Data Act Pioneer

EU DATA ACT

Implications, Strategic Responses, and Opportunities

August 29, 2025

funded by:

Interreg Alpenrhein-Bodensee-Hochrhein

Kofinanziert von der Europäischen Union

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

HTWG Hochschule Konstanz Technik, Wirtschaft und Gestaltung

Zürcher Hochschule für Angewandte Wissenschaften zhaw

OST Ostschweizer Fachhochschule

FHV Vorarlberg University of Applied Sciences

The EU Data Act – Implications, Strategic Responses, and Opportunities

Whitepaper

as part of the research project

Interreg VI ABH030 **"Data Act Pioneer"**

Prof. Dr. Marc Strittmatter, Johanna Meyer, LL.B., Eileen Gladis

Hochschule Konstanz Technik, Wirtschaft und Gestaltung (HTWG)

Dr. Jürg Meierhofer, Susana Soriano Ramírez

ZHAW School of Engineering (ZHAW SoE)

Prof. Dr. Petra Kugler

Ostschweizer Fachhochschule (OST)

Dr. Helen Vogt

ZHAW School of Management and Law (ZHAW SML)

Martin Dobler, BSc MSc

Fachhochschule Vorarlberg (FHV)

Publication date: August 29, 2025

Management Summary

The EU Data Act is a central pillar of the European data strategy. Its objective is to unlock previously untapped data potential to foster innovation and competition. At its core, the regulation aims to establish fair access and usage rights for data. The new European framework assigns the involved actors to the roles of data holders, users, and data recipients (third parties). In doing so, the Data Act lays the foundation for a new form of data value creation, while at the same time posing significant legal, technical, and strategic challenges for companies.

The research project "Data Act Pioneer" analyzes these dynamics of change through four complementary research perspectives:

1. **Legal Framework and Compliance Approaches**

   Since the Data Act establishes contracts as the primary governance mechanism for data allocation, new obligations arise for data holders and data recipients, for example regarding data provision duties, technical design requirements (data access by design), information obligations, and protection interests. At the same time, conflicts of objectives emerge between the mandatory data access provisions and the protection of trade secrets and personal data. While the Data Act prioritizes access, it allows for refusal in cases where adequate protective measures are lacking or economic harm is imminent. For practical implementation, a tiered internal data governance strategy is recommended, comprising data inventory, classification, legal assessment, and protective measures. Companies are therefore required to balance statutory data access rights with their own protection interests, while also establishing risk assessment processes and procedures to manage potential compliance and sanction risks.

2. **Open Data Innovation**

   The Data Act grants previously inaccessible industrial data a quasi-open character, thereby enabling new forms of innovation partnerships between data holders, users, and data recipients. However, successful utilization requires clarification regarding which types of data are to be shared within the ecosystem, how the new access provisions transform the innovation process, and what organizational prerequisites – particularly in terms of data literacy – must be established. This research perspective examines how data-driven innovation can be effectively fostered while simultaneously identifying and reducing potential barriers to its realization.

3. ICT Security and Protective Measures

The expansion of data access is accompanied by an increase in attack surfaces within industrial networks. Accordingly, the project analyzes typical attack vectors in industrial environments and develops strategic security concepts as well as technical and organizational measures (TOMs). In addition, the research identifies emerging security-related services and business models that may evolve as a result of the Data Act's implementation.

4. Data Valuation and Industrial Data Value Creation

The new rights granted to users to share industrial data with data recipients give rise to new data value flows and market mechanisms. This creates opportunities for more efficient services provided by third parties, but at the same time raises new questions of competition and financing for data holders. The project analyzes these economic effects, develops valuation models for data access, and formulates proposals for fair compensation mechanisms between the actors involved.

With these four research lines, the "Data Act Pioneer" project demonstrates comprehensive foundations and approaches to examine the impacts of the EU Data Act in a holistic way:

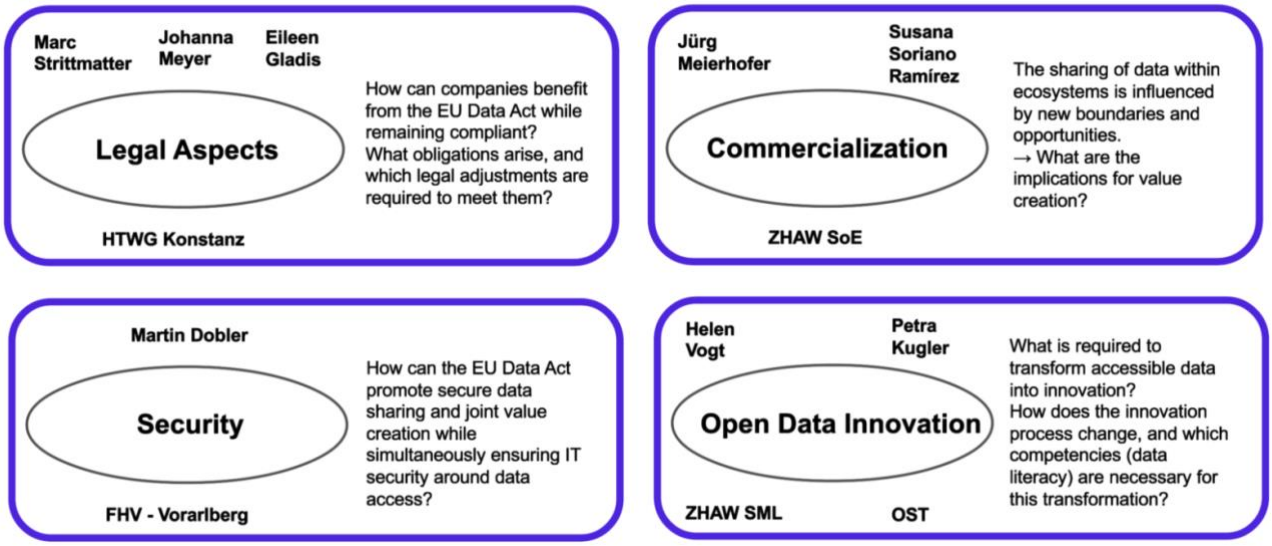


Table of Contents

1 About this Whitepaper

A guidance tool for the classification, impact analysis, and strategies in dealing with the new European legal framework.

This paper is aimed at companies and consultants who want to engage with one of Europe's most ambitious digital laws and are thus faced with the question: *What does the Data Act mean for our company and our business model – how can we respond, and what needs to be done?*

As of 12 September 2025, the EU Data Act (hereinafter: Data Act) will become applicable and enforceable, representing, for many companies, more of a leap into cold water. What remains unclear is how deep it is, how strong the current will be, and who is actually prepared to swim.

This whitepaper is aimed at companies, particularly in the manufacturing sector, that have connected products and related services in use or are customers of companies whose products and services collect data. The paper is intended to create understanding, provide guidance, and enable companies to identify the questions relevant for implementing the Data Act.

The aim of this paper is therefore to provide approaches and bring together different disciplinary perspectives on central questions. It presents initial approaches and strategic considerations from various viewpoints, but with a common goal: to increase actionable confidence and awareness in dealing with this complex, new legal framework. This paper serves as an interdisciplinary orientation framework, helping companies to understand the scope of application and complexity of the Data Act and to derive initial strategic considerations for their own practice. It is not a legal commentary, a technical guide, or a universally applicable recommendation for all situations that companies subject to the Data Act may encounter. Rather, it is intended as a structured approach to a highly complex regulatory framework that affects many different departments within companies – from legal issues and compliance to IT security and product development, as well as business model adaptation and development and insights for one's own data strategy. The aim of the whitepaper is to raise the necessary awareness of upcoming requirements, to highlight key terms, mechanisms, and challenges, and to address practical questions that are becoming relevant now, with a view to September 2025.

Throughout this paper, these distinct areas of research will be examined:

> **Focus HTWG Konstanz – Legal Aspects:** This section aims to systematically present the foundations and legal framework of the Data Act. It covers the requirements and obligations that apply to the various actors involved, addresses the management of inherent tensions between data utilization, trade secret protection, and personal data protection, and examines the implications for corporate data governance structures, which are essential for ensuring compliance with the Data Act.

Focus ZHAW SML und OST – Open Data Innovation: This section aims to understand the new legal regulation as a strategic opportunity, which enables access to previously scarcely accessible resources (data) and can thus lead to innovative business ideas. Ultimately, the goal is to convert data into innovative products, services, and business models in order to achieve advantages in the rapidly evolving competitive environment.

Focus FHV Vorarlberg - IT-Security: The multifaceted areas of cybersecurity are examined, which gain an additional specificity under the Data Act. The strategic role of IT security and threat management are addressed, typical attack vectors in industrial environments are analyzed, and effective technical and organizational measures (TOMs) are discussed. New business fields and services can emerge specifically from the requirements related to security.

Focus ZHAW SoE – Data Valuation and Monetization: The profound changes introduced by the Data Act in industrial data utilization for value creation are examined: Customers gain new rights to access and share equipment data, creating opportunities for external service providers to develop and monetize more efficient offerings, while simultaneously generating risks for manufacturers. Against this background, the emerging data flows and their implications for value creation are analyzed, and models for assessing economic effects and establishing fair compensation mechanisms are developed.

The present paper builds on the findings and discussions that have arisen in the context of the research conducted within the project Data Act Pioneer (Interreg ABH 030), as well as within expert communities, conferences, and workshops. The numerous responses from industry and academia have shown how great the need for structured information, interdisciplinary perspectives, and practice-oriented contextualization of this law is. This paper is a first step to address the need for orientation in dealing with the Data Act. What at first appears to be a clear legal framework reveals, upon closer examination, numerous questions concerning the impacts on business models, value chains, innovation processes, and IT security architectures. At the same time, the regulation opens up new opportunities for the market entry of new actors.

2 Key Provisions, Objectives, and Mechanisms of the EU Data Act

2.1 From Untapped Potential to New Obligations

Up to 80 percent of machine data generated in connected devices, IoT systems, and production facilities has so far remained largely unused (*European Commission, 2023; Podszun/Pfeifer, 2023*). This is due not only to technical barriers, but above all to the lack of legal frameworks governing access to and use of such data (*Specht-Riemenschneider, 2023*).

The EU legislator has already engaged in "market design" far beyond what would have been strictly necessary (*Strittmatter et al., 2025*). As a result, the legal framework will undergo significant further development. The Data Act aims to break open existing data silos in order to facilitate access to and the sharing of data, thereby creating new opportunities for innovation and value creation in the digital economy (*Heinzke, 2023*). While in recent years the focus has been on the protection of personal data, for example through the GDPR (General Data Protection Regulation), the Data Act for the first time establishes a comprehensive legal framework for access to and the sharing of non-personal data.

Data fundamentally differ from physical goods: unlike, for example, a mechanical component, they can be used simultaneously and multiple times for a wide variety of purposes without any loss of quality. In addition, data can be replicated an unlimited number of times without wearing out or being consumed. The EU Data Act addresses this and marks a paradigm shift in European data policy (*Hennemann et al., 2025*). The European legislator already points to this central characteristic of digital goods in the first recital of the Data Act. At the same time, the use of data is seen as offering considerable potential for innovation, competitiveness, and sustainable economic growth. Against this background, the Data Act aims to enable an "optimal allocation of data for the benefit of society" (*Recital 2 Data Act*).

In particular, companies in the manufacturing sector and data-driven business models will be affected by the new regulations, whether as providers, users, or managers of machine data. The scope of application will be examined in more detail below.

On 6 September 2024, the EU Commission published an initial FAQ document on the Data Act to provide guidance for practice even after its entry into force. The updated version, presented on 3 February 2025, now includes 74 individual questions, particularly providing explanations regarding the scope and application of key provisions of the regulation (*cf. press release of the EU Commission, 6 September 2024, available at: https://digital-strategy.ec.europa.eu/de/library/commission-publishes-frequently-asked-questions-about-data-act*).

2.2 Subject matter and scope of application

Art. 1 Data Act describes the subject matter and scope of application of the Data Act. The provision differentiates between regulatory focuses, the types of data covered, and the addressees, i.e., the actors within the Data Act's framework. At this point, the different types of data and the associated data concepts are addressed in order to classify them more clearly.

The comprehensive concept of "data" in the Data Act:

At its core, the Data Act addresses **non-personal data**. These are all types of data that do not allow conclusions to be drawn about natural persons. This primarily includes data generated through the operation of connected products in the **Internet of Things (IoT)**. Such data can comprise both raw data and pre-processed data, which are generated directly or indirectly through the operation of the devices.

In addition, the Data Act regulates access to certain **personal data**, provided that these are processed within the context of non-personal data sets. In such mixed data sets, which contain both personal and non-personal data, the data protection provisions of the GDPR continue to apply.

The Data Act, however, places particular emphasis on data generated in connection with **connected products** (*cf. Art. 2(5) Data Act*) and the related **services** (*cf. Art. 2(6) Data Act*). These products range from machines in industrial manufacturing to smart household devices and connected vehicles (*Recital 14 Data Act*). Accordingly, data within the meaning of the Data Act includes, for example, performance data (e.g., range), usage data (e.g., times of day, passengers during a trip), or environmental data (e.g., locations, temperature). It can be noted that once such products generate data, for example through the corresponding sensors, the question arises who is entitled to use this data.

The data covered by the Data Act can be classified as follows:

- **Data from connected products:** Data collected from machines, vehicles, or IoT devices, providing insights into their usage or condition.
- **Data from related services:** Data captured by services interacting with connected products, for example in the context of maintenance or optimization processes.
- **Machine-generated data:** Primarily data from production processes, which can be used to increase efficiency and improve collaboration along the value chain.

The Data Act regulates, among other things, the provision of product data and related service data to the user of the connected product or service, the disclosure of data by the **data holder** to **data recipients (third parties)**, and the implementation of protective measures against unlawful third-party access to non-personal data as well as measures to protect trade secrets (*see Sections 3.1.2 and 3.1.3*).

In order to avoid placing an excessive burden on SMEs, the Data Act generally exempts micro and small enterprises from the obligations of Chapter II of the regulation, provided they develop connected products or offer related services.

However, the exemption applies only if these companies do not have other partner or affiliated companies that are not themselves classified as micro or small enterprises.

Medium-sized enterprises also enjoy temporary protection: If they have been classified as medium-sized enterprises for less than one year, the obligations likewise do not yet apply. Furthermore, for products placed on the market by medium-sized enterprises, the corresponding obligations only take effect one year after market introduction (*Hennemann & Steinrötter, 2022; Schreiber et al., 2024*).

These three main actors (*see Section 3.1.3 for a detailed discussion*) and the data access mechanism of the Data Act become apparent in the following basic schema:

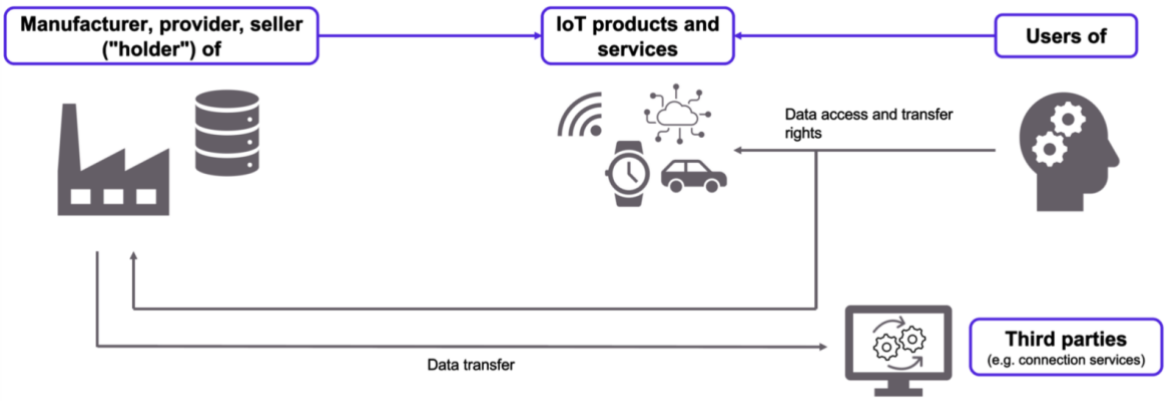


Figure 1

Simplified schema: Data access mechanism of the Data Act, showing the three main roles: data holder, user, and data recipient (third party)

Example Use Case:

An agricultural company uses connected agricultural machinery from a manufacturer, which continuously collects data on soil quality, machine performance, or environmental conditions during operation. When this data is collected or read by the manufacturer, it initially resides within the manufacturer's sphere; the manufacturer is the data holder within the meaning of the Data Act (Art. 2 No. 13 Data Act).

