even if adopted, would not enter into application until after a transitional period that extends beyond the CERTAIN project timeline. What adoption would trigger is an update cycle for the LDTM, and this is precisely why the model was built to be updated: modular, trigger-mapped, and open to new questions and new rows, so that legislative changes can be incorporated without rebuilding the model from scratch. D3.4 is not a fixed product. It is a living framework, and its value will grow as it is further validated against the CERTAIN use cases and updated to reflect the evolving regulatory landscape.

APPENDIX A: ABRIDGED CONSOLIDATED LEGAL REQUIREMENTS

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-001	DA-001	Data Act	Art. 3(1)	Connected products must be designed so that product data and related metadata are by default easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format, and directly accessible to the user	**1 — Data Access and Sharing Obligations**	Manufacturer / Connected Product Provider	When placing a connected product on the market	Microenterprises and small enterprises (Art. 7(1))
REQ-002	DA-004	Data Act	Art. 4(1)	The data holder must make readily available data and relevant metadata accessible without undue delay, free of charge, in a comprehensive, structured, commonly used and machine-readable format, of the same quality as available to the data holder, and where technically feasible, continuously and in real-time	**1 — Data Access and Sharing Obligations**	Data Holder	When data cannot be directly accessed by the user from the connected product or related service and the user submits a request	Microenterprises and small enterprises (Art. 7(1))
REQ-003	DA-004b	Data Act	Art. 4(2)	Users and data holders may contractually restrict or prohibit data access, use or further sharing where processing poses a serious security risk. Where the data holder refuses to share on this basis, it must notify the competent authority (Art. 37)	**1 — Data Access and Sharing Obligations**	Data Holder / User	When data sharing could undermine security requirements of the connected product under Union or national law, resulting in serious adverse effects on health, safety or security of persons	Microenterprises and small enterprises (Art. 7(1))

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-004	DA-014	Data Act	Art. 5(1)	The data holder must make readily available data and relevant metadata available to a third party without undue delay, free of charge to the user, of the same quality as available to the data holder, in a comprehensive, structured, commonly used and machine-readable format, and where technically feasible, continuously and in real-time	**1 — Data Access and Sharing Obligations**	Data Holder	Upon user request to share data with a third party	Microenterprises and small enterprises (Art. 7(1))
REQ-005	DA-024	Data Act	Art. 8(1)	The data holder must agree with the data recipient on arrangements for making data available under fair, reasonable and non-discriminatory (FRAND) terms and in a transparent manner	**1 — Data Access and Sharing Obligations**	Data Holder	When a legal obligation to share data with a data recipient exists in B2B relations	
REQ-006	DA-026	Data Act	Art. 8(3)	A data holder must not discriminate between comparable categories of data recipients regarding data sharing arrangements. Upon reasoned request from a data recipient who suspects discrimination, the data holder must without undue delay provide information demonstrating absence of discrimination	**1 — Data Access and Sharing Obligations**	Data Holder	When making data available to multiple data recipients	
REQ-007	DA-027	Data Act	Art. 8(4)	A data holder must not make data available to a data recipient on an exclusive basis unless requested to do so by the user under Chapter II	**1 — Data Access and Sharing Obligations**	Data Holder	When considering exclusive data sharing arrangements with a data recipient	
REQ-008	DA-044	Data Act	Art. 14	Data holders that are legal persons must make the requested data including relevant metadata available without undue delay	**1 — Data Access and Sharing Obligations**	Data Holder (legal persons, non-public sector)	When a duly reasoned request demonstrating exceptional need as defined in Art. 15 is received from a public sector body, the Commission, the ECB or a Union body	Microenterprises and small enterprises exempt from Art. 15(1)(b) non-emergency requests

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-009	DA-049	Data Act	Art. 18(1)	The data holder must make the data available without undue delay, taking into account necessary technical, organisational and legal measures	**1 — Data Access and Sharing Obligations**	Data Holder	When a valid exceptional need request is received from a public sector body under Art. 14	
REQ-010	DA-050	Data Act	Art. 18(2)	The data holder may decline or seek modification of a request within 5 working days for public emergency requests or 30 working days for other exceptional need requests	**1 — Data Access and Sharing Obligations**	Data Holder	When the data holder has valid grounds to decline or modify: the data holder does not control the requested data; a similar request for the same purpose was previously submitted and data not yet erased; or the request does not meet the conditions of Art. 17(1) and (2)	
REQ-011	DA-065	Data Act	Art. 33(1)	Data holders and data service providers participating in data spaces must comply with essential interoperability requirements: datasets must be sufficiently described including content, use restrictions, licences, collection methodology, quality and uncertainty in machine-readable format; data structures, formats, vocabularies and classification schemes must be described in a publicly available and consistent manner; technical means of access including APIs and their terms of use must be sufficiently described to enable automatic access and transmission; and where applicable, means to enable interoperability of tools for automating data sharing agreements including smart contracts must be provided	**1 — Data Access and Sharing Obligations**	Data Holder / Data Service Provider participating in a data space	When participating in a data space and offering data or data services to other participants	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-012	DGA-002	DGA	Art. 4(1)	Agreements or practices granting exclusive rights to re-use data held by public sector bodies, or having the effect of restricting availability of such data for re-use by others, are prohibited	**1 — Data Access and Sharing Obligations**	Public Sector Body	When granting or entering into agreements for re-use of protected public sector data	Exclusive rights granted for provision of general interest services where otherwise impossible, subject to conditions of Arts. 4(2-5)
REQ-013	DGA-004; DGA-005	DGA	Art. 5(1); Art. 5(2)	Public sector bodies must make publicly available the conditions for re-use and the procedure to request re-use via the single information point. Conditions for re-use must be non-discriminatory, transparent, proportionate and objectively justified. Conditions must not restrict competition	**1 — Data Access and Sharing Obligations**	Public Sector Body	When granting or refusing access for re-use of protected data categories	
REQ-014	DGA-015	DGA	Art. 9(1)	Competent public sector bodies must adopt a decision on a re-use request within two months of receipt, extendable by up to 30 days for exceptionally extensive or complex requests, with notification to the applicant of the delay and reasons	**1 — Data Access and Sharing Obligations**	Public Sector Body	When receiving a request for re-use of protected data categories	
REQ-015	GDPR-023	GDPR	Art. 20(1-2)	The data subject has the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format and to transmit it to another controller without hindrance, where processing is based on consent or contract and is carried out by automated means. The data subject has the right to have the data transmitted directly from one controller to another where technically feasible	**1 — Data Access and Sharing Obligations**	Controller (Data Holder)	When a data subject submits a data portability request and processing is based on consent or contract and carried out by automated means	Does not apply to processing for public interest tasks or exercise of official authority; must not adversely affect rights and freedoms of others

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-016	GDPR-001	GDPR	Art. 5(1)(a)	Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject	**2 — Personal Data Protection**	Controller (Data Holder)	When processing any personal data	
REQ-017	GDPR-002	GDPR	Art. 5(1)(b)	Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes	**2 — Personal Data Protection**	Controller (Data Holder)	When collecting personal data and when considering further processing or sharing	Further processing for archiving, scientific research, historical research or statistical purposes is not incompatible with original purposes subject to Art. 89(1) safeguards
REQ-018	GDPR-003	GDPR	Art. 5(1)(c)	Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	**2 — Personal Data Protection**	Controller (Data Holder)	When determining what personal data to collect or share	
REQ-019	GDPR-004	GDPR	Art. 5(1)(d)	Personal data must be accurate and where necessary kept up to date. Every reasonable step must be taken to ensure inaccurate personal data is erased or rectified without delay	**2 — Personal Data Protection**	Controller (Data Holder)	When storing or sharing personal data	
REQ-020	GDPR-005	GDPR	Art. 5(1)(e)	Personal data must be kept in a form permitting identification of data subjects for no longer than necessary for the purposes for which it is processed	**2 — Personal Data Protection**	Controller (Data Holder)	When storing personal data	Personal data may be kept longer for archiving, scientific research, historical research or statistical purposes subject to Art. 89(1) safeguards

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-021	GDPR-006	GDPR	Art. 5(1)(f)	Personal data must be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	**2 — Personal Data Protection**	Controller (Data Holder)	When processing personal data in any context including data sharing	
REQ-022	GDPR-007	GDPR	Art. 5(2)	The controller must be responsible for and able to demonstrate compliance with the data processing principles in Art. 5(1)	**2 — Personal Data Protection**	Controller (Data Holder)	When processing any personal data	
REQ-023	GDPR-008	GDPR	Art. 6(1)	Processing of personal data is lawful only if at least one of the following applies: consent of the data subject; necessity for contract performance; compliance with a legal obligation; protection of vital interests; performance of a public interest task; or legitimate interests of the controller or third party not overridden by data subject rights	**2 — Personal Data Protection**	Controller (Data Holder)	Before processing any personal data	Legitimate interests basis does not apply to processing by public authorities in performance of their tasks
REQ-024	GDPR-009	GDPR	Art. 6(4)	Where processing for a purpose other than the original collection purpose is not based on consent or Union/Member State law, the controller must assess compatibility by considering: link between original and new purposes; context of collection; nature of data especially special categories; possible consequences for data subjects; and existence of appropriate safeguards including encryption or pseudonymisation	**2 — Personal Data Protection**	Controller (Data Holder)	When considering processing personal data for a purpose different from that for which it was originally collected	Processing based on consent or Union/Member State law does not require compatibility assessment

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-025	GDPR-010; GDPR-011	GDPR	Art. 7(1); Art. 7(3)	Where processing is based on consent the controller must be able to demonstrate that the data subject has consented. The data subject has the right to withdraw consent at any time. Withdrawal must be as easy as giving consent. The controller must inform data subjects of this right before consent is given	**2 — Personal Data Protection**	Controller (Data Holder)	When relying on consent as the lawful basis for processing personal data	
REQ-026	GDPR-016	GDPR	Art. 11(1-2)	Where the purposes of processing do not or no longer require identification of a data subject, the controller is not obliged to maintain, acquire or process additional information to identify the data subject solely for GDPR compliance purposes. Where the controller cannot identify the data subject it must inform them accordingly where possible, and Arts. 15-20 do not apply	**2 — Personal Data Protection**	Controller (Data Holder)	When processing data where identification of individual data subjects is not required for the processing purpose	
REQ-027	GDPR-017	GDPR	Art. 12(1-4)	The controller must provide information and communications relating to data subject rights in a concise, transparent, intelligible and easily accessible form using clear and plain language, in particular for information addressed to children. The controller must respond to data subject requests without undue delay and within one month, extendable by two further months for complex requests	**2 — Personal Data Protection**	Controller (Data Holder)	When communicating with data subjects about their personal data or responding to data subject rights requests	Controller may charge reasonable fee or refuse manifestly unfounded or excessive requests bearing burden of proof
REQ-028	GDPR-018	GDPR	Art. 13(1-3)	Where personal data are collected directly from the data subject, the controller must provide at the time of collection: controller identity and contact details; DPO contact details where applicable; purposes and legal basis for processing; legitimate interests where applicable; recipients or categories of recipients; intended third	**2 — Personal Data Protection**	Controller (Data Holder)	When collecting personal data directly from data subjects	Where the data subject already has the information

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				country transfers with applicable safeguards; retention period; data subject rights; right to withdraw consent; right to lodge complaint; whether provision is statutory or contractual; and existence of automated decision-making. Where further processing for a different purpose is intended, the data subject must be informed prior to that processing				
REQ-029	GDPR-019	GDPR	Art. 14(1-4)	Where personal data have not been obtained directly from the data subject, the controller must provide within one month: controller identity and contact details; DPO contact details where applicable; purposes and legal basis; categories of personal data; recipients or categories of recipients; intended third country transfers; retention period; data subject rights; right to withdraw consent; right to lodge complaint; source of data; and existence of automated decision-making. Where further processing for a different purpose is intended, the data subject must be informed prior	**2 — Personal Data Protection**	Controller (Data Holder)	When processing personal data not collected directly from the data subject	Where data subject already has information; where provision would be impossible or disproportionate for archiving/research/statistical purposes subject to Art. 89(1); where obtaining or disclosure is laid down by law; where data must remain confidential under professional secrecy
REQ-030	GDPR-020	GDPR	Art. 15(1-3)	The data subject has the right to obtain confirmation of whether personal data concerning them is being processed and where so, access to the personal data and information about: purposes; categories of data; recipients including in third countries; retention period; data subject rights; right to lodge a complaint; source of data where not collected from the data subject; and existence of automated decision-making. The controller must provide a copy of the personal data undergoing processing free of charge in a	**2 — Personal Data Protection**	Controller (Data Holder)	When a data subject submits an access request	Right to copy shall not adversely affect rights and freedoms of others

