DiCiM

Digitalised Value Management for Unlocking the potential of the Circular Manufacturing Systems with integrated digital solutions

D1.3 – LEGAL REQUIREMENT SPECIFICATIONS REPORT

Project 101091536

Funded by the European Union

D1.3 – Legal requirement specifications report

Project acronym:	DiCiM
Project full title:	Digitalised Value Management for Unlocking the potential of the Circular Manufacturing Systems with integrated digital solutions
Grant agreement no.:	101091536
Author/s:	Maryna Henryson (KTH); Sayyed Shoaib-ul-Hasan (KTH); Farazee Asif (KTH); Bharghav Ganesh (KTH); Md Mahmudul Hasan (KTH)
Reviewed:	Gyorgy Szemeredi (LEX); Caíque de Carvalho (CHX); Alena Klapalová (MU); Michal Krčál (MU); Mario Lorenz (TUC); Markus Wagner (C-ECO); Álvaro Fernández Cisneros (IDENER)
Approved:	Alena Klapalová (MU)
Document type:	R
Dissemination Level:	PU
Version:	V1.0
Date:	29.11.2023

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Health and Digital Executive Agency (HaDEA). Neither the European Union nor the granting authority can be held responsible for them.

Funded by the European Union

History of Changes

Version	Date	Modification reason	Modified by
V0.1	02.10.2023	Initial Draft	Maryna Henryson; Sayyed Shoaib-ul-Hasan; Farazee Asif; Bharghav Ganesh; Mahmudul Hasan
V0.2	20-10-2023	Review and feedback	All partners
V0.3	08-11- 2023	Second draft (1st revision)	Maryna Henryson; Sayyed Shoaib-ul-Hasan; Farazee Asif; Bharghav Ganesh; Mahmudul Hasan
V0.4	10-11-2023	1st Quality check	Sayyed Shoaib-ul-Hasan
V0.5	21-11-2023	2nd Review and 2nd Quality check	Alena Klapalová
V0.6	27-11-2023	3rd draft (2nd revision)	Sayyed Shoaib-ul-Hasan; Bharghav Ganesh
V1.0	29/11/2023	Final reviewed deliverable submitted	Alena Klapalová

Funded by the European Union

Table of contents

1. Executive Summary 8

2. Introduction 9

2.1. Setting the Analytical Context for Legal and Regulatory Frameworks 11
2.2. Methodology 14
2.3. Structure of the report 16

3. Regulatory frameworks impacting circular product strategies for environmental compliance 17

3.1. Waste Electrical and Electronic Equipment (WEEE) Directive 17
3.2. Restriction of Hazardous Substances (RoHS) Directive 18
3.3. Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation 19
3.4. Ecodesign Directive for Sustainable Products (ESPR) 20

3.4.1. Digital Product Passport (DPP) 24

3.5. Proposal for a regulation on circularity requirements for vehicle design and on management of end-of-life vehicles (ELV) 25
3.6. Batteries Regulation 28

4. Legal and regulatory frameworks relevant for a circular economy from data perspective 30

4.1. The Data Governance Act 30
4.2. The Data Act 31
4.3. The Digital Services Act 36
4.4. The Digital Markets Act 37
4.5. The General Data Protection Regulation (GDPR) 38
4.6. The ePrivacy Regulation 40
4.7. The Open Data Directive 41
4.8. Regulation on the Free Flow of Non-personal Data 42
4.9. NIS2 Directive on Measures for a High Common Level of Cybersecurity across the Union 43
4.10. Artificial Intelligence Act 45
4.11. Liability Digital Technologies: Product Liability Directive (PLD), New Product Liability Directive and an AI Liability Directive (AILD) 46
4.12. Summary of Legal Acts Pertaining Data Governance in the EU 47

5. Relevance of the legal and regulatory frameworks for DiCiM project demonstrators and results 51

5.1. Circularity and environmental regulations compliance 51
5.2. Open access digital platform 54

5.2.1. Sharing data across the value chain and making data public 55
5.2.2. Access to data from used products 57

5.3. IoT solution for collecting data from products 57
5.4. Technological solutions for harvesting components from used products 59
5.5. Limitations and future research 61

6. Final conclusions and recommendations 63

7. Annexes 65

Funded by
the European Union

7.1. Annex 1 Documents Reviewed 65
7.2. Annex 2 Mapping of Legislative acts and individual clauses relevant to DiCiM Development 68
7.3. Annex 3 Interview Protocol 74
8. References 76

Funded by the European Union

List of Figures

Figure 1 Smart Circular Economy framework..... 14
Figure 2 Overview of Initiatives in the Circular Economy Package and the place of Ecodesign for Sustainable Product Regulation. 21
Figure 3 . A three-part regulatory system for AI in the EU, with upstream harm prevention provided by the AI Act and downstream harm redress provided by the proposed directives..... 47

Funded by
the European Union

List of tables

Table 1 Overview of EU Data Governance Legal Acts 47
Table 2 Relevance of Individual EU Legal Acts to the DiCiM Project Scopes 51
Table 3 A Mapping of Legislative Acts Individual Clauses to DiCiM Developments 68

Funded by
the European Union

List of abbreviations

Abbreviation	*Explanation*
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
API	Application Programming Interface
AR	Augmented Reality
DA	Data Act
DGA	Data Governance Act
DMA	Digital Market Act
DPP	Digital Product Passport
DSA	Digital Services Act
ePD	ePrivacy Directive
EoL	End-of-Life
FFoD	Free Flow of Non-Personal Data Regulation
ESPR	Ecodesign Directive for Sustainable Products
GDPR	General Data Protection Regulation
HRAIS	High Risk Artificial Intelligence Systems
IoT	Internet of Things
NIS2	Network and Information Systems Directive 2
OADP	Open Access Data Platform
PLD	Product Liability Directive
REACH	Registration, Evaluation, Authorization, and Restriction of Chemicals
RoHS	Restriction of Hazardous Substances
VR	Virtual Reality
WEEE	Waste Electrical and Electronic Equipment
XR	Extended Reality

Funded by
the European Union

1. Executive Summary

DiCiM is a Horizon Europe funded project with the objective to develop and demonstrate integrated digital solutions that enable tracking, tracing, and condition monitoring of products during their use phase, optimising the reverse logistics, and enhancing the efficiency and responsiveness of operations during the value recovery phase.

This Deliverable, D1.3, reports the work performed under Task 1.3 and serves a dual purpose. Firstly, it identifies relevant legal and regulatory frameworks applicable within the European Union (EU) and the operational areas of DiCiM project demonstrators. Specifically, the report focuses on regulatory and compliance considerations pertaining to development of technological solutions for circular value management proposed in the DiCiM Grant Agreement, and identified in Task 1.1 (Deliverable 1.1 is being prepared at the time of writing this report) and Task 1.2 (Deliverable 1.2) with a particular focus on open access digital platform (for storing, analysing and sharing data), IoT solution for collecting data from products (for condition monitoring and location tracing), and technological solutions for harvesting parts/components from the used products. These technological solutions for circular value management cover two key areas from a legal and regulatory perspective: i) data related; ii) product related. The report aims to shed light on EU policy and regulatory frameworks relevant to these two areas in the context of circular manufacturing systems.

The primary objective is to equip original equipment manufacturers and producers, digital technology developers, and other stakeholders in the manufacturing sector with insights into the implications of EU regulatory frameworks and legislation in the context of circular economy. It provides an overview of relevant regulatory frameworks and acts pertaining to environmental regulations and data governance considering circular manufacturing systems.

To provide a robust foundation for analysis of the legal documents, this report draws upon a desk analysis of pertinent EU legislation sourced from Eur-Lex and the Official Journal of the European Union, and other EU databases and public sources.

This report identifies the complex regulatory landscape within the EU and its implications for IoT products, AI-based technologies, data management, and product environmental compliance and product liability. It highlights the importance of comprehensive documentation, supply chain collaboration and third part-relationship management, proactive compliance, due diligence process and systematic record-keeping, and maintaining an accurate data system inventory. Organisations must engage proactively with these regulatory changes to ensure compliance and legal risk management in an evolving digital landscape.

This report will be instrumental in recommending and informing DiCiM project's developments from a legal and regulatory perspective. It is important to mention here that this report does not provide interpretation of the law. It only aims to establish relevance of the legal and regulatory frameworks for DiCiM project. Partner companies are expected to consult their legal departments for interpretation of the law in case a legal issue arises during the project.

Funded by
the European Union

2. Introduction

This document reports the outcome of Task 1.3, titled "Legal requirement specifications" within the Work Package 1 of DiCiM project. Task 1.3 is closely intertwined with other Tasks (i.e., Task 1.1 Technical requirement specifications and Task 1.2 Business requirement specifications). The primary objectives of Task 1.3 are as follows:

- To identify the relevant legal and regulatory frameworks within the EU where project demonstrators will operate.
- To understand the relevance between identified legal and regulatory frameworks and DiCiM demonstrators from a compliance perspective, particularly emphasizing data protection laws, considering the project's emphasis on open-access digital platform and data collection from products.
- To understand the legal and regulatory challenges for accessing data from used products, promoting data sharing across the value chain, and making data publicly accessible—all within the framework of existing legislation.
- To explore the legal ramifications of technological solutions for harvesting components from used products for repair, spare parts sales, remanufacturing, and the manufacturing of new products.

This document serves a pivotal purpose by offering an overview and clarification on legal and regulatory issues to various stakeholders, including Original Equipment Manufacturers (OEMs) and service providers (who act as demonstrators in this project), commercial technology developers, and other stakeholders. It provides insights into how existing EU legislation pertaining to circular economy implementation and data governance impacts the development and implementation of digital circular support solutions that are designed to streamline the generation, collection, management, and exchange of data.

In this regard, it is crucial to recognize the central role that data gathering and sharing among value chain partners plays in bridging information gaps within our current economic system. These practices are foundational for the transition towards a circular economy. The circular economy, in turn, demands deep integration and collaboration of value chain partners through digital solutions. Enhanced transparency and information accessibility are essential components of this transition, necessitating the resolution of existing information gaps as a fundamental prerequisite for advancing and expanding the circular economy (as emphasized by Wilts and Berg in 2017). Within the context of the EU, horizontal regulations play a pivotal role in establishing common rules and standards that span different sectors or areas of law. Their objective is to promote consistency and harmonization within the EU. These regulations often address overarching principles and requirements that are relevant to multiple industries, including but not limited to data protection, competition law, or fundamental rights.

This document identifies regulatory frameworks and acts that may carry legal risks and compliance implications for the OEMs, digital solution developers and other stakeholders in the project. It's crucial

Funded by
the European Union

to understand the distinction between two related but separate concepts: legal risks and compliance implications.

Legal risks revolve around the potential adverse outcomes an organisation might face if it fails to comply with applicable laws and regulations. These risks encompass a range of consequences, including legal actions, financial penalties, fines, lawsuits, and damage to an organisation's reputation due to legal non-compliance. In essence, legal risks are narrowly focused and specifically relate to potential legal challenges, liabilities, and negative repercussions stemming from legal non-compliance. Mitigating legal risks involves the implementation of various legal strategies, such as achieving and maintaining legal compliance, establishing contractual safeguards, securing insurance coverage, and developing effective dispute resolution mechanisms. The organisation's primary objective is to minimize the likelihood of legal actions and address legal challenges efficiently when they arise. Both the management of legal risks and ensuring regulatory compliance are fundamental components of risk management and regulatory adherence for organisations.

Regulatory compliance implications encompass a broader array of considerations, challenges, and adjustments that an entity must make to align its operations with regulatory requirements. These implications go beyond merely avoiding legal repercussions; they involve adherence to prescribed standards and regulations. Achieving compliance often requires significant changes to operational processes, investments in innovative technologies, personnel training, and a suite of additional measures aimed at harmonizing the organisation's activities with the regulatory framework. Compliance implications refer to the consequences or effects that regulatory requirements, such as laws, rules, and industry standards, have on an organisation's operations, products, or services. These implications may encompass compliance requirements, standards for quality or safety, and the need for specific permits or licenses. Moreover, regulatory implications are expansive in scope, considering the broader regulatory environment in which an organisation operates. This involves assessing how regulations impact various aspects of business operations, including compliance, market access, and product development. Organisations typically manage compliance implications through well-structured compliance programs, adherence to industry standards, and proactive engagement with regulatory authorities. The aim is to ensure that the organisation operates within the boundaries of applicable regulatory frameworks and acts.

This report has identified and discussed regulatory frameworks that have direct implications for companies participating in the DiCiM Project. Regulatory frameworks impacting circular product strategies for environmental compliance include the Ecodesign Directive for Sustainable Products (ESPR), which establishes performance and information requirements for various physical goods placed on the EU market, including IoT-connected products. The WEEE Directive is instrumental for IoT devices, as it governs the responsible disposal and recycling of electronic and electrical products, ensuring minimized environmental impact. The RoHS Directive mandates compliance with stringent regulations concerning restricted substances, necessitating data reporting and transparency. The REACH Directive obliges companies to register, evaluate, and potentially seek authorization for the use of certain chemical substances in their products, emphasizing transparency and responsible chemical handling throughout the supply chain. Companies operating in the EU market must navigate and

Funded by
the European Union

adhere to these regulations for regulatory compliance and to fulfil their environmental and social responsibility.

In summary, the regulatory landscape for open access digital platforms is influenced by several key acts, including the Data Act, Digital Services Act (DSA), Digital Markets Act (DMA), Open Data Directive (ODD), General Data Protection Regulation (GDPR), Free Flow of Non-Personal Data Regulation, E-Privacy Regulation, Data Governance Act (DGA), and Network and Information Systems Directive 2 (NIS2). These acts shape data sharing, privacy, transparency, and fair competition in the development of open access platforms. For data sharing and public data sets, the Data Act, DSA, DMA, ODD, GDPR, Free Flow Regulation, E-Privacy Regulation, and DGA play significant roles, promoting fairness, privacy, and competition landscape in the sharing and utilization of data. They impact various aspects of data access, use, and privacy, ensuring that user rights and regulatory boundaries are respected. In the context of accessing data from used products, the Data Act, DSA, GDPR, and E-Privacy Regulation are pivotal. These regulations require secure data management, consent, and adherence to privacy measures when handling data from used products, ensuring trust and compliance with user rights. For technological solutions for harvesting components from used products, relevant acts include the Data Act, DSA, GDPR, E-Privacy Regulation, and the AI Liability Directive, which will soon be under enforcement. These acts address data handling, privacy, and user rights, impacting the development and deployment of technologies involved in harvesting components from used products. Chapter 5 details the implications accordingly.

In summary, this document identifies legal and regulatory frameworks that may pose legal risks and compliance implications for partners during or after the project implementation. Understanding and effectively addressing both legal risks and compliance implications are essential components of risk management for organisations. This report, however, does not provide the interpretation of the law and regulations. This report serves only as a means to identify the legal and regulatory frameworks relevant for DiCiM project. Partner companies are expected to consult their legal departments for interpretation of the law in case a legal issue arises during the project.

2.1. Setting the Analytical Context for Legal and Regulatory Frameworks

The primary objective of this section is to establish the context for the analysis of legal and regulatory frameworks in the EU. The DiCiM project aims to develop and implement different technological solutions for circular value management as identified in the project proposal, Tasks 1.1 (Deliverable 1.1 is being prepared at the time of writing this report) and Task 1.2 (Deliverable 1.2). These technological solutions include development of an open access digital platform to store, analyse and share product lifecycle information, IoT solution for data collection for condition monitoring and location tracing, and technological solutions for harvesting components from the used products which could be used for repair, sell as spare parts, and used in remanufacturing as well as manufacturing of new products. Below we briefly discuss these technological solutions and their main objectives.

Funded by
the European Union

Open Access Digital Platform (OADP): In DiCiM project, the development of an OADP aims to achieve following objectives:

- Store, analyse and share product data and assess the condition of the products to increase their return.
- Provide support to optimize the reverse logistics.
- Increase product/core returns through more efficient handling of products/core information by developing standard product data structure.
- Lower time to provide product information including Eco reporting for products.
- Increase availability and utilization of refurbished parts for repairs.

IoT and ML-based solution to support decision making: These solutions aim to achieve following objectives:

- Tracking and tracing of products to optimizing the reverse logistics.
- Condition monitoring for predictive maintenance, to speed up products/parts end-of-life evaluation, and to decrease testing time for new product models.

Solutions for component harvesting: These solutions aim to achieve following objectives:

- Augmented Reality solution to decrease the error rates in disassembly/dismantling of products.
- Image processing solution recognising visual defects in used products/parts to decrease visual testing timeline.

These technological solutions fall under common categories within the realm of technology nomenclature, including open-access data platform, Extended Reality (XR) technologies, image processing technologies, and IoT technologies (specifically for tracking, tracing, and condition monitoring). This section aims to provide a rudimentary understanding of these technological components and their potential contributions to the circular manufacturing systems.

Digital technologies play a key role as technological enablers in the context of circular manufacturing systems. The utilization of digital technologies can significantly enhance the circularity in the manufacturing sector. Three primary application levels can be delineated within this context. *At the process level*, these technologies contribute to heightened efficiency and circularity in the processing of materials and the manufacturing of products. This encompasses automation through robotics, additive manufacturing, digital design, sensor technologies, and machine learning, among others. *At the product level*, digital technologies enable the tracking and tracing of products and components, optimizing value chains, facilitating the development of products as services, and promoting increased reuse, repair, and refurbishment. This is achieved through the deployment of technologies such as the Internet of Things (IoT), blockchain, and digital twins. Lastly, *at the platform level*, digital technologies serve as connectors between suppliers, consumers, and producers, facilitating the development of services and dematerialization, and fostering industrial symbiosis.

Funded by
the European Union

Implementing circular manufacturing systems in practice includes multiple stages such as value use, reverse logistics and value recovery where support solutions are needed. These support solutions encompass a spectrum of technologies, such as the Industrial Internet of Things (IIoT)/Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Image Processing, Augmented Reality (AR). These interconnected digital technologies collectively contribute to realizing circular manufacturing systems. For example, Extended Reality (XR) can be employed to repair and produce new parts, complementing traditional manufacturing methods. *AR* solutions can guide repairers (service providers) and repair technicians. AR solutions can also deliver real-time dismantling guidance. Utilizing various sensing technologies allows for proactive diagnosis of component health, signalling the need for repair before a failure occurs. Fault diagnostic technologies complement the repair process, with the potential for a continually updated fault diagnostic database through a *data-sharing platform* (open access or restricted access) aligned with federated data space principles. This database facilitates the collection and dissemination of information. It can include manufacturer-recommended guidelines alongside real-world fault data, symptoms, and corresponding repair solutions provided by product repairers and technicians. Solutions such as open data sharing platform can be used to collect data from products and components (including harvested). Digital marketplaces might serve as platforms for trading recycled materials, used components, parts or products. Leveraging *ML* from such databases and data-sharing platforms could enhance diagnostic capabilities. *IoT* allows to enhance efficiency, reduce costs, enable data-driven decision-making, predictive maintenance, and better control over the entire product lifecycle, ultimately benefiting both manufacturers and consumers. Efficient logistics and reverse logistics optimization play a crucial role in minimizing both costs and environmental impacts associated with material transfers during recycling and recovery activities. Thus, value recovery in manufacturing systems involves critical identification, sorting, and material recovery phases. Sensing and imaging technology coupled with data analytics and ML, can be employed in identifying and sorting diverse products and materials across the value chain.