Since the agricultural company generates this data through the use of the machinery, it is entitled to a data access right (Art. 4 Data Act). Furthermore, it can request that these data be transmitted to a third party, e.g., a specialized provider for agricultural data analysis, to derive, for example, more accurate crop forecasts or fertilization recommendations.

This interaction illustrates the central mechanism of the Data Act: factual control over the data remains with the data holder, while the discretionary authority over its transfer lies with the user. The third party has the opportunity to access data that is strategically valuable for its business model.

2.3 Market Location Principle of the Data Act

The market location principle in Art. 1 of the Data Act ensures that the applicability of the regulation is determined not by the location of the actors involved, but by the place of use or provision. The decisive factor is whether connected products, related services, or associated data are offered or used within the European Union. Accordingly, the Data Act also subjects non-European providers to European rules, provided their offerings are directed at the EU market. The market location principle thus significantly contributes to the scope of the Data Act and protects the European data space from regulatory loopholes (*Specht-Riemenschneider et al., 2025*). The market location principle is also the basis of the General Data Protection Regulation (GDPR).

This principle establishes that data holders and providers of corresponding services based outside the Union, for example in Switzerland, are also subject to the scope of the Data Act, provided their offerings are directed at the European market (*Strittmatter et al., 2024; Weinhold et al., 2024*). It remains unclear, however, whose actions are decisive for placing the product on the market in the EU, and whether the obligations already apply if a third party has placed the product on the market without the manufacturer's knowledge.

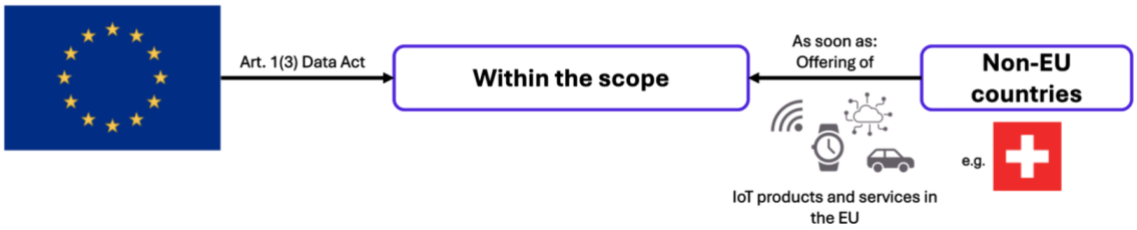


Figure 2

Visualization and country example of the marketplace principle under the Data Act

3 The different perspectives of the research project “Data Act Pioneer”

The research project “Data Act Pioneer” investigates the key regulatory innovations introduced by the EU Data Act and their impact on data-driven companies across various disciplines. These include legal aspects, obligations and implications for data governance structures, open data innovation, data monetization, and IT security.

By redefining access and usage rights to data, the Data Act promotes the development of new business models, products, and services, while simultaneously presenting significant challenges in these areas.

The research project deliberately focuses on four core dimensions. What makes this initiative distinctive is that the Data Act is not examined solely from a legal standpoint, but rather through the inclusion of additional aspects and diverse research disciplines.

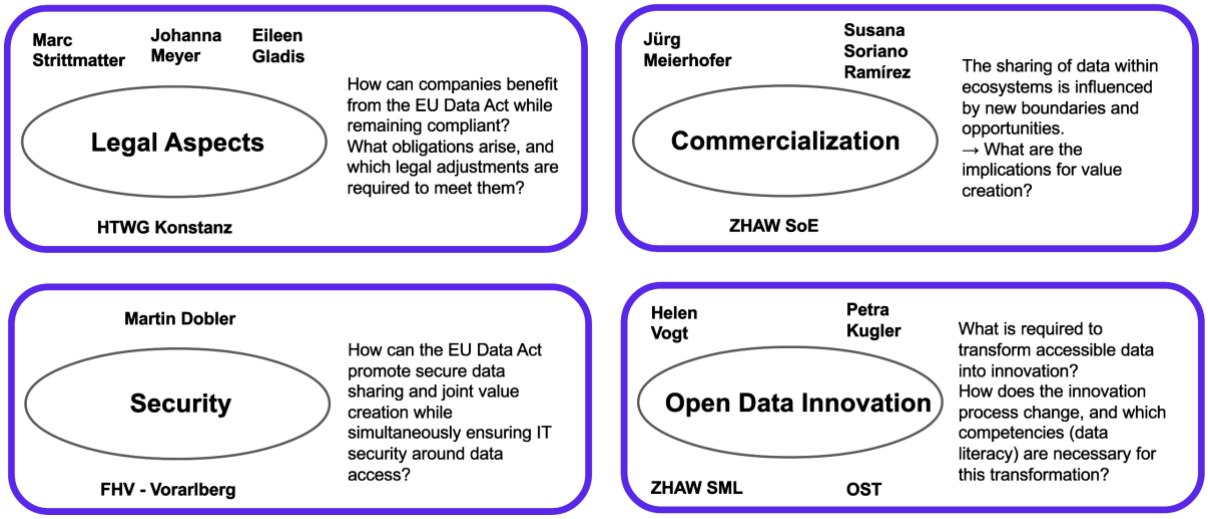


Figure 3

Research partners and their respective research focuses

Anyone wishing to leverage the associated potential and assess the risks must therefore integrate various perspectives: legal, economic, technical, and innovation-related. Further details are provided in the following table.

Research perspective	Explanation
Legal aspects and key areas of data governance (Section 3.1)	This subproject analyzes both the current state within companies in terms of awareness of and preparation for the requirements of the Data Act and the measures that should be taken to be prepared by the Act's implementation date (12 September 2025). This research perspective includes, for example, the adaptation and further development of contractual and internal data governance processes. Additionally, it examines the tensions that arise between mandatory data access and the protection of trade secrets, data protection requirements, and competition law aspects.
Open Data Innovation (Section 3.2)	This subproject focuses on the opportunities arising from the newly possible access to previously hardly accessible data in order to develop innovative products, services, and business models and thereby gain a competitive advantage. What is required for this, and which obstacles must be overcome? Against this background, it is expected that both the innovation process and the necessary competencies (literacy) will change, although it is still unclear in what way.
ICT security (Section 3.3)	This subproject addresses the multifaceted aspects of cybersecurity. It examines strategic consulting and threat management, analyzes typical attack vectors in industrial environments, and discusses effective technical and organizational protective measures (TOMs). In addition, it considers the development of novel services and business models from a security perspective.
Data-based value creation (Section 3.4)	This subproject focuses on the impact of the EU Data Act on industrial data-based value creation. New usage rights for customers over their plant data create opportunities for innovative services by third-party providers. At the same time, questions arise regarding fair remuneration and the economic effects for manufacturers. Which new value streams emerge, how can they be assessed, and which models are suitable for this purpose? The objective is to systematically analyze and quantify the opportunities and challenges of these regulatory changes in relation to value creation.

Table 1: Four research perspectives in relation to the challenges and opportunities of the EU Data Act

3.1 The legal framework of the Data Act

Tensions between data access in relation to the protection of trade secrets and personal data

Summary: The Data Act is a central component of the European data strategy. It aims to establish fair access and usage rights for data, particularly in the industrial and IoT sectors. No ownership right over data exists; however, protective positions arise from database law, trade secret protection, and contractual arrangements. Through the Data Act, the contract becomes the primary instrument for data allocation. The Data Act defines different roles: data holders (often the manufacturer or provider of connected products, though manufacturers and data holders will not always be identical), users (holders or authorized users), and data recipients (third parties receiving data from the user). Data holders have extensive obligations regarding provision, technical design ("Data Access by Design"), information duties, contractual binding, and protection interests. Third parties are also subject to obligations under the Data Act.

Key tension fields exist between the mandatory data access prescribed by the Data Act and aspects of trade secret protection and data protection. While the Data Act prioritizes access, it allows refusal in cases of insufficient protective measures or imminent serious economic harm. When personal data overlaps with Data Act data, the GDPR takes precedence. However, unclear boundaries between personal and non-personal data create practical risks.

For implementation, a staged data governance strategy is recommended: data inventory and classification, legal assessment and protective measures for sensitive datasets, and strategic design of access types. Companies must also decide which compliance strategy to adopt.

3.1.1 Starting point: Questions of legal protection for data

The debate on the protection of machine data and data pools has long shaped legal scholarship. However, it has largely subsided, as the European legislator deliberately refrained from introducing a data ownership right and instead, through the Data Act, agreed on the establishment of **data access and usage regulations** (*Wiebe, 2023; Hennemann & Steinrötter, 2024; Strittmatter, 2025*). At the same time, this marked a departure from the idea of an exclusive right over data, for example in the legal concept of data ownership (*Weiden, 2022; Denga, 2024*).

The legal classification of data and the assessment of statutory protection options remain a challenge for the data economy, as **protective positions for data** are limited: Data are not objects under § 90 of the German Civil Code (BGB) and are therefore considered intangible goods. They are generally excluded as computer programs under § 69a of the Copyright Act (UrhG) or as copyright-protected databases under § 4(2) UrhG. However, structured data collections can, under certain conditions, be recognized as databases within the meaning of § 87a UrhG. Protection then extends to the structure of the database itself (the so-called database producer right) and not to the individual data contained within (*Antonie, 2024*).

A prerequisite for this protection is a substantial investment in the acquisition, verification, or presentation of the contents; investments in the mere generation of data, however, do not confer a protective right (*see CJEU, Judgment of 9 November 2004 – C-444/02, GRUR 2005, 254; regarding the level of creativity: CJEU, Judgment of 1 March 2012 – C-604/10, GRUR 2012, 386*). Criminal law protection does not apply to the data themselves but primarily to their integrity and protection against unauthorized access. A similar situation exists in trade secret protection: here, access protection is paramount and is ensured through a combination of technical, organizational, and legal measures (*Grützmacher, 2024; see also Section ICT Security 3.3.4*).

In the EU, particularly in Germany, Austria, and Switzerland, no ownership rights exist for individual data, datasets, or unstructured data collections. Since statutory protection remains overall incomplete, the contract is the primary instrument for regulating data usage (*Wiebe, 2023; Denga, 2024*). The Data Act continues this approach with its provisions on contractual arrangements and the obligation to make data accessible and usable only on the basis of data license agreements (*Schmidt-Kessel, 2024*).

3.1.2 Classification of the Data Act within the European data strategy

With its ambitious data strategy and a multitude of new legal acts, the European Union has set itself the ambitious objective of establishing a unified, secure, and innovation-promoting data single market. Within this complex regulatory framework, the Data Act plays a pivotal role: it complements the Data Governance Act (DGA) and specifically regulates fair access to and the use of data, with a focus on the industrial and IoT sectors. While the DGA aims to create trustworthy data spaces and promote voluntary data sharing, the Data Act concretizes the rights and obligations of data holders and users, particularly in the relationships between businesses, consumers, and public authorities. Together with other regulatory instruments such as the Digital Services Act (DSA), the Digital Markets Act (DMA), and the AI Regulation, a complex regulatory framework for Europe's digital economy emerges:

Figure 4

The Data Act and adjacent legal acts of the European Commission's European digital strategy

3.1.3 Overview of Actors and Key Obligations

The Data Act aims to establish data access and usage rights and to ensure them through its various regulatory provisions. This creates a data access triangle encompassing three central groups of actors: data holders, users, and data recipients (third parties); see also the simplified data access scheme in Section 2.2. As the GDPR remains unaffected (see also Section 3.1.4), the lawful use of personal data will require a legal basis under the GDPR. Accordingly, an additional actor, the **data subject**, is introduced.

Who is data holder? The **data holder** (Art. 2 No. 13 Data Act) is the natural or legal person who is, by law or contract, obliged to provide access to certain product- or service-related data and to enable its transfer in accordance with the Data Act. Typically, this is the manufacturer or provider of a connected product or service, who, through their technical or legal control, has access to the generated data. It should be noted that manufacturer and data holder cannot be equated nor are they sharply distinguished under the Data Act (*Hennemann et al., 2025*). In most cases, however, the manufacturer will hold the right and obligation to make data accessible, as they are usually the person best able to control the data. Nonetheless, the equation *manufacturer = data holder* may not always be appropriate in industrial practice. The data holder thus represents a central interface within the data ecosystem: they manage access to the data and must enable users or third parties designated by the user to access the data (*Schmidt-Kessel, 2024*).

What obligations apply to data holders? (Excerpt from the obligations framework)

Technical design of connected products and related services: **Data Access by Design** Art. 3(1) Data Act Implementation deadline: 12 September 2026	Connected products must be designed and manufactured, and related services designed and provided, in such a way that they enable the user to access the data generated as a **standard feature**. This includes both product data and related service data, including all relevant metadata necessary for understanding and using the data. Access must be simple, secure, and free of charge for the user, provided in a comprehensive, structured, commonly used, and machine-readable format. Wherever technically feasible and reasonable, the data should also be **directly and immediately accessible**. This establishes a clear design mandate for manufacturers and digital service providers: user-centered data access becomes a technical and legal fundamental requirement.
Data information for the connected product Art. 3 (2) DA Implementation deadline: 12 September 2025	Before concluding a purchase, rental or leasing contract for a connected product, the user must be informed about the data-related characteristics of the product. The seller, lessor or leasing provider, which may also be the manufacturer, must provide at least the following information: the type, format and estimated volume of data generated by the product, whether the product can generate data continuously and in real time, and whether and where data are stored (locally or on a server), including the storage duration, as well as information on access, retrieval and, where applicable, deletion of the data, including the technical means, terms of use and quality of service.

Data information for the related service Art. 3 (3) DA Implementation deadline: 12 September 2025	Providers of related services must, prior to the conclusion of the contract, inform the user about how the data generated will be handled. The **mandatory information** shall in particular include: the type, scope and frequency of data collection, as well as information on access, storage and retention period of product and service data, the purposes of use of the data by the prospective data holder and, where applicable, by third parties, the identity and contact details of the potential data holder and any other data processors, the procedures by which the user can initiate or terminate data sharing with third parties, information on the right to lodge a complaint with the competent authority pursuant to Art. 37 Data Act, details of any trade secrets contained and their holders, as well as information on the contract duration and the conditions for early termination.
Data provision to the user Art. 4 (1) DA Implementation deadline: 12 September 2025	If the user cannot access the data directly via the connected product or the related service (by design), the data that are readily available, including the necessary metadata, must be made available to the user without delay, securely, free of charge, and in a commonly used, machine-readable format. This shall take place upon simple electronic request (user's **right of access to data**), continuously and in real time, and with the same quality as available to the data holder, insofar as this is technically possible.
Provision of personal data Art. 4 (12) DA Applicable from: 12 September 2025	If a personal reference exists, the provision of personal usage data shall only occur if a **valid legal basis** is present, in accordance with Art. 6 GDPR and, where applicable, Art. 9 GDPR.
Data usage only on the basis of a contract: **Mandatory data license** Art. 4 (13) DA Applies to contracts concluded after 12 September 2025.	The data holder may only use readily available non-personal data on the basis of a contract with the user. It is explicitly prohibited from using this data to gain insights into the user's economic situation, assets, or production methods nor in any manner that could affect the user's commercial position in relevant markets. Contractual clauses that deviate from statutory provisions to the detriment of a party in particular the user are not binding. Furthermore the contractual clauses are subject to strict scrutiny **standard terms and conditions law for data licenses** in particular to protect SMEs from unfair or disproportionate provisions (cf. Art. 12, 13 Data Act).
Data transfer to third parties Art. 5 (1) DA Applicable from: 12 September 2025	**At the request of the user** the data holder must provide a third party with the readily available data as well as the necessary metadata without delay free of charge securely and in the same quality. Provision is intended in a common structured and machine-readable format as continuously and in real time as possible. The provision is carried out in accordance with the requirements of Art. 8 and 9 Data Act.

Prohibition of processing readily available data Art. 5 (6) DA Applicable from: 12 September 2025	The data holder may not use readily available data to analyse the economic situation assets or production methods of the third party if this could endanger its competitive position. Such use is only permitted if the third party explicitly consents and can easily revoke this consent at any time Art. 5 (6) Data Act.

Who is the user? The **user** (Art. 2 no. 12 Data Act) is a natural or legal person who owns or is entitled to use a connected product under a contract or uses related services. Users are the central entitled parties of the Data Act and benefit from the essential data access and data provision obligations under Art. 3, 4, and 5 Data Act (*Hennemann et al., 2025*).

They not only have the right to access the data generated during the use of a product or service but can also decide whether these data should be shared by the data holder with a third party. Furthermore, data holders may only use non-personal data themselves if the user has previously consented to this contractually. Thus, the user holds the central decision-making power over the use of the data and becomes a key actor in the data access triangle.