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				commonly used electronic form where requested electronically				
REQ-031	GDPR-021	GDPR	Art. 17(1-2)	The data subject has the right to erasure of personal data without undue delay and the controller has an obligation to erase where: data is no longer necessary for the purposes collected; consent is withdrawn and no other legal ground exists; data subject objects and no overriding legitimate grounds exist; data has been unlawfully processed; erasure is required by Union or Member State law; or data was collected in relation to information society services to a child. Where the controller has made the data public it must take reasonable steps to inform other controllers processing the data of the erasure request	**2 — Personal Data Protection**	Controller (Data Holder)	When a data subject submits an erasure request on one of the listed grounds	Processing necessary for: freedom of expression; legal obligation or public interest task; public health reasons under Art. 9(2)(h)(i); archiving/research/statistical purposes under Art. 89(1); or establishment, exercise or defence of legal claims
REQ-032	GDPR-022	GDPR	Art. 19	The controller must communicate any rectification, erasure or restriction of processing to each recipient to whom the personal data have been disclosed unless this proves impossible or involves disproportionate effort. The controller must inform the data subject about those recipients if requested	**2 — Personal Data Protection**	Controller (Data Holder)	When rectification, erasure or restriction of processing has been carried out on personal data previously disclosed to recipients	Where notification is impossible or involves disproportionate effort
REQ-033	GDPR-024	GDPR	Art. 24(1-2)	The controller must implement appropriate technical and organisational measures to ensure and demonstrate that processing is performed in accordance with the GDPR, taking into account the nature, scope, context, purposes and risks of processing. These measures must be reviewed and updated	**2 — Personal Data Protection**	Controller (Data Holder)	When processing any personal data	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				where necessary and shall include appropriate data protection policies where proportionate				
REQ-034	GDPR-025	GDPR	Art. 25(1-2)	The controller must implement appropriate technical and organisational measures — such as pseudonymisation — designed to implement data protection principles including data minimisation in an effective manner, both at the time of determining processing means and at the time of processing itself. By default only personal data necessary for each specific purpose must be processed. Personal data must not by default be made accessible to an indefinite number of persons without individual intervention	**2 — Personal Data Protection**	Controller (Data Holder)	When determining the means of processing and when processing personal data	
REQ-035	GDPR-029	GDPR	Art. 30(1)	Each controller must maintain a written record of processing activities containing: controller identity and contact details; purposes of processing; categories of data subjects and personal data; categories of recipients including in third countries; third country transfers with applicable safeguards; envisaged erasure time limits where possible; and a general description of technical and organisational security measures	**2 — Personal Data Protection**	Controller (Data Holder)	When processing personal data as a controller	Enterprises or organisations with fewer than 250 employees unless processing is likely to result in risk to data subject rights, is not occasional, or involves special category or criminal conviction data
REQ-036	DA-011	Data Act	Art. 4(12)	Personal data may only be made available to the user where there is a valid legal basis under GDPR Art. 6, and where relevant Art. 9 and ePrivacy Directive Art. 5(3) are satisfied	**2 — Personal Data Protection**	Data Holder	When the user is not the data subject and the requested data contains personal data of third parties	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-037	DA-017	Data Act	Art. 5(7)	Personal data may only be made available to the third party where there is a valid legal basis under GDPR Art. 6, and where relevant Art. 9 and ePrivacy Directive Art. 5(3) are satisfied	**2 — Personal Data Protection**	Data Holder	When the user is not the data subject and data to be shared with a third party contains personal data	
REQ-038	DA-051	Data Act	Art. 18(4)	The data holder must anonymise the data unless disclosure of personal data is strictly necessary, in which case the data holder must pseudonymise the data	**2 — Personal Data Protection**	Data Holder	When an exceptional need request includes personal data	
REQ-039	DA-085	Data Act	Art. 37(3)	GDPR supervisory authorities are responsible for monitoring the application of the Data Act insofar as personal data protection is concerned	**2 — Personal Data Protection**	Data Holder / Data Recipient / Data Processing Service Provider	When processing of personal data is involved in the context of Data Act obligations	
REQ-040	DGA-031	DGA	Art. 12(m-n)	Where providing services to data subjects, the data intermediation services provider must act in data subjects best interest, informing and advising them in a concise, transparent and accessible manner about intended data uses and standard terms before consent is given. Where providing tools for obtaining consent or permissions, the provider must specify the third-country jurisdiction for data use and provide tools to give and withdraw consent or permissions	**2 — Personal Data Protection**	Data Intermediation Service Provider	When providing intermediation services involving personal data or consent mechanisms	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-041	DGA-039	DGA	Art. 21(1)	A recognised data altruism organisation must inform data subjects or data holders prior to any processing of their data in a clear and easily comprehensible manner of: the general interest objectives and specific purpose for which data will be processed; and the location and objectives of any processing carried out in a third country	**2 — Personal Data Protection**	Recognised Data Altruism Organisation	Before processing data provided by data subjects or data holders for altruistic purposes	
REQ-042	GDPR-012	GDPR	Art. 9(1)	Processing of special categories of personal data — including racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data for unique identification, health data, sex life or sexual orientation data — is prohibited	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When processing any data that falls within the listed special categories	All exceptions listed in Art. 9(2)
REQ-043	GDPR-013	GDPR	Art. 9(2)	The prohibition on processing special categories of personal data does not apply where one of the following applies: explicit consent; employment and social security law obligations; vital interests where consent impossible; not-for-profit body processing relating to members; data manifestly made public by data subject; legal claims; substantial public interest under Union or Member State law; preventive or occupational medicine; public health; or archiving, research or statistical purposes under Art. 89(1)	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When processing special category personal data and one of the listed exceptions applies	Each exception carries specific additional conditions
REQ-044	GDPR-014	GDPR	Art. 8(1-2)	Where processing is based on consent for information society services offered directly to a child, processing is lawful only where the child is at least 16 years old. For children below 16, consent must be given or authorised by the holder of parental responsibility. The controller must make reasonable efforts to verify that consent is given or authorised by	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When processing personal data of children under 16 based on consent in the context of information society services	Member States may lower the age threshold to a minimum of 13 years

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				the holder of parental responsibility taking into consideration available technology				
REQ-045	GDPR-015	GDPR	Art. 10	Processing of personal data relating to criminal convictions and offences or related security measures may only be carried out under the control of official authority or when authorised by Union or Member State law providing for appropriate safeguards. Any comprehensive register of criminal convictions must be kept only under the control of official authority	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When processing personal data relating to criminal convictions, offences or related security measures	Processing authorised by Union or Member State law with appropriate safeguards
REQ-046	GDPR-030	GDPR	Art. 32(1-2)	The controller and processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including as appropriate: pseudonymisation and encryption; ability to ensure ongoing confidentiality, integrity, availability and resilience of systems; ability to restore availability and access in a timely manner after incidents; and a process for regularly testing, assessing and evaluating the effectiveness of security measures	**3 — Special Category and Sensitive Data**	Controller / Processor (Data Holder / Data Space Operator)	When processing personal data — heightened obligation for special category data given elevated risk	
REQ-047	GDPR-031	GDPR	Art. 33(1-5)	In the case of a personal data breach the controller must notify the competent supervisory authority without undue delay and where feasible within 72 hours of becoming aware, unless the breach is unlikely to result in risk to data subject rights. The notification must describe: the nature of the breach including categories and approximate number of	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When a personal data breach occurs — heightened urgency for special category data given severity of potential harm	Where the breach is unlikely to result in risk to rights and freedoms of natural persons

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				data subjects and records affected; DPO or contact point details; likely consequences; and measures taken or proposed. The controller must document all personal data breaches				
REQ-048	GDPR-032	GDPR	Art. 34(1-2)	Where a personal data breach is likely to result in high risk to the rights and freedoms of natural persons the controller must communicate the breach to the data subject without undue delay in clear and plain language describing the nature of the breach, DPO contact details, likely consequences and measures taken	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When a personal data breach is likely to result in high risk to data subjects — special category data breaches are presumed high risk	Where appropriate technical protection measures render data unintelligible such as encryption; where subsequent measures ensure high risk is no longer likely; or where communication would involve disproportionate effort and public communication is used instead
REQ-049	GDPR-033	GDPR	Art. 35(1-3)	Where a type of processing using new technologies is likely to result in high risk to the rights and freedoms of natural persons the controller must carry out a Data Protection Impact Assessment prior to processing. A DPIA is required in particular for: systematic and extensive automated evaluation or profiling with legal or similarly significant effects; large-scale processing of special categories of personal data or criminal conviction data; and systematic large-scale monitoring of publicly accessible areas	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When processing is likely to result in high risk to data subjects, particularly when using new technologies, processing special category data at scale, or systematic profiling	A single DPIA may cover a set of similar high-risk processing operations
REQ-050	GDPR-034	GDPR	Art. 36(1)	Where a DPIA indicates that processing would result in high risk in the absence of controller mitigation measures the controller must consult the supervisory authority prior to processing	**3 — Special Category and Sensitive Data**	Controller (Data Holder)	When a DPIA under Art. 35 indicates high residual risk after mitigation measures	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-051	GDPR-035	GDPR	Art. 37(1)	The controller and processor must designate a Data Protection Officer where: processing is carried out by a public authority or body; the core activities require regular and systematic monitoring of data subjects on a large scale; or the core activities consist of large-scale processing of special categories of personal data or criminal conviction data	**3 — Special Category and Sensitive Data**	Controller / Processor (Data Holder / Data Space Operator)	When any of the three mandatory DPO designation conditions are met	
REQ-052	GDPR-049	GDPR	Art. 89(1-3)	Processing for archiving in the public interest, scientific or historical research or statistical purposes must be subject to appropriate safeguards including technical and organisational measures to ensure data minimisation. Pseudonymisation must be used where the purpose can be fulfilled in that manner. Where purposes can be fulfilled without identifying data subjects that approach must be used. Member State law may provide derogations from data subject rights under Arts. 15, 16, 18 and 21 for research and statistical purposes, and additionally from Arts. 19 and 20 for archiving purposes, where those rights would render the purposes impossible or seriously impair them	**3 — Special Category and Sensitive Data**	Controller (Data Holder) / Member States	When processing personal data for archiving in the public interest, scientific or historical research or statistical purposes	Derogations from data subject rights only available where those rights would render the research purpose impossible or seriously impair it
REQ-053	GDPR-048	GDPR	Art. 85(1-2)	Member States must reconcile the right to data protection with freedom of expression and information. For processing for journalistic, academic, artistic or literary expression purposes Member States may provide exemptions or derogations from the core GDPR chapters including principles, data subject rights, controller and processor obligations, and international transfer	**3 — Special Category and Sensitive Data**	Controller (Data Holder) / Member States	When processing is carried out for journalistic, academic, artistic or literary expression purposes	Exemptions must be necessary and proportionate to reconcile data protection with freedom of expression

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				rules where necessary to reconcile these rights				
REQ-054	AIA-001	AI Act	Art. 10(1)	High-risk AI systems using techniques involving training of AI models must be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in Art. 10(2-5)	**3 — Special Category and Sensitive Data**	Provider of High-risk AI System / Data Holder supplying training data	When a high-risk AI system uses techniques involving training of AI models with data	Non-high-risk AI systems; Art. 10(6) applies testing data requirements only to high-risk AI systems not using training techniques
REQ-055	AIA-002	AI Act	Art. 10(2)	Training, validation and testing data sets must be subject to appropriate data governance and management practices for the intended purpose, covering in particular: relevant design choices; data collection processes and origin including original purpose of personal data collection; data preparation operations such as annotation, labelling, cleaning, updating, enrichment and aggregation; assumptions about what the data measures and represents; assessment of availability, quantity and suitability of data sets; examination for possible biases affecting health and safety, fundamental rights or prohibited discrimination; appropriate measures to detect, prevent and mitigate identified biases; and identification of data gaps or shortcomings	**3 — Special Category and Sensitive Data**	Provider of High-risk AI System / Data Holder supplying training data	When developing a high-risk AI system using training data	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-056	AIA-003	AI Act	Art. 10(3-4)	Training, validation and testing data sets must be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose. They must have appropriate statistical properties regarding the persons or groups for whom the system is intended. Data sets must take into account characteristics particular to the specific geographical, contextual, behavioural or functional setting of intended use	**3 — Special Category and Sensitive Data**	Provider of High-risk AI System / Data Holder supplying training data	When preparing data sets for high-risk AI system development	
REQ-057	AIA-004	AI Act	Art. 10(5)	Where strictly necessary for bias detection and correction in high-risk AI systems, providers may exceptionally process special categories of personal data subject to: GDPR and other applicable data protection law; the bias correction cannot be achieved with other data including synthetic or anonymised data; technical limitations on re-use and state-of-the-art security and privacy-preserving measures including pseudonymisation; strict access controls and documentation; no transmission or transfer to other parties; deletion once bias is corrected or retention period ends; and documentation in records of processing of why special category processing was strictly necessary	**3 — Special Category and Sensitive Data**	Provider of High-risk AI System / Data Holder supplying training data	When special category personal data processing is strictly necessary for bias detection and correction in a high-risk AI system and no alternative data including synthetic or anonymised data can achieve the same purpose	
REQ-058	DA-007; DA-018	Data Act	Art. 4(6); Art. 5(9)	The data holder or trade secret holder must identify trade secret data including in metadata, and agree with the user or third party on proportionate technical and organisational measures to preserve confidentiality such as contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct. Trade	**4 — Trade Secret and Confidentiality Protection**	Data Holder / Trade Secret Holder	When data to be shared with a user or third party contains trade secrets	Microenterprises and small enterprises (Art. 7(1))

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				secrets may only be disclosed to the extent strictly necessary to fulfil the agreed purpose				
REQ-059	DA-008; DA-019	Data Act	Art. 4(7); Art. 5(10-11)	The data holder may withhold or suspend data sharing where no agreement on confidentiality measures is reached, or where the user or third party fails to implement agreed measures. The decision must be substantiated in writing without undue delay and the competent authority must be notified. In exceptional circumstances where disclosure would likely cause serious economic damage despite agreed measures, the data holder may refuse access on a case-by-case basis. Refusal must be substantiated in writing based on objective elements and the competent authority must be notified	**4 — Trade Secret and Confidentiality Protection**	Data Holder	When no agreement on confidentiality measures is reached, when agreed measures are not implemented, or when disclosure would likely cause serious economic damage in exceptional circumstances	Microenterprises and small enterprises (Art. 7(1))
REQ-060	DA-029	Data Act	Art. 8(6)	A data sharing obligation does not require the data holder to disclose trade secrets unless specifically provided for under Union or national law	**4 — Trade Secret and Confidentiality Protection**	Data Holder	When a data sharing obligation exists and the data to be shared contains trade secrets	
REQ-061	DA-035	Data Act	Art. 11(1)	A data holder may apply appropriate technical protection measures including smart contracts and encryption to prevent unauthorised access to data and ensure compliance with Arts. 4, 5, 6, 8 and 9 and contractual terms. Such measures must not discriminate between data recipients or hinder user rights to access or share data	**4 — Trade Secret and Confidentiality Protection**	Data Holder	When implementing technical measures to protect data including trade secrets	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-062	DA-036; DA-037	Data Act	Art. 11(2-3); Art. 11(4)	The data holder may require the offending party to: erase data and all copies, cease production of goods or services derived from that data, inform the user of the breach, and compensate the harmed party. This applies where a third party, data recipient or user has obtained data through deception or coercion, used data for unauthorised purposes, unlawfully disclosed data, failed to maintain agreed technical measures, or altered protection measures without agreement	**4 — Trade Secret and Confidentiality Protection**	Data Holder	When a third party, data recipient or user has misused or unlawfully accessed data — including trade secret violations	
REQ-063	DA-054	Data Act	Art. 19(3)	Trade secrets may only be disclosed to the extent strictly necessary for the purpose of the exceptional need request. The data holder or trade secret holder must identify trade secret data including in metadata. The receiving public sector body must implement all necessary technical and organisational measures to preserve confidentiality of trade secrets prior to disclosure	**4 — Trade Secret and Confidentiality Protection**	Data Holder / Public Sector Body / Commission / ECB / Union Body	When an exceptional need request involves data containing trade secrets	
REQ-064	DGA-008	DGA	Art. 5(5)	Re-users must adhere to a confidentiality obligation prohibiting disclosure of any information that jeopardises the rights and interests of third parties obtained through re-use. Re-users must not re-identify any data subject and must implement technical and operational measures to prevent re-identification. Re-users must notify any data breach resulting in re-identification to the public sector body. In case of unauthorised re-use of non-personal data, re-users must without delay inform affected legal persons	**4 — Trade Secret and Confidentiality Protection**	Data Re-user (Data Holder as re-user)	When re-using protected data obtained from a public sector body	Unless national law provides specific confidentiality safeguards