Figure 1 illustrates the Smart Circular Economy framework, demonstrating the interconnected role of digital technology within it. This framework employs a hierarchical organisation, showing how each level depends on the preceding one. For instance, in the context of data transformation, the connection of resources through IoT sensors is essential to generate data, which can then be transformed into information through integration with other data sources and contextualization, ultimately leading to increased ability to support decision-making. It outlines where in the hierarchy separate technologies are used for data collection, data integration and analysis.

Funded by
the European Union

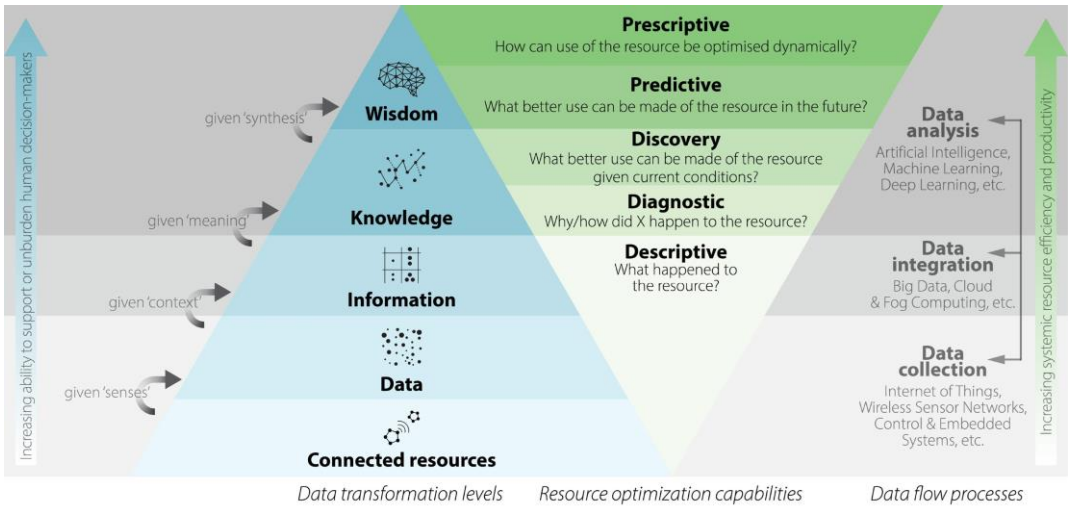

Figure 1 Smart Circular Economy framework (Kristoffersen et. al 2020)

The technological advancements, encompassing aspects related to the CE and sustainability within manufacturing and data-driven technologies, has led to the emergence of a set of legislative initiatives. Initially, these initiatives, predominantly focused on substances and products. With time, environmental regulations have expanded to encompass a broader range of materials and products. Compliance with the regulatory and legal requirements often include aspects related to data and information sharing as well as data governance requirements. This evolution prompted the establishment of multiple governance mechanisms since unrestricted sharing of data and information, as 'open data,' can potentially encroach upon the rights of private sector entities, including manufacturers' intellectual property rights and trade secrets, as well as the privacy and data protection of individuals, such as product consumers and users. The regulations that pertain to data governance take the form of horizontal regulations applicable across EU in line with the EU overall data strategy. Originally, these data and information obligations primarily targeted public authorities, particularly in relation to environmental issues, falling under the category of “open data”, yet as environmental concerns extend to the sustainability of the economic system, these obligations now increasingly affect the private sector and have grown in scope (Ducuing and Reich, 2023).

The above contextualization serves as a foundation to identify the relevant legal and regulatory frameworks within the EU salientto the development of these technological solutions for circular manufacturing systems.

2.2. Methodology

The process for preparing this report was divided into three stages:

1. We conducted a review and categorization of EU regulatory and legal acts related to the implementation of the circular economy within the sectors and activities outlined in sections 3 & 4.
2. Our approach involved a qualitative analysis of the gathered regulatory texts.

Funded by the European Union

3. To ensure a comprehensive evaluation, we engaged in stakeholder consultations, drawing from the insights gained through interviews and the textual analysis of the collected data.

The methodology employed in this study is based on a mixed-method approach to investigate the interplay between EU legislation, pertaining circular economy and data governance, and regulatory compliance within the manufacturing sector. It commenced with a text review of EU legal frameworks, drawing from the *Official Journal of the European Union*, is the official platform (EUR-Lex) that publishes all EU legal acts and other publicly accessible databases. Interviews with key stakeholders, including original equipment manufacturers (OEMs), digital technology developers, and DiCiM partners, serve for triangulation purposes and to gather additional data. This triangulation of data sources enhances the study's comprehensiveness. The synthesis and analysis of data from these diverse sources enable the identification of relevant legal and regulatory frameworks in EU in the context of circular economy. Through this mixed-method methodology, the study aims to provide an understanding of the topic, grounded in both legal foundations and practical industry experiences.

The methodology employed for conducting interviews in this study involved a structured approach to ensure robust data collection and analysis. The methodology used was informed by a combination of open-ended questionnaires, interviews, focus groups, and written feedback from participating companies, following the best practices in qualitative research (Adams and Cox, 2008; Bell, Bryman and Harley, 2022; Creswell and Creswell, 2017).

In the initial phase of our research, a set of open-ended questions was prepared. Following the preparation of the questions, we disseminated them in advance of the interview sessions. This not only allowed participants to familiarize themselves with the topics but also facilitated a more in-depth and reflective discussion during the actual interviews (Rubin & Rubin, 2012). The next step in our methodology involved conducting a series of three interviews with a group of company representatives. These interviews were structured as a form of focus group, with the aim of promoting interactive discussions and the exchange of diverse viewpoints (Krueger & Casey, 2015). The inclusion of multiple perspectives within a group setting added depth to the data collected and enabled the exploration of nuances that might have been missed in individual interviews (Morgan, 1997).

In addition to the interview-based data collection, some of the approached companies also contributed written feedback to answer the research questions. This mixed-methods approach ensured that we could capture a wide spectrum of responses and insights, accounting for the preferences and comfort levels of our participants (Tashakkori & Teddlie, 2010).

To enhance the validity and rigor of our research, we further disseminated the initial draft of this report to the participating companies. This step allowed for member checking, a technique employed to verify the accuracy and completeness of the data gathered (Lincoln & Guba, 1985). The feedback received from these companies played a crucial role in refining our analysis and ensuring that the results accurately represented their perspectives and experiences. The results of our study, informed by the data collected through interviews, focus groups, and written feedback, are presented in Section 5 of this report.

Funded by
the European Union

2.3. Structure of the report

The report is structured into five distinct chapters. Following this introductory section, Chapter 3 presents legal and regulatory aspects relevant to Circular Economy from a product perspective, offering insights into the existing legal landscape. Chapter 4 focuses on legislative instruments relevant from a data governance perspective within the EU, providing a comprehensive overview of the key instruments. Chapter 5 analyses the relevance of legal and regulatory frameworks for the DiCiM project demonstrators, combining a study of identified acts with stakeholder interview results. Chapter 6 presents final conclusions and recommendations.

Funded by
the European Union

3. Regulatory frameworks impacting circular product strategies for environmental compliance

This section describes legal aspects relevant for CE implementation in the EU and offers a review of the current legal landscape based on a mapping of regulatory initiatives and mechanisms that are pertinent to the implementation of CE in the manufacturing sector. The European Green Deal is a roadmap of key policies and measures needed to transform the EU into a fair and prosperous society, with a modern, resource-efficient, and competitive economy where there are no net emissions of greenhouse gases in 2050 and where economic growth is decoupled from resource use. The Circular Economy Action Plan (CEAP), one of the main building blocks of the European Green Deal, is a plan to develop measures that target how products are designed, promotes circular economy processes, encourages sustainable consumption, and aims to ensure that waste is prevented, and the resources used are kept in the EU economy for as long as possible. The Circular Economy Action Plan serves as a policy framework and roadmap for promoting a circular economy within the EU.

Many regulatory mechanisms and policies are still work in progress, yet these instruments play a pivotal role in driving sustainable production and consumption. These instruments serve as effective tools for encouraging industries to align with a collective path toward sustainable development, whether through direct or indirect incentives. Within the European context, a range of such instruments has been employed. Each of these instruments contributes to fostering a resource-efficient and competitive economy, aligning with the overarching goal of achieving climate neutrality by 2050 as set forth in the European Green Deal. Below we discuss some of the relevant legal frameworks that support CE implementation in the EU.

3.1. Waste Electrical and Electronic Equipment (WEEE) Directive

The WEEE Directive[1] serves as a comprehensive framework for the responsible management of waste electrical and electronic equipment within the EU. It places a strong emphasis on separate collection, proper treatment, and achieving specific collection rates, all with the overarching goal of promoting recycling and safeguarding environmental and public health interests. Compliance with these provisions is imperative for all stakeholders engaged in the recovery of components from WEEE.

The EU's Waste Electrical and Electronic Equipment (WEEE) Directive establishes critical provisions governing the handling and disposal of electrical and electronic equipment (EEE) when it becomes waste, commonly known as WEEE.

[1] Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast) Text with EEA relevance. The act has been changed and has a Consolidated text date 04/07/2018: Directive 2012/19/EU of the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE) (recast) (Text with EEA relevance)

Funded by the European Union

WEE directive established the definitions of EEE and WEEE. EEE encompasses equipment reliant on electric currents or electromagnetic fields, designed for use with specified voltage ratings not exceeding 1,000 volts for alternating current and 1,500 volts for direct current. WEEE comprehensively includes electrical or electronic equipment that has become waste, covering not only the primary product but also all its components, sub-assemblies, and consumables present at the time of disposal.

Another fundamental concept within the directive is that of "making available on the market." This pertains to the supply of products for distribution, consumption, or use within a Member State's market through commercial activities, whether for payment or free of charge.

Furthermore, the directive underscores the significance of "separate collection." Distributors play a pivotal role in ensuring that waste generated b can be returned, at least on a one-to-one basis, free of charge. The condition is that the returned equipment must be of an equivalent type and serve the same functions as the originally supplied equipment. Member States may make exceptions to this provision, provided that the return of WEEE remains both free and not more challenging for the final holder.

Proper treatment of WEEE constitutes another fundamental aspect of the directive. This encompasses the removal of all fluids and their selective treatment in accordance with specifications outlined in Annex VII of the directive. The selective treatment necessitates the removal of specific substances, mixtures, and components from separately collected WEEE. Examples include polychlorinated biphenyls (PCB) containing capacitors, mercury-containing components, batteries, and other materials as specified in Annex VII of the directive.

Under the WEEE Directive, EU Member States are mandated to establish individual registers for manufacturers of electrical appliances, necessitating separate registration of brand, manufacturer name, device type, and category in each Member State. This registration serves as a crucial step in holding producers accountable for the entire lifecycle of their electrical and electronic equipment, encompassing production, market placement, user retrieval, and ensuring proper recycling and recovery processes.

3.2. Restriction of Hazardous Substances (RoHS) Directive

The RoHS Directive's[2] primary goal is to mitigate the potential hazards to both human health and the environment associated with the disposal of electronic and electrical waste. RoHS is in the form of a directive, which mandates each member state to incorporate it into their national law, ensuring

[2] Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (recast) Text with EEA relevance. and Directive (EU) 2017/2102 of the European Parliament and of the Council of 15 November 2017 amending Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment (Text with EEA relevance.)

Consolidated text: Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (recast) (Text with EEA relevance) Text with EEA relevance, text is meant purely as a documentation tool and has no legal effect.

Funded by the European Union

uniformity of impact across all territories. This Directive lays down rules on the restriction of the use of hazardous substances in Electrical and Electronic Equipment (EEE) with a view to contributing to the protection of human health and the environment, including the environmentally sound recovery and disposal of waste EEE. RoHS Directive mandates that Member States take measures to ensure that EEE introduced into the market adheres to specific chemical restrictions or does not exceed maximum concentration values by weight, subject to certain exemptions. The RoHS Directive governs the presence of hazardous substances during the manufacturing of EEE. Conversely, the WEEE Directive pertains to the management and disposal of this identical equipment. RoHS represents a vertical, sector-specific legislation that targets EEE, with limited exclusions such as means of transport and equipment exclusively used for national security purposes. RoHS focuses on restricting the concentration of 10 specific substances within EEE products. The evaluation under RoHS is carried out at the homogenous material level. It achieves this objective by placing limitations on the use of specific dangerous substances in EEE, substances that can be replaced with safer alternatives. The substances subject to these restrictions encompass heavy metals, flame retardants, and plasticizers.

Additionally, the RoHS Directive encourages the recyclability of EEE. Recognizing the potential benefits, it emphasizes that limiting the use of hazardous substances is likely to enhance recycling opportunities for waste EEE and mitigate adverse health effects on workers in recycling facilities. This means that EEE and its constituent parts, once they become waste, contain fewer harmful substances. Simultaneously, it ensures fair competition among manufacturers and importers of EEE within the European market.

The directive's overarching approach involves a sector-specific, highly focused, scientifically grounded, and structured mechanism for granting exemptions to substance restrictions. This mechanism serves to uphold a robust standard of protection for both the environment and human health within the EU's internal market.

Manufacturers and suppliers must institute robust data management practices to fulfil their RoHS obligations. This not only ensures compliance but also promotes transparency within the supply chain, facilitating the provision of essential data to regulatory authorities, customers, and consumers alike.

3.3. Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation

The REACH Regulation encompasses a comprehensive set of guidelines governing various aspects related to substances, including registration procedures, bans or restrictions on substances, and prerequisites for authorizing particularly hazardous substances. REACH encompasses a broad horizontal scope, applicable to virtually all components and products available in the EU, albeit with certain exceptions like radioactive materials. It necessitates comprehensive written disclosure of all Substances of Very High Concern (SVHCs), currently numbering 209, found in products and packaging. Consequently, a multitude of EU-based companies fall within the REACH Regulation. Companies are obliged to conduct audits of their products and components to ensure compliance with the prohibited substances' manufacturing, marketing, and usage restrictions across the EU. They must also adhere to

Funded by
the European Union

the prescribed conditions for entry. If any of their product contains substances listed on the Authorization List, companies are required to obtain the necessary authorization for their use within the EU. It also prescribes regulations regarding the dissemination of information to customers. Business/entities handling manufacturing, importing, or selling of articles and chemical products within the EU or European Economic Area (EEA), must adhere to the relevant regulations applicable to their specific operations. The users of chemical products are also subject to compliance requirements outlined within the Regulation.

The REACH Regulation officially came into effect on 1 June 2007. The evaluation under REACH is conducted at the article level. REACH promotes the communication of information about chemicals in the supply chain. Manufacturers and importers are required to provide safety data sheets to downstream users, ensuring safe handling and use. Under REACH, manufacturers and importers of chemical substances are required to register them with the European Chemicals Agency (ECHA). Registration involves providing detailed information about the properties and hazards of the chemicals. This data helps assess the risks associated with their use.

In cases where substances cannot be employed safely, the EU reserves the authority to impose restrictions on their usage, either through outright bans or other restrictive measures. Additionally, authorisation requirements may be introduced for substances that pose a notably high level of hazard, with the intention of encouraging the adoption of less perilous alternatives.

Extensive guidance for the industry is available[3].

3.4. Ecodesign Directive for Sustainable Products (ESPR)

The Ecodesign Directive for Sustainable Products (ESPR) is an evolution of the existing Ecodesign Directive (2009/125/EC) and is one of the cornerstones of the EU Circular Economy Action Plan. ESPR is a horizontal product agnostic Ecodesign Regulation that introduces a more comprehensive set of Ecodesign criteria that apply to a broader range of products than its predecessor. Its primary goal is to establish sustainable products as the standard within the EU market. Of particular significance to circular manufacturing systems is the introduction of a novel mechanism known as the Digital Product Passport (DPP).

The key objectives of this regulation are to minimize the environmental impact of products across their life cycle and enhance the internal market's efficiency. These aims align with EU industrial policy goals, promoting sustainability in production and ensuring fair competition in the internal market. To achieve these objectives, the regulation calls for uniform requirements, efficient compliance methods, robust enforcement, and enhanced market surveillance based on risk analysis. This regulation will broaden

[3] https://echa.europa.eu/en/regulations/reach/understanding-reach'

https://echa.europa.eu/en/support/guidance

Funded by the European Union

the scope of the Ecodesign Directive in terms of products and new kinds of requirements. For reasons of legal clarity, the Ecodesign Directive should therefore be repealed.

ESPR creates the basis for new CE-related data and information sharing obligations by the OEM as eco-design requirements. Crucially, this Regulation's goals are in harmony with various other CEAP initiatives. It aims to complement and strengthen the requirements set by these initiatives, especially those related to key value chains, such as the EU's strategy for sustainable and circular textiles. Additionally, it aligns with initiatives aimed at empowering consumers for the green transition and enhancing the credibility of environmental claims about products, promoting reliability, comparability, and verifiability. These measures are substantiated using life-cycle analysis methods, including the Product Environmental Footprint method.

Figure 2 Overview of Initiatives in the Circular Economy Package and the place of Ecodesign for Sustainable Product Regulation. Source: EC (2023)

The proposed Regulation also finds common ground with upcoming legislation on Corporate Sustainable Due Diligence[4], particularly in its environmental due diligence provisions for businesses. This convergence of initiatives highlights a comprehensive approach to achieving sustainability, circularity, and responsible consumption and production across various economic sectors.

[4] This upcoming legislation is not included in the analysis in the report. Proposal for a Directive of the European Parliament and of the Council on Corporate Sustainability Due Diligence, amending Directive (EU) 2019/1937, with EEA relevance. (As presented in documents: SEC(2022) 95 final, SWD(2022) 38 final, SWD(2022) 39 final, SWD(2022) 42 final, SWD(2022) 43 final).

Funded by the European Union

The ESPR proposal places significant emphasis on Ecodesign requirements, which form its core. These requirements necessitate the adoption of a Commission delegated act specific to a product group, unless broader 'horizontal' requirements are established. Ecodesign requirements encompass a wide range of aspects aimed at enhancing product durability, reliability, circularity, and reducing their environmental footprint across their lifecycle. Additionally, the proposal introduces considerations for the social sustainability of products and due diligence aspects throughout the value chain. These Ecodesign requirements encompass both performance criteria (e.g., minimum recycled content) and information requirements, with the latter encompassing Digital Product Passports (DPPs) and Substances of Concern (SoC).