Who is the data recipient (third party)? The **data recipient** (Art. 2 no. 14 Data Act) is a natural or legal person acting in the course of their professional or economic activity but who is not themselves a user of a connected product or related service. This person receives data from the data holder at the explicit request of the user.

Data recipients are therefore typical actors in data reuse: they can act, for example, as maintenance service providers, platform operators, or analysis providers, provided that the user has granted access to the relevant data. Crucially, without the consent of the user, access to the data is not possible for them.

What obligations apply to data recipients (third parties)? (Excerpt from the obligations program)

Agreement on TOMs for the protection of trade secrets Art. 6 (9) DA Applicable from: 12 September 2025	Trade secrets are only disclosed to the extent strictly necessary for the contractually agreed purpose with the third party. The data holder or the trade secret owner identifies data worthy of protection including relevant metadata and agrees with the third party on appropriate technical and organizational measures to ensure their confidentiality. These include, for example, model contract clauses, confidentiality agreements, strict access protocols, and the application of recognized security standards.
Purpose limitation and restriction of use Art. 6 (1) DA Applicable from: 12 September 2025	The data recipient is obliged to process the data provided to them exclusively for the purposes contractually agreed with the user. As soon as the data are no longer needed for the agreed purpose, they must be deleted, unless the user.
Compliance with usage prohibitions Art. 6 (2) DA Applicable from: 12 September 2025	Data recipients may use the data received from the user exclusively within the framework of the agreed purpose and in compliance with the law. **Prohibited actions** include in particular restricting user rights, unauthorized profiling, sharing with third parties without a user contract, transmission to so-called gatekeepers (e.g., large platforms), use for the development of competing products, security-endangering uses, and the violation of trade secrets. If the user is a consumer, they must also not be prevented from sharing their data with additional parties (no exclusivity agreements).
Obligations in case of **unlawful data use** Art. 11 (2) DA Applicable from: 12 September 2025	In the event of unlawful use or disclosure of data, the third party or data recipient is obliged to comply immediately with the requests of the data holder, the trade secret owner, or the user. This includes, among other things, the deletion of all received data, the cessation and, if applicable, destruction of products or services derived therefrom, informing the user about the data breach, and appropriate compensation for any resulting damages. These obligations apply in particular if the data were obtained or processed through deception, unauthorized use, disclosure, disregard of technical protection measures, or security vulnerabilities.

3.1.4 Tension Between Data Access and the Protection of Trade Secrets and Personal Data

The Data Act establishes data access rights and thereby inevitably creates tensions in relation to trade secrets and the protection of personal data (*Antoine, 2024*). The following sections outline the requirements that companies should keep in mind regarding these issues.

3.1.4.1 Tension Between Data Access and the Protection of Trade Secrets

The objective of the European legislator, through the Data Act, to break up the previously one-sided data access of manufacturers in favor of users by means of legally enshrined provision and access rights, collides in key points with the protection of trade secrets (G*rützmacher, 2024*). The right to use these data is of interest both to users and to third parties, for example when it comes to opening up complementary service and data markets. For the data holder, this can mean undesired competition in these markets and raise concerns that valuable know-how could reach users or third parties in the context of data access or data sharing.

What are trade secrets within the meaning of the Data Act? Against this background, the question arises to what extent the protection of trade secrets is eroded by the data access claims or whether the Data Act adequately considers the protection of secrets.

A trade secret exists according to Art. 2 no. 18 Data Act if it meets the criteria of the EU Trade Secrets Directive (implemented in German law in § 2 no. 1 GeschGeh = Act on the Protection of Trade Secrets). Specific requirements are that information must (a) not be generally known or easily accessible and therefore have economic value, (b) be protected by appropriate confidentiality measures, and (c) there must be a legitimate interest in keeping it secret.

Whether the data covered by the Data Act that are readily available, i.e., unprocessed raw data, are protected under the GeschGehG is disputed in the literature (*Grützmacher, 2024*). The EU Commission, referring to a study, stated that this is precisely not the case (*European Commission/European Innovation Council and SMEs Executive Agency/Radauer/Bader/Aplin et al., Study on the legal protection of trade secrets in the context of the data economy - Final report, Publications Office of the European Union, 2022, p. 89*). However, this view is opposed by a large number of contrary opinions according to which raw data (at least under certain conditions) can also qualify as trade secrets within the meaning of the GeschGehG. Reference should be made to the case law of the Federal Administrative Court (*BVerwG, decision of 5 March 2020 – 20 F 3.19*), which recognizes that data can also be protected as trade secrets if trade secrets can be derived from these data. One could therefore assume that by combining data or technical parameters, such as temperatures and movement data of connected products, conclusions about their technical functioning are possible (*Pauly et al., 2024*). Furthermore, this could also apply to datasets from which particularly relevant trade secrets can be easily inferred, for example because they enable reverse engineering pursuant to § 3 para. 1 no. 2 GeschGehG.

The legislator has indeed recognized these tensions, but whether this actually works in practice in conjunction with the provisions of the Data Act remains to be seen. For the data holder, a conflict of objectives arises: on the one hand, they must fear the loss of their data assets, while on the other hand, they face a high fine (Art. 40 Data Act) if they unlawfully deny access due to a misjudgment of the requirements for trade secret protection (*Grützmacher, 2024*).

What protective measures does the Data Act provide in light of the protection of trade secrets? The Data Act provides that trade secrets remain protected. For this purpose, the Data Act provides for or at least suggests various protection mechanisms, such as the model contract clauses of the European Commission (*cf. Art. 41 Data Act)*, NDAs, strict access regulations, technical security requirements, and codes of conduct. Protection also includes the implementation of authorization concepts that ensure limited use as well as confidentiality obligations in the case of third-party access. It is therefore advisable to restrict data access on a need-to-know basis. If such protective measures are lacking (for example, a password-protected authorization concept) and employees have access to the relevant data far beyond the development department, it will hardly be possible to invoke trade secret protection (*Pauly et al., 2024*). The central element of the protection of data containing trade secrets will be contractual agreements between data holders and users or third parties (data recipients). These agreements will play a key role along the entire value chain of connected products and services, especially when several trade secret holders exist for the affected data. On the one hand, contractual safeguards prevent overclaiming of trade secrets. This is necessary because the concept of a trade secret is not clearly defined, and the Data Act (unlike, for example, Art. 20 (4) GDPR) does not contain a balancing provision that would relativize data access rights.

A closer look shows that the EU legislator assigns noticeably greater weight to data access than to the protection of trade secrets, even though large parts of European industry, such as plant and mechanical engineering, the automotive sector, or medical technology, are particularly dependent on the latter (*Antoine, 2024*). This observation will be the subject of intense discussion, and corresponding elaborations and guiding principles by the case law of the CJEU on the relationship between data and trade secret protection can be expected.

At the same time, it becomes even clearer that the contract is the central instrument for implementing the Data Act (*Wiebe, 2023*). In all constellations, whether between the user and the data holder or in relation to third parties, contractual provisions for the protection of trade secrets are essential. In order to grant the data holder control over the handling of their trade secrets, Art. 4 paras. 6–7 and Art. 5 (9) Data Act provide rules on the protection of trade secrets and the possibility of refusing data access or data sharing in individual cases for specific data (Art. 4 (8) and Art. 5 (11) Data Act).

What limitations and rights of refusal exist in favor of the protection of trade secrets under the Data Act? If a trade secret exists, the data holder may oppose the user's claim to data access or to the sharing of data with third parties. This is possible when a trade secret exists but the protection of the

secret cannot be ensured (despite the measures provided for in Art. 4 (7) and Art. 5 (10) Data Act). Even if the parties have agreed on protective measures, the data holder may withhold access until adequate protection is actually ensured. If the required measures are particularly demanding from a technical or organizational perspective, this may accordingly delay the provision of data (*Pauly et al., 2024*). Furthermore, refusal is also conceivable if exceptional circumstances exist and serious economic damage would likely occur (Art. 4 (8) and Art. 5 (11) Data Act; *Schulz, 2024*).

A **right of refusal** for the data holder therefore exists if the parties involved were unable to agree on appropriate protective measures, if agreed measures were not implemented, or if confidentiality has been breached. Even if users or third parties take sufficient measures to protect trade secrets, the data holder may refuse access pursuant to Art. 4 (8) or Art. 5 (11) Data Act if, in exceptional cases, there is a high probability of severe economic harm. According to Recital 31 of the Data Act, such harm exists when significant and irreparable economic losses are to be expected. The right of refusal, which was highly controversial during the legislative process, is described only vaguely in the recitals, leaving it unclear which specific criteria will be decisive in future practice and case law (*Grützmacher, 2024*). The Data Act provides several indications in this regard, including the enforceability of trade secret protection in third countries (outside the EU), the level of confidentiality and the type of data concerned, as well as the "uniqueness and novelty" of the connected product. In addition, possible negative implications for cybersecurity are also highlighted.

Are there indications of practically foreseeable difficulties and potential conflicts regarding data access versus the protection of trade secrets? It is already foreseeable that the application of the criteria established in the Data Act will lead to significant disputes:

On the one hand, proving that the data in question actually constitute a trade secret represents a major challenge. The data holder must present and substantiate this fact in order to defend against a claim to data access. However, the debate will often concern the fundamental question of whether certain types of data, such as machine data, can be considered trade secrets at all (see above). General statements that such data do not in principle constitute trade secrets cannot be upheld. Furthermore, it will often be difficult for the data holder to convincingly demonstrate the specific measures taken to maintain confidentiality (*Schulz, 2024*).

On the other hand, disputes are foreseeable regarding which protective measures are actually necessary and whether these have already been adequately implemented. The parties involved will often hold differing opinions on this matter. It will also remain to be seen who bears the responsibility for proving the implementation in the event of a dispute. Although Art. 4 (7) and Art. 5 (10) Data Act initially place the burden of proof on the data holder, in practice the latter often lacks sufficient insight into the circumstances of the user or third party. Therefore, at least in part, the latter may also bear a secondary burden of presentation. Another problem lies in the unclear definition of the term "serious economic

damage" (*Specht-Riemenschneider et al., 2025*). As already mentioned, Recital 31 of the Data Act provides only vague guidance, leaving it unclear when exactly such damage can be assumed.

For providers of devices, systems, or services, this is particularly problematic, as the thresholds for disclosure to third parties are low. In principle, a user can almost always be found with whom a purpose agreement pursuant to Art. 5 para. 10 Data Act can be concluded – a hurdle that appears hardly insurmountable. In such a case, the burden lies with the holder to prove that the third party has violated the agreed confidentiality obligations. Moreover, it will be extremely difficult to demonstrate that the third party has used the received information for the development of competing products. Therefore, in certain cases, it will be of little help that third parties are, according to Art. 9 para. 2 lit. (c) Data Act, obliged to maintain confidentiality (*Pauly et al., 2024*).

Although the Data Act provides for the possibility to deny data access in the event of a breach of confidentiality, there is a well-founded concern that such breaches will often only be detected once the damage has already occurred, or that providing corresponding evidence will be very difficult (*Schulz, 2024*).

3.1.4.2 The Tension Between Data Access and Data Protection

Although the Data Act addresses both personal and non-personal data, its main focus clearly lies on the use of machine-generated and industrial data. In the event of a conflict between the Data Act and the GDPR, the **GDPR takes precedence**. Consequently, the Data Act does not constitute an independent legal basis for the processing of personal data (*Schemmel, 2024; Hennemann et al., 2025*). Against this background, it is crucial for the practical application of the Data Act to determine whether a given dataset concerns personal or non-personal data. According to Art. 2 No. 1 Data Act, the regulation generally applies to all types of data. Nevertheless, it is necessary to determine the potential personal reference in order to establish whether the provisions of the GDPR apply to the access of a given dataset or not. The Data Act does not contain its own definition of personal data but instead refers in Art. 2 No. 3 Data Act to the definition provided in the GDPR (Art. 4 No. 1 GDPR).

Within the context of the Data Act, the term **personal data** covers digital representations of information relating to an identified natural person. Even if the person is not explicitly named, data are still considered personal if the data subject can be identified on the basis of the available information, that is, if identification is reasonably likely (*Art. 4 No. 1 GDPR; Specht-Riemenschneider, 2023*). **Non-personal data**, on the other hand, are defined negatively in the Data Act. They encompass all data that do not contain information relating to natural persons (Art. 2 No. 4 Data Act). However, it is questionable whether this negative delimitation of personal reference can be clearly made in practice. In many cases, the boundary between personal and non-personal data is fluid, for example, when data that initially appear to be anonymous may allow for re-identification of individuals through combination with additional information (Antoine, 2024). This creates significant uncertainty for data holders regarding the classification under data protection law and the related obligations, particularly with respect to data

protection compliance (Specht-Riemenschneider, 2023). Especially in the context of connected products and IoT applications, there is an increased risk that seemingly non-personal data could still allow inferences to be drawn about individual persons.

Thus, the following applies: If the data also constitute personal data within the meaning of Art. 4 No. 1 GDPR, the scope of data protection law is triggered. In this case, the data holder may only transfer personal (IoT) data to the user or a data recipient designated by the user subject to a **legal basis** under Art. 6 GDPR or an exception under Art. 9 GDPR.

Since the Data Act should not affect the personal rights of the data subjects, the legislator suggests in Recital 7 that data holders may grant data access in a data protection-compliant manner through anonymization or exclusion of personal data (*Baumann & Brunnbauer, 2025*). The advantage of anonymization is that the data are deprived of any personal reference, and thus the provisions of the GDPR do not apply. In contrast to anonymization, pseudonymized data remain fundamentally re-identifiable if corresponding additional information is available. While the right to data access may be weighted more heavily in the case of recognized pseudonymization, such data are still considered personal. From a data protection perspective, therefore, only anonymization offers a secure option.

Who is to be regarded as the **controller** within the meaning of data protection law (Art. 4 No. 7 GDPR) for the transfer of personal data depends on the individual case. In practice, both the user and the data holder are regularly considered as potential controllers. Under certain circumstances, joint controllership pursuant to Art. 26 GDPR may also exist, which is explicitly mentioned in Recital 34 (*Specht-Riemenschneider et al., 2025*).

In the context of the Data Act, **processors** (Art. 4 No. 8 GDPR) are not considered data holders. This is understandable, as the processor does not itself determine the purpose and means of data processing and therefore has no independent legal authority to grant access to the data. It acts solely on the instructions of the controller within the meaning of Art. 4 No. 7 GDPR and is only entitled to grant access if corresponding instructions from the controller exist (*Specht-Riemenschneider et al., 2025*).

Against this background, the practically relevant scenario must also be considered in which a request for data access in favor of a third party is made on the basis of the Data Act, but the data holder could refuse it by invoking data protection restrictions. This could occur, in particular, if datasets are deliberately contaminated with personal data, with the awareness that mixed datasets must be treated as personal data and are therefore excluded from the data access requirements of the Data Act (*Schemmel, 2024*). Since the GDPR takes precedence, the Data Act does not constitute an independent legal basis for the transfer of personal data. If a legal basis under Art. 6 GDPR is lacking, for example in the form of the explicit consent of the data subject or another statutory provision, the data holder is not only entitled but indeed obliged to refuse data access.

3.1.5 Overview: Approaches to Data Governance by the Data Holder

The following provides an overview of three levels of data governance with regard to the obligations of a data holder within the meaning of the Data Act.

Level 1: Data Inventory and Data Classification. The first step in establishing effective data governance structures (or central data management) consists of conducting a data inventory with the aim of gaining a systematic overview of all data available within the company. This includes both a structured recording of data and the classification of data according to defined criteria in order to assess their origin, relevance, and potential uses (*Hennemann et al., 2025*).

Within the framework of the Data Act, data holders are obliged to provide certain data under specified conditions. Without a prior structured data inventory, it is hardly possible to fulfill these obligations in a legally compliant and targeted manner. Above all, data holders must be able to identify, classify, and provide on request data from connected products, related service data, as well as **data that are readily available**. These differ as follows (see section 2.2 for a detailed discussion):

Product data represent a primary use case of the Data Act, as the access regime primarily applies to them (and to related service data). They are generated through the use of connected products, either actively through user interaction or passively as a by-product. **Related service data**, on the other hand, are data generated during the provision of connected services and reflect digital user actions in connection with the connected product. Examples include data about the environment or interactions of the connected product, such as location information at specific times for a connected navigation device. **Readily available data** are product and related service data that the data holder can lawfully obtain from the connected product or service without disproportionate effort. Particular attention must be paid to the origin of the data: only if it is traceable where the data come from, for example whether they are generated internally, provided by third parties, or obtained from connected devices, can a systematic classification in accordance with the Data Act be carried out (*Schreiber et al., 2024*).