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-065	DGA-011	DGA	Art. 5(8)	Public sector bodies must ensure confidential data including data protected by statistical confidentiality, trade secrets or intellectual property rights is not disclosed as a result of allowing re-use, unless re-use is allowed under Art. 5(6)	**4 — Trade Secret and Confidentiality Protection**	Public Sector Body	When allowing re-use of commercially or statistically confidential data	
REQ-066	DA-023; DA-038; DA-043	Data Act	Art. 7(2); Art. 12(2); Art. 13(9)	Any contractual term that excludes, derogates from or varies the effect of user rights under Chapter II, Chapter III obligations, or Article 13 contractual fairness provisions to the detriment of any party shall not be binding. Parties may not exclude the application of these provisions by contract	**5 — Contractual Fairness and FRAND Conditions**	Data Holder / Seller / Service Provider / Enterprise (any contracting party)	When drafting or enforcing contracts with users or data recipients	
REQ-067	DA-025	Data Act	Art. 8(2)	Contractual terms concerning data access, use, liability or remedies shall not be binding if they constitute unfair contractual terms within the meaning of Article 13 or if they derogate from user rights under Chapter II to the detriment of the user	**5 — Contractual Fairness and FRAND Conditions**	Data Holder / Data Recipient	When drafting or enforcing data sharing contracts	
REQ-068	DA-039; DA-040; DA-041	Data Act	Art. 13(1); Art. 13(3-4); Art. 13(5)	A contractual term concerning data access, use, liability or remedies that has been unilaterally imposed by one enterprise on another shall not be binding if it is unfair. A term is unfair if it grossly deviates from good commercial practice contrary to good faith and fair dealing. In particular terms are unfair if they: exclude or limit liability for intentional acts or gross negligence; exclude remedies available to the weaker party in case of non-performance; or give the imposing party exclusive right to determine data conformity or interpret contractual terms. A term is presumed unfair if it: inappropriately limits remedies or extends liability of the	**5 — Contractual Fairness and FRAND Conditions**	Enterprise (imposing party)	When a contractual term related to data access or use is unilaterally imposed by one enterprise on another	Terms reflecting mandatory Union law provisions; terms defining main subject matter or price adequacy

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				weaker party; allows detrimental access to commercially sensitive data; prevents use of data generated during contract; prevents termination within reasonable period; prevents obtaining data copy after termination; enables termination at unreasonably short notice; or enables substantial unilateral changes to price or data conditions without valid reason				
REQ-069	DA-042	Data Act	Art. 13(6)	The contracting party that supplied the contested contractual term bears the burden of proving that the term was not unilaterally imposed	**5 — Contractual Fairness and FRAND Conditions**	Enterprise (imposing party)	When the fairness of a unilaterally supplied contractual term is challenged	
REQ-070	DA-030; DA-031	Data Act	Art. 9(1); Art. 9(2-3)	Any compensation agreed between a data holder and data recipient for making data available must be non-discriminatory and reasonable and may include a margin. When agreeing on compensation parties must take into account: costs of making data available including formatting, dissemination and storage; investments in data collection and production; and the volume, format and nature of the data	**5 — Contractual Fairness and FRAND Conditions**	Data Holder / Data Recipient	When agreeing on compensation for B2B data sharing	
REQ-071	DA-032	Data Act	Art. 9(4)	Compensation charged to the data recipient must not exceed the direct costs of making the data available	**5 — Contractual Fairness and FRAND Conditions**	Data Holder	When the data recipient is an SME or not-for-profit research organisation without partner or linked enterprises that are non-SMEs	Data recipient must be SME or not-for-profit without non-SME linked enterprises

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-072	DA-033	Data Act	Art. 9(7)	The data holder must provide the data recipient with sufficient detail on the basis of compensation calculation so that the data recipient can assess whether FRAND requirements are met	**5 — Contractual Fairness and FRAND Conditions**	Data Holder	When compensation is charged for making data available	
REQ-073	DGA-023	DGA	Art. 12(b)	Commercial terms including pricing for data intermediation services must not be made dependent on whether the data holder or data user uses other services provided by the same provider or a related entity	**5 — Contractual Fairness and FRAND Conditions**	Data Intermediation Service Provider	When setting commercial terms and pricing for data intermediation services	
REQ-074	DGA-013; DGA-014	DGA	Art. 6(1-2); Art. 6(4-5)	Public sector bodies may charge fees for allowing re-use of protected data. Any fees must be transparent, non-discriminatory, proportionate, objectively justified and must not restrict competition. Where fees are charged, public sector bodies must provide incentives for re-use for non-commercial purposes including scientific research and by SMEs and start-ups. Fees must be derived from and limited to actual costs of: data reproduction, provision and dissemination; rights clearance; anonymisation and preparation; secure processing environment maintenance; and assisting re-users in seeking consent or permission	**5 — Contractual Fairness and FRAND Conditions**	Public Sector Body	When charging fees for re-use of protected public sector data	
REQ-075	DA-092	Data Act	Art. 41	The Commission will develop non-binding model contractual terms on data access and use including reasonable compensation and trade secret protection, and non-binding standard contractual clauses for cloud computing contracts to assist parties in drafting FRAND contracts	**5 — Contractual Fairness and FRAND Conditions**	Data Holder / Data Recipient / Data Processing Service Provider	When drafting or negotiating data access, use or cloud computing contracts	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-076	DGA-017	DGA	Art. 10	The provision of data intermediation services must comply with Art. 12 conditions and is subject to a notification procedure. This applies to: intermediation between data holders and data users; intermediation between data subjects or natural persons and data users; and services of data cooperatives	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When any entity intends to provide data intermediation services as defined in Art. 2(11)	Recognised data altruism organisations and not-for-profit entities collecting data for general interest purposes not aiming to establish commercial relationships (Art. 15)
REQ-077	DGA-018; DGA-020	DGA	Art. 11(1); Art. 11(6)	Any data intermediation services provider intending to provide data intermediation services must submit a notification to the competent authority before starting activities. The notification must include: name and legal status; ownership structure and subsidiaries; address of main establishment and any secondary branches or legal representative; public website URL with up-to-date information; contact details; description of the service and category under Art. 10; and estimated start date if different from notification date	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	Before commencing provision of data intermediation services	
REQ-078	DGA-021	DGA	Art. 11(12-13)	Data intermediation services providers must notify the competent authority of any changes to notification information within 14 days of the change. Where a provider ceases activities it must notify the competent authority within 15 days	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When notification information changes or when the provider ceases activities	
REQ-079	DGA-019	DGA	Art. 11(3)	A data intermediation services provider not established in the Union but offering services within the Union must designate a legal representative in one of the Member States where services are offered. The legal representative must cooperate with competent authorities	**6 — Data Space and Intermediary Governance**	Non-EU Data Intermediation Service Provider	When a data intermediation service provider not established in the Union offers services within the Union	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				and demonstrate compliance upon request				
REQ-080	DGA-022	DGA	Art. 12(a)	The data intermediation services provider must not use the data for which it provides intermediation services for purposes other than making them available to data users. The provider must provide data intermediation services through a separate legal person, legally distinct from any other services it provides	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When providing data intermediation services	
REQ-081	DGA-024	DGA	Art. 12(c)	Data collected about activity within the intermediation service including date, time, geolocation, duration and connections may only be used for developing the intermediation service itself including fraud detection and cybersecurity. Such data must be made available to data holders upon request	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When processing activity data collected in the course of providing data intermediation services	
REQ-082	DGA-025	DGA	Art. 12(d-e)	The data intermediation services provider must facilitate exchange of data in the format received, converting formats only to enhance interoperability, where requested by the data user, where mandated by Union law, or to ensure harmonisation with standards. An opt-out from format conversion must be offered to data subjects and data holders unless mandated by Union law. Additional tools such as temporary storage, anonymisation and pseudonymisation may only be used at the explicit request or approval of the data holder or data subject	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When handling and transmitting data within intermediation services	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-083	DGA-026	DGA	Art. 12(f-g)	The data intermediation services provider must ensure the procedure for access to its service is fair, transparent and non-discriminatory for data subjects, data holders and data users including with regard to prices and terms of service. The provider must have procedures in place to prevent fraudulent or abusive access practices	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When operating data intermediation services and granting access to participants	
REQ-084	DGA-027	DGA	Art. 12(h)	The data intermediation services provider must ensure reasonable continuity of services in the event of insolvency and must have mechanisms in place to allow data holders, data users and data subjects to access, transfer or retrieve their data	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When the data intermediation service provider faces insolvency or cessation of activities	
REQ-085	DGA-028	DGA	Art. 12(i)	The data intermediation services provider must take appropriate measures to ensure interoperability with other data intermediation services using commonly used open standards in the sector	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When operating data intermediation services	
REQ-086	DGA-029; DGA-030	DGA	Art. 12(j-k); Art. 12(l)	The data intermediation services provider must put in place adequate technical, legal and organisational measures to prevent unlawful transfer of or access to non-personal data. The provider must without delay inform data holders of any unauthorised transfer, access or use of their non-personal data. The provider must take necessary measures to ensure appropriate security for storage, processing and transmission of non-personal data, and must ensure the highest level of security for storage and transmission of competitively sensitive information	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When operating data intermediation services involving non-personal data	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-087	DGA-032	DGA	Art. 12(o)	The data intermediation services provider must maintain a log record of data intermediation activity	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider	When providing data intermediation services	
REQ-088	DA-065; DA-066	Data Act	Art. 33(1); Art. 33(3)	Data holders and data service providers participating in data spaces must comply with essential interoperability requirements: datasets must be sufficiently described including content, use restrictions, licences, collection methodology, quality and uncertainty in machine-readable format; data structures, formats, vocabularies and classification schemes must be described in a publicly available and consistent manner; technical means of access including APIs and their terms of use must be sufficiently described to enable automatic access and transmission; and where applicable, means to enable interoperability of tools for automating data sharing agreements including smart contracts must be provided. Participants meeting harmonised standards published in the Official Journal of the EU are presumed to conform with these requirements	**6 — Data Space and Intermediary Governance**	Data Holder / Data Service Provider participating in a data space	When participating in a data space and offering data or data services to other participants	
REQ-089	DA-069; DA-070	Data Act	Art. 36(1); Art. 36(2-3)	Smart contract vendors or deployers must ensure smart contracts comply with essential requirements of: robustness and access control to withstand manipulation and functional errors; safe termination and interruption mechanisms; data archiving and continuity for auditability; rigorous access control at governance and smart	**6 — Data Space and Intermediary Governance**	Smart Contract Vendor / Deployer	When developing or deploying smart contracts for executing data sharing agreements in a data space	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				contract layers; and consistency with the terms of the data sharing agreement being executed. Smart contract vendors or deployers must perform a conformity assessment against these requirements and issue an EU declaration of conformity upon fulfilling them				
REQ-090	DA-005; DA-006	Data Act	Art. 4(4); Art. 4(5)	Data holders must not make it unduly difficult for users to exercise their access rights, including through dark patterns or non-neutral interface design. Data holders must not require users to provide more information than necessary for verification purposes, and must not retain log data on user access beyond what is necessary for execution of the request and security and maintenance	**6 — Data Space and Intermediary Governance**	Data Holder	When providing user interface for data access and when verifying user identity for data access requests	Microenterprises and small enterprises (Art. 7(1))
REQ-091	DA-015	Data Act	Art. 5(3)	Gatekeepers designated under the Digital Markets Act must not be eligible third parties to receive data under Art. 5, and must not solicit or incentivise users to share or request data on their behalf	**6 — Data Space and Intermediary Governance**	Gatekeeper / User	When a gatekeeper attempts to access data via Art. 5 mechanism	
REQ-092	DGA-049	DGA	Art. 37	Entities providing data intermediation services on 23 June 2022 must have complied with all Chapter III obligations by 24 September 2025	**6 — Data Space and Intermediary Governance**	Data Intermediation Service Provider (existing at DGA entry into force)	When an entity was already providing data intermediation services at the time the DGA entered into force	New providers after 23 June 2022 must comply from the start
REQ-093	GDPR-038	GDPR	Art. 44	Any transfer of personal data to a third country or international organisation — including onward transfers — may only take place if the conditions of Chapter V are complied with by both controller and processor. The level of protection	**7 — International Data Transfers**	Controller / Processor (Data Holder / Data Space Operator)	When personal data is transferred or intended to be transferred to a third country or international organisation	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				guaranteed by the GDPR must not be undermined by the transfer				
REQ-094	GDPR-039	GDPR	Art. 45(1)	Personal data may be transferred to a third country or international organisation where the Commission has adopted an adequacy decision for that country or organisation. No specific authorisation is required for such transfers	**7 — International Data Transfers**	Controller / Processor (Data Holder)	When transferring personal data to a third country or international organisation covered by a Commission adequacy decision	
REQ-095	GDPR-040	GDPR	Art. 46(1-2)	In the absence of an adequacy decision a controller or processor may transfer personal data to a third country only if appropriate safeguards are provided and enforceable data subject rights and effective legal remedies are available. Appropriate safeguards may be provided without supervisory authority authorisation through: legally binding instruments between public authorities; binding corporate rules; standard data protection clauses adopted by the Commission; standard data protection clauses adopted by a supervisory authority; an approved code of conduct with binding commitments; or an approved certification mechanism with binding commitments	**7 — International Data Transfers**	Controller / Processor (Data Holder)	When transferring personal data to a third country in the absence of an adequacy decision	Subject to supervisory authority authorisation: contractual clauses between controller/processor and recipient; provisions in administrative arrangements between public authorities
REQ-096	GDPR-042	GDPR	Art. 49(1)	In the absence of an adequacy decision or appropriate safeguards a transfer may only take place on one of the following conditions: explicit consent of the data subject after being informed of risks; necessity for contract performance with the data subject; necessity for contract in	**7 — International Data Transfers**	Controller (Data Holder)	When transferring personal data to a third country in the absence of both an adequacy decision and appropriate safeguards	Derogations based on consent, contract and compelling legitimate interests do not apply to public authority activities in exercise of public powers