In summary, ESPR will harmonize with and support broader EU policies, emphasizing sustainability, circularity, and responsible consumption and production across various economic sectors. Article 2 of ESPR covers a broad range of definitions, where for the purpose of this report the most relevant include:

- *'Product' means any physical good that is placed on the market or put into service.*
- *'Consumer product' means any product, excluding components and intermediate products, primarily intended for consumers.*
- *'Component' means a product intended to be incorporated into another product.*
- *'Intermediate product' means a product that requires further manufacturing or transformation such as mixing, coating, or assembling to make it suitable for end-users.*
- *'Energy-related product' means any product that has an impact on energy consumption during use.*
- *'Product group' means a set of products that serve similar purposes and are similar in terms of use, or have similar functional properties, and are similar in terms of consumer perception; 'remanufacturing' means an industrial process in which a product is produced from objects that are waste, products or components and in which at least one change is made to the product that affects the safety, performance, purpose or type of the product typically placed on the market with a commercial guarantee*
- *'Upgrading' means enhancing the functionality, performance, capacity or aesthetics of a product.*
- *'Refurbishment' means preparing or modifying an object that is waste or a product to restore its performance or functionality within the intended use, range of performance and maintenance originally conceived at the design stage, or to meet applicable technical standards or regulatory requirements, with the result of making a fully functional product.*
- *'Maintenance' means an action carried out to keep a product in a condition where it is able to function as required.*
- *'Repair' means returning a defective product or waste to a condition where it fulfils its intended use.*
- *'Product passport' means a set of data specific to a product that includes the information specified in the applicable delegated act adopted pursuant to Article 4 and that is accessible via electronic means through a data carrier.*
- *'Data carrier' means a linear bar code symbol, a two-dimensional symbol or other automatic identification data capture medium that can be read by a device.*

Funded by
the European Union

- *'Unique product identifier' means a unique string of characters for the identification of products that also enables a web link to the product passport.*
- *'Unique operator identifier' means a unique string of characters for the identification of actors involved in the value chain of products.*
- *'Unique facility identifier' means a unique string of characters for the identification of locations or buildings involved in the value chain of a product or used by actors involved in the value chain of a product.*
- *'Manufacturer' means any natural or legal person who manufactures a product or who has such a product designed or manufactured, and markets that product under its name or trademark or, in the absence of such person or an importer, any natural or legal person who places on the market or puts into service a product.*
- *'Online marketplace' means a provider of an intermediary service using software, including a website, part of a website or an application, that allows customers to conclude distance contracts with economic operators for the sale of products*

Article 7 essentially underscores that products must adhere to the information requirements associated with these product aspects as defined in Article 5(1). These information requirements are vital for transparency and compliance, ensuring that products meet the established ecodesign standards throughout their lifecycle. These product aspects are established as part of ecodesign requirements, which are further defined in delegated acts under Article 4. Article 5(1) lays out a comprehensive set of ecodesign requirements that encompass various facets of product design and performance. These requirements aim to enhance the following product aspects:

(a) Durability

(b) Reliability

(c) Reusability

(d) Upgradability

(e) Reparability

(f) Possibility of maintenance and refurbishment

(g) Presence of substances of concern

(h) Energy use or energy efficiency

(i) Resource use or resource efficiency

(j) Recycled content

(k) Possibility of remanufacturing and recycling

(l) Possibility of recovery of materials

(m) Environmental impacts, including carbon and environmental footprint

(n) Expected generation of waste materials

Funded by
the European Union

3.4.1. Digital Product Passport (DPP)

The European Commission (EC) has introduced two legislative proposals addressing the requirement for DPPs. The first proposal concerns the Battery Regulation, specifically focusing on products and necessitating the creation of battery passports. The second proposal lays the foundation for potential future adoption of product (group) DPPs. Both legislative initiatives incorporate environmental and sustainability criteria as integral components of product legislation. While the current ESPR Directive is still undergoing revisions, and there is no current obligation for DPPs, there are already implications for the manufacturing sector that need to be considered. In particular, Chapter III, of the ESPR titled "Digital Product Passport," with Article 8, which focuses on the concept of the product passport and Article 9, outlines the general requirements that pertain to this product passport.

Manufacturers and EU importers of regulated products are obligated to ensure the availability of a product passport, as specified in the applicable delegated act, before placing a product on the market. The DPP serves as a decentralized tool for registering, processing, and sharing product-related information among supply chain stakeholders, authorities, and consumers.

Box 1. General requirements for the digital product passport

The product passport must fulfil the following conditions:

a) It must be linked to a unique product identifier through a data carrier.

b) The data carrier must be physically present on the product, its packaging, or accompanying documentation, as specified in relevant delegated acts issued under Article 4.

c) Both the data carrier and the unique product identifier must comply with the standard ISO/IEC 15459:2015.

d) All information contained in the product passport must adhere to open standards, use an interoperable format, and be machine-readable, structured, and searchable, in accordance with the essential requirements outlined in Article 10.

e) The information within the product passport must pertain to the specific product model, batch, or item, as detailed in delegated acts issued under Article 4.

f) Access to the information contained in the product passport must be regulated in accordance with the essential requirements specified in Article 10, and specific access rights at the product group level must be identified in relevant delegated acts issued under Article 4.

Funded by the European Union

The economic operator[5] responsible for placing the product on the market must provide dealers with a digital copy of the data carrier. This allows dealers to make the product information accessible to customers, particularly when physical access to the product is not feasible. The economic operator is obligated to provide this digital copy free of charge and within five working days upon the dealer's request. Data access is facilitated through a data carrier and a unique identifier.

3.5. Proposal for a regulation on circularity requirements for vehicle design and on management of end-of-life vehicles (ELV)

The proposed regulation[6] by European Commission is set to replace existing directives on end-of-life vehicles and reusability, recyclability, and recoverability. The regulation will emphasize circular design, require a substantial percentage of recycled content in vehicle production, enhance raw material recovery, improve governance through uniform Extended Producer Responsibility schemes, and expand its scope to include various vehicle categories, fostering sustainability and circular business models in the automotive industry. This initiative encompasses a comprehensive review of the ELV Directive and the 3R type-approval Directive, which were established in 2000 and 2005, respectively. The ELV Directive aims to ensure environmentally sound treatment of end-of-life vehicles, setting guidelines for collection, depollution, hazardous substance restrictions, and recycling and recovery targets. On the other hand, the 3R type-approval Directive connects the ELV Directive with design requirements for reusability, recyclability, and recoverability, especially during the type-approval process for new vehicles.

The proposed regulations pertaining to circularity requirements for vehicle design and the handling of end-of-life (EoL) vehicles play a crucial role in influencing the trajectory of circular strategies within the automotive sector. A concise overview outlining key proposals for the EU is presented below:

- Definition and determination of the end-of-life status of automobiles and their components are proposed.

[5] The term "economic operator" is defined in the context of European Union (EU) regulations, particularly related to various aspects such as product safety, customs, and trade. The precise definition may vary depending on the specific regulation, but in general, an "economic operator" refers to any person or business entity that is involved in economic activities. This typically includes a range of stakeholders in the supply chain, such as manufacturers, importers, distributors, wholesalers, and retailers.

For instance, in the EU Regulation (EU) 2019/1020 on Market Surveillance, which deals with market surveillance and compliance of products, the term "economic operator" includes: 1. Manufacturer: The natural or legal person who manufactures the product.2. Importer: The natural or legal person established within the EU who places a product from a third country on the EU market.3. Distributor: The natural or legal person in the supply chain, other than the manufacturer or the importer, who makes a product available on the market.4. Authorized representative: A person established in the EU who has received a written mandate from the manufacturer to act on their behalf. In different contexts, there may be variations in the definition of "economic operator," but the common interpretation is that it encompasses all the key players involved in bringing products to the market, ensuring they meet relevant regulatory requirements, and addressing issues related to safety, quality, and compliance. It is essential to refer to the specific regulation or directive in question to determine the exact definition and obligations associated with "economic operators" in that context.

[6] Proposal for a regulation of the European Parliament and of the Council on circularity requirements for vehicle design and on the management of end-of-life vehicles, amending regulations (EU) 2018/858 and 2019/1020 and repealing directives 2000/53/EC and 2005/64/EC - COM/2023/451 final.

Funded by the European Union

- Viability of repairing an end-of-life product is contingent upon the restoration cost being lower than the prevailing market value of the vehicle.
- Proposals for the traceability of vehicles and their components to the manufacturer and the final owner are put forth.
- Conditions are recommended for acceptable concentrations (mass function) of harmful substances in constituent components, such as Lead, Chromium, and Mercury, set at 0.1%, and 0.01% for Cadmium.
- Discussion of circular strategies and frameworks within the automobile sector, encompassing measures and methods for collaborating with manufacturers to enhance prolonged value recovery.
- Regular updating of circular strategies for manufacturers regarding technological advancements and disseminating these updates across the value chain to improve the industry overall, mandated every five years.
- Introduction of a unique identification key for simplified identification of components, which would also share technical information about the component.
- Establishment of requirements and standards for storage spaces and treatment sites for end-of-life products.
- Proposals for the depollution of harmful end-of-life components.
- Mandatory removal of specific components from end-of-life vehicles.
- Establishment of rules and regulations specifying which components can be used for value recovery and imposing restrictions on components not allowed for value recovery. For instance, components such as airbags, and other components that compromise the safety of end users, cannot be part of value recovery processes.

Following the proposal to the EU, the European Commission formulated amending regulations EU 2017/853 and 2019/1020, while simultaneously repealing directives 2000/53/EC and 2005/64/EC. The challenges identified in connection with the deficient adoption of sustainable practices, aligning with the EU Green Deal and Circular Economy Action Plan (CEAP), are delineated as follows:

- Lack of integration of circularity in vehicle design and production - The absence of circularity integration in the design and production of vehicles
- Suboptimal quality of treatment of EoL vehicles - Inadequate standards in the treatment of EoL vehicles, compromising their environmental impact
- Increasing numbers of EoL and non-road worthy vehicles which are termed as ‘missing vehicles’ are not treated under proper environmental conditions - A growing number of EoL and non-roadworthy vehicles categorized as 'missing vehicles' that are not subjected to proper environmental treatment.
- Plethora of unexploited circularity potential in the automobile space - Numerous untapped opportunities for circular practices within the automotive sector.

A synopsis of the EU document addressing these policy concerns is presented as follows:

- In the context of design and production of new vehicles, three policies are drafted.

Funded by the European Union

1. Better Compliance Verification: Enhanced compliance verification through type-approved processes and improved information exchange within the dismantling sector.
2. New Design Requirements for Dismantling: Introduction of new design requirements aimed at facilitating dismantling processes.
3. Development of Environmental Vehicle Passport: Creation of an Environmental Vehicle Passport to track and manage the environmental impact of vehicles throughout their lifecycle.

- In the context of recycled content, three policies are drafted,
    1. Moderate Targets for Recycled Plastics: Establishment of moderate targets for recycled contents of plastics.
    2. Mandate on Recyclates: Implementation of a mandate requiring 25% of recyclates on new products and a minimum of 20% recycled steel.
    3. Increased Recycled Content: Promotion of increased recycled content in both steel and plastics, with a target of up to 30%.
- In the context of EoL treatment, the 3 policy options are:
    1. Clarifications on ELV Waste Treatment: Clarifications of rules regarding the treatment of End-of-Life Vehicles (ELV) waste as outlined in the ELV directive.
    2. Ban on Mixing ELV Scrap with WEEE Scrap: Enforcement of a ban on the mixing of ELV scrap with Waste Electrical and Electronic Equipment (WEEE) scrap, incentivizing the support for the market of used spare parts.
    3. Removal of Small Electronic Components: Mandate for the removal of small electronic components before the scrapping process.
- In the context of collection, the 3 polices are summarized as follows:
    1. Enhanced Reporting Rules: Improvement of reporting rules by shredders and dismantlers.
    2. Improved Tracking through Digitalization: Utilization of digitalization for enhanced tracking of vehicle components.
    3. Export Requirement: Stipulation that the export of used vehicles outside the EU is permissible only with a valid roadworthiness certificate.
- In the context of incentivizing collection of ELV to improve the waste treatment and higher value recovery, the 3 policies are as follows:
    1. Extended Producer Responsibility (EPR): Introduction of Extended Producer Responsibility (EPR) for vehicle manufacturers, covering the costs associated with the collection of used and EoL vehicles for all EU member states.
    2. Harmonized Circularity Criteria for EPR Fees: Establishment of harmonized circularity criteria for adjusting EPR fees paid by vehicle manufacturers, ensuring effective functioning in cross-border situations within the EU.
    3. Additional Economic Incentives: Introduction of additional economic incentives, such as 'deposit return schemes,' and harmonized circularity criteria for Green Public Procurement of vehicles.

Funded by
the European Union

3.6. Batteries Regulation

The Batteries regulation[7] effective from August 17, 2023, starts to apply as of 18 February 2024. It applies universally to all "Economic Operators" involved in battery manufacturing, importation, and distribution within the EU market, encompassing various battery types, regardless of their origin. It directly impacts battery design, production, and waste management across all battery types within the EU. These regulations expand producer responsibility and mandate supply chain due diligence to evaluate social and environmental risks, particularly concerning cobalt, natural graphite, lithium, and nickel sourcing. The introduced labelling requirements aim to furnish consumers with enhanced insights into batteries' social and environmental implications. Notably, these regulations encompass all battery manufacturers, producers, importers, and distributors in the EU market, spanning industrial, automotive, electric vehicle, and portable batteries, irrespective of their origin.

The regulation introduces changes in four key areas: Enhanced Recycling and Reuse Measures, Heightened Utilization of Recycled Raw Materials and Open information on batteries and traceability Manufacturers will have an obligation to furnish access to control system data for automotive batteries exceeding 2 kWh in capacity. This provision aims to facilitate battery management, assess suitability for reuse or recycling, and ensure greater transparency. Furthermore, the EU mandates comprehensive information disclosure on material composition, quantities, and origin for automotive and industrial batteries.

The regulation introduces changes in four key areas:

1. *Sustainability and Safety: Batteries, such as EV batteries, LMT batteries, and certain industrial batteries, must bear a "clearly legible and indelible" carbon footprint declaration and label, disclosing recycled material levels, while restricting the use of mercury, cadmium, and lead.*
2. *Supply Chain Management: Economic Operators, excluding SMEs, selling batteries in the EU must establish due diligence policies compliant with international standards for sourcing and trading raw materials essential for battery production.*
3. *Labelling and Information: The introduction of a "digital battery passport" for specific batteries, alongside mandatory CE marking and label details related to capacity, performance, durability, and chemical composition.*
4. *Recycling – End of Life Management: Ensuring separate, high-quality recycling and addressing issues related to battery management system software.*

These changes are part of the EU's efforts to promote sustainability and safety in the battery industry, enhance supply chain accountability, and improve recycling practices, all of which have far-reaching implications for battery manufacturers, importers, and distributors.

[7] Regulation (EU) 2023/1542 of the European Parliament and of the Council, 12 July 2023, concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC (Text with EEA relevance).

Funded by the European Union

Beginning in 2027, battery labelling requirements will necessitate manufacturer identification, battery type, manufacturing date, hazardous substance presence, and other recycling or reuse-related data. Reconditioned batteries must be accompanied by status documentation, ownership transfer certificates, and technical records. Manufacturers will also be mandated to provide end-of-life batteries with information that promotes minimal waste generation, encourages material content reuse or recycling, and imparts guidelines for safe dismantling, transportation, and recycling of automotive batteries, along with disclosure of their environmental and health impact. The EU is in the process of introducing an electronic battery passport for industrial and automotive batteries exceeding 2 kWh in capacity, intended to encompass comprehensive battery information. Updates to this passport will be required whenever the battery undergoes status changes, such as repair or reuse.

Current regulations dictate that a minimum of 50% of a battery's weight must be recycled. Starting in 2025, this threshold will rise to 65% for lithium-ion batteries and further to 70% by 2030. Specific recycling mandates will also be introduced for lithium, cobalt, copper, nickel, and lead components within batteries. For instance, the prescribed recycling rate for lithium will escalate from 35% to 70% between 2026 and 2030. Furthermore, the EU is striving to establish a 90% recycling target for cobalt, copper, nickel, and lead, effective from 2026.

Manufacturers will be compelled to increase their collection of portable batteries by 45% by 2026 and by 70% by 2030. Furthermore, the export of used batteries beyond the EU will only be sanctioned if the recipient's battery management procedures align with EU requirements.

Member States must establish effective, proportionate, and dissuasive penalties for violations of this Regulation by August 18, 2025.

Funded by
the European Union

4. Legal and regulatory frameworks relevant for a circular economy from data perspective

According to the current legal framework, data access, portability, and sharing are primarily regulated by contract law, general competition law, a few sector-specific instruments with limited scope, and, regarding personal data, the GDPR (Leistner and Antoine, 2023). In this section, we will examine the legislative instruments that are relevant for circular economy from data perspective within the EU. The following sub-sections will provide an overview of the key instruments highlighting their relevant aspects.

4.1. The Data Governance Act

Regulation (EU) 2022/868, commonly referred to as the Data Governance Act (DGA)[8], serves the primary purpose of enhancing data accessibility for reuse and fostering data sharing across a diverse range of sectors including health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills. The DGA entered into application on September 23rd, 2023.

The overarching objective is to generate tangible benefits for both EU citizens and businesses. The regulation encompasses several key provisions, including the establishment of specific conditions for the reuse of protected data held by public sector entities, regulations governing companies providing data intermediation services, the introduction of a framework to facilitate data altruism, the provision for the establishment of the European Data Innovation Board (EDIB) as a pivotal entity, and the implementation of measures aimed at ensuring the secure cross-border flow of non-personal data from the EU. The DGA also amends Regulation (EU) 2018/1724[9] on the single digital gateway.

The DGA primarily regulates the reuse of certain categories of publicly held data by public sector bodies. Yet, notably, DGA also places regulatory oversight on entities offering data intermediation services, serving as impartial intermediaries that facilitate connections between data holders and data users. The regulatory framework for these services is designed to ensure that data intermediaries operate as reliable facilitators of data sharing. With the objective of fostering trust in data sharing, the DGA establishes a model cantered on the principles of neutrality and transparency for data intermediaries while also empowering individuals and companies to exercise control over their data. Entities seeking to provide data intermediation services must adhere to stringent requirements to ensure neutrality and prevent conflicts of interest, maintain structural separation from other value-added services, establish pricing terms independent of users' engagement with additional services,

[8] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (OJ L 152, 3.6.2022, pp. 1–44).

[9] Consolidated text: Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (Text with EEA relevance) Text with EEA relevance.