This first level, the inventory of data holdings, forms the basis for a differentiated categorization of data along legal and economic criteria. For example, it allows the identification of data subject to access obligations under the Data Act, as well as data for which the limitation of trade secret protection may potentially be asserted (*Hennemann et al., 2025; see also 3.1.4.1*).

Furthermore, such transparency regarding data flows and sources not only provides the foundation for legal classification but also promotes awareness of the economic value of the company's own data assets, an aspect that gains significant importance under the Data Act (*see also the supplementary chapter on Data Valuation 3.4*).

Level 2: Identification of Special Data Sets and Required Actions. Once transparency regarding the data available within the company has been achieved through a targeted data inventory, the next step is to assess their legal protection. The Data Act not only requires a clear assignment and categorization of data but also assumes that companies know whether and to what extent their data are protected against unauthorized use and which enforcement mechanisms under the Data Act are available.

Since **no ownership rights exist in individual data**, datasets, or unstructured collections of data, legal protection is only possible for structured data holdings under database law pursuant to Directive 96/9/EC or as a copyright-protected database work. For unstructured data, protection may at most be available under trade secret law (*Antoine, 2024*). This protection therefore primarily serves to **safeguard access** rather than to confer an exclusive right (*Antoine, 2024*). Against this background, it is essential for companies not only to technically record their data holdings but also to evaluate them legally: *Which data could fall under existing protection regimes, such as database law or trade secret law? What additional measures are required to establish and maintain a protection status at all?*

Even before data is shared under the Data Act, companies should maximize their internal leeway by systematically classifying data that require protection. Especially for strategically relevant data, whose significance results from the previously conducted data inventory and categorization, the second step requires an assessment of potentially existing tensions (*Antoine, 2024; see also 3.1.4*). Only when clarity exists can potential access requests under the Data Act be legally limited or even refused. The insights gained also form the basis for the design of contractual arrangements as well as for possible adjustments to internal company processes and business models in light of the new legal requirements. With the entry into force of the Data Act, the need for internal data classification within companies is significantly expanded:

In addition to the requirements for recording personal data already established by the GDPR, companies must now also identify all product-related and service-related IoT data that potentially fall under the data access and provision obligations of the Data Act. This applies regardless of whether the data are structured or unstructured, personal or non-personal. Based on the chosen protection category and the establishment of a clear procedure, concrete measures can then be derived, ranging from organizational and technical precautions to contractual protection mechanisms towards users and third parties.

Level 3: Design Regarding the Different Types of Data Access. In the course of implementing the European Union Data Act, the question of access to data comes to the center of corporate responsibility. At the latest after the application of the Data Act, the mere technical ability to provide data is no longer sufficient. Rather, an **organizational, legal, and strategic** integration of the requirements of the Data Act into a data governance structure is necessary (*Hennemann et al., 2025*). At the third conceptual level, the level of actual data access, companies should decide how to comply with statutory access claims while simultaneously pursuing legitimate protection interests, for example with regard to trade secrets. This

requires a balancing act between openness and protection, within which modern data governance structures must operate today (*Spießhofer, 2022; Ohly, 2019*).

The Data Act differentiates between two central forms of data access: direct access by the user (**Access by Design**) pursuant to Art. 3 (1) Data Act, and subsequent provision by the data holder under Art. 4 (1) DA. Both provisions obligate companies to make the data generated by a connected product or an related service easily, free of charge, structured, and machine-readable accessible to users. Art. 3 Data Act requires that access be embedded already in the product design. For companies, this entails a realignment of their development and design processes in the sense of Data Access by Design, which integrates technological, regulatory, and operational requirements (*Bomhard et al., 2025*).

A central component in this context is the so-called **in-situ data access** – that is, access to data directly at the location of their storage, without transferring a copy of the data. In legal literature, it is argued that such a right to read on a server controlled by the data holder can fundamentally satisfy the requirements of the Data Act. From the perspective of the data holder, this is a valuable instrument for maintaining control over the relevant data: the risk of aggregation and analysis of sensitive data sets by third parties is reduced, as is the risk of the leakage of trade secrets.

In-situ access is, however, partly rejected: While it is currently considered an acceptable minimum standard, it is unclear whether the mere read-only option will suffice in the long term for the underlying principle of effective and user-oriented data access, particularly if no further processing is effectively possible. Companies should therefore develop a flexible architecture: While highly sensitive data could preferably be made accessible exclusively in-situ, for less critical types of data the option to create a data copy can be granted, for example after successful negotiation or via a digital contractual relationship pursuant to Art. 4 (13) Data Act. This can be implemented, for instance, through a registration requirement or the acceptance of online terms of use directly in the user interface or in the user account.

Against this background, a dual design task arises: On the one hand, companies must establish an organizational framework in which legitimate access requests can be processed and implemented. On the other hand, a technical and contractual toolkit must be developed to safeguard existing protection interests.

3.1.6 Preliminary Conclusion of this Chapter and Further Research Questions

The current situation in companies regarding the preparation and implementation of the regulatory contents of the Data Act is heterogeneous and partly characterized by uncertainty, prolonged waiting, limited awareness, low willingness to adapt, and cautious investment behavior (*Podszun, 2021*). The implementation of efficient data-related processes is significantly hindered by the unclear legal development of the Data Act, which is also due to the hitherto missing relevant case law and established best practices that could serve as guidance for practical implementation.

Against this background, the question arises as to how companies can structure their **contractual and data management processes** to ensure compliance with legal obligations. Pursuant to Art. 41 Data Act, the EU Commission developed non-binding model contractual clauses for the data provision obligations regulated in Chapters II and III, as well as non-binding standard contractual clauses for cloud computing contracts under Chapter VI, prior to the entry into force of the regulation. To prepare these texts, the Expert Group on B2B Data Sharing and Cloud Computing Contracts was appointed, which presented its final report on 2 April 2025. The 183-page document contains the clause proposals developed by the expert group (*the final report is available at: https://www2.morihamada.com/ss/uploads/files/Final%20Report_Expert%20Group_02.04.2025.pdf)*.
A relevant aspect that is likely to crystallize in practice is the organizational embedding of data management within companies: Will the traditionally data-protection-focused department, which primarily handles personal data, in the future be expanded to include units for data access and data provision, even though these areas often have divergent interests? Or will instead independent data management teams be established, specifically tailored to the requirements of the Data Act?

Furthermore, the design of exceptions and priority rules in interaction with the GDPR and trade secret protection has not yet been definitively clarified. Here, there are tactical leeways that companies can use within the tension between compliance and avoidance strategies. Competition law issues are also relevant, particularly with regard to potential restrictions or opportunities that the Data Act provides for the use of data made accessible.

In addition, the strategic orientation of companies in dealing with the Data Act comes into focus. One **strategic decision** concerns the general positioning as an **early adopter** or **late adopter**. This results in different courses of action, ranging from full or partial implementation to targeted avoidance. Some companies consciously choose an **avoidance strategy** by attempting to design their products or services so that the scope of the Data Act is affected as little as possible.

Whether this is fully achievable remains to be seen. Others adopt a "**go-with-the-flow**" strategy, in which observation of legal developments, preliminary organization of data holdings, and risk-oriented prioritization of implementation measures enable a flexible response to regulatory specifications. A third group opts for **proactive implementation**, that is, the early systematic implementation of all requirements, including comprehensive compliance structures and adapted licensing and contractual models, since Data Act compliance can potentially provide a competitive advantage and possibly also serve as a selling point.

Which strategic option appears most appropriate largely depends on the role of machine and device data within the business model, the company's overall compliance culture, as well as its competitive positioning and sensitivity to reputation. Moreover, the incomplete and highly case-specific legal protection of non-personal data, such as machine and sensor data, can lead to considerable legal

uncertainty for companies. This uncertainty may negatively affect their willingness to share data (*Podszun, 2021*).

Against this background, the following **theses** can be formulated, which at the same time give rise to further research questions:

- **Thesis 1**: Companies with robust data governance structures are better able to comply with the legal requirements of the Data Act, manage data access and data access claims, and strategically leverage the opportunities created by the Data Act.
- **Thesis 2**: Small and medium-sized enterprises face greater challenges in achieving Data Act compliance than larger companies, due to limited resources, despite the privileges provided for SMEs in the Data Act.
- **Thesis 3**: Companies that select and pursue a strategy appropriate to their specific situation can derive long-term competitive advantages from implementing the Data Act, whereas failed or miscalculated avoidance strategies increase the risk of legal violations and associated sanctions.
- **Thesis 4**: The vague requirements regarding the design of data licenses under the Data Act, as well as the highly general model clauses of the European Commission, complicate contract drafting and represent an obstacle to the rapid practical implementation of data access and use agreements.

The current model contractual clauses, in their present draft form, offer only limited protection for trade secrets and require substantial additions to become practically applicable.

3.2 Open Data Innovation

The Impact of the EU Data Act on Corporate Innovation Capacity: Seizing Opportunities, Mitigating Risks

Summary: This chapter examines the impact of the EU Data Act on the innovation process and the innovation capacity of companies. It summarizes the current state of this project perspective as of August 2025.

The primary goal of the EU Data Act is to translate the vast amounts and potential of previously unused data into innovation. This becomes possible because the new regulation redefines access to previously inaccessible or scarcely available data, giving them the status of quasi-open data (instead of de facto ownership). This applies particularly in the specific form of an ecosystem of data holders, data users, and third parties.

However, data does not automatically become innovation. Enabling conditions must first be created and potential barriers reduced. It is essential to understand how the EU Data Act transforms value creation both within ecosystems and within companies. The starting point includes the different types of data shared within ecosystems, the new access to these data, how these data change the innovation process, and what competencies (literacy) and organizational frameworks are needed to handle them. From the perspective of "Open Data Innovation," these aspects are at the heart of the next phases of the project.

3.2.1 Objective of the EU Data Act: Turning Data into Innovation

Embracing Change and Innovation as an Opportunity. The primary objective of the EU Data Act is to provide companies with access to data that has so far been scarcely or not at all accessible for many firms. In most cases, this refers to machine data obtained through sensors. With the help of this data, and thus access to new knowledge and insights, innovation should ultimately be enabled and stimulated to establish new products, services, or business models on the market (*European Commission 2022a, 2024*). This represents one way to become or remain competitive in a rapidly changing environment. Against this background the EU Data Act is not only a response to numerous changes that companies currently face, but the accompanying new legal requirements themselves constitute a form of change (not always easy to grasp) for companies.

Today, companies and individuals are confronted with numerous changes and uncertainties, often described by the term VUCA (volatile, uncertain, complex, ambiguous) or similar concepts. At its core, this depicts a situation that develops quickly and makes (strategic) planning nearly impossible. In such circumstances, flexibility and entrepreneurial spirit are required. New (often digital) technologies play a central role in many developments and new trends, as they serve as the trigger for these changes, such as Artificial Intelligence. Innovative technologies have the potential to fundamentally change both established rules of the market and the way value creation is structured and carried out.

For companies, this entails both opportunities and challenges. **Challenges** arise in the sense that established functioning processes, competences, business models, or even business relationships may become obsolete and need to be renegotiated and redesigned. **Opportunities** arise in the sense that they can inspire or stimulate the further development of one's own company and create new options on the market—provided they are identified and seized in time. Change and innovative ideas can then lead to an improved market position or new competitive advantages in general.

Young, small companies (startups) often proactively focus on emerging opportunities, while established companies tend to interpret changes as challenges or threats to the status quo, and thus they behave more defensively. Startups have little to lose but much to gain, whereas established companies risk leaving a strong market position behind. From a strategic perspective, however, it is worthwhile even for established companies to see change as an opportunity to proactively reposition themselves in the market – because defensive behavior often merely postpones necessary entrepreneurial changes, which are not always implemented in time. It is therefore more uncomfortable but often more effective to engage with changes early and act proactively, even as an established company. This also applies in the context of the EU Data Act, which is primarily intended to stimulate innovation.

Artificial Intelligence (AI) and Data: Two Sides of the Same Coin. Different types of innovation play a central role in this process: innovative products, processes, and services address customer needs in new, often better, smarter, or faster ways than before. They are often part of innovative business models or associated with innovative management and working methods, which they make possible in the first place. This creates a paradoxical situation: the faster changes occur, the more innovation is needed to remain competitive; and the more innovations are implemented, the faster the situation changes again, creating even more uncertainty (*Furr & Dyer, 2014*).

With the public release of OpenAI's large language model ChatGPT in November 2022, there has been no doubt that Artificial Intelligence has significant potential to fundamentally challenge many established processes, products, and business models. Although companies have been continuously confronted with new technologies or changing political conditions in recent years, the current situation is different. This is because artificial intelligence is not only a complex technology, but its development is also progressing at an unprecedented pace, thereby acting as a catalyst, as described above.

Artificial intelligence is developing rapidly while companies search for feasible use cases to benefit from the technology. However, suitable use cases do not automatically emerge, as they can fundamentally interfere with existing value creation systems. To leverage their potential, fundamental modifications of value creation configurations (e.g., new business models or

ecosystems) are required, which still need to be defined. Many questions therefore remain unanswered in such a situation. And yet, it is clear that AI has the potential to restructure established value creation and establish a new logic of how value creation is structured. AI is thus also considered a typical case of disruption (*Christensen, 2016*).

Data and AI are two sides of the same coin. The mere application of AI does not in itself create a competitive advantage. Rather, its use will establish a new standard in many industries, normalizing and eventually requiring the use of the technology. It will become commonplace to use AI for certain tasks and processes, such as boosting productivity. While many competitors may then have access to the same technology, meaning no direct competitive advantage is generated and rather, a new technological standard emerges. It is possible, though, to achieve better results than competitors through the quantity and quality of the data that is available for training AI. The more data is available and the higher its quality, the better the outcomes. The use of AI therefore creates a strong demand for data.

To satisfy this demand, large amounts of data not only need to be accessible but often must also be shared with other companies. These data can then serve as a source to stimulate innovation (*e.g., Aaser et al., 2020*). Data in an industrial context often arises precisely at the interface between different actors – for example, when a machine is delivered by the manufacturer to a customer and put into operation. The EU Data Act can therefore be seen as a trigger for changes that may be associated with numerous uncertainties and risks for companies, but at the same time as an opportunity to access data (i.e., new resources) that were previously unavailable. In the spirit of the European Commission, these data can ideally be transformed into innovations. But is it really this simple?

From Data to Innovation: Barriers and Preconditions. A data-based innovation process fundamentally differs in some characteristics from traditional innovation processes, and companies should first gain an overview of the interrelationships they are confronted with. Understanding these causalities, processes and interrelationships is the subject of our ongoing research project “Data Act Pioneer” (2024–2027) and the objective for the coming months of research.

At the core of the perspective “Open Data Innovation” are the key elements and interconnections outlined in figure 6, which are relevant for the journey that data undergoes on the way to innovation: **(1) Characteristics of data, (2) Data access and data sharing, (3) Innovation process, (4) Data competency (literacy) & enabling organizational framework conditions.**

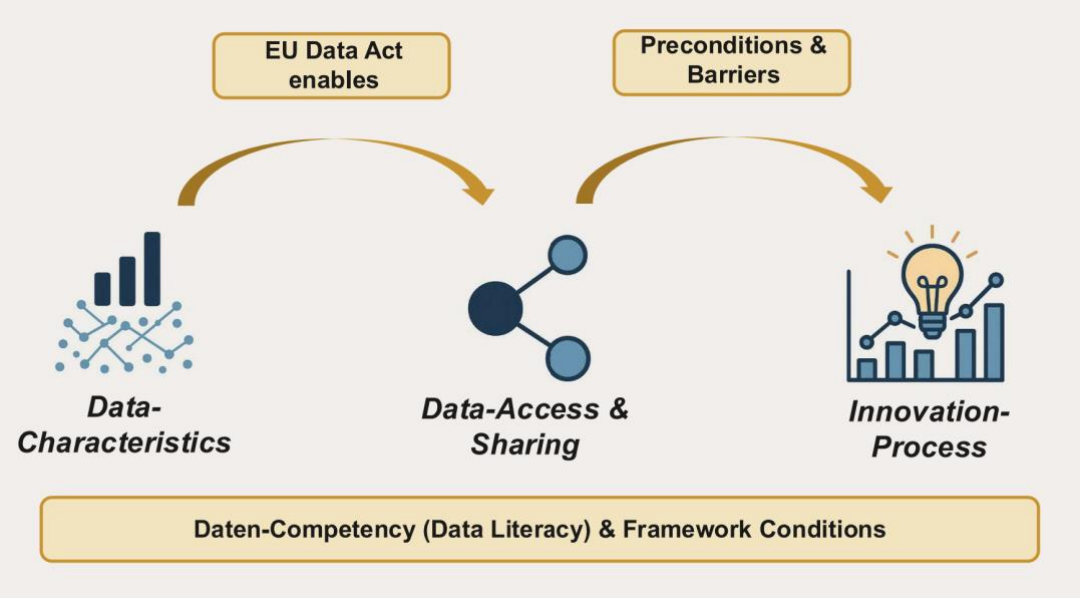


Figure 5

From Data to Innovation: Preconditions and Barriers. Own illustration, created with the help of ChatGPT.