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				the interest of the data subject; important reasons of public interest recognised in Union or Member State law; establishment, exercise or defence of legal claims; protection of vital interests where the data subject cannot consent; or transfer from a public register. Where none of these apply, a non-repetitive transfer of limited scope may be made on the basis of compelling legitimate interests after assessment and notification to the supervisory authority				
REQ-097	DA-061; DGA-044	Data Act / DGA	Art. 32(1); Art. 31(1)	Providers of data processing services, public sector bodies, re-use right holders, data intermediation services providers and recognised data altruism organisations must take all reasonable technical, legal and organisational measures including contracts to prevent international governmental access to or transfer of non-personal data held in the Union where such access or transfer would conflict with Union or national law	**7 — International Data Transfers**	Data Processing Service Provider / Data Intermediation Service Provider / Recognised Data Altruism Organisation / Public Sector Body / Data Re-user	When non-personal data held in the Union is subject to potential third-country governmental access or transfer	
REQ-098	DA-062; DGA-045	Data Act / DGA	Art. 32(2-3); Art. 31(2-3)	A third-country decision requiring transfer of or access to non-personal data held in the Union may only be complied with where it is based on an international agreement in force between the third country and the Union or a Member State, or where specific conditions regarding proportionality, right of objection and judicial review are met in the third country legal system: the third-country system must require reasons and proportionality to be set out and the decision to be specific in character; the reasoned objection of the addressee must be subject to review by a	**7 — International Data Transfers**	Data Processing Service Provider / Data Intermediation Service Provider / Data Re-user	When a third-country court, tribunal or administrative authority issues a decision requiring transfer of or access to non-personal data held in the Union	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				competent third-country court or tribunal; and the competent court must be empowered to take into account the relevant legal interests of the provider protected under Union law				
REQ-099	GDPR-041	GDPR	Art. 48	A third-country court or administrative authority decision requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable if based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the Union or a Member State	**7 — International Data Transfers**	Controller / Processor (Data Holder / Data Space Operator)	When a third-country court or administrative authority issues a decision requiring transfer or disclosure of personal data	
REQ-100	DA-063; DGA-046	Data Act / DGA	Art. 32(4); Art. 31(4)	Where conditions for complying with a third-country request are met, only the minimum amount of data permissible must be provided in response, based on a reasonable interpretation of the request	**7 — International Data Transfers**	Data Processing Service Provider / Data Intermediation Service Provider / Data Re-user / Public Sector Body	When a third-country data access request must be complied with under the conditions of Art. 32(2-3) or Art. 31(2-3)	
REQ-101	DA-064; DGA-047	Data Act / DGA	Art. 32(5); Art. 31(5)	Providers of data processing services, data intermediation services providers and recognised data altruism organisations must inform the data holder about the existence of a third-country authority request to access its data before complying with that request	**7 — International Data Transfers**	Data Processing Service Provider / Data Intermediation Service Provider / Recognised Data Altruism Organisation / Public Sector Body	When a third-country authority requests access to a data holder's data held by any of the listed entities	Except where the request serves law enforcement purposes and notification would compromise law enforcement effectiveness

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-102	DGA-012	DGA	Art. 5(9-10)	Where a re-user intends to transfer non-personal protected data to a third country, the re-user must inform the public sector body of its intention and purpose at the time of requesting re-use. The public sector body must not allow re-use unless the affected legal person gives permission for the transfer. Re-users must contractually commit to: complying with re-use obligations even after transfer to the third country; and accepting jurisdiction of courts of the Member State of the transmitting public sector body	**7 — International Data Transfers**	Data Re-user (Data Holder as re-user) / Public Sector Body	When a re-user intends to transfer non-personal protected data originally held by a public sector body to a third country	Third countries designated by Commission as providing equivalent protection
REQ-103	DA-076	Data Act	Art. 28(1-2)	Providers of data processing services must make publicly available on their website and keep up to date: the jurisdiction to which their ICT infrastructure is subject; and a general description of technical, organisational and contractual measures to prevent unlawful international governmental access to or transfer of non-personal data held in the Union. This information must be referenced in all contracts	**7 — International Data Transfers**	Data Processing Service Provider	When providing data processing services involving data held in the Union	
REQ-104	AIA-001	AI Act	Art. 10(1)	High-risk AI systems using techniques involving training of AI models must be developed on the basis of training, validation and testing data sets that meet the quality criteria referred to in Art. 10(2-5). For high-risk AI systems not using training techniques, Art. 10(2-5) apply only to testing data sets	**8 — AI Data Governance**	Provider of High-risk AI System / Data Holder supplying training data	When a high-risk AI system uses techniques involving training of AI models with data	Non-high-risk AI systems; Art. 10(6) applies testing data requirements only to high-risk AI systems not using training techniques

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-105	AIA-002	AI Act	Art. 10(2)	Training, validation and testing data sets must be subject to appropriate data governance and management practices for the intended purpose, covering in particular: relevant design choices; data collection processes and origin including original purpose of personal data collection; data preparation operations such as annotation, labelling, cleaning, updating, enrichment and aggregation; assumptions about what the data measures and represents; assessment of availability, quantity and suitability of data sets; examination for possible biases affecting health and safety, fundamental rights or prohibited discrimination; appropriate measures to detect, prevent and mitigate identified biases; and identification of data gaps or shortcomings and how they can be addressed	**8 — AI Data Governance**	Provider of High-risk AI System / Data Holder supplying training data	When developing a high-risk AI system using training data	
REQ-106	AIA-003	AI Act	Art. 10(3-4)	Training, validation and testing data sets must be relevant, sufficiently representative, and to the best extent possible free of errors and complete in view of the intended purpose. They must have appropriate statistical properties regarding the persons or groups for whom the system is intended. Data sets must take into account characteristics particular to the specific geographical, contextual, behavioural or functional setting of intended use	**8 — AI Data Governance**	Provider of High-risk AI System / Data Holder supplying training data	When preparing data sets for high-risk AI system development	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-107	DA-010; DA-021	Data Act	Art. 4(10); Art. 6(2)(e)	Users must not use accessed data to develop a connected product competing with the connected product from which the data originates, share data with a third party for that purpose, or use data to derive insights about the manufacturer or data holder. Third parties must not use received data to develop a competing connected product or derive insights about the data holder, nor share such data with another third party for those purposes	**8 — AI Data Governance**	User / Third Party (Data Recipient)	When user or third party receives data under Art. 4(1) or Art. 5(1) and considers using it for AI-driven competitive intelligence or competing product development	
REQ-108	GDPR-002; GDPR-003; GDPR-004	GDPR	Art. 5(1)(b); Art. 5(1)(c); Art. 5(1)(d)	Where AI training data includes personal data: it must have been collected for purposes compatible with AI training use (purpose limitation); it must be limited to what is necessary for the AI training purpose (data minimisation); and it must be accurate and up to date (accuracy). Where AI training represents a new purpose incompatible with original collection, a compatibility assessment under Art. 6(4) is required or consent must be obtained	**8 — AI Data Governance**	Controller (Data Holder) / Provider of High-risk AI System	When personal data is used or supplied for AI system training, validation or testing	
REQ-109	DGA-006; DGA-008	DGA	Art. 5(3); Art. 5(5)	Where data re-used from public sector bodies under DGA Chapter II is intended for use in AI system development: the public sector body must ensure the protected nature of the data is preserved through anonymisation or secure processing environment access before re-use is permitted. Re-users must adhere to confidentiality obligations and must not re-identify any data subject. Where the data will be used to train an AI system, this use must be within the scope of the re-use purpose agreed with the public sector body	**8 — AI Data Governance**	Data Re-user (Data Holder as re-user) / Public Sector Body	When re-used public sector data is intended for AI system training or development	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-110	DA-034	Data Act	Art. 10(1)	Users, data holders and data recipients must have access to a certified dispute settlement body to resolve disputes about data access, FRAND conditions and data sharing arrangements. Dispute settlement bodies must be impartial, independent, have expertise in FRAND conditions, be accessible electronically, and be capable of adopting swift and cost-effective decisions	**9 — Enforcement, Remedies and Penalties**	Data Holder	When disputes arise regarding data access, FRAND conditions or data sharing arrangements	
REQ-111	DA-088; DGA-042; GDPR-044	Data Act / DGA / GDPR	Art. 38(1); Art. 27(1); Art. 77(1)	Natural and legal persons have the right to lodge a complaint with the relevant competent authority where they consider their rights under the Data Act, DGA or GDPR have been infringed. This right exists individually or collectively. The competent authority must inform the complainant of progress and outcome of proceedings and of available judicial remedies	**9 — Enforcement, Remedies and Penalties**	Any natural or legal person / Data Subject	When a person considers their rights under any of the three instruments have been infringed	
REQ-112	DA-089; DGA-043; GDPR-045	Data Act / DGA / GDPR	Art. 39(1-2); Art. 28(1-3); Art. 79(1)	Any affected natural or legal person has the right to an effective judicial remedy regarding legally binding decisions by competent authorities or where a competent authority fails to act on a complaint. Data subjects also have the right to a judicial remedy directly against a controller or processor where they consider their GDPR rights have been infringed	**9 — Enforcement, Remedies and Penalties**	Any natural or legal person / Data Subject	When a competent authority takes a legally binding decision, fails to act on a complaint, or when a data subject considers their GDPR rights have been infringed	
REQ-113	GDPR-043	GDPR	Art. 58(1-2)	Supervisory authorities have investigative powers including: requiring controllers and processors to provide any necessary information; conducting data protection audits; accessing all personal data and information necessary for their tasks; and accessing premises and equipment. They have corrective powers including: issuing warnings and	**9 — Enforcement, Remedies and Penalties**	Controller / Processor (Data Holder / Data Space Operator)	When a supervisory authority investigates or finds non-compliance with GDPR	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				reprimands; ordering compliance with data subject rights requests; ordering processing to be brought into compliance; ordering communication of breaches to data subjects; imposing temporary or definitive limitations including bans on processing; ordering rectification, erasure or restriction; withdrawing certifications; imposing administrative fines; and ordering suspension of data flows to third countries				
REQ-114	DA-087	Data Act	Art. 37(14)	Competent authorities have the power to request from users, data holders or data recipients all information necessary to verify compliance with the Data Act. Any such request must be proportionate and reasoned	**9 — Enforcement, Remedies and Penalties**	Data Holder / Data Recipient / User	When a competent authority requests information to verify compliance	
REQ-115	GDPR-046	GDPR	Art. 82(1-4)	Any person who has suffered material or non-material damage as a result of a GDPR infringement has the right to receive compensation from the controller or processor. Any controller involved in processing is liable for damage caused by non-compliant processing. A processor is liable where it has not complied with processor-specific GDPR obligations or acted outside controller instructions. Where multiple controllers or processors are involved in the same processing each is liable for the entire damage to ensure effective compensation	**9 — Enforcement, Remedies and Penalties**	Controller / Processor (Data Holder / Data Space Operator)	When a person suffers material or non-material damage as a result of a GDPR infringement	Controller or processor exempt from liability if it proves it is not in any way responsible for the damage-causing event

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
REQ-116	DA-090; DA-091	Data Act	Art. 40(1); Art. 40(3)	Penalties for Data Act infringements must be effective, proportionate and dissuasive. When imposing penalties, competent authorities must take into account: nature, gravity, scale and duration of the infringement; mitigation actions taken; previous infringements; financial benefits gained; and the infringing party's annual turnover in the Union	**9 — Enforcement, Remedies and Penalties**	Member States / Competent Authority	When implementing national penalty rules and when imposing penalties for Data Act infringements	
REQ-117	DGA-048	DGA	Art. 34(1)	Penalties for DGA infringements covering international transfer obligations, notification obligations, conditions for providing data intermediation services and conditions for data altruism registration must be effective, proportionate and dissuasive. Criteria include: nature, gravity, scale and duration; mitigation actions; previous infringements; financial benefits gained	**9 — Enforcement, Remedies and Penalties**	Member States	When implementing national penalty rules for DGA infringements	
REQ-118	GDPR-047	GDPR	Art. 83(4-5)	Infringements of Arts. 8, 11, 25-39, 42 and 43 are subject to fines up to €10 million or 2% of global annual turnover whichever is higher. Infringements of the basic processing principles under Arts. 5, 6, 7 and 9, data subject rights under Arts. 12-22, and international transfer provisions under Arts. 44-49 are subject to fines up to €20 million or 4% of global annual turnover whichever is higher	**9 — Enforcement, Remedies and Penalties**	Supervisory Authority	When a GDPR infringement is found and administrative fines are being determined	
REQ-119	DA-086	Data Act	Art. 37(10-11)	Entities falling within the scope of the Data Act that are not established in the Union but make connected products available or offer services in the Union must designate a legal representative in one of the Member States	**9 — Enforcement, Remedies and Penalties**	Non-EU established Data Holder / Data Processing Service Provider / Connected	When an entity not established in the Union makes connected products available or offers services in the Union	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
						Product Manufacturer		
REQ-120	DGA-016	DGA	Art. 29(1)	Any natural or legal person directly and individually affected by a decision of a public sector body on a re-use request under DGA Chapter II must have access to an effective right of redress before a competent body in the Member State where the relevant public sector body is located. This includes the right to challenge a refusal of re-use, the conditions imposed on re-use, or the fees charged for re-use.	**9 — Enforcement, Remedies and Penalties**	Any natural or legal person / Data Re-user	After receiving a decision from a public sector body on a DGA Chapter II re-use request	
REQ-121	DA-022	Data Act	Art. 7(1)	The obligations of Data Act Chapter II do not apply to data generated by connected products or related services of microenterprises or small enterprises, provided they have no partner or linked enterprise that does not qualify as micro or small, and are not subcontracted to manufacture or provide the connected product or service. The same applies to medium-sized enterprises for one year after qualifying as medium, and to connected products for one year after being placed on the market by a medium-sized enterprise	**10 — Exemptions and Compliance Timelines**	Microenterprise / Small Enterprise	When the data holder qualifies as a microenterprise or small enterprise with no non-qualifying linked enterprises and is not subcontracted	
REQ-122	DA-094	Data Act	Art. 50	The Data Act applies from 12 September 2025. The product design obligation under Art. 3(1) applies to connected products placed on the market after 12 September 2026. Chapter III B2B sharing obligations apply only to data sharing obligations under Union law entering	**10 — Exemptions and Compliance Timelines**	Data Holder / Connected Product Manufacturer / Data Processing Service Provider	When determining which Data Act obligations currently apply and from when	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				into force after 12 September 2025. Chapter IV unfair terms obligations apply to contracts concluded after 12 September 2025, and from 12 September 2027 to pre-existing contracts of indefinite duration or due to expire at least 10 years from 11 January 2024				
REQ-123	DGA-050	DGA	Art. 38	The DGA applies from 24 September 2023. All DGA obligations including Chapter III data intermediation services requirements and Chapter IV data altruism registration requirements are fully in force	**10 — Exemptions and Compliance Timelines**	All entities within scope of DGA	When determining which DGA obligations apply and from when	
REQ-124	DGA-001	DGA	Art. 3(1)	DGA Chapter II applies only to re-use of data held by public sector bodies that is protected on grounds of: commercial confidentiality including trade secrets; statistical confidentiality; intellectual property rights of third parties; or personal data outside the scope of the Open Data Directive. Data held by public undertakings, broadcasters, cultural and educational establishments, data protected for security or defence reasons, and data outside the public sector body's public task scope are excluded	**10 — Exemptions and Compliance Timelines**	Public Sector Body / Data Re-user	Before applying any DGA Chapter II requirement — determines whether the chapter is applicable at all	Data held by public undertakings, broadcasters, cultural/educational establishments, data protected for security/defence/national security, data outside public task scope
REQ-125	DGA-033	DGA	Art. 18(a-e)	To qualify for registration as a recognised data altruism organisation an entity must: carry out data altruism activities; be a legal person established to meet general interest objectives; operate on a not-for-profit basis and be legally independent from for-profit entities; carry out data altruism activities through a functionally separate structure; and comply with the rulebook within 18 months of its entry into force.	**10 — Exemptions and Compliance Timelines**	Entity seeking data altruism recognition	When an entity wishes to register as a recognised data altruism organisation	Entities not seeking recognised status may still conduct data altruism activities without registration and without being subject to Chapter IV obligations