Funded by the European Union

and register with a competent authority. This regulatory approach underscores the significance of data intermediation services within the broader context of data governance.

Additionally, GDA incorporates provisions related to data altruism, a concept that comes into play when individuals and companies willingly grant consent to make the data, they generate accessible for public interest purposes, without expecting any form of compensation in return. The primary objective of this data altruism provision is to establish trusted mechanisms that simplify the sharing of data for the benefit of society.

In accordance with the European Strategy for Data, the DGA introduces the concept of "common European data spaces." These data spaces are organized by data intermediaries with the responsibility of safeguarding the data, and they are strategically focused on sectors such as health, environment, energy, agriculture, mobility, finance, manufacturing, public administration, and skills. This framework, as articulated by the European Commission, presents an alternative model to the data handling practices of dominant Big Tech platforms, which wield significant market power due to their control over extensive datasets.

4.2. The Data Act

The Data Act[10], introduced by the European Commission in a proposal on February 23, 2022, and subsequently agreed upon by the European Parliament and the Council of the EU on June 28, 2023, constitutes a substantial legislative instrument within a larger legal framework. It intersects with various legal initiatives, including the Digital Markets Act (DMA), GDPR, Free Flow of Non-Personal Data Regulation, ePrivacy Directive, and Database Directive. While both the DMA and the Data Act (DA) share a core objective of promoting equitable and transparent digital markets, the Data Act goes further by explicitly addressing data sharing and utilization, an aspect not covered by the DMA. The EU Data Act entails profound implications for both custodians and consumers of non-personal data and datasets. Consequently, the scope of this legislation extends well beyond the boundaries defined by the GDPR. The Data Act is expected to take effect approximately 20 months after its publication in the Official Journal of the European Union, impacting various aspects of businesses, including data management systems, contracts, and security measures.

As the EU is introducing and revising a series of data-focused legislative initiatives at the EU level, alongside existing practices, aimed at addressing the evolving needs of the economy. The Data Act, along with other acts like the DSA, DMA, and DGA, aims to foster fair competition and innovation in the data-sharing economy through measures such as:

1. *Making data generated by products and related services available to users.*

[10] European Parliament P9_TA(2023)0069 Data Act Amendments adopted by the European Parliament on 14 March 2023 on the proposal for a regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act) (COM(2022)0068 – C9-0051/2022 – 2022/0047(COD))1

Funded by the European Union

2. *Ensuring fair, reasonable, non-discriminatory, and transparent data-sharing terms and conditions.*
3. *Simplifying the process of switching between data processing service providers.*
4. *Mandating business-to-government data sharing in exceptional cases.*
5. *Protecting non-personal data held by specific service providers within the EU, including commercially sensitive data like trade secrets.*

The Data Act's Scope[11] extends to manufacturers of devices, digital service providers, companies involved in connected device production, and EU public authorities. It encompasses personal and non-personal data collected by connected products and related services. This legislation introduces new regulations alongside the existing GDPR, focusing on personal data. Additionally, it applies to physical products capable of collecting data and communicating via electronic services. These regulations combined ensure accessible data, promote innovation, and support a circular economy model.

The EU's Data Act is designed to:

1. *Enable data sharing among businesses (B2B), businesses and consumers (B2C), and businesses and governments (B2G), with a primary focus on data generated by connected devices.*
2. *Strike a balance between data access and trade secret protection, allowing companies to refuse data sharing in exceptional circumstances where disclosing specific data could result in severe economic harm despite protective measures.*
3. *Provide access to data generated by IoT devices for users, promoting transparency and business benefits.*
4. *Encourage GDPR-compliant data sharing among businesses, with a particular advantage for small and medium-sized enterprises (SMEs).*
5. *Encourage data sharing related to public interest issues, such as climate change or health emergencies, while strictly adhering to GDPR and emergency-related limitations.*
6. *Establish a framework for data intermediaries, neutral entities that facilitate data sharing between data holders and users, subject to stringent regulations to prevent misuse.*
7. *Safeguard trade secrets by allowing companies to refuse data sharing when they can demonstrate potential serious economic damage, subject to competent authority scrutiny.*
8. *Align with other legal initiatives like the Digital Markets Act and GDPR within the broader legal framework.*

[11] See for detail clarification: 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 (Data Act) SWD/2022/34 final.

Funded by the European Union

In particular, the Data Act defines data generation as a function of manufacturers and specifies which manufacturers are within the scope and defines the products (including home equipment and consumer goods) that are subject to the DA:

It further stipulates that sector-specific regulations tailored to address the unique requirements and goals of particular industries, or antitrust rulings, should dictate the data that a connected product can potentially provide to data holders or recipients at the time of purchase. On the other hand, the Data Act should not apply to content or data that is acquired, produced, or retrieved from the connected product or sent to it for storage or processing on behalf of third parties. This includes situations such as when servers or cloud infrastructure are involved, and the data is intended for use by an online service, among other scenarios.

The Data Act also refers to data intermediation services. "Data intermediation services," as delineated in Regulation (EU) 2022/868, are designated to provide support to users or data recipients in the formation of commercial associations for lawful objectives, predicated on data encompassed by the purview of this Regulation. These services can assume a pivotal role in access to data derived from many individual data users, thereby expediting comprehensive big data analyses or machine learning processes. Nevertheless, the users must retain unmitigated agency in determining whether to contribute their data to such aggregation and maintain control over the commercial stipulations governing the utilization of their data. Data intermediation services providers are entities that seek to facilitate commercial interactions intended for data sharing between an unspecified multitude of data subjects and data holders on one side and data users on the other side, which can include open data management platforms and entities utilising advanced technologies for B2B data sharing and data marketplaces. In practice, under DA data intermediaries are those parties that will function as neutral third parties that connect individuals and companies with data users.

Moreover, the Data Act revisits certain elements of the Database Directive [12], initially established in the 1990s to safeguard investments in the structured presentation of data. It clarifies that the Database Directive should not be exploited to impede access to data produced by connected products or related services. Without this clarification, data holders could assert de facto exclusivity over such data, obstructing the effective application of access and portability rights as outlined in the Data Act.

This Regulation focuses on ensuring that manufacturers of connected products and providers of related services enable users in the EU to access and use the data generated by these products or services. It mandates data holders to provide data to users and their chosen data recipients under fair, reasonable, and transparent terms. The Regulation also incorporates private law rules to address contractual imbalances hindering data access and use. Additionally, it allows data holders to provide data to public sector bodies and Union institutions when there is an exceptional need. The Regulation aims to enhance data sharing mechanisms, facilitate switching between data processing services, and

[12] Directive 96/9/EC of the European Parliament and of the Council of March 1996 on the legal protection of databases (Reviewed in 2018).

Funded by the European Union

improve data interoperability within the Union. It does not grant data holders inherent rights to hold, access, or process data, but acknowledges that users may grant them access and use permissions, often via contractual agreements to perform related services.

Data generation stems from the design of connected products, user actions, and related services. This data, which can be non-personal and valuable, raises questions about fairness in the digital economy, given its importance for various services and applications. To unlock economic benefits and foster data-driven growth, a general approach to assigning data access and usage rights is preferred over exclusive rights. However, voluntary data sharing agreements remain essential for the development of data-driven value in European companies.

The Data Act, as part of the European Strategy for Data, promotes "data sharing by design" among manufacturers, enhancing user access and regulating data processing services, international data transfer, and interoperability criteria. It complements existing EU data regulations, such as the GDPR, Free Flow of Non-Personal Data Regulation, and Open Data Directive, by facilitating data sharing and elucidating the value creation aspects of data.

The Regulation covers physical products that collect, generate, or transmit data about their performance, use, or environment through electronic communications services, physical connections, or on-device communication, excluding prototypes. A "user" of a connected product refers to the legal or natural person, such as a business, consumer, or public sector body that acquires the product or receives related services. Data recipients who access data may be natural or legal persons, enterprises, research organisations, not-for-profit organisations, or intermediaries, including data intermediation services and data altruism organisations as defined in Regulation (EU) 2022/868.

Implications: The Data Act is a complex law that will have noticeable effects on businesses and their operation, no matter their size. It aims to balance the rights and responsibilities of different groups involved with data, like those who have the data, those who use it, and the people, referred to as natural persons, the data is about. The ‘user rights’ mechanism as the key instrument of the DA (Kerber, 2023; PC1. 2023)

As this law comes into effect, businesses will need to review their products, data practices, and policies carefully to make sure they follow the rules. This will probably mean they have to make changes to how they manage data, update their contracts, and put in place security measures to keep data safe. With data being more accessible, it's important to have strong security to protect it from unauthorized access, use, or any harm. This might include using encryption, controlling who can access data, and using secure methods to move data around. The current version of the law hasn't completely addressed the concerns that companies have raised about protecting their confidential information when sharing data with competitors during the consultation process. Businesses must adapt to comply with the Data Act while navigating trade secret protection concerns. Moreover, expanding digital practices and spaces regulations raises questions about balancing rights and obligations for mixed data sets and clarifying whether it covers raw data or data that has undergone further processing.

Additionally, there are concerns about protecting trade secrets and valuable data sets within the Act's definition of data, despite some limited safeguards for trade secrets. The interpretation of the Data

Funded by
the European Union

Act's scope in practice remains uncertain, even after political consensus on its wording. Under the Data Act, manufacturers, and providers of IoT products and services, as well as their users, will be subject to several obligations that aim to ensure access, sharing, and portability of data regarding the use of these products and services. To be more precise, a fundamental policy objective is to facilitate horizontal data sharing among various entities, including Business-to-Business (B2B), Government-to-Business (G2B), Business-to-Government (B2G), and Consumer-to-Business (C2B), not only within individual countries but also among the European Member States. This data can subsequently undergo annotation, analysis, and processing, primarily to train artificial intelligence (AI) models in the process of machine learning. The Data Act contains an explicit right to data processing.

The Data Act does not resolve the implications arising from the existing legal ambiguity surrounding data ownership. In practice, there exists a de facto economic ownership of data, but the concept of legal ownership, as defined by EU primary and secondary legislation and property law, remains absent. Notably, the European framework regulation suggests a parallel between data and tangible goods, albeit in the context of property law. However, despite sharing some characteristics with property, data is distinct from real property or intellectual property.

Data ownership regulations vary not only among different countries but also within the EU itself. For instance, German law excludes intangible assets from certain rights, while French law provides comprehensive protection for intangible assets. Consequently, digital data has not yet acquired formal recognition as a legally possessable entity, resulting in the absence of established property rights concerning data. This lack of clarity concerning both economic and legal ownership leaves stakeholders uncertain about the rightful ownership of data and the permissible actions of data holders.

This issue becomes significantly more intricate in cases involving datasets created collaboratively by multiple companies in diverse geographical locations over an extended period or datasets encompassing a mixture of personal, governmental, and industrial data. Furthermore, it is worth noting that distinct economic sectors, such as Logistics, Energy, Creative Industry, and Life Sciences and Health, introduce unique challenges concerning both sector-specific and cross-sectoral data sharing and the utilization of machine learning datasets. Companies will have to figure out how to deal with this uncertainty and consider if they should move their data out of the scope of this law, especially when it comes to sensitive business data. They might need to take steps to avoid mixing user data with other data that could give away important details about their products or services. Additionally, the companies will have to take steps to define data strategies in dealing with companies outside of EU.

The Data Act mandates that companies share the data collected through their products and associated services with other entities within the value chain. Non-compliance and infringements of the obligations laid down in the Data Act will result in the imposition of penalties.

Several challenges and implications remain, including concerns about protecting trade secrets within the Act's data definition and uncertainty about the Act's scope in practice. To prepare for the enforcement of the Data Act, data holders and providers must:

Funded by
the European Union

1. Gain a comprehensive understanding of their market presence, considering whether it's global, EU, or local, and identify specific services that generate or utilize data across the value chain. Including those that are relevant for the circular value management systems specifically.
2. Ensure consistency in data-sharing practices to prevent discrimination and promote fairness.
3. Openly evaluate whether their practices encourage fair competition and innovation.

Failure to anticipate and comply with these regulations could lead to limited market access, financial and legal liabilities, and reduced financing opportunities and impact data sharing for the purpose of enhancing efficiency and responsiveness of operations during the use, reverse logistics, and value recovery phases.

4.3. The Digital Services Act

The Digital Services Act (DSA) [13] is an EU regulation that focuses on regulating digital services acting as intermediaries, connecting consumers with goods, services, and content, including online marketplaces. Its primary aim is to enhance user protection and safeguard fundamental rights online while establishing a comprehensive transparency and accountability framework for online platforms. The DSA applies across the EU and encompasses various obligations for intermediaries, such as countering illegal content, ensuring traceability of products on online marketplaces, safeguarding user rights, and implementing transparency measures for online platforms. Furthermore, it introduces a unique oversight structure for very large online platforms and search engines, allowing for EU-wide cooperation among national regulators and the European Commission. Importantly, the DSA does not define what constitutes illegal online content but rather sets out rules for its detection, flagging, and removal. It does not replace sector-specific legislation but complements existing regulations, addressing the changing digital landscape, and providing a harmonized approach to digital service regulation in the EU. The DSA entered into force on November 16, 2022, following a political agreement reached on April 23, 2022, between the European Parliament and Council, with the publication of the act in the EU Official Journal on October 27, 2022.

Article 29 of the regulation focuses on the obligations of online marketplaces and online search engines, with a particular emphasis on how data is treated and exchanged for effective market surveillance. In summary, Article 29 outlines the responsibilities of online marketplaces, particularly concerning data exchange and cooperation with market surveillance authorities to ensure product compliance. It also highlights the need for accessible product information and compliance with other relevant regulations. Some of the DSA requirements include:

[13] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) PE/30/2022/REV/1

Funded by the European Union

1. Online marketplaces are required to cooperate with market surveillance authorities, ensuring effective market surveillance measures. This cooperation includes:

   (a) Avoiding obstacles to market surveillance measures.

   (b) Informing authorities of actions taken.

   (c) Exchanging information on removed offers.

   (d) Granting access to interfaces for identifying non-compliant products.

   (e) Allowing authorities to scrape data if technical obstacles are created by marketplaces.

2. Online marketplaces must design their interfaces to enable dealers and economic operators to fulfil their obligations. Information should be readily accessible for each product offered, including any required electronic information for specific products.

3. Member States empower market surveillance authorities to order the removal or restriction of illegal content related to non-compliant products from online marketplaces. Such orders must comply with the DSA.

4. Online marketplaces are obliged to receive and process these orders in accordance with the DSA.

5. Online marketplaces must establish a single contact point for direct communication with Member States' market surveillance authorities regarding compliance with the regulation and its delegated acts. This contact point may align with existing regulations, such as the General Product Safety Regulation or the DSA.

4.4. The Digital Markets Act

The main legislative texts for the Digital Markets Act (DMA) are Regulation (EU) 2022/1925[14] of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and the Implementing Regulation. The Procedural Implementing Regulation (EU) 2023/824 details procedural aspects related to the implementation and enforcement of the DMA. The DMA seeks to identify and regulate large online platforms that have significant market power. These platforms are referred to as "digital gatekeepers". They are characterized by their size, user base, and impact on the digital ecosystem.

The DMA addresses entities commonly termed as "digital gatekeepers," denoting their prominence in the digital landscape, as discerned by their dimensions, user reach, and consequential influence on the digital ecosystem. The thematic focus, encapsulated by the overarching principles of the regulation, pertains to the pivotal role these platforms assume as integral conduits between business entities and

[14] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) PE/17/2022/REV/1

Funded by the European Union

end users. This thematic emphasis is underscored by the acknowledgment that entities meeting specific criteria, delineated in the regulatory framework, qualify for the designation of a 'gatekeeper.' In adhering to the provisions of the regulation, these gatekeepers are subject to constraints designed to curb unfair and anti-competitive practices, fostering a more equitable digital marketplace. According to Article 3 DMA, an undertaking shall be designated as a gatekeeper if: (a) it has a significant impact on the internal market; (b) it provides a core platform service which is an important gateway for business users to reach end users. The DMA prohibits certain unfair and anti-competitive practices by digital gatekeepers. These practices include self-preferencing (promoting their own products or services over others), blocking or hindering third-party interoperability, and leveraging data collected on their platform to gain a competitive advantage. Digital gatekeepers are required to ensure data portability and interoperability with smaller businesses and competing platforms. This aims to reduce barriers to entry for smaller players and foster competition. Digital gatekeepers are required to notify the European Commission of any proposed mergers or acquisitions, which could potentially harm competition in the digital market. They are also subject to regular reporting obligations.

The DMA empowers the European Commission to conduct market investigations into digital markets. If competition concerns are identified, the Commission can impose remedies on digital gatekeepers to address these issues. Digital gatekeepers are prohibited from treating their own services or products more favourably than those of their competitors. This is aimed at ensuring a level playing field for all market participants. Competing businesses are entitled to access certain data and algorithms from digital gatekeepers under specific conditions, allowing for fair competition. The DMA includes provisions for significant fines for non-compliance with its rules. These fines can amount to a percentage of the gatekeeper's global turnover.

The DMA establishes a European Digital Markets Authority (EDMA) responsible for monitoring and enforcing compliance with the regulation. Currently, it applies solely to 22 core platforms and 6 gatekeepers (EC, 2023). Therefore, it does not extend its applicability to open data-sharing platforms as envisioned within the scope of the DiCiM project.

4.5. The General Data Protection Regulation (GDPR)

The GDPR is founded on the fundamental principles outlined in the European Convention on Human Rights and the EU Charter of Fundamental Rights, particularly emphasizing the right to privacy and the protection of personal data. To safeguard individual interests, data subjects possess several rights to access their processed personal data, whether held by entities such as companies or authorities. However, it is essential to clarify that these rights do not impose a general obligation on organisations processing personal data to share data generated by individuals, such as website users.

Nonetheless, organisations are bound by specific transparency obligations concerning an individual's personal data. This includes the data subjects' right to request data register extracts, ensuring they receive confirmation regarding the processing of their personal data and granting access to copies of such data within a data register extract. Furthermore, the right to data portability allows individuals to transfer their personal data from one data controller to another, either directly or through their own

Funded by
the European Union

involvement. Within the data processing domain, organisations are obligated to demonstrate respect and adherence to these rights, recognizing their pivotal role in safeguarding personal data.

The scope of the GDPR encompasses companies involved in the processing of personal data within the EU, irrespective of their physical presence. Companies operating from outside the EU that offer goods or services, whether on a paid or free basis, or that monitor individuals within the EU.