The starting point consists of various **types of data**, which, through analysis, can yield knowledge that provides information, for example, about device usage, customer behavior, or other phenomena. Often, data from different sources must be combined for analysis. But what data is available, and what data is needed? The **EU Data Act** newly enables access to data that has so far been unavailable or only partially accessible, since it was available to only one actor. Between the involved actors (data holders, data users, third parties), certain data will now be disclosed due to the new legislation (**data access**), turning these data into **open data** within the ecosystem. These can, on the one hand, flow into the **innovation process** and fundamentally reshape it. So, how does innovation occur on this basis? On the other hand, this may also lead to a new configuration of the relationship between **actors in the ecosystem**: are they in a relationship of competition, cooperation, or both—i.e., co-opetition (see, e.g., Kugler & Plank, 2021)? Finally, employees must be enabled to handle data in their daily work. They require the necessary **data literacy** and the organizational conditions to do so.

The following sections discuss these elements in more detail.

3.2.2 How Does the Stage-Gate® Innovation Process Change Through Data Access?

To plan and manage product development projects, companies have established process-oriented structural models that systematize the timeline along defined development phases (*Schuh, 2012*). For this purpose, companies use structured models such as the widely adopted Stage-Gate® model by R.G. Cooper (2008). This process represents an established approach to structured product development. It subdivides the innovation process into a sequence of phases (stages), in which defined activities are carried out, and decision points (gates), where continuation of the project is decided (*Cooper,*

2008). Throughout each phase of the Stage-Gate® process, the systematic collection, processing, and analysis of data plays a central role. Companies have a wide range of data sources available, differentiated by their degree of structure and origin (*Babu et al., 2024*). These data sources include:

- **Unstructured data** such as texts from social media activities, audiovisual content, or customer feedback;
- **Structured data** such as transaction or master data from internal databases;
- **Machine-generated data**, e.g., collected through sensors in the context of Industry 4.0 applications.

In industrial innovation processes, machine-generated data plays an increasingly central role. They enable companies to gain real-time insights into physical and operational processes, thereby improving operational efficiency, detecting anomalies early, and identifying innovation potential (*SECO, n.d.; Stucki et al., 2024*). In industrial manufacturing, for example, the following data are typically collected through sensor technology:

- **Acoustic signals** (e.g., for machine monitoring);
- **Visual features** (e.g., image data for quality control);
- **Process-related data** such as energy consumption, vibrations, pressure, temperature, and electrical voltage, to name only the most important.

The systematic analysis of these data provides profound insights into the functioning and condition of technical systems. These insights can be used both to optimize existing installations and to develop novel products and processes (*Babu et al., 2024*). The increasing integration of the Internet of Things (IoT) as well as broader access to machine data fundamentally change the role of **innovation managers**. With the planned Data Act, the European Union aims to actively promote this development. The legislative proposal is intended to facilitate access to machine data generated through the use of connected products or associated services, both for manufacturers and users as well as for third parties (*Pliauskaite, n.d.; Strittmatter et al., 2025*).

For **innovation management**, this gives rise to far-reaching consequences in three central areas:

- **data-driven decision-making processes;**
- **accelerated innovation cycles;**
- **customer-centric business model innovation**

With improved access to machine data in the context of increasing IoT integration, established **innovation processes** are also facing transformation. In particular, the classical Stage-Gate process, long established as a standard model for managing innovation projects, needs to be rethought (*Tesch et al., 2017; Trott et*

al., 2022; tntra.com, n.d.). The availability of real-time data and continuous feedback from connected products creates new requirements – and new opportunities – for **process design**:

- **agile and hybrid process models;**
- **data-driven and dynamic decision points;**
- **iteration and prototyping**

The innovation process of the future is therefore likely to be not rigid, but dynamic, learning-oriented, and data- and AI-based. However, not every project benefits from the same innovation model. While digital, data-driven, or highly uncertain innovation projects require a flexible and adaptive process approach, projects with clear requirements and low complexity can still benefit from the classical Stage-Gate® discipline. The future lies in context-sensitive process design. Innovation managers face the challenge of creating structures that enable both targeted control and agile response to new insights – particularly those obtained from real-time data. A central role is played, as a consequence of the EU Data Act, both by freely accessible data (Open Data) and by the special form of an ecosystem with the three aforementioned actors (data holders, data users, data recipients (third parties)).

3.2.3 The Importance of Open Data

Manufacturers have so far secured de facto control over the Internet of Things (IoT) data generated by their products through technical design. This so-called de facto ownership of such data enables them to maintain an exclusive position, even though no formal ownership rights exist (*Eckardt & Kerber, 2023*). The resulting data silos hinder innovation as well as competition and stand in the way of developing open data ecosystems. This may be one reason why a large proportion of collected data (estimated at around 80% by the European Commission, 2023) is not further utilized.

The EU Data Act (Regulation (EU) 2023/2854) aims to dismantle these structures. Recital 32 emphasizes that the decision against exclusivity of data serves the regulation's purpose of fostering innovation in the data economy. By regulating access to non-personal IoT data, innovation is to be enabled that was previously blocked by exclusive data control (*Strittmatter et al., 2025*). At the same time, competition is to be strengthened, particularly in so-called secondary markets such as maintenance, repair, or data analytics, where data-driven services have so far struggled to gain a foothold (*Ridgway et al., 2025*). Another aim is to ensure a fairer distribution of value creation between manufacturers, users, and data-processing service providers (*Martens, 2023*).

IoT data are **non-rivalrous resources** – their use by one actor does not preclude simultaneous use by others (*Bertschek et al., 2021*). This characteristic gives them special potential in the data-driven economy, since the same data can be used multiple times and in diverse combinations. Against this backdrop, the EU Data Act (Regulation (EU) 2023/2854) plays a central role. It aims to facilitate the use of data across sectors and clarifies that interoperable data from different domains can increase the competitiveness of

the European economy. **Interoperability** here means that data from different sources—such as machines, digital platforms, or complex supply chains – are technically and semantically compatible and can thus be efficiently integrated and utilized. Combined use of such data generates new analysis and value creation potentials, which in turn can spur innovation.

In this context, the concept of **Open Data Innovation** is gaining increasing importance (*see, e.g., European Union, 2025*). It refers to the deliberate opening of non-personal IoT data to external actors to enable new applications, services, and data-driven business models through regulated access (European Commission, 2022b). This creates a framework that systematically unlocks the economic potential of interoperable data. The focus here is not on full openness in the sense of "open access," but on structured shareability that respects legitimate interests such as data protection and trade secrets. The aim is to intensify the use of existing data resources by promoting liquid data markets.

3.2.4 Data Literacy and Organizational Requirements

To use data effectively in the outlined innovation process, certain prerequisites within the company must be met, or barriers removed or avoided. Interestingly, the greatest hurdles to translating data into value in companies are not found in the so-called "hard factors" (e.g., lack of resources, company too small, technology) or in the data itself (e.g., volume or quality of data). Instead, the main obstacles are the so-called "soft factors" (e.g., organization, lack of vision, culture) (*Kugler et al., 2020*).

The following discussion focuses on two of these factors**: (1) Data literacy and (2) Data culture and mindset.** To work with data effectively within a company—especially in the context of the innovation process – companies and their employees must first be empowered to do so. Data is a special type of resource that fundamentally differs from physical products. At the core lies, on the one hand, the data literacy of employees, and on the other hand, an enabling data culture and mindset within the company—i.e., the implicit and explicit values, norms, and assumptions that shape thinking (*mindset, logic; see also on culture: Kugler, 2025; Kugler et al., 2024; on mindset: Kugler, 2023; 2020*).

Data Literacy, AI Literacy. As data becomes an increasingly integral part of the innovation process, **data literacy** becomes a key qualification for companies. Data literacy is generally understood as the ability to understand data in context, question it critically, analyze it, and translate it into action (*Schüller, 2020*). It is essentially about making decisions based on data and enabling employees to understand and carry out this process. In data-driven organizations, this competence is increasingly relevant across all employees, hierarchies, and departments – from product development to marketing or to strategic management. Data are thus moving from the periphery to the core of organizational value creation (*Kugler, 2020*).

In the innovation process, data play a dual role: on the one hand, they help identify new needs, trends, and developments; on the other, they can contribute to the implementation of innovations through continuous idea generation, evaluation and optimization, as well as the communicative preparation and visualization of ideas and prototypes. Companies with a high level of data literacy are overall better able to develop

data-driven business models, interpret customer data meaningfully, and deliberately steer data-driven innovations. Increasingly, this also involves the use of machine learning models, generative AI, and AI agents that increasingly automate the innovation process (*e.g., Bouschery et al., 2023; Eapen et al., 2023*). Closely related is **AI literacy**, which is often equally relevant for companies. AI literacy is the ability to critically reflect on and competently apply Artificial Intelligence. It involves understanding how AI systems work, assessing their potential and risks, and evaluating their organizational and societal impacts. This goes beyond technical knowledge and basic understanding to include ethical, legal, and social aspects of AI use—such as data protection in companies or in a broader societal context (*e.g., Long & Magerko, 2020; Ng et al., 2021*).

For companies, this creates a clear mandate: data literacy must be strategically understood and promoted as an organization-wide key qualification—through internal training programs, the integration of data-related competences into leadership roles or embedding data literacy objectives in innovation strategies. Only when employees can use data confidently and reflect critically can data unfold their full potential in the innovation process. (See also table 2).

Competence Area	Data Literacy	AI Literacy
Understanding & Classifying	Understanding of data types, sources, and quality	Basic understanding of AI, ML, algorithms, and training data
Collecting & Generating	Collecting, curating, and structuring data	Knowledge of data fundamentals for AI models and their collection
Analyzing & Interpreting	Data analysis, statistical thinking, pattern recognition	Interpretation of AI results, understanding algorithmic processes
Evaluating & Reflecting	Critical evaluation of data sources, bias, and context	Reflection on fairness, bias, and transparency of AI
Communicating & Visualizing	Preparing and presenting data (e.g., through visualizations)	Explaining AI systems and their decision-making
Applying & Implementing	Using data-driven insights for decision-making	Applying AI tools in daily life/work (e.g., chatbots, recommendation systems)
Ethical & Legal Aspects	Data protection, data ethics, copyright	AI ethics, GDPR, accountability for automated decisions

Table 2: Elements of data literacy and AI literacy.

Data Culture, Mindset, and Organization. The organizational culture of a company plays a centra – perhaps even decisive – role in handling data in general and especially in the innovation process. Working with or sharing data follows a different logic than handling physical products or traditional services: it follows a **data-dominant logic** (*Kugler, 2020*). In such a logic, data moves to the center of organizational

value creation, rather than merely representing one of many resources. But what characterizes such a culture, and what should companies pay special attention to?

Organizational culture generally describes the values, norms, and beliefs that guide the thinking and actions of members of an organization – both explicitly and implicitly (*Schein, 1992*). In data-driven companies, this culture manifests in decisions increasingly based on analyses and data (via data literacy), rather than personal intuition or experience. For this reason, the term decision culture is often used in this context (*Vidgen et al., 2017*). However, a data-oriented culture goes far beyond decision-making—it influences structures, roles, and the organizational self-concept. Three characteristics are central: **(1) recognizing data as a special resource, (2) shaping organizational boundaries to be permeable, and (3) adapting structures, roles, and processes** (*see also Kugler, 2025; 2023; Kugler et al., 2024*).

(1) Recognizing data as a special resource

A data-oriented culture begins with acknowledging data as a resource that fundamentally differs from physical or intangible company resources. Not all data are equally valuable. Operational data that enhance efficiency differ from strategic data that enable innovation (Kugler & Plank, 2021). Raw data usually holds less value than analyzed and interpreted results. If data are to be shared with other companies, this can both enable competitive advantages and risk losing them. Companies are therefore often uncertain about how to leverage data without sacrificing control or exclusivity. Thus, the first step is to understand and acknowledge the potential value of data and shared use within ecosystems – both within one's own organization and with partner companies. Often, the true value of data becomes evident only when new knowledge is generated from them.

(2) Shaping organizational boundaries to be permeable

The organizational self-concept and the way internal and external boundaries are defined are equally important. Companies often act strongly department-oriented or focus narrowly on themselves – but data-driven value creation requires broader, ecosystem-based thinking that goes beyond an understanding of the organization within clearly defined boundaries of the company. Only by combining (raw) data with existing knowledge can new potentials for value creation arise.

Within a company, this requires close integration between technological data analysis and business perspectives, particularly in developing data-based business models or value propositions. Within ecosystems, it requires partnership-based collaboration to jointly identify potential use cases or synergies. For example, real product usage data can provide new insights into customer behavior when combined with technical expertise and business model knowledge – forming the basis for new services, innovations, or use cases.

(3) Adapting structures, roles, and processes

Finally, organizational infrastructure must evolve. A data-oriented culture requires that data be accessible – both technically and procedurally. It is often unclear who is allowed to access which data, especially with sensitive information such as customer data. Data-driven organizations are characterized by transparent, low-threshold access regulations – across hierarchies and functions. This understanding fundamentally changes organizational roles, processes, and structures. Value creation with data requires both recognizing the value of data and the ability to capture it – through analysis, interpretation, and visualization. Internal structures must be flexible enough to integrate new roles and responsibilities. Organizational structure ultimately reflects the symbolic importance of topics such as data.

Recommendations: Step-by-Step Cultural Change. Developing a data-friendly organizational culture is a long-term process that cannot be mandated. A step-by-step approach is therefore recommended, leveraging different levers: first, employees should be sensitized to the potential of data – e.g., through internal ambassadors who make the topic tangible. Building on this, competencies in handling data should be systematically developed.

In the next step, access to data should be facilitated, and existing boundaries – both internally and within the ecosystem – should be opened towards an open organization. Finally, it is important to actively spread and scale successful best practices and early use cases. Through concrete experiences, a sustainable change in the cultural anchoring of data can be stimulated.

3.3 ICT-Security

Security Approaches and New Risks in the Age of the Data Act

Summary: ICT security is multifaceted and has become even more complex with the introduction of the Data Act. It is therefore important to examine strategic considerations and threat management, analyse typical attack vectors in the industrial environment, and discuss effective **technical and organisational measures (TOMs)**. We will also take a look at the development of innovative services and business models from a security perspective.

This chapter deals with the complex aspects of cyber security. It examines strategic consulting and threat management, analyses typical attack vectors in the industrial environment and discusses effective technical and organisational protective measures. One focus is on responsiveness to security incidents and damage limitation. The topics of load management and compliance within the framework of IT security standards are also addressed. In addition, we take a look at the development of innovative services and business models based on security requirements.

When considering ICT security aspects, there are different levels of security requirements. A possible distinction could be made between critical infrastructures, adjacent critical infrastructures and other companies. Critical infrastructures generally include public safety, electrical power supply, nuclear energy, chemical production, agricultural and pharmaceutical production and distribution, and in some cases banking and finance (*Knapp, 2024*). Joint value creation and the development of innovative services at this level can be hampered by compliance with regulations and standardisation frameworks and their strict approaches to data integrity and data exchange. Sectors adjacent to critical infrastructures include sectors that are not explicitly classified as critical infrastructures by regulatory authorities - such as governments or supranational blocs such as the EU - but nevertheless play a crucial role in maintaining societal functionality and continuity. Examples include the food industry (*Hetzenauer et al., 2023*) or suppliers to critical infrastructure providers, as well as providers of software and solutions for supply chain management (*Topping et al., 2021*).

When jointly developing new services, the impacts prescribed by each level must be taken into account. It should be noted that although a company (or SME in particular) may not be classified as critical infrastructure or adjacent to critical infrastructure, it may be a supplier or service provider for critical infrastructure.

The following section primarily presents considerations that are relevant for all companies. In the case of critical or system-preserving infrastructures, additional measures may be necessary.
It should also be noted that the following considerations only refer to specifics related to the Data Act. A thorough examination and implementation of established IT security standards (in particular ANSI/ISO standards and protective measures of the BSI or the Austrian Information Security Manual) is

recommended. In general, it may also be helpful to bear in mind that, according to the Data Act, the data owner and the owner of a trade secret do not have to be the same person.