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				DGA Chapter IV obligations only apply to entities that choose to register — unregistered entities conducting altruistic activities are not bound by the Chapter IV framework				
REQ-126	GDPR-016	GDPR	Art. 11(1-2)	Where the purposes of processing do not or no longer require identification of a data subject, the controller is not obliged to maintain, acquire or process additional information to identify the data subject solely for GDPR compliance purposes. Where the controller cannot identify the data subject it must inform them accordingly where possible, and Arts. 15-20 do not apply unless the data subject provides additional identification information enabling identification	**10 — Exemptions and Compliance Timelines**	Controller (Data Holder)	When processing data where identification of individual data subjects is not required for the processing purpose	
REQ-127	DA-093	Data Act	Art. 43	The sui generis database right under Directive 96/9/EC does not apply to data obtained from or generated by a connected product or related service falling within the scope of the Data Act. Database owners cannot use the sui generis right to prevent or restrict data sharing under Data Act Arts. 4 and 5	**10 — Exemptions and Compliance Timelines**	Data Holder / Connected Product Manufacturer	When data is obtained from or generated by a connected product or related service covered by the Data Act	
REQ-128	GDPR-036; GDPR-037	GDPR	Art. 40(1-2); Art. 42(1-4)	Codes of conduct may be drawn up to contribute to proper GDPR application, specifying application in areas including pseudonymisation, data subject rights, children's data and parental consent, Arts. 24 and 25 measures, breach notification, and third country transfers. Adherence to approved codes may be used to demonstrate compliance. Data protection certification mechanisms, seals and marks may be established to demonstrate compliance with the GDPR.	**10 — Exemptions and Compliance Timelines**	Controller / Processor / Industry Associations	When seeking to demonstrate GDPR compliance through an approved code of conduct or certification mechanism	

ID	Original ID	Source	Location	Requirement Text	Cluster	Addressee	Trigger	Exemptions
				Certification is voluntary and transparent but does not reduce the responsibility of the controller or processor for GDPR compliance				

APPENDIX B: ABRIDGED SOCIAL & ETHICAL BEST PRACTICES

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
ELSA-001	1 — Data Access and Sharing Obligations	*Risk of reinforcing gender bias due to unequal representation or exclusion in shared datasets. Where data sharing obligations are met without attention to dataset composition, structurally unequal patterns may be reproduced or amplified in downstream uses.*	Proactively ensure that data made available under access and sharing obligations is balanced and representative. Where feasible, provide gender-disaggregated data and document known representational gaps in metadata. Do not treat legal compliance with access obligations as sufficient where the underlying dataset excludes or under-represents groups.	Data holders (private and public); data space operators
ELSA-002	1 — Data Access and Sharing Obligations	*Risk of reinforcing structural inequalities if access conditions — both technical and financial — disproportionately favour large or well-resourced actors. Users with low digital literacy, individuals with disabilities, and actors in low-resource environments may be formally entitled to access but effectively excluded from using it.*	Ensure access is not only legally compliant but practically usable. Provide accessible formats including assistive technologies for individuals with disabilities. Offer support and guidance for effective data use by less technically mature participants. Monitor data access practices for discriminatory patterns. Practically usable access is the standard — formal availability without usability does not meet the spirit of the access obligations.	Data holders (private and public); data space operators; public sector bodies
ELSA-003	2 — Personal Data Protection	*Heightened exposure of certain genders and vulnerable groups to privacy harms including harassment, profiling, and misuse of personal data. Legal compliance with GDPR principles does not prevent harms that arise from patterns within lawfully processed data.*	Apply gender-sensitive and vulnerability-aware risk assessments when designing or reviewing data processing activities. Implement enhanced safeguards for categories of processing that carry disproportionate risks for specific groups, including profiling, automated decision-making, and large-scale behavioural analysis. Do not limit the risk assessment to data types — assess the impact on specific affected populations.	Controllers; processors; data space operators processing personal data
ELSA-004	2 — Personal Data Protection	*Risk that transparency and notice obligations are met formally but are not understood by data subjects, particularly those with low digital literacy, disabilities, or language barriers. Consent flows are often designed to minimise refusals rather than to enable genuine informed choice.*	Use layered privacy notices — a short, plain-language summary plus a detailed version. Provide just-in-time notices at key decision points rather than only at sign-up. Include visual aids and accessible formats. Ensure no pre-checked boxes and no dark patterns in consent flows. Introduce reconfirmation steps for high-impact processing such as data sharing and profiling. Conduct user testing of consent flows including with vulnerable users to verify comprehension.	Controllers processing personal data; data holders presenting consent to users

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
ELSA-005	**2 — Personal Data Protection**	*Data subject rights exist in law but may not be practically exercisable, particularly for individuals who face technical, linguistic, or access barriers. Response time obligations are legal minima — not a benchmark for responsible practice.*	Enable one-click tools for data download, deletion, and correction via a user dashboard. Provide accessible alternative channels to exercise rights. Implement response time tracking and escalation for data subject requests. Include a human review option where automated processing significantly affects individuals. Provide clear, simple instructions on how to exercise each right.	Controllers; data holders processing personal data at scale
ELSA--006	**2 — Personal Data Protection**	*Privacy-invasive practices are often enabled by permissive default settings. Data minimisation principles in law are frequently interpreted as minima rather than as active design obligations.*	Set privacy-protective defaults with minimal data collection as the default state. Conduct periodic data minimisation audits to identify and remove data that is no longer needed or was never necessary. Implement data protection by design as an active engineering standard, not a compliance checkbox.	Controllers; data holders; product designers; data space architects
ELSA-007	**3 — Special Category and Sensitive Data**	*Risk of misuse or exposure of gender-related and other sensitive personal data leading to discrimination, stigmatisation, or targeted harm. The categories protected under GDPR Article 9 are particularly susceptible to being processed under narrow exceptions in ways that enable discriminatory profiling or exclusion.*	Minimise collection of special category data to the strictest necessary scope. Apply explicit ethical oversight — including an independent review function or ethics board — for any processing of gender data, health data, or other Article 9 categories. Document the ethical justification for each processing activity involving sensitive data beyond the legal basis requirement. Ensure that processing for AI purposes involving special category data is subject to an enhanced ethical review in addition to the legally required DPIA.	Controllers processing special category data; AI system providers; research organisations
ELSA-008	**3 — Special Category and Sensitive Data**	*Risk that secondary use of health and sensitive data benefits some populations more than others due to underrepresentation of minorities, rural populations, women, and rare disease patients. Patients and data subjects may not understand or meaningfully control how their sensitive data is reused. Re-identification risks are heightened for small populations such as rare disease patients.*	Ensure representative inclusion in sensitive datasets by actively assessing and addressing gaps across demographic and clinical groups. Implement dynamic and accessible consent models with clear explanations of secondary use and withdrawal options. Provide data subject-facing transparency tools such as portals explaining how sensitive data is used. Apply strong de-identification techniques with regular re-identification risk testing. Include rare disease and small population considerations explicitly in DPIAs. Prioritise interoperability standards to enable pooling of scarce data for rare disease research.	Controllers processing health and sensitive personal data; research organisations; healthcare providers; AI developers using health data

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
ELSA-009	4 — Trade Secret and Confidentiality Protection	*Strong confidentiality protections may enable opaque practices and limit accountability. Risk of over-classification of data as confidential to avoid scrutiny rather than to protect genuine proprietary interests.*	Clearly define and document trade secret scope using objective criteria. Separate genuinely sensitive elements from shareable data using redaction or aggregation rather than blanket withholding. Maintain justification logs for withheld or restricted data. Provide explanation to requesters when access is refused or restricted.	Data holders with commercially sensitive data; public sector bodies applying confidentiality restrictions
ELSA-010	4 — Trade Secret and Confidentiality Protection	*Blanket refusal to share data containing trade secrets denies the value of the access framework. Those with limited negotiation power — including SMEs, researchers, and civil society — are disproportionately affected by unreasonable confidentiality claims.*	Apply tiered access and controlled environments as alternatives to full refusal. Use standardised and balanced confidentiality agreements that avoid one-sided clauses. Implement explainability and audit mechanisms that enable accountability without compromising legitimate proprietary interests.	Data holders sharing data containing trade secrets; data recipients; re-users of public sector data with commercially sensitive content
ELSA-011	5 — Contractual Fairness and FRAND Conditions	*Power asymmetries and complex contractual terms undermine fairness and informed consent, particularly for smaller actors. Opaque pricing and bundled services create hidden access barriers. SMEs and newer market entrants are most adversely affected.*	Use standardised contract templates as a baseline. Require clear, itemised pricing breakdowns without bundled or hidden costs. Document and justify deviations from FRAND conditions. Conduct internal review of contracts involving SMEs or parties with weaker bargaining power. Ensure negotiation timelines are reasonable. Offer simplified contract pathways for SMEs such as pre-approved standard terms. Embed accessible and affordable dispute resolution mechanisms into all data sharing agreements. Monitor contract outcomes for discriminatory patterns across actor types.	Data holders; data recipients; SMEs; data intermediaries; contracting parties
ELSA-012	6 — Data Space and Intermediary Governance	*Risk of concentration of power in data intermediaries affecting neutrality and fair access. Dependency on intermediaries may limit autonomy of participants. Onboarding processes may create barriers for less technically mature participants, particularly SMEs and civil society organisations.*	Ensure clear, auditable functional separation between intermediation and other commercial services. Implement auditable neutrality controls. Publish transparent access criteria and onboarding procedures. Provide onboarding guidance and support for less technically mature participants. Monitor access decisions for discriminatory patterns across actor types.	Data space operators; data intermediaries; data altruism organisations
ELSA-013	6 — Data Space and Intermediary Governance	*Lack of interoperability may fragment ecosystems and exclude smaller actors. Absence of clear continuity and exit procedures creates dependency risks for all participants in a data space.*	Provide standardised and documented APIs to enable interoperability. Establish contingency and exit procedures including tested data retrieval processes in case of intermediary failure or insolvency. Ensure participants can extract their data and transition to alternative intermediaries without undue technical barriers.	Data space operators; data intermediaries; data holders entering data spaces

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
ELSA-014	7 — International Data Transfers	*Cross-border data transfers may expose individuals to gender-based and other identity-based risks in destination contexts with weaker legal protections. The adequacy and safeguards framework does not automatically account for the heightened risk profile of specific groups in specific destination countries.*	Conduct gender-specific and vulnerability-specific risk assessments as part of transfer impact assessments before transferring personal data to third countries. Where the destination context presents heightened risks for specific groups — including LGBTQ+ individuals, ethnic or religious minorities, political dissidents, or journalists — apply additional technical and organisational safeguards beyond those legally required. Do not treat an adequacy decision or standard contractual clauses as a sufficient substitute for a contextualised risk assessment.	Controllers and processors transferring personal data internationally; data space operators with international participants
ELSA-015	7 — International Data Transfers	*Risk of reduced protection when data is transferred outside the EU. However, overly restrictive transfer practices may also impair cross-border cooperation including mutual legal assistance and transnational crime investigation. The balance between these two risks requires active management.*	Conduct and document transfer impact assessments including human rights and public interest considerations. Distinguish clearly between lawful cooperation channels such as mutual legal assistance treaties and unlawful access requests. Implement clear internal procedures for timely response to legitimate law enforcement requests. Maintain logs of third-country requests and decisions. Limit data to the necessary scope while avoiding blanket refusals that create unintended barriers to legitimate cooperation. Apply encryption and pseudonymisation where feasible.	Data holders; data space operators; data processing service providers; re-users of public sector data transferring internationally
ELSA-016	8 — AI Data Governance	*Training data may reflect historical inequalities, embed structural biases, and underrepresent minorities, women, and marginalised groups. Dataset composition problems are often invisible at the legal compliance stage.*	Meticulously document dataset composition and known limitations including underrepresented groups. Conduct gender audits and representativeness testing using validated methods such as SGIA. Use diverse and balanced data sources where feasible. Implement dataset review checkpoints before training including human oversight. Apply systematic data cleaning and error detection. Perform bias and fairness testing before the data is supplied or used for training.	Data holders supplying AI training data; AI system providers; data spaces for AI development
ELSA-017	8 — AI Data Governance	*Bias and representation problems in AI systems are not fully detectable before deployment. Continuous monitoring is needed to identify and address harms as they emerge. Data contributors often receive no transparency or feedback on how their data was used or what outcomes it produced.*	Perform bias and fairness testing at multiple lifecycle stages including after deployment. Include impact-focused risk assessments for high-risk use cases. Provide transparency summaries on training data characteristics to downstream users. Enable feedback or complaint mechanisms for affected stakeholders. Monitor downstream use and impacts where possible.	AI system providers; data holders with ongoing supply relationships; data spaces for AI development

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
ELSA-018	9 — Enforcement, Remedies and Penalties	*Complaint and enforcement mechanisms exist in law but may not be practically accessible for vulnerable groups due to complexity, cost, digital barriers, or lack of awareness. Gender-related harms and harms to marginalised groups are disproportionately underreported.*	Provide clear, accessible information on complaint rights and enforcement mechanisms in plain language and accessible formats. Ensure simple, user-friendly complaint submission processes including both online and assisted channels. Ensure no retaliation for individuals exercising rights. Provide affordable alternative dispute resolution as a complement to formal complaint channels.	All data holders; data space operators; entities subject to supervisory authority oversight
ELSA-019	9 — Enforcement, Remedies and Penalties	*Organisations often treat complaints as isolated incidents rather than as signals of systemic issues. In multi-actor data spaces, responsibility for handling complaints may be unclear, leading to delays or non-resolution.*	Set internal procedures to handle complaints promptly and transparently with defined timelines and escalation paths. Track and analyse complaints to identify systemic issues and trigger process improvements. Maintain clear allocation of responsibility for complaint handling in multi-actor data spaces. Train staff on handling complaints and interactions with supervisory authorities in a gender-responsive and inclusive manner.	Data space operators; data holders with ongoing user relationships; data intermediaries
ELSA-020	10 — Exemptions and Compliance Timelines	*Anonymisation claims may not reflect genuinely robust de-identification. Structurally unequal patterns in data may persist even in technically anonymised datasets. Delayed compliance timelines may create temporary protection gaps for affected individuals.*	Apply robust anonymisation techniques and regularly test for re-identification risk. Do not use anonymisation as a binary claim — document the technical method, the risk assessment, and residual risks. Plan phased compliance to minimise protection gaps during transition periods. Monitor the impact on affected groups and adjust practices where risks emerge.	All actors using anonymisation; all actors subject to compliance timelines
ELSA-021	10 — Exemptions and Compliance Timelines	*SME and similar exemptions may be claimed incorrectly or may be used to avoid safeguards rather than to reduce disproportionate compliance burden. Over-reliance on exemptions may lead to weaker protection in practice for individuals whose data is processed by exempt actors.*	Clearly document and justify use of any exemption including SME status using objective criteria. Implement internal checks to verify ongoing eligibility — exemptions lapse when the triggering conditions no longer apply such as when the enterprise scales, enters subcontracting arrangements, or joins a group exceeding the thresholds. Avoid using exemptions to bypass core safeguards. Provide simplified compliance guidance to help SMEs progressively align with full obligations.	Microenterprises; small enterprises; data holders relying on exemptions
ELSA-022	Health / medical data	*Risk that secondary use of health data benefits some populations more than others due to underrepresentation of minorities, rural populations, women, and rare disease patients. Particularly acute for rare disease patients who may be both*	Ensure representative inclusion by actively assessing and addressing demographic and clinical gaps across the dataset. Prioritise interoperability standards to enable pooling of scarce data for rare disease research. Include rare disease and small population considerations explicitly in DPIAs and risk assessments. Monitor	Healthcare providers; research organisations; health data spaces; AI developers using health data