The GDPR incorporates provisions that address the processing of special categories of personal data (Article 9), processing without identification (Article 11), transparency in data collection (Article 13), joint controllers (Article 26), cross-border data transfers (Article 44), and reporting (Article 59). These provisions collectively underscore the importance of Original Equipment Manufacturers (OEMs) exercising prudence when handling special categories of personal data, determining the necessity of identifying data subjects in the context of data processing, the need for transparent data collection, the establishment of transparent arrangements for joint control of data, the adherence to stipulated conditions for cross-border data transfers, and the imperative to avoid actions that might lead to violations of GDPR regulations. The legal presumption supported by the European Data Protection Board (EDPB) which clarifies that, in essence, aggregate data are not within the scope of the GDPR.

Below we report some relevant and important provisions of GDPR.

Data Protection for Special Categories of Data (Article 9): OEMs must be particularly cautious when dealing with special categories of personal data, such as health data or biometric data. They should ensure that their products or services comply with the strict prohibition on processing these types of data, unless specific exceptions or additional conditions are applicable under national laws.

Processing without Identification (Article 11): When OEMs design products or services that involve the processing of personal data, they should consider whether it's necessary to identify the data subjects. If not, they can avoid the burden of maintaining, acquiring, or processing additional information for identification purposes.

Transparency in Data Collection (Article 13): When OEMs collect personal data directly from individuals (e.g., through IoT devices), they must provide clear and transparent information to data subjects about the identity of the controller, the purposes of data processing, and the legal basis for processing. This requires clear and user-friendly privacy notices and consent mechanisms.

Joint Controllers (Article 26): If OEMs collaborate with other entities (e.g., software providers or service partners) to jointly determine the purposes and means of data processing, they need to establish transparent arrangements for GDPR compliance. This includes defining responsibilities for data subject rights and information provision. OEMs must ensure that they have agreements in place to clarify these roles and responsibilities.

Cross-Border Data Transfers (Article 44): If OEMs transfer personal data across borders, whether to third countries or international organisations, they must ensure that the conditions and safeguards specified in the GDPR are met. This often involves conducting assessments of the destination country's data protection laws and putting in place appropriate contractual clauses, binding corporate rules, or other safeguards to protect the data.

Funded by
the European Union

Reporting (Article 59): OEMs should be aware that supervisory authorities are required to produce annual activity reports, which may include information on data protection infringements. OEMs should aim to avoid any actions or practices that could result in violations of GDPR regulations and may attract the attention of supervisory authorities.

In conclusion, OEMs must diligently incorporate robust data protection practices into their product development processes, ensuring unwavering compliance with GDPR regulations and readiness to furnish evidence of their adherence to these provisions. Non-compliance carries substantial financial penalties and reputational risks, accentuating the pivotal significance of GDPR compliance for OEMs operating within the EU or engaging with data related to EU residents. Some products and services relying on aggregate data necessitate the processing of personal data, which cannot always be directly obtained with informed consent, as reflected in Article 13 of the GDPR. Frequently, such activities are conducted by private entities that may lack the same institutional safeguards and ethical standards as public entities. In such cases, it is reasonable to inquire about the threshold at which data ceases to be considered "personal". Therefore, there is a need to explore and address the risks associated with this presumption when developing machine learning models and AI products, despite its presence in the non-binding Recitals of the Regulations, creating a grey area (Podda, 2021[15]).

4.6. The ePrivacy Regulation

The ePrivacy Regulation (ePR) will replace the ePrivacy Directive of 2002[16] and is a pivotal legal framework that safeguards privacy and personal data protection in the digital age, with a specific focus on communication confidentiality and regulations concerning tracking and monitoring. Designed to complement and specify areas covered by the GDPR, this directive aims to achieve three main objectives:

1. Ensuring effective confidentiality of all electronic communications through technologically neutral and future-proof legislation.

2. Providing robust protection from unsolicited commercial communications, including a prohibition on anonymous marketing calls.

3. Promoting greater harmonization and simplification of the existing legal framework.

The ePrivacy Regulation will apply to "electronic communications content," encompassing exchanged content like text, voice, videos, and images, and "electronic communications metadata," which includes data used for tracing communication source and destination, device location, date, time, duration, and communication type. It also extends to legal entities. Collectively, these categories form "electronic communications data" transmitted through methods such as email, SMS, MMS, and

[15] Podda, E., 2021. Shedding light on the legal approach to aggregate data under the GDPR & the FFDR. In conference of European statisticians Expert Meeting on Statistical Data Confidentiality.

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Funded by the European Union

equivalent applications and techniques. Regulation's scope is thus more extensive than that of the GDPR, which solely pertains to the personal data of individuals.

The ePrivacy Regulation introduces foundational principles governing data processing, particularly concerning the use of pseudonymized or anonymized data. Under this framework, content is categorized as "anonymous" when it cannot be linked to any identifiable natural person or legal entity, leading to the non-application of the ePrivacy Regulation. Conversely, content is regarded as "pseudonymous" if it remains possible to identify a natural person or legal entity through additional information. In such instances, the ePrivacy Regulation retains its applicability.

In the context of Artificial Intelligence and Internet of Things (IoT) devices, the ePrivacy Regulation establishes fundamental rules and principles for their development and deployment. It allows for necessary actions without explicit consent for specific service provision. However, when data stored on IoT devices serves purposes beyond core services, explicit user consent becomes mandatory, striking a balance between essential IoT functionalities and data protection rights within the regulatory framework.

Infringements of the ePrivacy Regulation may result in substantial fines, similar to GDPR-infringements, with potential penalties of up to EUR 20 million or 4% of the organisation's total global annual turnover. This regulation introduces a fine system comparable to GDPR:

1. Lesser violations may incur fines of up to 2% of the company's annual global turnover or up to €10 million.

2. More severe violations may lead to fines of up to 4% of the company's annual global turnover or up to €20 million.

These fines will be administered and adjudicated by the EU's Data Protection Authorities (DPAs), who also possess a range of non-financial penalties at their disposal.

4.7. The Open Data Directive

The Open Data Directive, also known as the Open Data and re-use of Public Sector Information Directive (EU) 2019/1024[17] had to be transposed into national law by 17 July 2021. It establishes rules on the re-use of data held by the public sector and of publicly funded research data made publicly available through repositories. This directive plays a pivotal role in strengthening the EU's data economy by promoting the release of public sector data in free and open formats, thereby fostering fair competition, facilitating easy access to public sector information, and promoting cross-border innovation driven by data. At its core, the directive emphasizes the principle of openness in government data, with provisions covering the release of non-personal data in open formats and to

[17] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public-sector information (recast) (OJ L 172, 26.6.2019, pp. 56–83).

Funded by the European Union

open standards, real-time data availability through Application Programming Interfaces (APIs) where feasible, new rules regarding charges for data re-use, and the re-use of publicly funded research data.

Additionally, the directive outlines the creation of a list of High Value Datasets (HVDs) through an Implementing Act, discourages exclusive arrangements to prevent data lock-in, and promotes the re-use of data held by public undertakings, including public utilities and transport providers. Consequently, the Open Data Directive applies to the scientific research results of the DiCiM project.

4.8. Regulation on the Free Flow of Non-personal Data

Regulation (EU) 2018/1807[18], known as the Regulation on the Free Flow of Non-personal Data, came into effect in late 2018. Its primary objective is to ensure the unimpeded cross-border movement of non-personal data within the EU. The Free Flow of Non-Personal Data Regulation (FFoD) ensures that non-personal data can be stored, processed and transferred anywhere in the EU. It achieves this by establishing guidelines pertaining to data location, competent authority access, and data portability for professional users among other measures.

Non-personal data, as defined within the context of the Regulation, pertains to electronic information that lacks the potential for traceability to an identified or identifiable natural person, or has undergone anonymization to achieve this state. For example, aggregated and anonymized datasets employed in extensive big data analytics, information related to precision farming, which aids in the monitoring and optimization of pesticide and water usage, as well as data concerning maintenance requirements for industrial machinery.

This regulation explicitly prohibits data localization requirements at the national level, unless they can be justified on the grounds of public security, adhering to the principle of proportionality embedded in EU law principles. Justifications for such requirements encompass aspects of national and external security, alongside other public security concerns, including criminal prosecution. These justifications necessitate the presence of a tangible and substantial threat capable of jeopardizing fundamental societal interests.

Data localization requirements may take various forms, including prohibitions, conditions, or restrictions that mandate data processing within a specific EU Member State or hinder processing within the territory of another Member State. As such, any restrictions on the free flow of data within the EU are not permissible.

Furthermore, the FFoD governs competent authority access to data, ensuring that access cannot be denied on the grounds that the data are processed in a different Member State. In relation to data portability or data transmission, the regulation obliges the European Commission to encourage and facilitate the development of self-regulatory codes of conduct at the EU level. This initiative aims to

[18] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union.

Funded by the European Union

foster a competitive data-driven economy rooted in principles such as transparency and interoperability. The Regulation presently enables and encourages EU enterprises to formulate self-regulatory codes of conduct with the aim of enhancing the competitive data economy. This enhancement is predicated on the fundamental tenets of transparency, interoperability, and the adoption of open standards.

The interaction between the Regulation and the GDPR concerning "mixed datasets" is as follows: When a dataset comprises both personal and non-personal data, the Regulation pertains specifically to the non-personal data portion of the dataset. However, in cases where personal and non-personal data within a dataset are intricately interconnected, the GDPR takes precedence and must be applied to the entire dataset.

Regarding compliance issues, while the Regulation may not present immediate compliance challenges for businesses and organisations, it underscores the significance of clearly distinguishing between personal and non-personal data, even in instances where the personal data may appear to be of minor significance.

4.9. NIS2 Directive on Measures for a High Common Level of Cybersecurity across the Union

A The NIS 2 Directive[19], in effect since January 16, 2023, requires EU Member States to transpose it into national law by October 17, 2024. It mandates security measures and incident reporting for key industry operators, with significant expansions compared to its predecessor (NIS 1 Directive). Changes include a broader scope, more specific measures, enhanced incident reporting rules, stricter sanctions, and accountability at the senior management level.

The directive covers entities if they operate in listed (sub)sectors and meet certain size criteria. For comprehensive details, exceptions, and nuances, refer to Articles 2 & 3 and Annexes I & II of the Directive.

The NIS 2 Directive extends its scope to new sectors and entity types within existing sectors, categorized into two groups: sectors of high criticality (Annex I of the Directive) and other critical sectors (Annex II of the Directive). The distinction between "essential" and "important" entities is now based on size and type, affecting the level of supervision and sanctions. Essential entities are large companies in high-criticality sectors, defined as having ≥250 employees OR an annual turnover of ≥50 million euros or an annual balance sheet total of ≥43 million euros. Important entities include medium-sized enterprises in high-criticality sectors or large/medium-sized enterprises in Annex II sectors not categorized as essential. The sectors of high criticality and critical sectors include the following: Manufacturing (including medical devices and in vitro diagnostic medical devices; computer,

[19] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity in the Union (amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148)

Funded by the European Union

electronic, and optical products; electrical equipment; machinery and equipment not elsewhere classified; motor vehicles, trailers, and semi-trailers; and other transport equipment), Digital providers, Research, Digital infrastructure, and ICT service management.

Article 24 of the Directive on measures for a high common level of cybersecurity across the Union addresses the use of European cybersecurity certification schemes for essential and important entities. It grants Member States the authority to require these entities to use specific ICT products, ICT services, and ICT processes that are certified under European cybersecurity certification schemes established under Regulation (EU) 2019/881[20].

The Commission has the power to issue delegated acts to further specify which categories of essential entities should be mandated to use certified ICT products, ICT services, or ICT processes or obtain certification through these schemes. These delegated acts are necessary when there are identified inadequacies in cybersecurity levels and come with implementation periods. Before enacting such delegated acts, the Commission is obliged to conduct an impact assessment and engage in consultations as outlined in Regulation (EU) 2019/881.

In cases where there is no suitable European cybersecurity certification scheme available, the Commission can, after consulting relevant bodies, request ENISA (European Union Agency for Cybersecurity) to develop a candidate scheme as per the provisions of Regulation (EU) 2019/881. This article underscores the importance of certified cybersecurity measures in safeguarding critical ICT assets. The supervisory boards or top management of Entities falling within the scope of this Directive are required to provide their consent to cybersecurity risk management measures, supervise their execution, and could be subject to legal responsibility in the event of any violations. The relevant entities have reporting obligations and are required to promptly report any significant incident to the competent national authorities as specified in the Directive. This notification obligation applies to incidents that significantly impact services within the sectors or sub-sectors listed in Annexes I and II of the Directive. Noncompliance with risk management measures or failure to report incidents may result in penalties.

The new obligations for relevant entities should not become effective until the end of the transposition period, which is set for October 2024. Nevertheless, it is advisable for companies to proactively prepare for the general requirements outlined in the Directive, taking into consideration the growing cybersecurity threats and risks. Hence, it is recommended that entities that will clearly be subject to these new obligations begin enhancing their cybersecurity measures promptly, without waiting for the transposition of legislation.

[20]Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) PE/86/2018/REV/1

Funded by the European Union

4.10. Artificial Intelligence Act

On June 14, 2023, Members of the European Parliament (MEPs) adopted the Parliament's negotiating position concerning the Artificial Intelligence (AI) Act, initiating negotiations with EU member states in the Council to determine the final legislative framework. Currently, there is no definitive negotiating text available for the Artificial Intelligence Act. It is anticipated that an agreement will be reached by the conclusion of 2023.

The European Commission has introduced a comprehensive regulatory framework governing artificial intelligence systems within the EU. This framework provides a technology-neutral definition of AI systems and follows a risk-based approach, categorizing AI into four risk levels:

1. Unacceptable Risk AI: AI systems engaging in harmful activities that violate EU values, such as government-implemented social scoring, will be strictly prohibited due to their unacceptable risk.
2. High-Risk AI: A specific set of AI systems significantly impacting people's safety or fundamental rights, detailed in an Annex, will be classified as high-risk. These systems will be subject to a range of mandatory requirements, including conformity assessments, to ensure consistent safety and protection of fundamental rights.
3. Limited Risk AI: Some AI systems will face a limited set of obligations, primarily focusing on transparency and disclosure.
4. Minimal Risk AI: All other AI systems with minimal risk will be permitted for development and use within the EU without additional legal obligations beyond existing legislation.

The proposal is presently under deliberation by the European Parliament and the Council, engaging in a legislative process to determine its final adoption and implementation.

Article 1, subject matter of the Regulation, lays down harmonized rules for the market placement, commissioning, and utilization of AI systems in the Union, along with prohibitions on certain AI practices, specific requirements for high-risk AI systems, and obligations for their operators. It also covers transparency rules, market monitoring, market surveillance, governance, and measures supporting innovation. The Regulation applies to providers, users, importers, distributors, product manufacturers, and authorized representatives of AI systems within and outside the Union. It encompasses scenarios where AI system outputs are used within the Union, irrespective of physical presence or establishment.

The AI Act primarily targets AI systems posing significant risks to fundamental rights and safety. Some "unacceptable risk" systems are completely prohibited, aligning with core EU values and fundamental rights. The extent to which specific technologies, like real-time facial recognition for public services, will be banned remains uncertain, as negotiations are ongoing.

The implications of this regulation in the manufacturing sector have been discussed yet remain uncertain, introducing significant ambiguity concerning its potential impact. It aims at reducing risks for safety and fundamental rights, such rules do not prohibit AI systems posing a residual risk to safety and fundamental rights being placed on the market.

Funded by
the European Union

4.11. Liability Digital Technologies: Product Liability Directive (PLD), New Product Liability Directive and an AI Liability Directive (AILD)

The existing EU liability framework encompasses the Product Liability Directive 85/374/EEC (the 'PLD').[21] and parallel national liability rules, offering various paths for victims to claim compensation, including fault-based liability, strict liability, and claims against producers of defective products. The rollout of IoT and AI-based technologies necessitates safeguards to minimize potential harm, and the EU commonly relies on product safety regulations to ensure the safety of all products in the European market. The European Commission has introduced a companion to the PLD in the form of an AI Liability Directive, aiming to establish uniform regulations for non-contractual fault-based liability concerning damages resulting from AI, especially high-risk AI systems (HRAIS). It's important to note that, as of the current writing, the AI Liability Directive is still in the early stages of the legislative process.

The AI liability directive aims to improve the internal market's functioning by establishing uniform requirements for non-contractual civil liability involving AI systems.

The PLD sets an EU liability regime for financial compensation claims due to damage caused by products intended for private use above a certain threshold. Member States can impose a maximum compensation limit, which may not be less than €70 million (Article 16(1)). Article 4 of the proposed Directive includes software in the scope of EU product liability laws, encompassing operating systems, firmware, computer programs, applications, and AI systems. Article 7 extends liability to manufacturers of defective components, distributors, fulfilment service providers, and online platforms. Articles 8 and 9 introduce a disclosure regime and presumptions to aid claimants. Additionally, there is a liability exemption for software manufacturers categorised as microenterprises or small enterprises when placing the product on the market, and provisions for joint and several liability in cases involving multiple economic operators liable for the same damage.

Historically, uncertainty surrounded the application of PLD requirements to software, seen as a limitation of the existing framework. While expanding the PLD's scope from "all movables" to "electricity, digital manufacturing files, and software" appears to enhance liability claims from a consumer's perspective, the inclusion of software applications and AI systems introduces new legal uncertainties and increased operational expenses for firms involved in software commercialization within the EU (Bauer and Sisto, 2023). Additional changes proposed by policymakers, such as treating "digital services" as products, incorporating psychological health and data loss as (immaterial) damage, shifting the burden of proof, easing access to evidence for plaintiffs, and introducing strict liability for complex products, amplify these legal risks. Figure 3 provides a three-part regulatory system for AI in the EU.