3.3.1 Strategic Cybersecurity Considerations & Threat Management in the Context of the Data Act

Joint value creation can be achieved through the development of services by ensuring ICT security. Despite the success of digital transformation, ICT security often remains a secondary consideration. From a holistic strategic perspective, it should be noted that, in addition to the additional requirements for ongoing ICT operations, the Data Act can also offer an opportunity for holistic value creation in the area of cybersecurity. The introduction of the Data Act primarily underlines the importance of implementing automated data exchange in compliance with legal requirements. Apart from its technological and administrative implications, this development has the potential to be used to increase co-creation value. Specific strategic considerations for information security include managing data retrieval in accordance with the Data Act, incident response protocols, and the operational management of ICT security considerations. Overall, a balance must be struck between costs and benefits and the company's risk tolerance (*Meier & Burda, 2019*).

At the strategic level of threat classification (*Jouini & Rabai, 2016*) for risk and threat management (*Al-Mhiqani et al., 2019*), at least the following threat categories must be considered:

- **Local operational threats** that jeopardise ongoing operations (example: machine availability is jeopardised due to numerous requests or infiltration of the machine)
- Operational **threats to companies** (example: interfaces for automated Data Act queries are used for infiltration)
- **Data leakage** (example: unintentional leakage of security-relevant or business-critical (meta) data as part of machine data)
- **Data integrity** (example: damage to reputation or consequential damage resulting from data manipulation using vulnerabilities in interfaces)
- **Reconnaissance** (example: use of (meta)data to conduct reconnaissance of internal company information or ICT security measures)

All risk categories can be addressed from the perspective of the providing company/data owner or the operating company/data user.
Finally, it is important to understand that the above risk categories are not new, but that the implementation of the Data Act creates potentially new attack vectors for these categories. In particular, the risk categories of data leakage and reconnaissance are to be considered critical due to the nature of the requirements of the Data Act.

3.3.2 Critical, common attack vectors in the machine-based industrial context

In the machine-based industrial context, the focus is on the attack vectors of data leakage and reconnaissance, as the Data Act explicitly promotes the exchange of machine-generated data.

Data leakage as an attack vector. Data exfiltration refers to the unauthorised copying, moving or transferring of sensitive data from a protected network. In an industrial context, this could include trade secrets, intellectual property, production data or personal information. Gateways can be created because interfaces for data retrieval that were created for legitimate purposes can also be misused by malicious actors. A typical attack vector is the exploitation of vulnerabilities in the APIs (application programming interfaces) or in the protocols used for data exchange. It is important to note that both data and meta-data (e.g. database schema, domain models, process steps, etc.) can be leaked.

Reconnaissance of technical infrastructure as an attack vector. Reconnaissance or reconnaissance measures are often the first step in cyber-attacks, in which malicious actors collect information about the target system in order to identify vulnerabilities. In the context of the Data Act, this vector is particularly critical, as the data provided Ð including metadata Ð can provide valuable insights into a company's system architecture, the software it uses and its security measures. Attackers can use this information to map out the IT infrastructure, locate potentially vulnerable systems and prepare tailored attacks. The data accessible via the Data Act could, for example, provide information about which machine types or software versions are in use, which communication paths exist, and how load management (e.g., content delivery networks, CDN) works. This information makes it easier to find zero-day exploits or known vulnerabilities in order to carry out targeted attacks.

Reconnaissance using data. Reconnaissance in the context of the Data Act can also take on a new dimension when freely available or easily accessible machine-generated data contains a wealth of derivable information. Malicious actors can use data science methods and statistical tools to gain valuable, security-critical insights. For example, a malicious actor can analyse the operating data of a machine that can be retrieved via an interface. Simply by statistically evaluating metadata such as data collection frequency, data volume or time stamps, conclusions can be drawn about utilisation, production cycles, maintenance intervals, shift intervals or geographical location, among other things. Anomalies in the data streams can also provide information about vulnerabilities or unusual configurations. Such information obtained from the data can serve as the basis for cyber-attacks that are specifically tailored to the company's vulnerabilities.

Effective examples of cyber-attacks based on the use of this statistically determined information are social engineering attacks. For example, knowledge of shift changes can be used to exploit reduced attention levels; phishing emails can be sent specifically before or after a maintenance interval; spear phishing attacks can be targeted at relevant individuals based on real-time data; malicious actors can credibly pose as maintenance personnel by telephone or at the production site; and much more.

In general, all reconnaissance measures can also be used to gather publicly available information that is not related to security in order to gain a business advantage.

3.3.3 Response to security incidents & damage limitation

A proactive approach to cybersecurity is essential, but complete prevention of all security incidents is usually impossible in practice. Effective incident management and rapid damage control or containment are therefore crucial to minimise the impact of attacks and ensure business continuity.

Incident management is a structured process for detecting, analysing, resolving and documenting security incidents. As part of the (technical) implementation of the Data Act, it makes sense to align measures with established IT security standards (in particular responsibilities, guidelines, procedures, checklists) for dealing with incidents. In organisational terms, this includes detecting the incident, isolating affected systems and then eliminating the cause of the problem. Detailed documentation of the incident is crucial in order to be able to take countermeasures, prevent future attacks and meet compliance requirements.
Ensuring business continuity in the event of damage is usually implemented by creating emergency plans. It may make sense to adapt these emergency plans for the Data Act, in particular to ensure the necessary due diligence for data disclosure.

Every security incident must undergo a thorough risk assessment to understand its actual impact on the company and its partners. This requires a holistic view that goes beyond the company's own infrastructure. In complex data ecosystems such as the Data Act, potential impacts usually relate to the company's own direct infrastructure, adjacent infrastructure (especially suppliers and partners) and other companies.

In order to minimise damage resulting from **due diligence and reputation**, it is advisable to supplement business continuity communication plans with specifics resulting from the Data Act. Communication plans should include sub-areas and possible contact points for internal, external and regulatory communication (especially in the case of reporting obligations).

3.3.4 Technical and Organisational Protective Measures

Technical and organisational measures (**TOMs**) are already known from the General Data Protection Regulation (GDPR) in its Article 32. However, technical and organisational measures in the context of the Data Act are much more than just a compliance requirement. They are evolving into a **strategic tool** that addresses the discrepancy between the required data transfer and the protection of sensitive information. The key question is: How can TOMs be used to protect one's own security level without violating the obligations of the Data Act? Or, in other words: How high can the defensive fence around a sensitive data container be?

This creates a tension between data security and data access. The Data Act obliges data owners to disclose data to third parties under certain conditions. At the same time, the legislator demands adequate cyber security. This conflict gives rise to a potential safety and security handbrake, which is explicitly addressed in the FAQs on the Data Act (question 25). Data owners can restrict or refuse the transfer of data if there is a risk that security requirements could be undermined. This can legitimise the use of high security standards as an argument against uncontrolled data transfer.

The challenge is to find a balance:

- Refusal due to high security requirements: A data owner could refuse to share data with a third party on the grounds that their own TOMs - which ensure a high level of security - would be compromised by the sharing.
- Ensuring an adequate level of security: The Data Act requires that an adequate level of security be maintained throughout the entire transfer chain. This raises the question of how the data owner can verify the security standards of the data recipient and ensure that they meet their own standards.

The legal basis for this area of tension can be found in various sections of the Data Act:

- Article 4(2) and (6): These deal with restrictions on use and transfer based on security requirements (para. 2) and the protection of trade secrets (para. 6).
- Article 11: A separate Article 11 in the Data Act is devoted to technical safeguards against unauthorised use or disclosure of data. This highlights the importance of technologies such as smart contracts and encryption. These can serve as essential TOMs to ensure data integrity and confidentiality throughout the data exchange process.
- Recitals 31, 42, 82 and 83: These emphasise the importance of protecting trade secrets and highlight the implications for cybersecurity.
- Recitals 8, 20, 35 and 46: These set out the importance of technical and organisational measures.

3.3.5 Designing Innovative Services and Business Models in the Context of Security

Joint value creation in the development of services can be achieved by providing and ensuring ICT security. Over the past decade, the growth of digital solutions has been driven primarily by digital transformation, resulting in a variety of strategies that all attempt to combine multidisciplinary approaches to creating business value and move away from purely technical considerations (*Verhoef et al., 2021*). ICT security, which is often not at the centre of digital transformation efforts, continues to offer considerable opportunities for the development of holistic shared value creation (*Stewart, 2023*). The entry into force of the Data Act further underscores this assertion when considering the technological and administrative implications for implementing the legally mandated automatic data sharing and exchange.

With the introduction of the Data Act, we foresee the following areas where new, jointly created services could flourish all in different forms, depending on the requirements arising from regulatory compliance or infrastructure integration considerations.

Planning and operations management services:

- Cybersecurity consulting & training: Consulting firms or service providers can offer strategic security policies for data services that are published under the Data Act. In addition, advanced automated threat detection tools can be provided at the technical level, enabling customers to identify and mitigate risks. These activities can be extended to corporate networks or supply chains involving multiple parties.
- Incident response and damage control: In the event of security incidents, rapid response and remedial action may be required. Specific incidents related to the Data Act may include unintentional or forced data breaches and maliciously induced high numbers of data retrieval requests, including (distributed) denial-of-service attacks ((D)DoS). Another common attack vector is the intentional or unintentional retrieval of third-party data that can be used for industrial espionage or reconnaissance.
- Compliance design and services: Services may include specialised compliance services that help customers meet legal data protection requirements or design ICT infrastructures that comply with both standards and legal frameworks.
- Resilience/business continuity design and services: These services may include strategies, consulting or technical solutions to ensure the continuous operation of Data Act-related services or to recover from a cyberattack.

Technical services:

- Managed On-Premises Secured Services: A service provider can develop solutions for hosting server infrastructure, including automated software solutions at the customer's site, to respond to Data Act requests. This category can be expanded to include maintenance solutions (i.e., trained personnel).
- Secured Managed Cloud Services: Similar to secured on-premises services, cloud software infrastructure could be developed to provide solutions for Data Act requests. This category can be expanded to include maintenance solutions (e.g. trained personnel).
- Threat data: Threat intelligence could include databases of known vulnerabilities or real-time assessment of security threats against published Data Act solutions.
- Penetration tests: Penetration tests can include the assessment of data protection-specific security measures and vulnerability testing.
- (Automated) counter-intelligence: Early detection of coordinated attacks or reconnaissance operations by third parties or malicious actors.

3.4 Data Evaluation, Monetisation and Models

New data flows and new opportunities

Summary:

The EU Data Act fundamentally changes industrial data value creation: Customers are given new rights to use and share their equipment data. This opens up opportunities for more efficient services by third parties, but also poses risks for manufacturers. The "Data Act Pioneer" project analyzes these new value streams and develops models for evaluating economic effects and remuneration.

3.4.1 Data-Based Value Creation in Industrial Contexts Before the Data Act

In industrial B2B markets, data-based value creation has typically taken place along the following value streams: Machine manufacturers develop, produce and sell equipment to business customers (equivalent to "users" in Data Act terminology). Business customers use these systems to manufacture their own products. In the course of digitalization, modern machines are equipped with sensors, actors and digital controls. Networking via IoT can offer additional services such as remote monitoring, condition-based or predictive maintenance. The connection to IoT platforms means that customers share their plant data with the manufacturer. The manufacturer thus becomes the data holder.

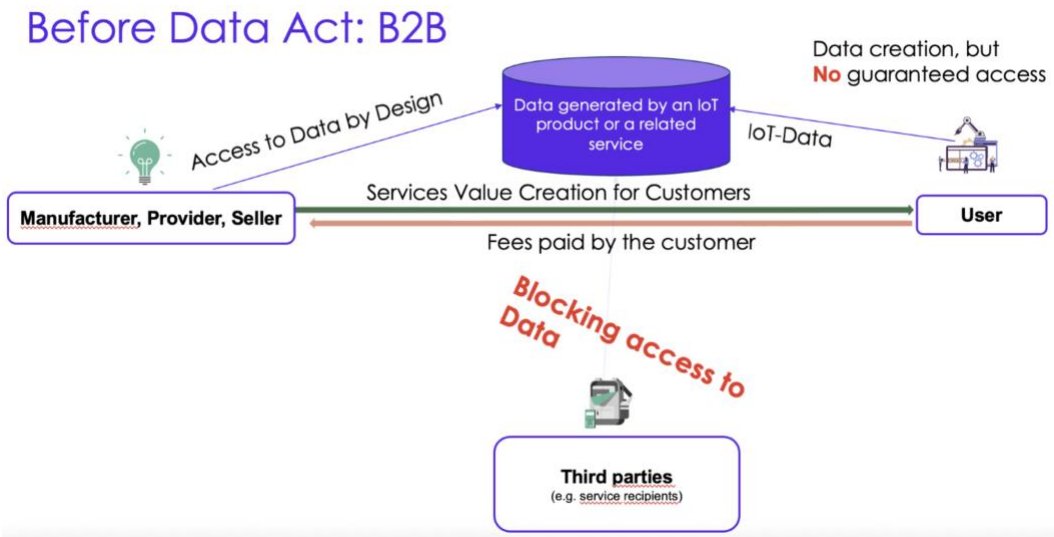


Figure 6

Simplified representation of the unbalanced data and value flows prior to the applicability of the Data Act.

This constellation brings both benefits and challenges. Potential disadvantages for customers include an unbalanced flow of value: Customers pass on their production data to manufacturers on a broad basis.

This can be used to derive benefits for manufacturers in various ways:

- They can use the data to offer value-added services to customers, which can drive customer loyalty and additional revenue.
- They gain valuable insights into the use of their systems and can derive improvements or requirements for a next product generation.
- Manufacturers can also use the data to deduce which usage patterns of their equipment are more efficient or lead to longer lifetime of the equipment, and use these patterns for a consulting service for other customers.
- Customers also give the manufacturer insight into their economic condition. Providers can, for example, anticipate economic booms or downturns and respond to them with targeted additional offers.
- Potenziell geben die Kunden sogar geistiges Eigentum preis, wenn z.B. aus den Produktionsdaten Informationen über das Design von Endprodukten ersichtlich werden.
- In addition, manufacturers are potentially remunerated for the resulting service benefits through service fees.

The benefit for customers is essentially improved performance with the equipment used, e.g. through:

- optimized operation, e.g. more output per time, less raw material and energy consumption per output.
- Improved quality of output, fewer defective parts produced including downstream benefits due to fewer complaints from end customers.
- Longer equipment lifetime, e.g. due to avoided failures and optimized maintenance of the systems.
- Tailor-made offers and innovative products, as the manufacturer knows the needs exactly from the data.

Even though both sides receive significant benefits from the shared data, there is a mismatch in some cases, especially because the manufacturer can scale the insights derived from one customer to many other customers. The effect is intensified if the manufacturer obtains the data from the customer and captures value for itself, but only creates a sub-optimal service for the customers. This circumstance opens up the opportunity for third-party providers to step in and generate create added value for customers from the data.

3.4.2 Changes in the Value Creation Ecosystem as a Result of the Data Act

The EU Data Act fundamentally changes these data streams. Customers (users) are given the right to use their equipment data themselves or to pass it on to third parties.

Use of data by the customers themselves: With the Data Act, customers are to be enabled by the manufacturer to obtain the data from their plants themselves and to use it further, e.g. for integration into their production control systems (such as MES, Scada, etc.) or for their own evaluations (e.g. their own management dashboards). Customers are also entitled to pass on this data to third parties who create added value from it, for example, by acting as an external service provider for plant maintenance or operational analyses.

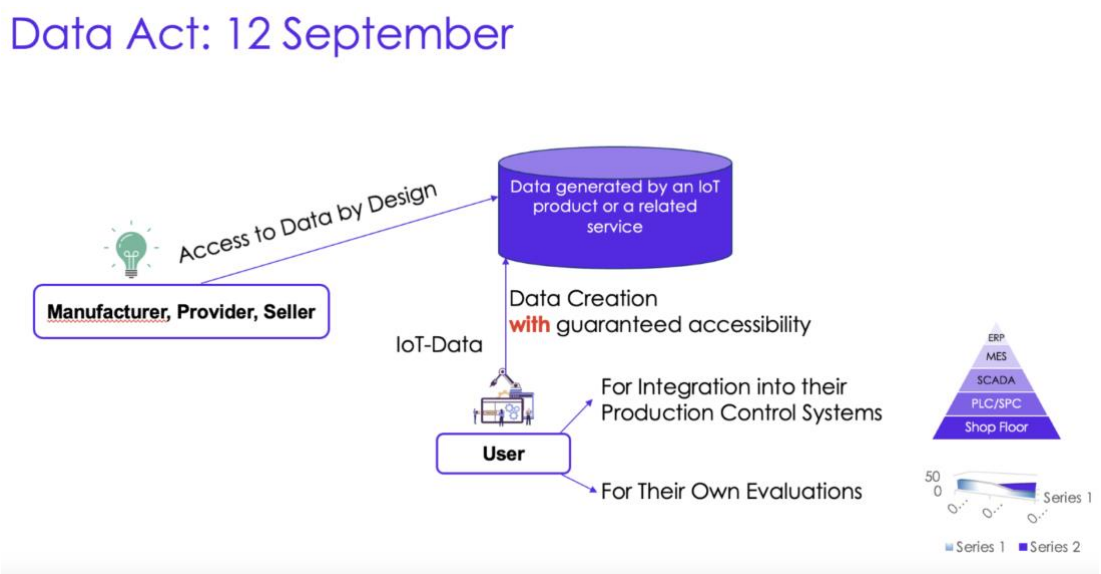


Figure 7

Simplified representation of data access and user opportunities enabled by the Data Act.