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
		underrepresented and highly identifiable due to small population size.	outcomes of research and AI systems for differential impact across groups.	
ELSA-023	**Health / medical data**	*Patients may not understand or meaningfully control how their health data is reused for secondary purposes. Trust deficits undermine participation in data sharing for research and AI development. Re-identification risks from sensitive health information can cause stigma or harm.*	Implement dynamic and accessible consent models with clear explanations of secondary use and withdrawal options. Provide patient-facing transparency tools such as portals explaining data use and sharing. Engage patient groups and public representatives in governance of data use through advisory boards. Apply strong de-identification techniques with regular re-identification risk testing and transparent communication to patients about residual risks. Enable patient-tailored feedback and complaint mechanisms.	Healthcare providers; research organisations; health data spaces
ELSA-024	**Health / medical data**	*Re-identification risk for health data is technically significant and is often underestimated. Standard pseudonymisation may be insufficient for rare conditions or small populations. Cross-border sharing amplifies this risk.*	Apply strong de-identification techniques and regularly test for re-identification risk using current state-of-the-art methods. Ensure accessibility of participation including offline options, assisted consent, and multilingual materials. Apply additional safeguards for highly sensitive conditions including mental health and rare diseases.	Research organisations; health data spaces; organisations sharing health data internationally
ELSA-025	**Children's data (under 16)**	*Children have limited capacity to understand data use and long-term consequences. Risk that parental consent does not fully reflect the child's best interests or that children are excluded from any meaningful participation in decisions about their data.*	Implement dual-layer consent and assent models — parental consent combined with meaningful child involvement appropriate to age and developmental maturity. Regularly refresh consent and provide easy withdrawal options. Provide age-appropriate layered explanations using child-friendly formats. Provide accessible mechanisms for children themselves to exercise rights and raise concerns. Engage children and youth advisory groups in data governance design.	Educational platforms; healthcare providers for minors; children's device manufacturers; researchers studying children
ELSA-026	**Children's data (under 16)**	*Children face heightened risks from profiling, behavioural manipulation, and overexposure of their data. Differential access and digital literacy across families may affect inclusion. Long-term harms from childhood data collection are often not foreseeable at the point of processing.*	Apply strict data minimisation and avoid unnecessary profiling or tracking of children. Build privacy-protective default settings for all child users. Conduct a Digital Child Rights Impact Assessment (UNICEF D-CRIA) to assess risks to children's rights across the full data lifecycle. Apply enhanced safeguards for high-risk contexts including education, health, and connected devices. Ensure no adverse consequences such as exclusion from services for non-consent or withdrawal. Monitor impacts of AI or analytics on children's outcomes.	Educational platforms; healthcare providers for minors; children's device manufacturers

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
ELSA-027	**Genetic and biometric data — general**	*Genetic data is inherently identifying and may affect not only individuals but also their families or broader genetic groups. High and often irreversible re-identification risk. Potential misuse for surveillance, profiling, or discrimination. Unequal representation in genomic datasets leading to biased research outcomes.*	Apply strict necessity and proportionality tests before processing or sharing. Use tiered or controlled access models such as data enclaves and secure research environments rather than open sharing. Apply enhanced de-identification and small-group protection measures. Include group-level risk assessment — not only individual-level DPIA — especially for identifiable communities. Engage affected communities in governance and consent models. Ensure datasets are diverse and representative while avoiding overexposure of small populations.	Biobanks; genomics research organisations; biometric authentication providers; healthcare organisations; AI developers using biometric data
ELSA-028	**Genetic and biometric data — forensic genetic genealogy (FIGG)**	*Forensic investigative genetic genealogy poses distinct risks: disproportionate impact on communities overrepresented in law enforcement databases; risk of misidentification from partial matches; cross-border data use without clear jurisdictional safeguards; risk of unexpected or distressing identification outcomes for families; cultural and religious sensitivities around human remains.*	Limit FIGG (Forensic investigative genetic genealogy) use to investigations of serious crime only where other investigative avenues have been exhausted, and to humanitarian identification purposes. Require judicial authorisation before use. Restrict to opt-in genealogy databases with explicit, informed consent for law enforcement access. Ensure sensitive family notification protocols including trained professionals and psychosocial support. Minimise data use and avoid unnecessary retention of genealogical trees or inferred relationships.	Law enforcement; forensic genetics laboratories; genealogy database operators; biobanks subject to law enforcement access requests
ELSA-030	**Research and academic use**	*Risk that research benefits are unevenly distributed across populations. Underrepresentation of certain groups leads to biased or non-generalisable findings. Risk of extractive research practices where communities contribute data without receiving any return of benefits or results.*	Ensure inclusive and representative dataset design by actively identifying and addressing gaps. Implement FAIR data principles responsibly — for sensitive data use controlled access rather than full openness. Establish benefit-sharing or feedback mechanisms such as return of results and public summaries. Apply ethics review processes that include social and group-level impacts rather than only legal compliance. Respect cultural and contextual sensitivities in data use. Monitor research outcomes for differential impacts across populations.	Universities; research institutes; public health bodies; statistical offices; research data repositories
ELSA-031	**SME data holders**	*Limited financial, technical, and legal capacity of micro and small enterprises to understand and implement complex data governance requirements. Risk of over-reliance on exemptions leading to weaker protection in practice. Vulnerability to unfair contractual terms due to limited bargaining power.*	Provide simplified, SME-tailored compliance tools including templates, checklists, and standard policies. Use standardised contracts to avoid complex negotiations. Prioritise proportionate compliance focusing on high-risk data processing. Offer shared or external support such as sectoral DPO services and compliance helpdesks. Include	Microenterprises; small enterprises; startups; small manufacturers of connected devices; small service providers

ELSA ID	Cluster / Scenario	Consideration / Risk	Best Practice	Addressee
			internal checks to ensure exemptions are correctly applied and not used to bypass essential safeguards. Include advisory support or ombudsperson mechanisms for SMEs facing unfair conditions.	
ELSA-032	**Non-EU actors entering EU data spaces**	*Risk of uneven protection standards across jurisdictions. Exposure to conflicting legal obligations between third-country government access requirements and EU safeguards. Barriers to participation for smaller non-EU actors due to complexity of EU requirements.*	Ensure clear internal alignment with EU data protection standards regardless of local legal requirements. Designate knowledgeable EU-based representatives with real oversight capacity. Implement internal policies to assess and respond to third-country government access requests in line with EU safeguards. Provide transparent information to EU users about data processing locations and applicable safeguards. Conduct jurisdictional risk assessments for transfers and access scenarios.	Non-EU companies entering EU data spaces; non-EU data intermediaries; non-EU AI developers serving EU market
ELSA-033	**AI training data supply**	*Training data may reflect historical inequalities creating risk of amplifying gender stereotypes and intersectional discrimination. Multiple actors create unclear responsibility for bias and harm.*	Conduct a Sex and Gender Impact Assessment (SGIA) — assess gender representation and bias risks, identify structural inequalities embedded in datasets, and go beyond binary gender categories. Define strict purpose limitation and usage controls in data supply agreements. Enhance transparency and documentation of data governance choices throughout the supply chain. Apply Gender Audit Tool principles to the full data lifecycle.	Data holders supplying AI training datasets; AI system providers
ELSA-034	**AI training data supply**	*Risk that supplied data embeds or amplifies existing biases. Underrepresentation of certain groups in training data affects system performance and fairness. Limited transparency for data subjects on secondary use of their data for AI.*	Document dataset composition, provenance, and known limitations using standardised formats such as datasheets and model cards. Perform bias and representativeness testing before supplying data. Apply data minimisation and exclude unnecessary sensitive data. Use special category data only as a last resort with enhanced safeguards.	Data holders supplying AI training datasets; AI system providers
ELSA-035	**AI training data supply**	*Data contributors often do not benefit from the AI systems built on their data. Harmful or unintended uses of supplied data may occur beyond the original supply agreement. Affected stakeholders have no mechanism to raise concerns or receive feedback.*	Include clear restrictions and permitted uses in data sharing agreements for AI training, particularly for high-risk AI. Implement traceability mechanisms linking training data to model outputs. Monitor downstream use and impacts where possible. Enable feedback or complaint mechanisms for affected stakeholders. Include provisions to prevent harmful or unintended uses.	Data holders with ongoing AI data supply relationships; AI system providers

APPENDIX C: LDTM COMPLETE QUESTION SET

Logical Decision Tree Model – Complete Question Set with Legislative Definitions

This document sets out all questions in the Logical Decision Tree Model as properly formulated sentences, together with all answer options and their legislative definitions. It serves as the textual layer of the LDTM. Legislative definitions are drawn from: Regulation (EU) 2023/2854 (Data Act); Regulation (EU) 2022/868 (Data Governance Act – DGA); Regulation (EU) 2016/679 (GDPR); Regulation (EU) 2024/1689 (AI Act). Where no single definition exists in the legislation, the characterisation is drawn from the relevant provisions and the established interpretive framework.

SECTION 1 – IDENTIFYING YOUR ORGANISATION

Questions in this section establish your role, your organisation's size, and your EU establishment status. These answers determine which instruments apply to you and whether any exemptions are available.

Q1. What best describes the primary role of your organisation in relation to data?

Select the single role that most accurately describes why you are using this tool. If your organisation performs multiple roles – for example, you are both a data holder and a data intermediary – please complete the tool separately for each role.

→ **Data holder (private sector)** *(Data Act Art. 2(6))*

A natural or legal person who has the right or obligation, in accordance with applicable Union or national law, access control, or contractual arrangements, to make available data that was obtained or generated during the provision of a related service or in the course of carrying out their activities, and who makes that data available. Private sector data holders are subject to the full data sharing framework of the Data Act (Chapters II, III and IV) and the GDPR where personal data is involved.

⚑ *If you select this option, you will be asked Q1a to clarify your specific private sector activity.*

→ **Data holder (public sector body)** *(DGA Art. 2(18), Data Act Art. 2(7), Art. 17)*

A State, regional or local authority, a body governed by public law, or an association formed by one or more such authorities or bodies, that holds data generated in the exercise of its public tasks. Public sector data holders are primarily subject to DGA Chapter II obligations regarding re-use of protected public sector data and may also be subject to the Data Act's exceptional need provisions (Chapter V).

→ **Data intermediary / data space operator** *(DGA Art. 2(11), Art. 10)*

A provider of data intermediation services – meaning services that aim to establish commercial relationships for the purposes of data sharing between data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the exercise of the rights of data subjects in relation to their personal data. This includes operators of data spaces, data marketplaces, data pools, and similar platforms facilitating data exchange between multiple parties.

→ **Data altruism organisation** *(DGA Art. 2(16), Art. 18)*

An entity that collects and processes data made available voluntarily by data subjects or data holders for objectives of general interest – such as scientific research purposes, improving public services, or policy-making – without seeking to make profit from such data, and that has registered or seeks to register as a recognised data altruism organisation under DGA Chapter IV.

→ **Data re-user (seeking access to public sector data)** *(DGA Art. 2(6))*

A natural or legal person seeking to re-use data held by public sector bodies under DGA Chapter II for commercial or non-commercial purposes other than the initial purpose for which the data was held. This includes researchers, companies and other organisations that apply for permission to re-use protected categories of public sector data.

→ **Provider of data processing services** *(Data Act Art. 2(8), Chapters VI and VII)*

A provider of a digital service other than an online social networking service, an online search engine, or an online intermediation platform, which enables on-demand administration and broad remote access to

a scalable and elastic pool of shareable computing resources of a centralised, distributed or highly distributed nature – including cloud and edge computing services. Such providers are subject to specific international data transfer restrictions and switching obligation requirements under the Data Act.

→ **Data recipient / user of connected product data** *(Data Act Art. 2(10), Art. 4(13), Art. 5(8))*

A natural or legal person that receives data from a data holder under the Data Act framework – either as a user of a connected product (a person who has purchased, rented or leased a connected product or received a related service) exercising their access rights, or as a third party to whom the data holder makes data available under Art. 5. Data recipients are subject to specific obligations under the Data Act, including a prohibition on using data received to develop competing products (Art. 4(13)), an obligation to delete data when no longer needed, and restrictions on re-sharing data with further parties.

Q1a. Which of the following most accurately describes your organisation's activity as a private sector data holder?

This question appears only if you selected "Data holder (private sector)" at Q1. Your answer affects which specific Data Act obligations apply to you.

→ **Manufacturer or provider of connected products** *(Data Act Art. 2(5))*

An organisation that manufactures or provides a connected product – meaning a physical object whose primary function does not depend solely on data processing, but which is capable of communicating data via electronic communications networks, including via the internet. Examples include manufacturers of smart home devices, industrial IoT equipment, medical devices, vehicles, and consumer electronics.

→ **Provider of related services** *(Data Act Art. 2(4))*

An organisation that provides a digital service, including software, which is connected to the connected product at the time of purchase, rent or lease, and whose absence would prevent the connected product from performing one or more of its functions, or which is subsequently connected to the connected product by the manufacturer or provider and whose function is to collect and process data generated by the connected product.

→ **Private sector data holder in another capacity** *(Data Act Art. 2(6), general)*

An organisation that holds data generated during the course of its activities – not as a connected product manufacturer or related service provider – but which may be subject to the Data Act's contractual fairness, B2G exceptional need, or interoperability provisions, or to the GDPR and AI Act as a controller or processor.

Q1b. In addition to your primary role, does your organisation also act as a data processor – processing personal data strictly on behalf of and under the instructions of another organisation (a controller), without determining the purposes or means of that processing yourself?