[21] Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (commonly referred to as the 'PLD' or Product Liability Directive)

Funded by the European Union

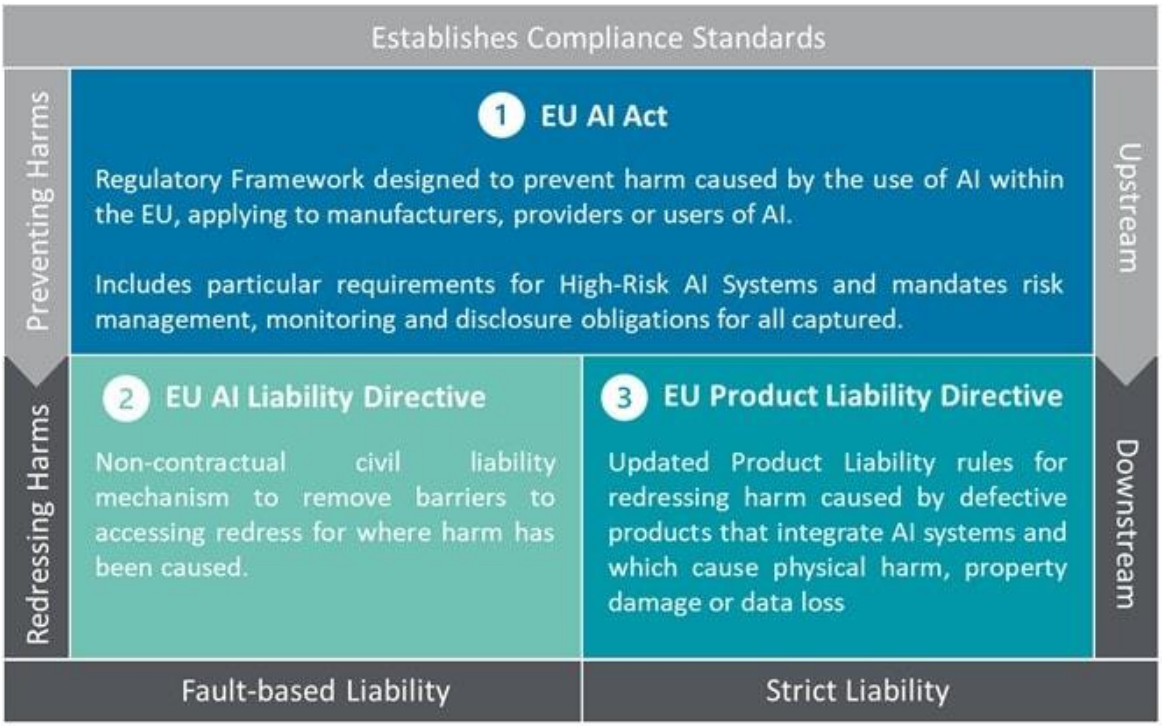

Figure 3 . A three-part regulatory system for AI in the EU, with upstream harm prevention provided by the AI Act and downstream harm redress provided by the proposed directives. (Source: Deloitte 2023[22])

4.12. Summary of Legal Acts Pertaining Data Governance in the EU

The following table serves as a comprehensive summary of the legal acts pertaining data governance in the EU covered in this report. It outlines the specific data types they address, highlights potential overlaps among them, and provides information on their respective objectives, scope, and current enforcement status.

Table 1 Overview of EU Data Governance Legal Acts

Legal Act	Aim	Type of Intervention	Type of data	Overlap	Status
Digital Markets Act or DMA	Remove barriers to access of data Regulate gatekeepers	Asymmetric Direct obligation and enforcement	Personal data and non-personal data Portability of data (will apply mostly to simple data storage	Access to search data in compliance with the GDPR only Transparency obligations on top of Article 13 and 14 of GDPR	Proposed by the commission in December 2020, agreed by the European Parliament in March 2022, in effect from May 2023. Obligatory

[22] Available: https://www2.deloitte.com/uk/en/blog/auditandassurance/2023/ai-updated-eu-liability-legislation.html

Funded by the European Union

			services operated by gatekeepers)		compliance from March 2024
	Preserve incentives to invest in data generation			Restricting combination of personal data Data Sharing obligations	
Digital Services Act or DSA	Proper functioning of the internal market for intermediary services	Asymmetric	Caching data, reporting data in aggregated form, personal data	Revising the e-commerce framework, GDPR-compliant data sharing	Proposal published on 15 December 2020; Political agreement was reached on 23 April 2022; needs approval still by European Parliament and Council
	Set out uniform rules for a safe, predictable and trusted online environment				Applicable (in force) since Augist 2023
Data Act or DA	Proper use and access of data	Symmetric	Mixed data, mainly IoT data; Cloud/edge switching	The GDPR prevails, with the exception of data sharing to gatekeepers in the DMA	To take effect approximately in 20 months after its publication in September 2023, with expected effect in early-mid 2025
		Framework conditions + interoperability standardisation	Includes switching of data, applications, and services		
				Rules for transfer of non-personal data	
General Data Protection Regulation (EU) 2016/679 **(GDPR)**	Protect personal data, create a solid framework for digital trust	Asymmetric	Personal data	All acts that regulate personal or mixed data sets overlap to some degree with the GDPR	Published on 27 April 2016. Applicable since 25 May 2018
Directive on open data and the re-use of public sector information (EU) 2019/1021 **(Open Data Directives)**	Enable reuse of data held by public-sector bodies. The directive is based on the general principle that public and publicly funded data should be reusable for commercial or non-commercial purposes.	Symmetric	Non-personal data; public sector information	The GDPR prevails Overlap with the DGA in so far as reuse of non-personal data is concerned Minor overlap regarding data	Applicable since 17 July 2021

Funded by the European Union

				portability with the DA	
Regulation on a framework for the free flow of non-personal data in the EU 2018/1807 **(Free Flow Regulation)**	Free movement of data Encourage porting of data for professional users Restriction of data localization rules in the EU	Asymmetric	Non-personal data; aggregate data	The GDPR prevails Overlap with the DGA in so far as reuse of non-personal data is concerned In the case of a data set composed of both personal and non-personal data, the Regulation applies to the non-personal data part of the data set. Slight overlap regarding data portability with the DA	In force, applicable since 28 May 2019
e-Privacy Regulation	Privacy in electronic communications	Asymmetric	Personal data, non-personal data	The GDPR prevails: can be applied simultaneously with the GDPR Includes more specific provisions on protecting privacy in the context of electronic communications	Proposal published on 10 January 2017; Trilogue since spring 2021 Possibly applicable in the second half of 2024, 24 months after entry into force
Data Governance Act or DGA	Make more data available and create governance models for sharing Increase trust in data intermediaries	Symmetric	Personal data, non-personal data, confidential data, data for IoT providers	The GDPR and the Free Flow Regulation prevail	The Data Governance entered into force on 23 June 2022 and, following a 15-month grace period, is applicable since September 2023.
Proposal for a Regulation laying down harmonized rules on artificial intelligence **(Artificial**	Improve predictability, optimize operations, and resource allocation, and personalise service delivery of the use of AI	Symmetric	Mixed data, personal data, non-personal data	The GDPR prevails exceptions for sensitive personal data	Proposal on 21 April 2021 Currently under negotiations

Funded by the European Union

Intelligence Act or AIA)	Categorization of AI according to risk			Transparency obligations on top of Articles 13 and 14 of GDPR	Possibly applicable in 2024, 24 months after entry into force
NIS 2 Directive on Measures for a High Common Level of Cybersecurity across the Union	Increase cyber resilience across essential service providers, streamline cyber resilience through stricter security requirements and penalties for violations, and improve the EU's preparedness to deal with cyber-attack	Symmetric	Incident reporting within critical supply chains, non-personal data	Some overlap, NIS is about protecting the infrastructure and GDPR is about personal data	in effect since January 16, 2023; transposition period, is set for October 2024
Product Liability Directive (PLD) and AI Liability Directive (AILD)	Establish uniform regulations for non-contractual fault-based liability concerning damages resulting from HRAIS. Improve the functioning of the internal market by setting uniform requirements for non-contractual civil liability involving AI systems.	Asymmetric	digital manufacturing files, software applications, and AI system files – all corresponding to non personal data segment	PLD overlaps with the GDPR AILD overlaps with the EU AI act	The PLD, proposed in September 2022, awaits full implementation details after the Council's June 2023 adoption. The AILD, proposed in September 2022, awaits consideration by the European Parliament and Council; once finalized, it enters into force, with Member States given two years for domestic implementation.

Funded by the European Union

5. Relevance of the legal and regulatory frameworks for DiCiM project demonstrators and results

The key technological developments in DiCiM project, as mentioned in section 2, include open access digital platform (for storing, sharing, and analysing data), IoT solution for collecting data from products (for condition monitoring and location tracing), and solutions for harvesting components from the used products. Based on the review of different legal and regulatory frameworks in section 3 and 4 and interviews with DiCiM stakeholders, an analysis is performed to map the relevance of legal and regulatory frameworks to different areas of developments in DiCiM project, as summarised in Table 2 below.

Table 2 Relevance of Individual EU Legal Acts to the DiCiM Project Scopes

DiCiM Scope	Data Act	Digital Services Act or DSA	Digital Markets Act or DHA	Open Data Directives	GDPR	Free Flow Regulation	E-Privacy Regulation	Data Governance Act or DGA	NIS2	Artificial Intelligence Act or AIA	ESPR	WEEE Directive/ROHS and REACH	Vehicle Design & Management of EoL	Battery Regulation	Product Liability & AI Liability Directives
Open access data platform	Relevant	Relevant	Limited relevance – related to right stakeholder(s) to have access to data	Relevant - in compliance with DGA and DA	Relevant	Relevant - with National Regulation as well as harmonized regulations	Relevant - correlation with personal data	Relevant	Relevant	-	-	-	-	-	-
Collecting data from products (for condition monitoring and location tracing)	Relevant	Relevant – only for commercial purposes	Relavant – Ownership of collected data	No relation with data collection for Businesses - only publicly accessible data	Relevant	-	Relevant - personal data such as location tracking	-	-	Relavant only when deploying AI for ML processing of IoT sensor data	Relevant - (DPP requiremenst)	-	-	-	Relevant - only when deploying AI for ML processing of IoT sensor data
Harvesting components from the used products[i]	Relevant – considering exceptions	-	-	-	No correlation	Relevant - Conditionally applicable for exemption components	Relevant - Conditionally applicable for exemption components	-	-	-	Relavant (DPP requiremenst)	Relevant (distinguishement between new products and waste)	Relevant	Relevant	-
Access to the (used) products[i]	Relevant	Relevant	-	-	Relavant - implication on exceptions only	-	Relevant - Conditionally applicable for exemption components	-	-	-	Relevant (DPP requiremenst)	Relevant (distinguishement between new products and waste)	Relevant - Development of Environmntal Vehicle Passport	Relevant	-
Sharing data across the value chain and making the data public[ii]	Relevant	Relevant	Relavant – ownership of data & right stakeholders	Relevant - B2B sharing of non sensitive data	Relevant	Relevant - Applicable with National Regulation as well as harmonized regulations	Relevant	Relevant	-	-	Relevant (DPP requiremenst)	-	Relevant - Development of Environmntal Vehicle Passàort	Relevant - for batteries exceeding 2kWh capacity	-

[i] Only equipment that does not contain data – Exceptions for Data Storage Devices (Hard Disk, SSD etc.). The WEEE, RoHS and REACH will be applicable.
[ii] In the context of a public data market

In the following sections we discuss implications of identified legal and regulatory frameworks for these technological developments.

5.1. Circularity and environmental regulations compliance

The regulatory framework concerning environmental requirements has evolved and matured over time, aligning with the prolonged development of EU legislation. Despite continuous updates and refinements, respondents in the EU market have garnered substantial experience in maintaining compliance. However, challenges and contradictions persist, particularly when translating EU horizontal regulations and individual directives into various national contexts. This complexity becomes particularly apparent in the context of waste-related directives and the utilization of refurbished components in new products.

Funded by the European Union

As pointed out by stakeholders, assessing, and controlling the adherence of partners and suppliers to these regulations remains a significant challenge. The respondents acknowledge that legal and regulatory compliance challenges related to environmental regulations, such as REACH, WEEE, Ecodesign, and RoHS directives, primarily pertain to supply chain management. This necessitates thorough tracking, testing, and material management to ensure compliance. Divergent sets of regulations across regions and countries add complexity to compliance efforts, given the non-harmonization of global regulations. The upcoming ESPR changes will necessitate enhanced information and transparency within the supply chain. Ensuring complete product lifecycle tracking, down to the serial number, presents an additional challenge, with responsibility often lying with customers.

Notably, a unified EU-wide registration system is unfeasible due to variations in the directive's implementation across Member States. Some countries provide publicly accessible national registers for electrical appliance manufacturers, enabling quick verification of registration status. The public accessibility of these registers aligns with enforcement measures undertaken by national authorities, ultimately incentivizing producers to fulfil their obligations as responsible manufacturers in compliance with the WEEE Directive. Manufacturers should consider these registration requirements and the associated enforcement measures when providing data on their products within the EU. In the context of WEEE, EPR principles ensure that manufacturers take responsibility for the proper disposal and recycling of electronic products they produce.

Several respondents have taken proactive measures to mitigate regulatory and legal challenges. They've implemented a Supplier Declaration of Conformity, which suppliers must complete at least once annually. Additionally, they enhance transparency by making REACH and RoHS declarations publicly accessible through a digital passport. Moreover, the suppliers of components, assemblies, and products are obligated to adhere to the Company Product Environmental Specification (CPES), which mandates compliance with global regulatory requirements, international treaties, conventions, and customer stipulations. An internal council of subject matter experts conducts periodic reviews of the CPES, leading to annual updates. Suppliers are promptly notified of revisions and are required to confirm their adherence by signing a declaration of conformity.

The respondents foresee that those responsible for Company Compliance Operations will be deeply involved in all aspects of ESPR, requiring careful consideration of workload, resources, and investments. The challenge of aggregating data presents an opportunity, as the companies aim to harmonize their digital passport approach within a standardized framework.

For instance, the upcoming ESPR framework will reset various requirements concerning product durability, substance presence, energy efficiency, recycled content, and environmental footprints. Some companies have already started addressing product durability as part of their design principles, emphasizing sustainability within their organization’s mission.

Anticipating the implementation measures under the Ecodesign and Energy Labelling Working Plan 2022-2024, the respondents foresee impacts on the organisation, particularly within compliance, design, and supply chain processes. This may require an increase in patents to protect trade secrets

Funded by
the European Union

and intellectual property. Most respondents aim to maintain awareness of new legislation and take proactive measures to ensure compliance, aligning with the company's commitment to legal and regulatory compliance.

The regulatory frameworks discussed in this report directly relate to the DiCiM Project in the following ways:

- **ESPR:** The ESPR enable the setting of performance and information requirements for almost all categories of physical goods placed on the EU market, including IoT-based data connected products such as washing machines, printers, refrigerators, and automobiles.
- **The WEEE (Waste Electrical and Electronic Equipment) Directive** plays a crucial role in shaping the landscape for individual products, including IoT devices, in the EU market. Just as the ESPR (Ecodesign and Energy Labelling Regulations) empower the establishment of performance and information standards for a wide range of physical goods sold in the EU, including items like washing machines, printers, refrigerators, and automobiles, the WEEE Directive governs the responsible disposal and recycling of electronic and electrical products, ensuring their environmental impact is minimized. This means that IoT-based data-connected products, like smart home devices, must adhere to WEEE regulations, not only in terms of their design and energy efficiency but also in terms of end-of-life management to minimize electronic waste and promote sustainability. WEEE: The directive requires manufacturers to design products that are more environmentally friendly and easier to recycle and recover. In case of accessing any parts of the product, or product itself, which contains user data should be protected by environmental safety. Article 49 of the WEEE Directive provides an exemption that permits the treatment and storage of specific categories of WEEE for the purpose of repair or refurbishment. This exemption applies to waste electronic and electrical equipment specified in Tables 11A and 11B of Schedule 2, Part 1 of the Waste Management Licensing Regulations 2003. These specified waste streams include various types of WEEE, such as equipment containing hazardous components or substances like chlorofluorocarbons (CFCs), hydrochlorofluorocarbons (HCFCs), and hydrofluorocarbons (HFCs). This exemption allows for the responsible handling and treatment of these WEEE categories to facilitate their repair or refurbishment processes, contributing to the circular economy's objectives within the context of waste management regulations.
- **RoHS Directive:** Products within the scope of RoHS must comply with strict regulations regarding the content of restricted substances, requiring manufacturers, importers, and distributors to demonstrate adherence. Manufacturers and suppliers of EEE, falling under the purview of the RoHS Directive, are obligated to adhere to data reporting requirements. These obligations necessitate the provision of comprehensive information concerning the conformity of their products with RoHS restrictions. This information encompasses explicit details regarding the presence or absence of restricted substances. Typically, this data is submitted to regulatory authorities, and in certain instances, it may also be made accessible to the public.
- **REACH Directive**: Companies must register, evaluate, and, if necessary, seek authorization for the use of certain chemical substances in their products. This regulation promotes transparency and the responsible handling of chemicals throughout the supply chain, covering not only the

Funded by
the European Union

production of chemicals but also their usage in various products. As with other EU regulations, navigating and adhering to the requirements of REACH is an obligation for companies operating within the EU market.

- **Vehicle Design and Management of EoL Directive -** Key action for companies in the EU automobile sector: Embrace circular design, increase recycled content in production, adhere to regulations on harmful substances, collaborate with manufacturers for value recovery, and comply with updated circular strategies every five years. New design requirements, moderate targets for recycled plastics, and environmentally sound treatment of end-of-life vehicles are essential. Extended Producer Responsibility (EPR) covers collection costs, and economic incentives like 'deposit return schemes' are encouraged for higher value recovery. Compliance is crucial for sustainable and circular business models.
- **Battery regulation:** The EU's Batteries Regulation, impacts all economic operators in battery manufacturing, importation, and distribution within the EU market. It expands producer responsibility, mandates supply chain due diligence, and introduces labelling requirements for social and environmental implications. Four key areas of change include enhanced recycling measures, increased use of recycled raw materials, supply chain management, and labelling and information disclosure such that manufacturers must comply with sustainability and safety standards, establish due diligence policies, and introduce digital battery passports. Regulations on labelling requirements will include detailed data, and a minimum recycling for lithium-ion batteries is set in place. Collection targets for portable batteries will increase, and violators face penalties by August 18, 2025. Complying with these regulations is crucial for sustainability, supply chain accountability, and improved recycling practices in the battery industry.
  Within the framework of the DiCiM project, it is pertinent to clarify that the products encompassed by the project's scope do not presently incorporate batteries. Nevertheless, a meticulous examination of the document assumes paramount significance from a strategic perspective, as it serves as a proactive measure for future-proofing and aligns with the intersection of batteries within the automotive sector. This discerning review ensures that the project remains resilient and adaptable to forthcoming developments, thereby enhancing its overall efficacy and relevance.

5.2. Open access digital platform

This section outlines the relevance of different Acts for developing open access digital platform.

- **Data Act:** The EU Data Act provides a framework for data sharing within the EU, ensuring fairness, legal certainty, and abuse prevention. For an open access data platform between OEMs, it can establish clear guidelines for data sharing and usage. It also provides legal clarity for data generators and prevents abuse of contractual imbalances. However, additional considerations such as proprietary information and technical compatibility may need to be addressed.
- **Digital Service Act:** The Digital Services Act aims to create a safer digital space and establish a level playing field for businesses. Open access data platform aligns with these goals by fostering transparency and accountability among OEMs. By facilitating the exchange of data, your platform

Funded by
the European Union

can enhance innovation, competitiveness, and user protection, all of which are key objectives of the DSA.