This form of data use by customers is not remunerated to manufacturers [*European Parliament, 2023*]. This form of use of the data for one's own purposes or for disclosure to third parties requires that the customers have their own competencies in data processing or then commission external suppliers (e.g. IT service providers) to do so on their behalf. Even for the transfer to third parties, interfaces (like API, application programming interface) or transmission protocols must be created, whereby relevant questions of data protection and IT security arise. The development and operation of these interfaces mean additional work for customers or even hurdles that are difficult to overcome, especially for SMEs. If customers want to avoid this, they have the option of passing the data on to third parties directly by the manufacturer.

Disclosure of data by manufacturers to third parties: Customers can oblige manufacturers to transfer their equipment data to third parties designated by them. These are typically service providers who add value to the data and create a new business from it:

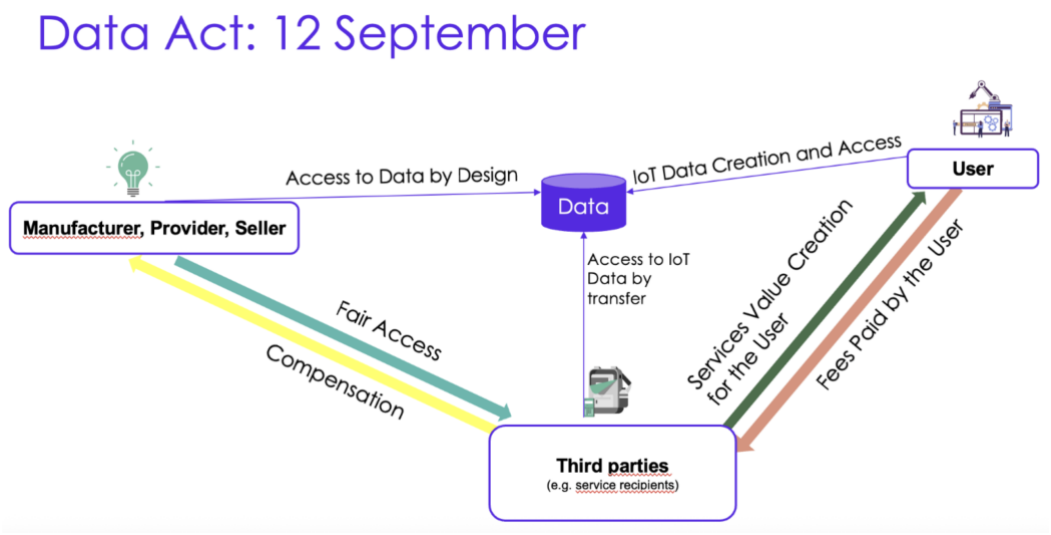


Figure 8

Simplified representation of data access and third-party opportunities enabled by the Data Act.

A very interesting and obvious form for customers arises if this third party provides better service than the manufacturer itself. This includes options such as those listed earlier in the text under "Benefits for customers". This can be the case, for example, if the third party specializes in deriving particularly effective or efficient maintenance activities from the productive data. Common examples in this context are remote monitoring and maintenance ("*remote service*") or condition-based or predictive maintenance. The latter form, in particular, is based on advanced machine learning and artificial intelligence methods, both of which are competencies that are difficult to tap into, especially for SME customers. Third parties specializing in this type of analytics can then derive significantly more benefit from the data and thus, for example, significantly reduce plant downtime at the customer's site, which can create direct economic benefits. It can also increase the resource efficiency and service life of the equipment, which creates not only economic but also environmental benefits. When third parties have their core competence in analyzing data from industrial equipment, they can learn from a wide range of types of production facilities, customer situations and plants and optimize their data models. This can result in a quality of service that cannot be achieved in a manufacturer-customer relationship.

In the language of industrial services, this use of data mitigates or relieves customer pains. **Typical pains are:** downtime, low plant efficiency, low quality, high energy consumption. The economic and environmental benefits from mitigating or relieving these pains can be quantitatively determined using the "*value-of-pains*" framework, which is described in (*Meierhofer et al. 2024*) and is briefly summarized here:

- The unresolved pains result in measurable economic loss ("impact") for the customers, e.g. reduced number of end products, overtime shifts, rework, waste of energy.
- The pains have a frequency with which they occur (e.g. daily, weekly, ...).

- By multiplying damage and frequency, we get the expected value of the pain in a given time period.
- With a data-driven service, a proportion of these pains can be avoided. This reduces the financial value of the pain by this proportion.

Example:

- A production plant with machine costs of 200 euros per hour typically stands still for 5 hours in the event of a failure, i.e. a breakdown costs 1,000 euros.
- Such failures occur on average four times a year. This results in the expected value of this pain at 4,000 euros per year.
- Predictive maintenance and remote monitoring can prevent about 50% of failures.
- This results in the business benefits of these services at 2,000 euros per year.
- In the sense of value-based pricing, the maximum willingness of customers to pay can be derived from this benefit: they pay part of the benefit received, i.e. their willingness to pay in the form of service fees is <= 2,000 euros per year in the example.

- In addition to the financial benefit, there is a potential environmental benefit if the services avoid, for example, travel, energy waste or scrap material. This can be calculated in CO2 equivalents expressed using the same methodology.

It can also be inferred from the foregoing considerations that the customers of the third party will potentially pay higher service fees if they receive higher service benefits from the third party.

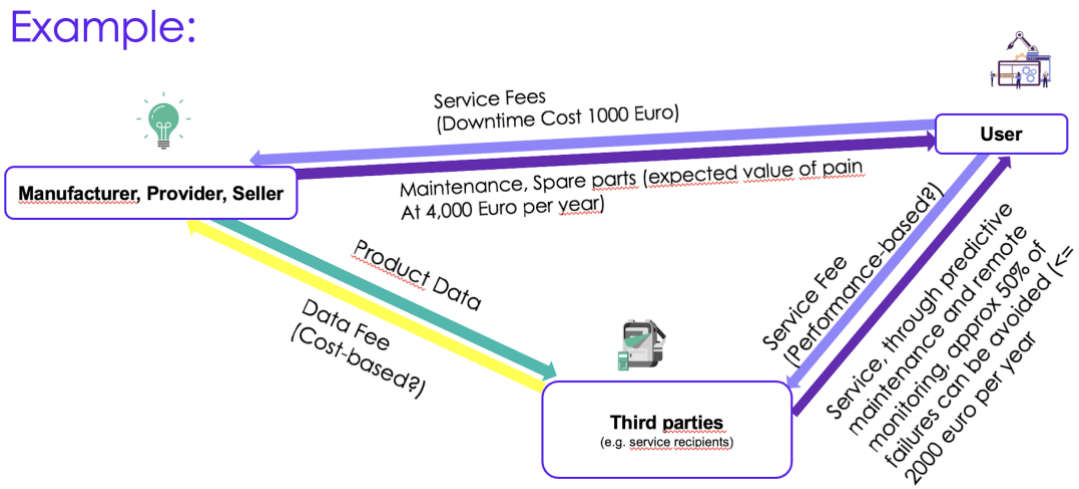


Figure 9

Simplified representation of the example: higher service fees

In summary, it can be said that customers receive a service benefit from either the provider or the third party to eliminate pains such as performance losses or interruptions of the system. In return, they are willing to pay a service fee for this, either to the provider or to the third party. Either the manufacturer provides the service to the customers itself by using the production data from the equipment. Alternatively, the third party obtains data from the manufacturer (or from the customer) and thus provides the service to the customer. The manufacturer is entitled to appropriate remuneration for this data transfer to third parties. The level of this remuneration is currently the subject of regulatory and economic clarification. These third-party services may substitute for or supplement existing services by the provider.

Whether it is more interesting for customers to purchase services from the third party instead of the manufacturer depends largely on whether the third party achieves better **service performance** (e.g. less downtime, more service for customers) than the manufacturer or whether it can provide service performance more efficiently (i.e. at lower costs) and thus at a lower service fee for customers. This means that the manufacturer can prevent customers from wanting to give the data to third parties if it is already efficiently providing good service performance itself. This also demonstrates the potential of the Data Act to promote the efficient and innovative use of data.

3.4.3 Opportunities and Risks for Actors in the Ecosystem

The new regulations create both risks and opportunities for all parties involved. **Manufacturers run the risk** of having to hand over data in exchange for potentially low remuneration. **At the same time, manufacturers have the following opportunities**:

- They can expand their own service competence and retain the service business with their customers.
- In addition, they can act as a third party in the market of other manufacturers and offer data-driven services. This opportunity is still very rarely recognized and used in practice, but it holds great potential, because the development and operation of industrial services benefit greatly from economies of scale. If, for example, service or data platforms from one manufacturer are also used for the customers of other providers, the fixed costs for development and operation can be better covered.
- An interesting possibility also exists if a provider has geographically distributed field technology resources with strongly fluctuating utilization, which can be smoothed out by an increased customer base.
- In addition, the situation can also arise that a manufacturer does not want to place any strategic emphasis on service and a third party can jump into this gap on the basis of the Data Act.

For third parties, there are opportunities to develop more efficient or customer-oriented services and to win new customers. However, there is a **risk for third parties** that manufacturers will catch up with their own service offerings and win back customers, which can lead to unamortized investments.

Customers benefit from better or cheaper services, but bear the risk of lock-in effects when switching providers and uncertainty about long-term service quality.

3.4.4 Contribution of the Data Act Pioneer project

As part of the "Data Act Pioneer" project, the new value streams are systematically analysed and analytically modelled. The aim is to create a basis for decision-making for the actors involved. Central project topics include the modelling of value streams in the business ecosystem, scenario analyses to assess the impact of data-based business models and the quantitative assessment of the economic effects for manufacturers, customers and third parties.

Initial findings from case studies show that data sharing with third parties can be economically advantageous, albeit at the expense of the manufacturer, under the following conditions: If the third party can provide the same service benefit more efficiently (more cost-effectively) or generate a higher service value. Success factors for third parties include superior data analytics capabilities and efficient service delivery.

The valuation models developed in the project can support the determination of adequte remuneration and the creation of transparency in regulatory and economic decision-making processes.

4 Conclusion

The forthcoming implementation of the EU Data Act marks an important turning point for the industrial data economy. Companies are required to analyse their role within the new regulatory framework and to integrate the resulting obligations at an early stage into product and service design. In particular, the rights to data access, as well as the requirements for data sharing and interoperability, necessitate consistent consideration already during the planning and development phases. In this context, the principle of "Data Access by Design" is gaining significance. The multitude of obligations and the potential scope of sanctions make the implications comparable to those experienced under the GDPR, so that timely engagement with the content of the regulation and the development of appropriate implementation strategies is advisable. In addition to technical implementation, contractual arrangements are also becoming a central instrument of the Data Act: existing customer and partner agreements should be reviewed for compliance with the requirements of the Data Act and adjusted where necessary. Likewise, the instruments and models proposed in this paper for assessing data value and monetisation should not be underestimated in their relevance.

From the perspective of the innovation process and the competencies required for it, the new regulation establishes a regulated access within the ecosystem to data that have so far been largely inaccessible, thereby granting them a quasi–open data status. However, as data do not automatically lead to innovation, suitable framework conditions must be created and barriers reduced. The key issue is how the EU Data Act will transform value creation within the ecosystem and within companies. The focus lies on the types of data shared, the new modes of data access, their impact on the innovation process, as well as the necessary competencies and organisational prerequisites.

In practical implementation, numerous uncertainties remain. Although the clear allocation of product and service data provides users with a strong initial position, the Data Act simultaneously grants data holders a degree of flexibility, provided they are adequately prepared. Essential steps include the systematic analysis and classification of data, the establishment of user and third-party management, and the definition of internal purposes of use and procedures for handling data access requests. This research therefore leaves many open questions — for instance, regarding fair remuneration for data sharing, the long-term development of service quality, and the assessment of technology platforms used for service delivery.

Given the direct applicability of the Data Act from **12 September 2025**, the preparation period remains limited. Early action is therefore essential not only to minimise risks but also to leverage the new economic potential. The implementation of the EU Data Act will have a lasting impact on the industrial data economy. Companies should therefore engage with the new obligations at an early stage in order to establish fact-based technical and organisational safeguards that are regularly reviewed and adjusted. At the same time, it is important to recognise the opportunities that the Data Act offers, particularly for smaller enterprises.

These aspects of the paper offer valuable points of reference for further research and cooperation. At the same time, the results of the research project "**Data Act Pioneer**" provide practical approaches from which both the associated partner companies and other interested enterprises can directly benefit.

References

Cited and further sources:

Aaser, M., Kanagasabai, K., Roth, M., & Tavakoli, A. 2020. Four ways to accelerate the Creation of Data Ecosystems. McKinsey Analytics, November.

Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. 2019. Review of cyber attacks classifications and threats analysis in cyber-physical systems. International Journal of Internet Technology and Secured Transactions, 9(3), 282-298.

Antoine, L. (2024). Datenzugang im Spannungsfeld zwischen DSGVO, Geschäftsgeheimnisschutz und Datenbankherstellerrecht, Computer und Recht, 73 ff.

Babu, M. M., Rahman, M., Alam, A., & Dey, B. L. 2024. Exploring Big Data-driven Innovation in the Manufacturing Sector: Evidence from UK Firms. Annals of Operations Research, 333(2), 689-716.

Baumann, J.; Brunnbauer, J. (2025). Datenschutzrechtliche Anforderungen bei der Bereitstellung von IoT-Daten nach dem Data Act, Herausforderung für Dateninhaber im Spannungsfeld zwischen DS-GVO und DA. Zeitschrift für Datenschutz, (3), 131-137.

Bertschek, I., H. Bonin, J. Kühling, J., G. Thüsing & Wenzel, T., 2021. Entwicklung eines Konzepts zur Datenallmende: IZA Research Report No. 119. Expertise im Auftrag des Bundesministeriums für Arbeit und Soziales.

Bomhard, D.; Siglmüller, J. (2025), Das Verhältnis von Access by design und Datenzugangsanspruch nach dem Data Act. Recht Digital, (7), 353-357.

Bouschery, S.G.; V. Blazevic & F.T. Piller, 2023. Augmenting human innovation teams with artificialintelligence: Exploring transformer-based language models. Journal of Product Innovation Management 40(2): 139–153. https://doi.org/10.1111/jpim.12656

Christensen, C., 2016. The Innovator's Dilemma: When new Technologies cause great Firms to fail. Harvard Business Review Press.

Cooper, R. G. 2008 Perspective: The Stage-Gate® idea-to-launch Process—update, what's new, and nexgen systems. Journal of Product Innovation Management, 25(3), 213-232.

Denga, M. (2024). Verträge über digitale Produkte zwischen Unternehmen. Zeitschrift für die gesamte Privatrechtswissenschaft, (4), 427-464.

Eapen, T.T.; D.J. Finkenstadt; J. Folk; L. Venkataswamy, 2023. How generative AI can augment Human Creativity. Harvard Business Review, July-August.

Eckardt, M., & Kerber, W. 2023. The EU Data Act and the Re-Allocation of Data Rights in the IoT Ecosystem. European Journal of Law and Economics, 56(3), 405–433. https://doi.org/10.1007/s10657-023-09791-8

Ehlen, T.; Sebulke, P. (2024). Der Data Act: Zwischen Markt- und Vertragsgestaltung. Computer und Recht, (2), 84-90.

EU-Kommission, COM(2020) 66 final v. 19.02.2020, Brüssel: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Eine europäische Datenstrategie, abrufbar unter: https://eurlex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52020DC0066.