This question is shown to all users. Many organisations are simultaneously controllers for some data and processors for other data. For example, a data space operator is a controller for its own governance data but may act as a processor for personal data it handles on behalf of its participants. A cloud provider is typically a processor for its customers' data. Answering Yes will cause processor-specific obligations – particularly around data processing agreements, security measures, and liability – to be included in your output alongside the obligations relevant to your primary role.

→ **Yes – my organisation also acts as a data processor for another controller** *(GDPR Art. 4(8), Art. 28, Art. 29, Art. 32)*

A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors must only process data on documented instructions from the controller, must ensure persons authorised to process data are bound by confidentiality, must implement appropriate technical and organisational security measures, must assist the controller in fulfilling data subject rights and DPIA obligations, must delete or return data upon termination of services, and must make available all information necessary to demonstrate compliance. Processing without a controller's instructions or beyond them constitutes acting as a controller for those purposes, with the associated full controller liability.

⚑ *If Yes, processor-specific obligations under GDPR Art. 28 (data processing agreement), Art. 29 (processing on instructions), Art. 32 (security), and Art. 82 (liability) will be flagged in your output.*

→ **No – my organisation determines the purposes and means of all its data processing** *(GDPR Art. 4(7))*

Your organisation acts solely as a controller – it determines why and how personal data is processed. Controller obligations under the GDPR apply in full. No additional processor-specific flags will be added to your output.

Q2. What is the size of your organisation?

Organisation size determines whether the Data Act Chapter II exemption for micro and small enterprises applies. Calculate size on the basis of staff headcount and either annual turnover or annual balance sheet total as defined in Commission Recommendation 2003/361/EC. Where your organisation is part of a group, see Q2a below before answering.

→ **Microenterprise** *(Commission Recommendation 2003/361/EC, Art. 2(3))*

An enterprise that employs fewer than 10 persons and whose annual turnover or annual balance sheet total does not exceed EUR 2 million.

→ **Small enterprise** *(Commission Recommendation 2003/361/EC, Art. 2(2))*

An enterprise that employs fewer than 50 persons and whose annual turnover or annual balance sheet total does not exceed EUR 10 million.

→ If you select micro or small enterprise, you will be asked Q2a about linked enterprises before the exemption is confirmed.

→ **Medium enterprise** *(Commission Recommendation 2003/361/EC, Art. 2(1))*

An enterprise that employs fewer than 250 persons and whose annual turnover does not exceed EUR 50 million or whose annual balance sheet total does not exceed EUR 43 million. Medium enterprises are not exempt from Data Act Chapter II obligations.

→ **Large enterprise** *(Commission Recommendation 2003/361/EC, Art. 2(1), by exclusion)*

An enterprise that exceeds the thresholds for medium enterprises – i.e. employs 250 or more persons, or has an annual turnover exceeding EUR 50 million and a balance sheet total exceeding EUR 43 million. Large enterprises are subject to all applicable obligations.

→ **Public sector body** *(Not subject to SME size thresholds)*

Size thresholds for private enterprises do not apply to public sector bodies. Select this option if you identified as a public sector data holder at Q1.

Q2a. Is your organisation linked to or partnered with one or more other enterprises in a way that would affect the calculation of your size?

This question appears only if you selected micro or small enterprise at Q2. Under EU SME rules, enterprises that are not independent – because they are owned by or have significant stakes in other enterprises – must aggregate their data with those enterprises when calculating size. An enterprise is "linked" if another enterprise holds more than 50% of its capital, voting rights, or can exercise dominant influence. It is a "partner enterprise" if another enterprise holds between 25% and 50%.

→ **Yes – my organisation has linked or partner enterprises** *(Commission Recommendation 2003/361/EC, Art. 3)*

If yes, your size must be recalculated by adding the headcount and financial figures of all linked enterprises (100%) and partner enterprises (proportionate share). This may mean you exceed the micro or small enterprise thresholds and therefore do not qualify for the Data Act Chapter II exemption.

⚑ *If Yes and recalculation takes you above the small enterprise threshold, the Data Act Chapter II SME exemption does NOT apply to your organisation. Proceed to Q2b.*

→ **No – my organisation is independent** *(Commission Recommendation 2003/361/EC, Art. 3(1))*

Your organisation has no linked or partner enterprises, or any shareholding relationships fall below the 25% threshold. Your size classification at Q2 stands.

⚑ *If No, proceed to Q2b.*

Q2b. Does your organisation carry out more than 25% of its activities as a subcontractor for one or more enterprises that are not themselves micro or small enterprises?

This question appears only if you answered No at Q2a. Even an independent enterprise may lose its SME status if it primarily works as a subcontractor for large enterprises, unless this reflects a normal market relationship.

→ **Yes – more than 25% of activities are subcontracted from larger enterprises** *(Commission Recommendation 2003/361/EC, Art. 3(2))*

If yes, your organisation may not qualify as an independent SME for the purposes of the Data Act exemption, depending on whether this reflects a normal market relationship. Seek legal advice on your specific situation.

⚑ *If Yes, the Data Act Chapter II SME exemption may NOT apply. Treat your organisation as a medium enterprise for the purposes of this tool and proceed accordingly.*

→ **No – less than 25% of activities are subcontracted from larger enterprises** *(Commission Recommendation 2003/361/EC, Art. 3(2))*

Your organisation qualifies as an independent micro or small enterprise. The Data Act Chapter II exemption applies to your connected product data sharing obligations.

⚑ *If No, the Data Act Chapter II SME exemption APPLIES. The tool will flag which obligations do not apply to you on that basis.*

Q3. Is your organisation established in the European Union, or does it offer products or services within the EU?

This question determines whether EU data law applies to your organisation at all, and whether you need to designate an EU legal representative. "Established" means having a stable arrangement – such as a registered office, branch, or subsidiary – in the EU through which you carry out a real and effective activity.

→ **Yes – my organisation is established in the EU** *(GDPR Art. 3(1); Data Act Art. 1(4); DGA Art. 1(2))*

Your organisation has a registered office, branch, or effective place of business in one or more EU Member States. All applicable obligations under the Data Act, DGA, GDPR and AI Act apply directly to your organisation.

→ **No – my organisation is not established in the EU, but it offers products or services in the EU, or processes data of persons located in the EU** *(GDPR Art. 3(2); Data Act Art. 1(4), Art. 37(10); DGA Art. 11(3))*

Non-EU organisations may still fall within the territorial scope of EU data law where they offer goods or services to persons in the EU, or monitor the behaviour of persons in the EU (GDPR), or make connected products or related services available in the Union (Data Act), or provide data intermediation or altruism services within the Union (DGA). Such organisations are generally required to designate a legal representative established in the EU.

⚑ *If your organisation is not EU-established but falls within scope, additional obligations regarding legal representative designation will be flagged in your output.*

→ **No – my organisation has no connection to the EU** *(GDPR Art. 3; Data Act Art. 1(4))*

If your organisation is not established in the EU and does not offer products or services in the EU, and does not process data of persons in the EU, EU data law does not apply. This tool is not relevant to your situation.

SECTION 2 – CHARACTERISING YOUR DATA

Questions in this section establish the nature of the data your organisation holds or processes. You may answer Yes to more than one question in this section. Each Yes answer activates a corresponding set of requirements in your output.

Q4. Does your organisation process, hold, or intend to share personal data – that is, data relating to an identified or identifiable natural person?

Answer Yes if any of the data your organisation handles relates to a natural person who can be identified directly or indirectly – for example, through a name, identification number, location data, online identifier, or factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. This includes pseudonymised data that can be re-identified using a key held by your organisation or another party.

→ **Yes**

If Yes, Q4a through Q4d will ask about specific categories of personal data that attract heightened obligations. You will also be asked about your lawful basis for processing at the relevant output stage.

→ **No**

If No, GDPR obligations do not apply to this data. Proceed to Q5.

Q4a. Does the personal data include health data, or data concerning the physical or mental health of a natural person?

This question appears only if you answered Yes at Q4. Health data is a special category of personal data subject to a prohibition on processing under GDPR Art. 9(1), unless one of the exceptions in Art. 9(2) applies.

→ **Yes – data concerning physical or mental health** *(GDPR Art. 4(15), Art. 9(1))*

Health data means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveals information about their health status. This includes medical records, diagnostic data, biometric health readings, mental health assessments, psychiatric disorder data, disability data, and data from wearables or monitoring devices measuring health parameters.

→ **No**

Q4b. Does the personal data include data concerning children – that is, persons under the age of 18?

This question appears only if you answered Yes at Q4. Processing personal data of children attracts specific obligations regarding consent, transparency and age verification. A child is any person under 18 years of age, unless Member State law sets a lower age of digital consent (minimum 13 years).

→ **Yes – data concerning persons under 18** *(GDPR Art. 8(1-2), Art. 12(1))*

Where the processing of personal data of a child is based on consent for information society services, the consent must be given or authorised by the holder of parental responsibility over the child where the child is under 16 years of age (or a lower age set by Member State law, with a minimum of 13 years). Additional obligations apply regarding transparency – notices must be written in a clear and plain language that the child can understand. The special category prohibition in GDPR Art. 9(1) may also apply where the child's data reveals health, genetic or other special category information.

→ **No**

Q4c. Does the personal data include genetic data, biometric data processed for the purpose of uniquely identifying a person, or data concerning a person's racial or ethnic origin, political opinions, religious beliefs, trade union membership, or sex life or sexual orientation?

This question appears only if you answered Yes at Q4. These are the remaining special categories of personal data under GDPR Art. 9 not covered by Q4a. All attract the same heightened prohibition and exception framework.

→ **Yes – one or more of these special categories** *(GDPR Art. 4(13-14), Art. 9(1-2); AI Act Art. 10(5))*

Special categories of personal data under GDPR Art. 9(1) are: data revealing racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data processed for the purpose of uniquely identifying a natural person; data concerning health (see Q4a); and data concerning a natural person's sex life or sexual orientation. Processing is prohibited unless one of the exceptions in Art. 9(2) applies, including explicit consent, vital interests, public interest, or – for AI systems – the specific conditions in Art. 10(5) of the AI Act.

→ **No**

Q4d. Does the personal data include data relating to criminal convictions, offences, or related security measures?

This question appears only if you answered Yes at Q4. Data relating to criminal convictions and offences is subject to a separate, stricter restriction under GDPR Art. 10 – it may only be processed under the control of official authority, or when authorised by Union or Member State law.

→ **Yes – data relating to criminal convictions or offences** *(GDPR Art. 10)*

Personal data relating to criminal convictions and offences or related security measures may only be processed under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Unlike the special categories in Art. 9, there is no list of exceptions – the legal basis must come from law.

→ **No**

Q5. Does any of the data your organisation holds or intends to share qualify as a trade secret?

Answer Yes if any data your organisation holds has commercial value precisely because it is secret, and your organisation takes reasonable steps to keep it confidential. If you are uncertain whether particular data qualifies, err on the side of Yes and the tool will guide you through the relevant identification and protection obligations.

→ **Yes – the data includes trade secrets** *(Directive (EU) 2016/943 Art. 2(1); Data Act Art. 4(6), Art. 5(9-11))*

A trade secret is information that: (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with this kind of information; (b) has commercial value because it is secret; and (c) has been subject to reasonable steps by the person lawfully in control of it to keep it secret. Trade secret protection under the Data Act does not override obligations to share data, but data holders may require confidentiality agreements and may withhold data if adequate measures cannot be agreed.

→ **No**

Q6. Does the data your organisation holds or intends to re-use originate from a public sector body, or is it data held by a public sector body that you wish to access?

Answer Yes if you are seeking to access data held by public sector bodies under the DGA Chapter II framework, or if data you already hold was obtained from a public sector body under that framework and is subject to conditions of re-use.

→ **Yes – the data originates from or is held by a public sector body** *(DGA Art. 3(1), Art. 2(18))*

DGA Chapter II applies to re-use of data held by public sector bodies that is protected on grounds of: commercial confidentiality (including business, professional or company secrets); statistical confidentiality; protection of intellectual property rights of third parties; or protection of personal data. Data that is freely available – such as open data published without restrictions – is not subject to the DGA Chapter II re-use conditions.

⚑ *If Yes, DGA Chapter II obligations will be included in your output – both the conditions imposed on public sector bodies and the obligations on you as a re-user. This applies whether you are actively seeking access (also answer Yes at Q10) or already hold data obtained under DGA Chapter II re-use conditions. Confidentiality obligations, third-country transfer notification requirements, and the DGA scope gate will all be triggered.*

→ **No**

Q7. Is the data generated by or through a connected product or related service – for example, a smart device, industrial IoT sensor, vehicle, wearable, or similar object capable of collecting and communicating data?

Answer Yes if any of the data your organisation holds was generated by a physical product capable of communicating data via electronic communications networks, including via the internet. The Data Act specifically governs access to data generated by connected products and the right of users to access such data.

→ **Yes – data generated by or through a connected product or related service** *(Data Act Art. 2(5), Art. 3, Art. 4)*

A connected product is a physical object whose primary function does not depend solely on data processing, but which is capable of communicating data via electronic communications networks – including via the internet – either autonomously or by being activated by the user, and whose primary purpose is not the storage, processing, transmission, display, playback or communication of data. Examples include: smart home devices, industrial machinery with embedded sensors, connected vehicles, medical devices, wearable technology, agricultural IoT equipment, and energy meters. The Data Act establishes the right of users of connected products to access data generated by those products and to have it shared with the data holder and authorised third parties.

→ **No**

SECTION 3 – YOUR INTENDED ACTIVITIES

Questions in this section ask about what your organisation intends to do with data. Unlike Section 1, these questions are independent of each other – you may answer Yes to several. Each Yes answer activates the corresponding set of obligations in your output.

Q8. Does your organisation intend to enter, participate in, or operate as part of a data space or data ecosystem – that is, an environment in which data is shared or exchanged between multiple participants according to common rules?

Answer Yes if your organisation is entering any multi-party data sharing arrangement with common governance, technical standards, or contractual frameworks – regardless of whether it is formally called a "data space". This includes sector-specific data spaces (health, agriculture, energy, mobility, financial), cross-sector industrial data platforms, and data pooling arrangements.

→ **Yes – my organisation participates in or operates a data space** *(Data Act Art. 2(13), Art. 28, Art. 33-35)*

A data space is a decentralised data sharing environment built on common standards, policies and governance frameworks that enables trustworthy data exchange between participating organisations. Participants in data spaces may act simultaneously as data holders (contributing data), data users (consuming data), and data intermediaries (facilitating exchange). The Data Act (Art. 28 et seq.) establishes interoperability requirements for data spaces and requires data processing services to enable switching between providers.

→ **No**

Q9. Does your organisation intend to share data with one or more third parties on a commercial basis – that is, to make data available to another company or organisation under a contractual arrangement?

Answer Yes if your organisation intends to sell, license, or otherwise provide data to another private sector entity under a contract. This includes both direct B2B data sharing and data sharing as part of a supply chain, outsourcing arrangement, or commercial partnership.