- **Digital Markets Act:** The aim of this act is to establish an unbiased market for data ensuring that the sharing and access of data with the right stakeholder. The implications for the company lie in liability and indemnification: there is a need to learly define liability and indemnification clauses in contracts and agreements to address potential legal disputes, data breaches, or other issues.
- **Open Data Directive:** The EU Open Data Directive provides a common legal framework for making public sector information available for re-use. This directive can facilitate the establishment of an open access data platform between OEMs by ensuring transparency and fair competition. It encourages the re-use of information and stimulates the publishing of dynamic data via Application Programme Interfaces (APIs), which could be pivotal in sharing and accessing data across different OEMs.
- **GDPR:** The GDPR ensures data privacy and protection standards for an open access data platform. It assists in managing data, policies, and handling processes, particularly during data breaches. It also encourages 'Privacy by Design' and 'Security of Processing'. Another notable relevance is 'protection of personal data'.
- **Free flow regulation:** The Free Flow of Non-Personal Data Regulation supports an open access data platform between OEMs by removing data localization requirements and promoting data mobility. It also encourages self-regulatory codes and best practices for data processing.
- **E-Privacy Regulation:** The EU's E-Privacy Regulation aims to reinforce trust and security in the digital communication service. The regulation ensure customers with clear and concise information about how their data will be used and who it will be shared with. In addition, customer can share option to withdraw their consent at any time.
- **DGA:** The DGA proposes rules to ensure fairness in data-sharing contracts and to allow public sector bodies to use data held by enterprises where there is an exceptional need, such as a public emergency. The act provides provisions regarding user rights of data, data by design, right to share data with third parties, limitations on use of data, and exceptions.
- **NIS2:** NIS2 ensures appropriate security measures and notify relevant national authorities of serious incidents for business and customer perspective for securing data form third parties.

5.2.1. Sharing data across the value chain and making data public

The sharing of data across value chain has been viewed from 2 scenarios: Instance 1: Sharing data across intended supply chain network for R&D purposes within the scope of the participating organisations. Instance 2: Creating a public data set such as a data market for extended supply chain including third party clients.

- **Data Act:** the EU Data Act can facilitate the establishment of a data platform for OEMs. It encourages the re-use of information and stimulates the publishing of dynamic data via Application Programme Interfaces (APIs), which could be pivotal in sharing and accessing data across different OEMs. For the second instance, the EU Data Act establishes detailed rules to rectify the power imbalance between data holders and SMEs in relation to data access and sharing

Funded by the European Union

arrangements. This can support the goal of making collected data available on a public platform for reproduction and utilization by other manufacturers and third-party service providers.

- **DSA:** the EU Digital Services Act (DSA) doesn't directly regulate data sharing between OEMs, but it does create a safer digital space with new rules on privacy, security, and data sharing. This could indirectly influence how OEMs handle and share data. For the second instance, the DSA requires large online platforms to give access to publicly available data to vetted researchers. This could potentially extend to other manufacturers and third-party service providers, allowing them to utilize this data for engineering and development purposes.
- **DMA:** the EU Digital Markets Act targets "gatekeepers" to ensure fair competition. If the platform becomes significantly influential, it may face additional regulations.
  For the second instance, the Act promotes interoperability and data portability, facilitating data sharing between your platform and other services. However, it applies only to "gatekeepers".
- **Open Data Directive:** the EU Open Data Directive encourages re-use of information and publishing of dynamic data, facilitating data sharing among OEMs.
  For the second instance, it establishes rules for data access and sharing, supporting your goal of making data available for reproduction and utilization by other manufacturers and third-party service providers.
- **GDPR:** The EU GDPR ensures that activities related to IoT data collection adheres to data privacy and protection standards, particularly when handling personal data. For the second instance, GDPR mandates that any individual or company contributing to the generation of IoT data has the right to access it. The data should be made available on fair, reasonable, and non-discriminatory terms. If the company collects and processes personal data, it must comply with data protection laws relevant to its jurisdiction. This includes obtaining consent, providing data subjects with access and control over their data, and ensuring the security of the data.
- **The regulation on Free Flow of Personal Data Regulation** can facilitate the establishment of a data platform for OEMs. It ensures that every organisation should be able to store and process data anywhere in the EU. Furthermore, the regulation encourages service providers to develop codes of conduct specifying the terms and conditions for transferring data between cloud service providers and back into an organisation's own IT environments. This promotes the companies' objective of making the data they collect accessible on a public platform, allowing other manufacturers and third-party service providers to reproduce and use it.
- **E-Privacy Regulation:** The regulation ensure that data platform have obtained explicit consent from the customers before collecting their data. It must have implemented appropriate security measures to protect the data collected form the customer.
- **Data Governance Act:** The company operating the data platform must ensure that it comply with the act's provisions regarding user rights of data, data by design, right to share data with third parties and the necessary limitations on use of data.

Funded by
the European Union

5.2.2. Access to data from used products

- **Data Act:** The EU Data Act can significantly impact product-as-a-service model for white goods and electronics. It empowers users to have more control over the data they generate, including data stored on devices like hard disks and solid-state drives. This means that at the end of a product's lifecycle, data must be handled in a way that respects user rights and privacy. Therefore, the service must ensure secure data management and adhere to these regulations to maintain trust and compliance.
- **DSA:** The EU Digital Services Act (DSA) primarily focuses on digital services and online intermediaries. While it doesn't directly regulate the lifecycle of physical products or components, it does have implications for data stored on devices like hard disks and solid-state drives. The DSA ensures a safer digital space where the rights of all users are protected. Therefore, any personal data stored on your products must be handled in a way that respects user rights and privacy.
- **GDPR:** The EU's GDPR plays a pivotal role in shaping your product-as-a-service model. It necessitates the incorporation of privacy and data protection measures at the inception stage of IoT devices. This encompasses the execution of robust technical safeguards to secure personal data and guarantees that data subjects are not subjected to decisions based purely on automated decision-making. Moreover, the GDPR stipulates a lawful basis for the processing of personal data, frequently necessitating explicit consent, particularly in scenarios where substantial data protection risks are present.
- **E-Privacy Regulation** ensures that data platforms operators have obtained explicit consent from the customers before collecting their data. It must have implemented appropriate security measures to protect the data collected form the customer.

5.3. IoT solution for collecting data from products

IoT data can be personal and non-personal, with personal data governed by GDPR, while non-personal data lacks de jure rights, meaning that IoT device manufacturers can choose designs granting them de facto control over all generated data, limiting user access and hindering other entities from using the data (Kerber, 2023).

In the context of IoT solutions, manufacturers often have significant control over non-personal and automatically generated data from these devices, potentially limiting users' access and usage rights. This concern led to the European Commission's Communication on building a European data economy and as a continuation of discussions in the stakeholder dialogue, the Commission introduced a set of principles in the Communication titled "Towards a common European data space" and its

Funded by
the European Union

accompanying staff working document[23],[24]. These principles are intended to guide contractual agreements and promote fairness and competition in markets involving IoT objects and the products and services relying on the non-personal data generated by these devices.

The following legislative acts currently apply to Business-to-Business (B2B) data sharing: the GDPR (see section 4.1.3), the Regulation on the Free Flow of Non-personal Data and the EU Cyber Security Act. Balancing data sharing while respecting GDPR and privacy regulations is a complex challenge for businesses. For instance, when determining the level of granularity for capturing IoT data from machines, it's crucial to consider GDPR regulations, including geographic granularity. Data ownership and privacy concerns often lead organisations to be cautious about open data sharing. To avoid overstepping boundaries, companies tend to apply GDPR more restrictively than required. In the domain of B2B data sharing, legal barriers can significantly impede the process. One common issue companies encounter is the denial of access to the data they need. The study by EC performed in 2018 reinforces earlier findings by highlighting that the primary data-sharing challenges are rooted in legal aspects.

Legally, challenges arise due to uncertainties about data ownership and what can be lawfully done with it. Moreover, complying with data protection regulations in a B2B context can be intricate. When it comes to reusing data, companies often face obstacles such as being denied access to the necessary datasets. Sometimes, even when access is granted, it may come with expensive and complex conditions. These legal complexities can pose significant hurdles to effective B2B data sharing and reuse.

In the Business-to-Consumer (B2C) domain, the e-Privacy Regulation plays a crucial role in governing IoT devices, establishing fundamental rules and principles for their development and deployment. One key principle is that accessing and utilizing the processing and storage capacities of IoT devices, as well as accessing information stored on them, does not require explicit consent if these actions are deemed necessary for delivering the specific service requested by the end-user. In such cases, the need for prior consent is waived. However, when information stored on IoT devices is intended for purposes that extend beyond the core service provision, obtaining explicit consent from users becomes mandatory. These guidelines seek to strike a delicate balance between enabling essential IoT functionalities and upholding user privacy and data protection rights, all within the bounds of the regulatory framework. Below we discuss relevance of different Acts for developing IoT solution for collecting data from products.

[23] SWD/2018/125 final. Commission Staff Working Document on Sharing Private Sector Data in the European Data Economy Accompanying: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, titled "Towards a Common European Data Space". {COM(2018) 232 final}

[24] The guidance provided in this document is intended for application across all sectors of the economy. IT should be noted that this document does not constitute a legal statement and should not be taken as a definitive interpretation of EU law, which falls under the purview of the Court of Justice of the European Union (CJEU). Furthermore, it does not impose binding obligations on the European Commission in its application of EU law, particularly in relation to the competition rules outlined in Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU).

Funded by the European Union

- **Data Act:** The EU Data Act impacts your IoT data collection platform in several ways. It mandates that any individual or company contributing to the generation of IoT data has the right to access it. The Act also stipulates that IoT devices should be designed to make data directly accessible to the user. Furthermore, it allows users to request the data holder to make the data available to a third party. These regulations ensure fair and transparent data sharing, which your platform must comply with.
- **DSA** primarily focuses on digital services, online intermediaries and issues related to content moderation which may be relevant for commercial purposes only. Hence it is a weak relevance.
- **DMA:** The regulation implies the ownership and trade of data. Furthermore, the Act promotes interoperability and data portability, which could facilitate data sharing between your platform and other services. Context with respect to anticompetitive practices are discussed in the DMA.
- **Open Data Directive:** When the collected data is made public information, the ODD elucidates the unbiased access to public data. Hence an extended relevance exists.
- **GDPR:** The EU GDPR requires your IoT data collection platform to implement privacy and data protection measures from the design stage. It mandates technical measures to protect personal data and ensures that data subjects are not subject to decisions based solely on automated decision-making. Furthermore, it requires lawful grounds for the processing of personal data, often requiring explicit consent.
- **E-Privacy regulation:** The EU's E-Privacy Regulation aims to reinforce trust and security in the digital communication service in the end products. Customers can ensure their info, daily user meta data, with clear and concise about how their data will be used and who it will be shared with. At any point customer can withdraw their consent with opinion.
- **AIA:** The act identifies "high-risk" AI systems that warrant special security precautions of user personal any IOT connected equipment.
- **ESPR:** The ESPR enable the setting of performance and information requirements for almost all categories of physical goods placed on the EU market, including IoT-based products such as washing machines, printers, refrigerators, and automobiles.

5.4. Technological solutions for harvesting components from used products

DiCiM aims to develop two technological solutions to support harvesting of parts/components from used products.

- Augmented Reality solution to decrease the error rates in disassembly/dismantling of products
- Image processing solution to recognise visual defects in used products/parts to decrease visual testing time

Commercial adopters of Extended Reality (XR) technologies, which involve the processing of personal data pertaining to EU individuals, must adhere to the GDPR and the ePrivacy Directive. The data gathered through XR technologies, including user interactions and representations in virtual

Funded by the European Union

environments, frequently pertains to a readily identifiable or identifiable natural person. Moreover, it is plausible that interfaces like Head-Mounted Displays (HMDs) would be categorized as "terminal equipment" according to the ePrivacy Directive. This directive generally imposes restrictions on the collection of data from such devices, permitting only the acquisition of information objectively necessary for service provision.

Given that EU data protection legislation remains neutral concerning the specific devices and interfaces employed for data processing, it inherently extends its applicability to encompass most commercial applications utilizing XR technologies. XR technology deployments with data processing implications must adhere to stringent EU data protection and privacy regulations, as these technologies inherently involve the handling of personal data, necessitating compliance with the GDPR and ePrivacy Directive provisions. This regulatory framework (and its individual regulatory acts) ensures that XR applications prioritize the safeguarding of individuals' privacy and data protection rights within the EU.

In particular, the Digital Services Act (DSA) is likely to encompass XR technology deployers, especially those operating centralized immersive environments. Under this legislation, intermediaries qualifying as online platforms are restricted from presenting profiling-based advertisements to users who may be minors or using sensitive data for such purposes. If these intermediaries employ automated systems for content recommendations, they may be required to offer users a non-profiling-based alternative for receiving suggestions.

Furthermore, XR deplorers may fall under the purview of the Digital Markets Act (DMA) if they meet specific criteria and qualify as 'gatekeepers.' This applies when they provide 'core platform services' and reach defined thresholds. In such cases, they are prohibited from utilizing insights gained from user interactions with other businesses for targeted advertising, as well as from combining or cross-utilizing personal data. The DMA also extends users' GDPR portability rights, potentially encompassing telemetry data generated by XR platforms, including detailed information such as eye movement patterns.

Additionally, the categorization of Extended Reality (XR) technologies within the framework of the EU's Artificial Intelligence Act will potentially exert a substantial influence on the methodologies and procedures governing the development and implementation of these technologies within the EU. Below we discuss relevance of different Acts for developing technological solutions for harvesting components from used products.

- **Data act:** The EU Data Act can significantly impact product-as-a-service model for white goods and electronics. It empowers users to have more control over the data they generate, including data stored on devices like hard disks and solid-state drives. This means that at the end of a product's lifecycle, data must be handled in a way that respects user rights and privacy. Therefore, the service must ensure secure data management and adhere to these regulations to maintain trust and compliance.
- **DSA:** The EU Digital Services Act primarily focuses on digital services and online intermediaries. While it doesn't directly regulate the lifecycle of physical products or components,

Funded by
the European Union

it does have implications for data stored on devices like hard disks and solid-state drives. The DSA ensures a safer digital space where the rights of all users are protected. Therefore, any personal data stored on your products must be handled in a way that respects user rights and privacy.

- **GDPR** plays a pivotal role in shaping a product-as-a-service model. It necessitates the incorporation of privacy and data protection measures at the inception stage of IoT devices. This encompasses the execution of robust technical safeguards to secure personal data and guarantees that data subjects are not subjected to decisions based purely on automated decision-making. Moreover, the GDPR stipulates a lawful basis for the processing of personal data, frequently necessitating explicit consent, particularly in scenarios where substantial data protection risks are present.
- **E-Privacy regulation:** For harvesting any legal components from the used product it has to obtain explicit consent from customers before collecting their data and appropriate security measures need to be implemented to protect the collected data. Additionally, customers should have clear and concise information about how their data will be used and who it will be shared with.
- **AI Liability Directive (AILD):** Under the AI EU liability legal act, these changes and amendments to the Updated Product Liability Directive have s implications for IoT products driven by AI systems by explicitly including AI systems and AI-enabled goods and services under the definition of products, ensuring that if defective AI causes harm, compensation is accessible without the need to establish the manufacturer's fault. The expanded liability coverage also holds software providers and digital service providers accountable for their impact on AI-related products, emphasizing that modifications, even through software updates or machine learning, can render them responsible. The directive stresses that a lack of necessary software updates or upgrades affecting a product's safety does not exempt the responsible party from liability. This directive is designed to offer individuals seeking compensation for damage caused by high-risk AI systems clear and effective methods to pinpoint those who might be responsible and gather relevant evidence. The PLD review concerns the adaptation of the producers' strict liability regime for defective products to allow for compensation for damages without the need to prove a fault. It will apply to high-risk AI systems (as defined in Article 6 of the AI Act). The AI liability directive would give national courts the power to order disclosure of evidence about high-risk AI systems. Some experts believe that AI system providers will struggle to protect themselves from liability due to the need to adhere to various safety and liability regulations, including potential claims under the new AI liability directive.

5.5. Limitations and future research

The limitations of this analysis stem from several factors. Firstly, it is important to consider that certain legal and regulatory instruments and surrounding documentation have undergone recent revisions by EU regulatory bodies, while others have not yet come into force (not published in the Official Journal of the EU) and remain unpublished in their final form with drafts in progress available in the Eur-lex database at the moment of the analysis alone. Consequently, this analysis in certain instances relies

Funded by
the European Union

on the text of proposed submissions that are currently under negotiation, such as the AI Act and the ESPR Directive intended to replace the Ecodesign Directive. Additionally, there is a lack of peer-reviewed and empirical evidence derived from real-world business practices within the manufacturing sector that adopt circular value management principles through the utilization of cutting-edge digital technologies. Moreover, the sample of stakeholders interviewed is largely limited to the entities participating in the DiCiM project.

Despite an extensive interview protocol, the study encountered limitations as respondents had not yet initiated the development of products under the purview of new and emerging EU data regulations. Consequently, their responses often remained general in terms of the regulations' applicability to their specific operations, in contrast to responses regarding the well-established environmental and product regulations where companies demonstrated specific experiences and clear compliance measures. Additionally, respondents were aware of upcoming legal and regulatory acts. They expressed a plan to familiarize themselves with them when they arise, leading to a lack of in-depth analysis in the house. Moreover, the respondents from the interviewed companies underscored the continuous evolution of data-related regulations, noting numerous concurrent processes. The apparent overlap in these processes was exemplified by the predominant coverage of personal data under the GDPR, prompting concerns regarding the necessity for additional legislative acts regulating analogous domains. It is imperative to acknowledge that this report while addressing concerns raised by interviewees, does not explicitly delve into the intricacies of national regulations, nor does it explicitly elucidate potential conflicts and incoherencies across EU member states.

Based on the analysis, it is evident that there are several avenues for future research that can enhance our understanding of the intersection between Circular Economy Governance Framework and Data Governance Framework within the context of the EU and their legal and compliance implications. The next steps should include the revision of the outlined regulatory acts and policy frameworks that pertain Circular Economy Governance Framework in the EU with the recognition of the upcoming legislative and regulatory proposals as well as a broader body of legislation that concerns EU Green Transformation and Green Deal ambitions.

Funded by
the European Union

6. Final conclusions and recommendations

The DiCiM project revolves around two major dimensions: the Data Dimension and the Product Dimension. In the Data Dimension, various legal acts come into play, such as the GDPR, Data Act, and ePrivacy Regulation, designed to protect consumers from threats like unauthorized data access and privacy violations while promoting a safer, more transparent digital environment. On the other hand, the Digital Market Act, Digital Service Act, Data Governance Act, and Free Flow Regulation are dedicated to establishing a level playing field for digital companies, facilitating data use and sharing, regulating digital markets, and fostering innovation while ensuring data security. The deliverable explored the regulatory landscape within the EU, emphasizing its dynamic evolution and the impact on data and product management. The relevance of EU regulations for the DiCiM project's Data and Product dimensions underscores the pivotal role of legal frameworks in circular economy and circular manufacturing systems.

As the Data Regulatory Framework becomes active, businesses will need to adapt their products and data management practices to ensure compliance. This entails data handling procedure adjustments, contract updates, and robust security measures to safeguard data. The regulations also raise questions about balancing rights and obligations for mixed data sets and their coverage, and the data ownership aspects.

Conversely, the Product Dimension encompasses regulations like the Ecodesign Directive, RoHS, REACH, WEEE Directives, and the Digital Product Passport, aiming to create a sustainable digital ecosystem. These regulations synergistically contribute to shaping a more sustainable and circular manufacturing system integrated with a digital environment.

The report emphasizes the intricate nature of the regulatory landscape in the EU and its far-reaching consequences for a spectrum of domains, including IoT products, AI-driven technologies, data governance, environmental compliance, and product liability. As the proposed directives continue to evolve within the EU legislative process and become part of Member States' national laws, stakeholders must proactively prepare for forthcoming regulatory requirements. It underscores that comprehensive documentation, effective supply chain collaboration, and adept management of third-party relationships, proactive compliance initiatives, rigorous due diligence processes, methodical record-keeping, and the maintenance of a precise data system inventory are all imperative.

The report underscores the need for organisations to be proactive in engaging with these regulatory transformations to ensure compliance and adept legal risk management in the ever-evolving digital terrain. These steps are not merely a matter of conforming to regulations; they represent a strategic approach to not only meet current legal requirements but also to safeguard a company's reputation, foster trust among stakeholders, and thrive in a swiftly evolving digital ecosystem. In this regard, the ongoing commitment to regulatory adherence and the proactive management of legal risks will be instrumental in enabling organisations to navigate the multifaceted EU regulatory landscape successfully.

Funded by
the European Union

Recommendations:

1. As we envision future developments and innovations, specialized legal expertise and due diligence will be essential to navigate the evolving regulatory terrain. Stakeholders and companies, including OEMs, software developers, and end-users, must remain vigilant, considering existing regulations and pending proposals under negotiation. *We recommend engaging qualified legal counsel to gain a comprehensive understanding of regulatory nuances and ensure seamless legal compliance within the context of the DiCiM project.*
2. To effectively navigate the intricate landscape of evolving environmental and data legislation and maintain a proactive stance, the companies should continue to leverage their memberships in trade and industrial associations, and professional partnerships and engage with external legal counsel. To stay ahead of regulatory changes and effectively align its operations with the evolving legal landscape, a company should actively monitor regulatory alterations, comprehend their implications and the relevant areas of application, and be cognizant of the legislation's enactment timeline. This approach enables manufacturers and product and service developers to seamlessly integrate the necessary requirements related to data regulations, product design circularity, and environmental performance, allowing for a more holistic and efficient compliance strategy.
3. Supply chain collaboration is key. For instance, the Batteries Regulation necessitates a collaborative effort involving manufacturers, producers, importers, and distributors of various battery types operating within the EU market. These stakeholders are mandated to implement substantial alterations encompassing labelling, end-of-life management, and the instatement of due diligence within their supply chains. Businesses engaged in battery production are encouraged to proactively scrutinize the ratified legislation and initiate preparations to ensure compliance.
4. Record-keeping and accurate inventory: To proactively prepare for evolving regulatory demands, organizations should prioritize robust documentation practices. As an example, in compliance with the Al Liability Directive and the Updated Product Liability Directive, ensuring the accurate, timely, and comprehensive maintenance of data and documentation related to Al systems. In addition, organizations operating Al systems, regardless of their risk level, should systematize record-keeping processes to meet EUAIA requirements, facilitating responses to disclosure requests and compliance evidence provision. Moreover, maintaining a thorough inventory of all Al systems is essential, given the growing prevalence of algorithmic and Al systems, ensuring compliance with the broad EU definition for Al systems and meeting the EUAIA and Al Liability Directive's focus on regulatory and legislative requirements. Similarly, maintaining accurate and comprehensive records is a fundamental aspect of regulatory compliance for various other domains discussed in this report, including digital product passports (DPP). The importance of accurate, timely, and well-documented data management remains relevant in ensuring compliance with digital passport-related regulations, facilitating responses to disclosure requests, and providing evidence of adherence to regulatory requirements.

Funded by
the European Union

7. Annexes

7.1. Annex 1 Documents Reviewed

1. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (OJ L 186, 11.7.2019, p. 57).
2. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of the terrorist content online (OJ L 172, 17.5.2021, p. 79).
3. Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (OJ L 274, 30.7.2021, p. 41).
4. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).
5. Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws and repealing Regulation (EC) No 2006/2004 (OJ L 345, 27.12.2017, p. 1).
6. Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011 (OJ L 169, 25.6.2019, p. 1).
7. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety (OJ L 11, 15.1.2002, p. 4).
8. Proposal for a regulation of the European Parliament and of the Council on circularity requirements for vehicle design and on the management of end-of-life vehicles, amending regulations (EU) 2018/858 and 2019/1020 and repealing directives 2000/53/EC and 2005/64/EC - COM/2023/451 final.
9. Regulation (EU) 2023/1542 of the European Parliament and of the Council, 12 July 2023, concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC (Text with EEA relevance).
10. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (OJ L 149, 11.6.2005, p. 22).

Funded by the European Union

11. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council (OJ L 304, 22.11.2011, p. 64).
12. Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (OJ L 165, 18.6.2013, p. 63).
13. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).
14. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22.6.2001, p. 10).
15. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004, p. 45).
16. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, p. 92).
17. Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (OJ L 321, 17.12.2018, p. 36).
18. Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).
19. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA (OJ L 335, 17.12.2011, p. 1).
20. Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (OJ L 101, 15.4.2011, p. 1)
21. Directive EU Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88, 31.3.2017, p. 6).
22. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).
23. Council Directive (EU) 2021/514 of 22 March 2021 amending Directive 2011/16/EU on administrative cooperation in the field of taxation (OJ L 104, 25.3.2021, p. 1).
24. Directive 98/6/EC of the European Parliament and of the Council of 16 February 1998 on consumer protection in the indication of the prices of products offered to consumers (OJ L 80, 18.3.1998, p. 27).

Funded by
the European Union

25. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure (OJ L 157, 15.6.2016, p. 1).
26. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC (OJ L 409, 4.12.2020, p. 1).
27. Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).
28. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39).
29. SWD (2018) Guidance on sharing private sector data in the European data economy Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space" {COM(2018) 232 final
30. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, pp. 15–69)
31. Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, pp. 1–38)
32. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, pp. 39–98).
33. Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products (commonly referred to as the 'PLD' or Product Liability Directive)

Funded by the European Union

7.2. Annex 2 Mapping of Legislative acts and individual clauses relevant to DiCiM Development

Table 3 A Mapping of Legislative Acts Individual Clauses to DiCiM Developments

DiCiM Scope	Legislative Act	Article	Clause
Open Access Data Platform	Data Act	Article 2: Definition	1,2
		Article 3: Obligation to make data generated by the use of products or related services accessible	1
		Article 4: The right of users to access and use data generated by the use of products or related services	1
		Article 5: Right to share data with third parties	1,6
		Article 11: Technical protection measures and provisions on unauthorised use or disclosure of data	2(a)
		Article 15: Exceptional need to use data	(a)
		Article 17: Requests for data to be made available	2(c)
		Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs	1
		Article 25: Gradual withdrawal of switching charges	1
		Article 27: International access and transfer	1
		Article 28: Essential requirements regarding interoperability	1
		Article 30: Essential requirements regarding smart contracts for data sharing	1
		Article 33: Penalties	1
	GDPR	Article 9: Processing of special categories of personal data	1,4
		Article 11: Processing which does not require identification	1
		Article 13 Information to be provided where personal data are collected from the data subject	1(a)(b)(c)
		Article 26: Joint controllers	1
		Article 44: General principle for transfers	

Funded by the European Union

		Article 59: Activity reports	
	ePrivacy Regulation	Article 2: Definitions Article 4: M2 Security of processing Article 9: Location data other than traffic data Article 13: Unsolicited Communications	M2 (c,d,f) 3 1
	NIS 2 Directive	Article 35: Infringement entailing a personal data breach	1,2,3
	Digital Service Act (DSA)	Article 15: Transparency reporting obligations for providers of intermediary services Article 24: Transparency reporting obligations for providers of online platforms Article 29: Exclusion for micro and small enterprises Article 32: Right to information Article 33: Pertaining to Very large online platforms and very large online search engines	
Collecting data from products (for condition monitoring and location tracing)	Data Act	Article 2: Definition Article 3: Obligation to make data generated by the use of products or related services accessible Article 4: The right of users to access and use data generated by the use of products or related services Article 5: Right to share data with third parties Article 11: Technical protection measures and provisions on unauthorised use or disclosure of data Article 15: Exceptional need to use data Article 17: Requests for data to be made available Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs Article 25: Gradual withdrawal of switching charges Article 27: International access and transfer Article 28: Essential requirements regarding interoperability	1,2 1 1 1,6 2(a) (a) 2(c) 1 1 1 1

Funded by the European Union

		Article 30: Essential requirements regarding smart contracts for data sharing Article 33: Penalties	1 1
	GDPR	Article 9: Processing of special categories of personal data Article 11: Processing which does not require identification Article 13 Information to be provided where personal data are collected from the data subject Article 26: Joint controllers Article 44: General principle for transfers Article 59: Activity reports	1,4 1 1(a)(b)(c) 1
	ePrivacy Regulation	Article 2: Definitions Article 4: M2 Security of processing Article 9: Location data other than traffic data Article 13: Unsolicited Communications	M2 (c,d,f) 3 1
	Artificial Intelligence Act	Article 3: Definitions Article 6: Classification rules for High Risk AI systems Article 9: Risk management system for high risk AI Article 10: Data and data governance Article 13: Transperency and provission of information to users Aricle 14: Human oversight for high risk AI Article 16 & Article 27: Obligations for AI service provider; distributors and users of service Article 24: Obligations for product manufacturers	
	NIS 2 Directive	Article 6: Definitions Article 21 Cybersecurity risk management measures Article 36: Penalties aplicable to infrinegments of national measures adopted pursuiant ti the Directive	
Harvesting components from the used products1	Data Act	Article 2: Definition Article 3: Obligation to make data generated by the use of products or related services accessible Article 4: The right of users to access and use data generated by the use of products or related services	1,2 1 1

Funded by the European Union

		Article 5: Right to share data with third parties	1,6
		Article 11: Technical protection measures and provisions on unauthorised use or disclosure of data	2(a)
		Article 15: Exceptional need to use data	(a)
		Article 17: Requests for data to be made available	2(c)
		Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs	1
		Article 25: Gradual withdrawal of switching charges	1
		Article 27: International access and transfer	1
		Article 28: Essential requirements regarding interoperability	1
		Article 30: Essential requirements regarding smart contracts for data sharing	1
		Article 33: Penalties	1
	Free flow of Non-personal Data Regulation	Article 3: Definitions	1,2,4,8,9
		Article 4: Free movement of data within the union	1
		Article 5: Data availability for competent authorities	2
	ePrivacy Regulation	Article 2: Definitions	M2 (c,d,f)
		Article 4: M2 Security of processing	3
		Article 9: Location data other than traffic data	1
		Article 13: Unsolicited Communications	
Access to the (used) products	ePrivacy Directive(ePD) 2002/58/EC	Article 2: Definitions	M2 (c,d,f)
		Article 4: M2 Security of processing	3
		Article 9: Location data other than traffic data	1
		Article 13: Unsolicited Communications	
	Data act 2022	Article 2: Definition	1,2
		Article 3: Obligation to make data generated by the use of products or related services accessible	1
		Article 4: The right of users to access and use data generated by the use of products or related services	1

Funded by the European Union

		Article 5: Right to share data with third parties	1,6
		Article 11: Technical protection measures and provisions on unauthorised use or disclosure of data	2(a)
		Article 15: Exceptional need to use data	(a)
		Article 17: Requests for data to be made available	2(c)
		Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs	1
		Article 25: Gradual withdrawal of switching charges	1
		Article 27: International access and transfer	1
		Article 28: Essential requirements regarding interoperability	1
		Article 30: Essential requirements regarding smart contracts for data sharing	1
		Article 33: Penalties	1
	GDPR	Article 9: Processing of special categories of personal data	1,4
		Article 11: Processing which does not require identification	1
		Article 13 Information to be provided where personal data are collected from the data subject	1(a)(b)(c)
		Article 26: Joint controllers	1
		Article 44: General principle for transfers	
		Article 59: Activity reports	
	ePrivacy regulation	Article 2: Definitions	M2 (c,d,f)
		Article 4: M2 Security of processing	3
		Article 9: Location data other than traffic data	1
		Article 13: Unsolicited Communications	
Sharing data across the value chain and making the data public	Data Act	Article 2: Definition	1,2
		Article 3: Obligation to make data generated by the use of products or related services accessible	1
		Article 4: The right of users to access and use data generated by the use of products or related services	1
		Article 5: Right to share data with third parties	1,6

Funded by the European Union

		Article 11: Technical protection measures and provisions on unauthorised use or disclosure of data	2(a)
		Article 15: Exceptional need to use data	(a)
		Article 17: Requests for data to be made available	2(c)
		Article 21: Contribution of research organisations or statistical bodies in the context of exceptional needs	1
		Article 25: Gradual withdrawal of switching charges	1
		Article 27: International access and transfer	1
		Article 28: Essential requirements regarding interoperability	1
		Article 30: Essential requirements regarding smart contracts for data sharing	1
		Article 33: Penalties	1
	Digital Service Act (DSA)	Article 15: Transparency reporting obligations for providers of intermediary services Article 24: Transparency reporting obligations for providers of online platforms Article 29: Exclusion for micro and small enterprises Article 32: Right to information Article 33: Pertaining to Very large online platforms and very large online search engines	
	Open Data Directive	Article 1: research data	(c)
	GDPR	Article 9: Processing of special categories of personal data	1,4
		Article 11: Processing which does not require identification	1
		Article 13 Information to be provided where personal data are collected from the data subject	1(a)(b)(c)
		Article 26: Joint controllers	1
		Article 44: General principle for transfers	
		Article 59: Activity reports	
	ePrivacy regulation	Article 2: Definitions	M2 (c,d,f)
		Article 4: M2 Security of processing	3

Funded by the European Union

		Article 9: Location data other than traffic data Article 13: Unsolicited Communications	1
	Data Governance Act (DGA)	Article 2: Definition Article 8: Single information point Article 18: General requirements for registration Article 31: International access and transfer	9, 10, 11(a)(b)(c) 1 (a,b,c,d,e) 1
	NIS 2 Directive	Article 6: Definitions Article 21 Cybersecurity risk management measures Article 36: Penalties aplicable to infrinegments of national measures adopted pursuiant ti the Directive	

7.3. Annex 3 Interview Protocol

The objective of the interview is to gain a comprehensive understanding of the legal risks and regulatory compliance aspects that individual companies within the DiCiM project are navigating. This task is critical given the multifaceted nature of the project, which spans various technological domains such as open-access digital platforms, IoT solutions, and product component harvesting. The interview is centred around the questions below and we aim to address both aspects related to data (non-tangible products) and physical assets and products.

Questions:

1. How does your company approach the data-relevant spectrum of regulations? Can you provide an overview of your company's data management and compliance practices, especially concerning regulations like GDPR and other legal acts relevant to operations and processes that involve data?
2. What are the most significant legal and regulatory compliance challenges that your company faces regarding data privacy and protection, management and ownership in your industry?
3. What measures does your legal department take to ensure that your company's data practices align with EU-wide horizontal regulations like GDPR and Data Act, for example, and other relevant national regulations?
4. What are the most significant legal and regulatory compliance challenges your company faces when carrying out activities related to harvesting components from your company's products and securing access to products?

Funded by the European Union

5. Among the regulations listed in Table 2, which do you consider applicable and significant for your business? How do the regulations listed in Table 2 (and any other relevant legal acts) directly affect and influence your company's operations and conduct?
6. In addition to the regulations listed in Table 2, can you describe any other legal acts or requirements that substantially influence your company's operations and conduct?
7. Are there any specific data-related risks or compliance challenges unique to your industry that your legal team is particularly concerned about?
8. Could you provide examples of instances (in generic terms) where your legal department has had to navigate the complexities of data regulation compliance while ensuring business operations continue smoothly?
9. How does your company approach the set of regulations that are relevant to managing the products? In particular, can you provide an overview of your company's legal practices related to harvesting components from products and access to products?
10. How does your company approach compliance with environmental regulations such as REACH, WEEE, Ecodesign (future ESPR Directive) and RoHS directives in the context of your products and services?
11. What are the most significant legal and regulatory compliance challenges your company faces regarding implementing the requirements of environmental regulations such as REACH, WEEE, Ecodesign (future ESPR Directive) and RoHS directives?
12. Could you provide examples of instances (in generic terms) where your legal department has had to navigate the complexities of environmental regulation (such as WEEE, Ecodesign Directive, RoHS and REACH) compliance while ensuring business operations continue smoothly?
13. Are your operations impacted by changes in Ecodesign Directive (ESPR)? If you answer positively, elaborate on how the new ESPR legislation will affect your legal and compliance operations.
14. What strategies and processes do you have in place for managing legal risks related to data regulations and environmental legislation, both proactively and reactively?

Funded by
the European Union

8. References

Adams, A. and Cox, A.L. (2008). *Questionnaires, in-depth interviews and focus groups*. Cambridge University Press.

Bauer, M., and Sisto, E. (2023). Increasing Systemic Legal Risks in the EU: The Economic Impacts of Changes to the EU's Product Liability Legislation (Occasional Paper No. 03/2023). European Centre for International Political Economy (ECIPE).

Bell, E., Bryman, A. and Harley, B. (2022). Business research methods. Oxford University Press.

Creswell. J.W. and Creswell, J.D. (2017). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th Edition, Sage, Newbury Park.

De Luca,S. 2023. "New Product Liability Directive." European Parliamentary Research Service, EU Legislation in Progress, PE 739.341, May.

Ducuing, C., & Reich, R. H. (2023). Data governance: Digital product passports as a case study. *Competition and Regulation in Network Industries*. https://doi.org/10.1177_17835917231152799

Kerber, W. (2023). Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives. GRUR International, 72(2), 120-135. https://doi.org/10.1093/grurint/ikac107

Kristoffersen, E., Blomsma, F., Mikalef, P., & Li, J. (2020). The smart circular economy: A digital-enabled circular strategies framework for manufacturing companies. *Journal of Business Research*, *120*, 241-261. https://doi.org/10.1016/j.jbusres.2020.07.044

Leistner, Matthias and Antoine, Lucie. "IP Law and Policy for the Data Economy in the EU" Economics, vol. 17, no. 1, 2023, pp. 20220043. https://doi.org/10.1515/econ-2022-0043

PC1 (2023). Personal Communication: Conversation with a representative of an EU regulator, 17 October.

Funded by the European Union