→ **Yes – my organisation shares or intends to share data commercially with third parties** *(Data Act Art. 8-13, Art. 4(1), Art. 5(1))*

B2B data sharing under the Data Act covers the sharing of data between undertakings for commercial purposes under contractual terms. The Data Act establishes FRAND conditions (fair, reasonable and non-discriminatory) for access terms and pricing, prohibits unfair contractual terms, and requires data holders to not discriminate between comparable data recipients. The GDPR applies in full where shared data includes personal data.

If Yes, Q9a will ask whether smart contracts are used in your data sharing arrangements.

→ **No**

Q9a. Does your organisation use, or intend to use, smart contracts to automate any aspect of your data sharing or data space participation arrangements – for example to automate access conditions, payment, or data deletion upon expiry of a sharing agreement?

This question appears if you answered Yes at Q8 or Q9. Smart contracts used in data sharing contexts are subject to specific essential requirements under the Data Act. A smart contract in this context is a computer program stored on a digital ledger (such as a blockchain) used to automate the execution of data sharing agreements.

→ **Yes – my organisation uses or intends to use smart contracts in data sharing** *(Data Act Art. 36(1-3))*

A smart contract used for data sharing must satisfy the following essential requirements under Data Act Art. 36: robustness and fault-tolerance (able to function safely despite errors); safe termination and interruption mechanisms (the deployer must be able to terminate or interrupt the contract to avoid unintended consequences); data archiving and continuity (data and instructions must be retained in the event of termination); access control (strict access management and audit trails); and use of open interoperability standards where applicable. Vendors and deployers of smart contracts used for data sharing must be able to demonstrate compliance with these requirements.

→ **No – my organisation does not use smart contracts** *(Data Act Art. 36 – not applicable)*

Smart contract essential requirements under Data Act Art. 36 do not apply. Data sharing arrangements are governed by standard contractual obligations under the FRAND and contractual fairness provisions of the Data Act.

Q10. Does your organisation intend to request access to, or re-use, data held by a public sector body – for example for research, product development, or other commercial or non-commercial purposes?

Answer Yes if your organisation is seeking to obtain and use data from a government body, public authority, or other public sector entity, where that data is not already available as open data.

→ **Yes – my organisation seeks to access or re-use public sector data** *(DGA Art. 3-9)*

DGA Chapter II establishes the framework for re-use of data held by public sector bodies that is protected on grounds of commercial confidentiality, statistical confidentiality, intellectual property rights of third parties, or personal data protection. Re-users must apply to the relevant public sector body, which may impose conditions on re-use including technical requirements, confidentiality obligations, and fees. The DGA explicitly prohibits public sector bodies from granting exclusive re-use rights to single parties.

→ **No**

Q11. Does your organisation intend to supply data for use in the development, training, validation or testing of an AI system – or does your organisation itself develop an AI system using data held by your organisation or obtained from others?

→ **Yes – my organisation supplies data for AI development or develops AI systems using data** *(AI Act Art. 3(1), Art. 10; Annex III)*

AI system means a machine-based system designed to operate with varying levels of autonomy that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers from the input it receives how to generate outputs such as predictions, content, recommendations, or decisions, that can influence physical or virtual environments. Where an AI system is classified as high-risk under Annex III of the AI Act, Art. 10 imposes specific data governance obligations on training, validation and testing datasets – including quality standards, representativeness requirements, bias assessment and, where strictly necessary, the use of special category data for bias detection and correction.

⚑ If Yes, Q16 in Section 4 will ask whether the AI system is classified as high-risk, which determines whether AI Act Art. 10 applies.

→ **No**

Q12. Does your organisation provide, or intend to provide, data intermediation services – that is, services that facilitate the exchange of data between data holders and data users, without itself acquiring rights to use the data?

Answer Yes if your organisation operates or plans to operate as a neutral third-party facilitating data exchange between two or more parties, acting in the interests of both sides of the exchange without itself acquiring rights to use the data for its own purposes. This covers data marketplaces, personal data stores, data brokerages operating in a neutral capacity, and data space operators providing intermediation as their primary service.

Answer No if your arrangement falls into one of the following categories, which are excluded from the DGA Chapter III regime: (i) services used exclusively by a single data holder to enable the use of its own data; (ii) closed-group sharing arrangements where all participants belong to the same legal group or where the data holder is also the data user; (iii) services whose primary function is to process, enrich, or add substantial value to data rather than to facilitate its exchange between independent parties; or (iv) services provided in the context of open data or government-to-public data publication, which are governed by separate frameworks.

→ **Yes – my organisation provides or intends to provide data intermediation services** *(DGA Art. 2(11), Art. 10-15)*

> Data intermediation services means services that aim to establish commercial relationships for the purposes of data sharing between data subjects and data holders on the one hand and data users on the other, through technical, legal or other means, including for the exercise of the rights of data subjects. This explicitly excludes: services where data is obtained from data holders and aggregated, enriched or transformed to create a derived product sold to users (these are data brokers, not intermediaries); services where data is obtained for the purpose of being used for news media; and data altruism services covered by DGA Chapter IV. Providers of data intermediation services must notify the competent authority and comply with the conditions in DGA Art. 12.

→ **No**

Q13. Does your organisation collect data made available voluntarily by individuals or companies for purposes of general interest – such as scientific research, improving public services, or public health – on a not-for-profit basis, and does it seek or hold registration as a data altruism organisation?

→ **Yes – my organisation is or seeks to become a recognised data altruism organisation** *(DGA Art. 2(16), Art. 18-23)*

> Data altruism means the voluntary sharing of data by data subjects and data holders, based on consent or permission, for objectives of general interest without seeking a reward that goes beyond compensation for the costs they incur when making their data available. A recognised data altruism organisation must be established as a not-for-profit entity, carry out data altruism activities as its primary objective, register in the Union register of recognised data altruism organisations, and comply with the governance and transparency conditions in DGA Art. 18-23.

→ **No**

Q14. Has your organisation received, or does it expect to receive, a request from a public sector body, the Commission, the European Central Bank, or a Union body to make data available on grounds of exceptional need – for example to respond to a public emergency, prevent a public emergency, or assist in recovery from a natural disaster?

Answer Yes only if you have received or anticipate a formal request invoking the Data Act's exceptional public interest mechanism. This is a specific legal procedure distinct from ordinary public procurement or data purchase requests.

→ **Yes – my organisation has received or expects a B2G exceptional need data request** *(Data Act Art. 15-20)*

Under Data Act Chapter V, public sector bodies, the Commission, the European Central Bank and Union bodies may request data holders to make data available where there is an exceptional need – defined as a public emergency (such as a public health emergency, major natural disaster, or serious cybersecurity incident), or where data is needed to fulfil a specific task carried out in the public interest and cannot reasonably be obtained in a timely manner through normal channels. The request must specify the legal basis, the data requested, and the purpose. Data holders may not use the data for other purposes and must receive fair compensation. The obligation to share does not require disclosure of trade secrets beyond what is strictly necessary.

→ **No**

SECTION 4 – ADDITIONAL CONTEXT

Questions in this section capture cross-cutting factors that activate specific additional obligations regardless of your primary role or activity. These questions apply to all actor types.

Q15a. Does your organisation transfer personal data to a recipient located outside the European Union or the European Economic Area, or does it use processors or sub-processors established outside the EU or EEA to process personal data on its behalf?

This question applies only if you answered Yes to Q4 (personal data). If you answered No to Q4, proceed to Q15b. Answer Yes if any of the following apply:

You send, transmit, or otherwise make personal data accessible to an entity, whether a controller, processor, or sub-processor, that is established in a country outside the EU or EEA, regardless of the technical means used

You use cloud services, IT infrastructure, or data processing services provided by an entity established outside the EU or EEA, where personal data is processed on that infrastructure

Personal data you hold is accessible to or retrievable by a non-EU or non-EEA entity, even if it is not formally "sent" to that entity

You facilitate onward transfers of personal data – that is, personal data received from an EU entity is further transferred to a non-EU recipient

Answer No if all recipients, processors, and sub-processors involved in the processing of personal data are established within the EU or EEA, and no personal data is accessible to entities outside the EU or EEA.

→ **Yes – my organisation transfers or intends to transfer personal data to a recipient outside the EU/EEA, or uses non-EU/EEA processors or sub-processors (GDPR Art. 44–49)**

International transfers of personal data are governed by GDPR Chapter V. A transfer may only take place where one of three conditions is met. First, the European Commission has adopted an adequacy decision in respect of the destination country or territory (Art. 45). Second, where no adequacy decision exists, the transfer may proceed where appropriate safeguards are in place, including standard contractual clauses adopted by the Commission, binding corporate rules approved by a supervisory authority, or an approved certification mechanism with binding enforceable commitments (Art. 46). Third, in the absence of both an adequacy decision and appropriate safeguards, a transfer may only take place on the basis of one of the narrow derogations in Art. 49 –such as explicit informed consent of the data subject, necessity for the performance of a contract, or important reasons of public interest – and these derogations may not be used for repetitive, large-scale, or structural transfers. Regardless of the transfer mechanism used, the data exporter remains responsible for ensuring the level of protection guaranteed by the GDPR is not undermined in the third country.

→ **No – all personal data processing takes place within the EU/EEA**

15b. Does your organisation store, process, or make available non-personal data using infrastructure or service providers that are subject to the laws, regulations, or binding judicial or administrative orders of a non-EU country?

This question applies to all actors regardless of your answer to Q4. Answer it independently of Q15a. Answer Yes if any of the following apply:

- You use cloud computing services, data processing services, or storage infrastructure provided by a company incorporated in or operationally subject to the jurisdiction of a non-EU country, even if the servers are physically located within the EU
- You are aware that a non-EU government, court, or administrative authority has issued or could issue a binding order requiring access to non-personal data you hold or that is held on your behalf
- You have received a request from a non-EU governmental authority for access to or transfer of non-personal data held in the Union
- Your data processing service provider has disclosed that it is or may be subject to non-EU governmental access obligations

Answer No only if your non-personal data is stored and processed exclusively on infrastructure provided by entities subject solely to EU or EEA jurisdiction and you have no indication of exposure to non-EU governmental access requests.

→ **Yes – my organisation uses infrastructure subject to non-EU jurisdiction or has been or may be subject to third-country governmental access requests for non-personal data (Data Act Art. 27–32; DGA Art. 31)**

International transfers of and governmental access to non-personal data held in the Union are governed by Data Act Articles 27 to 32 and DGA Article 31. Data processing service providers must take all reasonable technical, legal, and organisational measures to prevent the transfer of or access to non-personal data held in the EU where such transfer or access would conflict with EU or Member State law. Where a third-country court or administrative authority issues a decision requiring transfer or access, the provider must inform the requesting authority that the request conflicts with EU law and seek clarification before complying. Compliance is only permissible where the third-country legal system requires it, the request is not broader than necessary, the data subject or data holder has been given advance notice where possible, and the competent supervisory authority in the Member State has been notified. Data holders and data space participants should ensure that their contractual arrangements with data processing service providers include explicit provisions addressing third-country governmental access risks.

Note: If you have received or anticipate a specific governmental access request from a non-EU authority, also answer Yes to Q18.

→ **No – all non-personal data is stored and processed on infrastructure subject solely to EU or EEA jurisdiction**

Q16. Is the AI system for which you are supplying data, or which you are developing, classified or likely to be classified as a high-risk AI system under Annex III of the EU AI Act?

This question appears only if you answered Yes at Q11. High-risk AI systems attract the full data governance obligations of AI Act Art. 10. If you are uncertain whether your system qualifies, the key categories are listed below.

→ **Yes – the AI system is or is likely to be classified as high-risk** *(AI Act Art. 6, Annex III, Art. 10)*

High-risk AI systems are those listed in Annex III of the AI Act, covering systems used in: biometric identification and categorisation of natural persons; management and operation of critical infrastructure; education and vocational training; employment and workers management; access to essential private and public services including health and social benefits; law enforcement; migration, asylum and border control management; and administration of justice and democratic processes. Systems that are safety components of regulated products (medical devices, machinery, vehicles) may also be high-risk. Where a system is high-risk, AI Act Art. 10 imposes mandatory data governance requirements on training, validation and testing datasets.

→ **No – the AI system is not high-risk or does not fall within Annex III categories** *(AI Act Art. 6)*

AI systems that are not classified as high-risk are not subject to AI Act Art. 10 data governance requirements. However, GDPR obligations continue to apply in full where the training data includes personal data.

→ **Uncertain – I am not sure whether the AI system qualifies as high-risk** *(Seek legal advice on Annex III classification)*

⚑ *If Uncertain, the output will present the AI Act Art. 10 obligations as conditional – applicable if the system is later classified as high-risk.*

Q17. Is the purpose for which your organisation processes or intends to use the data a scientific research, statistical, archiving in the public interest, or historical research purpose?

Answer Yes if the primary purpose of your data processing activity is research or archiving, as these purposes attract specific derogations from certain GDPR obligations – particularly data minimisation, storage limitation, and the prohibition on processing special categories of data.

→ **Yes – the purpose is scientific research, statistics, public interest archiving, or historical research** *(GDPR Art. 89(1-3), Art. 9(2)(j))*

> GDPR Art. 89(1) permits derogations from certain data subject rights (access, rectification, restriction, objection) for processing carried out for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, subject to appropriate safeguards such as pseudonymisation. GDPR Art. 9(2)(j) permits processing of special category data for scientific or historical research or statistical purposes where it is necessary and subject to Art. 89(1) safeguards. These derogations must be implemented through Union or Member State law.

→ **No**

Q18. Has your organisation received, or does it anticipate receiving, a request from a government authority of a non-EU country requiring access to or transfer of data held by your organisation?

Answer Yes if a foreign government authority, court, regulator, or law enforcement agency – outside the EU/EEA – has made or may make a formal request for access to or disclosure of data your organisation holds.

→ **Yes – my organisation has received or anticipates a third-country governmental access request** *(GDPR Art. 48; Data Act Art. 32; DGA Art. 31)*

> Where a third-country court or administrative authority issues a decision requiring access to or transfer of personal data held in the EU, that decision is only recognised or enforceable if based on an international agreement – such as a mutual legal assistance treaty – between the requesting country and the EU or the relevant Member State (GDPR Art. 48). For non-personal data, Data Act Art. 32 and DGA Art. 31 require that the receiving party must not comply with the request unless it meets specific conditions, including: the third-country system provides for the establishment of grounds and proportionality of the decision; the data holder or provider notifies the data owner or controller; and only the minimum data necessary is disclosed. Compliance with a request that does not meet these conditions is prohibited.

→ **No**

End of questions.

Based on the given answers, the guidelines' user will receive a personalised compliance output across two tiers: Tier 1 (mandatory legal obligations) and Tier 2 (responsible compliance best practices based on ethical and social standards).

The output will reference the specific requirements from the D3.4 consolidated requirements database that apply to a specific combination of answers, grouped by thematic cluster and ordered by compliance tier.