Europäische Kommission, 2022. Proposal for a Regulation on harmonised Rules on fair Access to and use of Data (Data Act). COM(2022) 68 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068

European Commission 2023. Boosting data sharing in the EU: what are the benefits? https://www.europarl.europa.eu/topics/en/article/20220331STO26411/boostingdata-sharing-in-the-eu-what-are-the-benefits

European Commission, "Frequently Asked Questions Data Act." European Union, Feb. 03, 2025. Accessed: Apr. 14, 2025. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act

European Commission, 2022. Data Act: Commission proposes Measures for a fair and innovative Data Economy. Press Release, 23 February, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113.

European Commission, 2024. Data Act. Shaping Europe's digital Future. https://digital-strategy.ec.europa.eu/en/policies/data-act

European Parliament, "Data Act: MEPs back new rules for fair access to and use of industrial data." EP_Industry, Mar. 14, 2023. Accessed: Nov. 03, 2023. [Online]. https://www.europarl.europa.eu/news/en/press-room/20230310IPR77226/data-act-meps-back-new-rules-for-fair-access-to-and-use-of-industrial-data

European Union, 2025. European Data: Open Data as a Catalyst for Innovation. https://data.europa.eu/en/academy/open-data-catalyst-innovation.

Furr, N., & J. Dyer, 2014. The Innovator's Method: Bringing the Lean Start-up into Your Organization. Boston: Harvard Business Review Press.

Götz, M., Blöink, S. (2024). Datenvertrag: Lösungsansatz für das Spannungsfeld zwischen Data Act und DS-GVO. Multimedia und Recht, (6), 451-456.

Grützmacher, M. (2024). Data Act: Datenzugang und Geschäftsgeheimnisschutz, Computer und Recht, (5), 281-292.

Hartmann, B., McGuire, M. & Schulte-Nölke, H. (2023). Datenzugang bei smarten Produkten nach dem Entwurf für ein Datengesetz (Data Act). Recht Digital, (2), 49-59.

Heinzke, P.; Herbers, B.; Kraus, M. (2024). Datenzugangsansprüche nach dem Data Act. Betriebs-Berater, (12), 649-655.

Hennemann, M., Specht-Riemenschneider, L. (2025). Data Act – Data Governance Act – Handkommentar, 2. Auflage, Nomos Verlagsgesellschaft, Baden-Baden.

Hennemann, M., Steinrötter, B. (2022). Data Act – Fundament eines neuen EU-Datenwirtschaftsrechts? Neue Juristische Wochenschrift, (21), 1481-1486.

Hennemann, M., Steinrötter, B. (2024). Der Data Act – Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen. Neue Juristische Wochenschrift (1), 1 – 8.

Hennemann, M., Steinrötter, B. (2024). Der Data Act – Neue Instrumente, alte Friktionen, strukturelle Weichenstellungen. Neue Juristische Wochenschrift (1), 1 – 8.

Hetzenauer, C., Dobler, M., & Simma, A. (2023, June). Information security chal-lenges in the digitalisation of the austrian food industry: Assessment of food Suppli-ers and implications. In 2023 IEEE International Conference on Engineering, Tech-nology and Innovation (ICE/ITMC) (pp. 1-7).

Jouini, M., & Rabai, L. B. A. (2016). Threats classification: state of the art. Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security, 368-392.

Knapp, E. D. (2024). Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems. Elsevier.

Kugler, P., & T. Plank, 2021. Coping with the double-edged Sword of data sharing in Ecosystems. Technology Innovation Management Review, 11(11/12), 5-16. https://www.timreview.ca/article/1470.

Kugler, P., 2020. Approaching a Data-Dominant Logic. Technology Innovation Management Review, Vol. 10(10), 16-28. http://doi.org/10.22215/timreview/1393.

Kugler, P., 2023. Aus Big Data wird Big Value: Warum es eine Daten-dominante Logik braucht. Schallmo, D.R.A.; K. Lang; T. Werani; B. Krumay (Hrsg.): Digitalisierung: Fallstudien, Tools und Erkenntnisse für das digitale Zeitalter. Wiesbaden: Springer Fachmedien, 553-568. https://doi.org/10.1007/978-3-658-36634-6

Kugler, P., 2025. Datengetriebene Organisationskultur: Unternehmen neu denken und Daten im Ökosystem teilen. In: Kugler et al. (Hrsg.): Data Sharing für KMU: Voraussetzungen und Instrumente für die gemeinsame Nutzung von Daten. Berlin, Heidelberg: Springer Gabler, 27-49.

Kugler, P.; H. Vogt; J. Meierhofer; M. Dobler; M. Strittmatter; M. Treiterer; & S. Schick, 2024. Daten im B2B-Ökosystem teilen und nutzen: Wie KMU Voraussetzungen schaffen und Hürden überwinden. In: Schallmo, D., S. Kundisch, K. Lang, D. Hasler (Hrsg.): Digitale Plattformen und Ökosysteme im B2B-Bereich: Fallstudien, Ansätze, Technologien und Tools. Springer Nature, Schwerpunkt Business Model Innovation, 209-240. ISBN 978-3-658-43129-7, DOI 10.1007/978-3-658-43130-3.

Kugler, P.; M. Dobler, J. Meierhofer, M. Strittmatter, M. Treiterer, H. Vogt (2025). Data Sharing für KMU - Voraussetzungen und Instrumente für die gemeinsame Nutzung von Daten, Wiesbaden: Springer Nature.

Long, D., & B. Magerko, 2020. What is AI Literacy? Competencies and Design Considerations. In: CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, https://doi.org/10.1145/3313831.3376727

Martens, B., 2023. Pro-and anti-competitive Provisions in the proposed European Union Data Act (No. 01/2023). Bruegel Working Paper.

Meier, D. A., & Burda, D. (2019). Cybersicherheit als Führungsaufgabe in Schweizer KMU: Herausforderungen und Chancen im Zuge der Digitalisierung. In Digitale Transformation und Unternehmensführung: Trends und Perspektiven für die Praxis (pp. 83-104). Wiesbaden: Springer Fachmedien Wiesbaden.

Müller, J. (2024). Der Schutz faktischer Kontrolle durch die Rechtsordnung, Recht Digital, (7), 297 – 304.

Ng, D.T.K.; J.K.L. Leung; S.K.W. Chu; M.S. Qiao, 2021. Conceptualizing AI literacy: An exploratory review. Computers and Education: Artificial Intelligence, 2, 2021, 100041, https://doi.org/10.1016/j.caeai.2021.100041

Ohly, A. (2019). Das neue Geschäftsgeheimnisgesetz im Überblick, Gewerblicher Rechtsschutz und Urheberrecht, 441 ff.

Pauly, D., Wichert, F., Baumann, J. (2024). Schutz von Geschäftsgeheimnissen nach dem Data Act. Multimedia und Recht, (3), 211-216.

Pliauskaite, L. o.J. EU Data Act: 101. https://iapp.org/media/pdf/resource_center/eu-data-act-101-chart.pdf

Podszun, R. (2021). Handwerk in der digitalen Ökonomie – Rechtlicher Rahmen für den Zugang zu Daten, Software und Plattformen (Bd. 5). Nomos Verlag.

Podszun, R.,Pfeifer, C. 2023. Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission, Gewerblicher Rechtsschutz und Urheberrecht, (13), 953 – 961.

Ridgway, W. E., Simon, D. A., Kerr-Shaw, N., Werry, S., Aleksiev, A. J., & Éles, K., 2025. EU Data Act: Three months to go before new rules on data access and sharing take effect [PDF]. Skadden, Arps, Slate, Meagher & Flom LLP. https://www.skadden.com/-/media/files/publications/2025/06/eu_data_act_three-months_to_go_before_new_rules_on_data_access_and_sharing_take_effect.pdf?rev=19bad942e61b4d14b647c54e05456151

Schein, E.H., 1992. Organizational Culture and Leadership, 2nd edition. Jossey-Bass Publishers.

Schemmel, F. (2024). Data Act und DS-GVO: ziemlich beste Feinde? Spannungsfeld und Wechselbeziehung in der Praxis. Compliance-Berater, (8), 301-308.

Schmidt-Kessel, M. (2024). Heraus- und Weitergabe von IoT-Gerätedaten. Multimedia und Recht, 75-82.

Schreiber, K., Pommerening, P., /Schoel, P. (2024). Der neue Data Act – mit Data Governance Act, 2. Auflage, Nomos Verlagsgesellschaft, Köln.

Schuh, G. (Ed.), 2012. Innovationsmanagement: Handbuch Produktion und Management 3. Springer-Verlag.

Schüller, K. 2020. Future Skills: A Framework for Data Literacy. Stifterverband & Hochschulforum Digitalisierung. https://hochschulforumdigitalisierung.de/wp-content/uploads/2023/09/HFD_AP_Nr_53_Data_Literacy_Framework.pdf

Schulz, M. (2024). Datenzugang nach dem Data Act - Überblick und Schnittstellen zum Kartellrecht. Neue Zeitschrift für Kartellrecht, (8), 426-433.

Schwamberger, S. (2024). Die Klauselkontrolle in Art. 13 Data Act. Multimedia und Recht, 96-101.

Seco.com, o.J.. Industrial innovation, how an OEM evolves thanks to AI and IIOT. https://www.seco.com/blog/details/industrial-innovation-how-an-oem-evolves-thanks-to-ai-and-iiot

Specht-Riemenschneider, L. (2023). Datennutz und Datenschutz: Zum Verhältnis zwischen Daten-wirtschaftsrecht und DSGVO, Zeitschrift für Europäisches Privatrecht, S. 638 ff.

Spießhofer, B. (2022). Sustainable Corporate Governance, Neue Zeitschrift für Gesellschaftsrecht, S. 435 ff.

Steinrötter, B. (2021). Gegenstand und Bausteine eines EU-Datenwirtschaftsrechts. Recht Digital, (10), 480-486.

Stewart, H. (2023). Digital transformation security challenges. Journal of Comput-er Information Systems, 63(4), 919-936.

Strittmatter, M., Meyer, J., Meierhofer, J., Vogt, H., Kugler, P., Dobler, M. 2025. The EU Data Act: Opportunities and Research Perspectives for Data-Driven Companies. In: West, S., Meierhofer, J., Buecheler, T., Wally Scurati, G. (eds) Smart Services Summit. SMSESU 2024. Progress in IS. Springer, Cham. https://doi.org/10.1007/978-3-031-86958-7_2

Stucki, M., Meierhofer, J., Gal, B., Gallina, V., & Eisl, S. 2024. Data driven value creation in industrial services including remanufacturing. Procedia Computer Science, 232, 2240-2248.

Tesch, J. F., Brillinger, A. S., & Bilgeri, D. 2017. Internet of things business model innovation and the stage-gate process: An exploratory analysis. International Journal of Innovation Management, 21(05).

The European Parlament, “MODEL CONTRACTUAL TERMS for contracts between data holders and data recipients on making data available at the request of a user.” Dec. 2024.

The European Parlament, “REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act),” 2023/2854, p. 71, Dec. 2023, [Online]. Available: https://eur-lex.europa.eu/eli/reg/2023/2854/oj

Tntra.com. o.J. The Future of Work: IoT-Driven Innovations in Manufacturing Industries. https://www.tntra.io/blog/future-of-work-iot-driven-innovations-in-manufacturing-industries/

Topping, C., Dwyer, A., Michalec, O., Craggs, B. and Rashid, A., 2021. Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks. Computers & Securi-ty, 108, p.102324.

Trott, P., Baxter, D., Ellwood, P., & van der Duin, P. (2022). The changing context of innovation management. Prometheus, 38(2), 207-227.

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A multidisciplinary reflection and research agenda. Journal of business research, 122, 889-901.

Verordnung (EU) 2023/2084, Erwägungsgrund 32, https://data-act-law.eu/de/erwg/32/

Verordnung (EU) 2023/2854 des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung sowie zur Änderung der Verordnung (EU) 2017/2394 und der Richtlinie (EU) 2020/1828 (Datenverordnung) v. 13.12.2023, abrufbar unter: http://data.europa.eu/eli/reg/2023/2854/oj.

Verordnung (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data (Data Act), OJ L, 2023/2854, 22.12.2023, p. 1–65. https://eur-lex.europa.eu/eli/reg/2023/2854/oj

Vidgen, R., Shaw, S., & Grant, D.B. 2017. Management challenges of creating value from business analytics. European Journal of Operational Research, 261: 626-639. https://doi.org/101016/j.ejor.2017.02.023

Von Ditfurth, L. (2024). Datenmärkte, Datenintermediäre und der Data Governance Act – Eine Analyse der europäischen Regulierung von B2B-Datenvermittlungsdiensten (Bd. 4). Verlang De Gruyter.

Weiden, H. (2022). EU Data Act und Tool zur Visualisierung von Datenströmen öffentlich. Gewerblicher Rechtsschutz und Urheberrecht, 16(5), 313–315.

Weinhold, R.; Schröder, C. (2024). Data Act - (R)Evolution oder vergebene Chance?. Zeitschrift für Datenschutz, (6), 306-311.

Wiebe, A (2023). Der Data Act als vertragsrechtlicher Rahmen für Datennutzungsverträge, Computer und Recht, S. 777 ff.

Wiebe, A. (2023). Der Data Act – Innovation oder Illusion? Gewerblicher Rechtsschutz und Urheberrecht, (22), 1569-1578.

Prof. Dr. Marc Strittmatter holds a professorship in Business Law at HTWG Konstanz, with a focus on IT Law and Data Protection Law. His research focuses on legal issues of the data economy and artificial intelligence (AI). Before being appointed to HTWG Konstanz, he was Head of Legal at IBM Germany and worked as an attorney in a law firm specialized in IT law. His teaching focuses on data law, legal issues of AI, negotiation theory, antitrust law, and IT and data protection law.

Johanna Meyer studied Business Law at HTWG Konstanz, graduating with a Bachelor of Laws (LL.B.). During her studies, she was involved in various research projects and was part of the university's data protection office team. In addition to her position as a research associate for the research project "Data Act Pioneer," she has been working since 2021 as a freelance collaborator for a boutique law firm specializing in technology, IP, and media. Her main focus there is on IT law and EU regulation.

Eileen Gladis is currently pursuing her LL.B. at HTWG Konstanz. Since September 2024, she has been working as a student assistant at the chair of Marc Strittmatter, where she is deeply involved in the Interreg-funded project "Data Act Pioneer." Her particular interests lie in data economy law, IP law, and competition law, which she also explored in her thesis at the chair.

Interreg
Alpenrhein-Bodensee-Hochrhein
Kofinanziert von der Europäischen Union
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Data Act Pioneer

Zürcher Hochschule für Angewandte Wissenschaften

zh aw

Dr. Jürg Meierhofer is Head of the Expert Group “Smart Services” of the Data Innovation Alliance and Program Director for Industry 4.0 (MAS) and Smart Services (CAS) at the ZHAW Zurich University of Applied Sciences. The design of data-driven service value creation runs as a common thread through his professional activities. After holding various leadership positions in the service sector, he has been teaching and conducting research at ZHAW since 2014. He earned his PhD at ETH Zurich and obtained an EMBA from the University of Fribourg.

Dr. Helen Vogt is a lecturer in Innovation and Product Management at the Zurich University of Applied Sciences (ZHAW) in Winterthur. A trained materials scientist, she has extensive experience in business development and industrial product management in Swiss and international companies. At ZHAW, she heads the Master’s program in Product Management and is actively involved in continuing education in the field of innovation management. Her research focuses on the circular economy and entrepreneurship, with an emphasis on the development of sustainable business models.

Susana Soriano Ramirez has been a research associate at the Zurich University of Applied Sciences (ZHAW) since 2022. She holds a Master’s degree in Business Information Technology from ZHAW and a Master of Advanced Studies in Applied Technology from ETH Zurich. Her research focuses on sustainable and automated software development, empirical studies on related challenges, and data-driven value creation. Previously, she worked as a systems engineer in Mexico, the USA, and Switzerland, and founded her own IT company in Mexico.

Interreg Alpenrhein-Bodensee-Hochrhein

Kofinanziert von der Europäischen Union

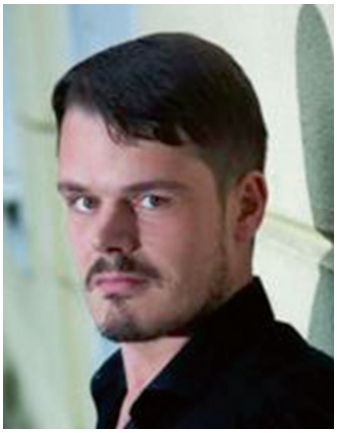
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Data Act Pioneer

OST Ostschweizer Fachhochschule

Prof. Dr. Petra Kugler is a Professor of Strategy and Management at the Institute of Corporate Management. Her work focuses on the intersection of innovation, strategy, and management, and on how companies can generate and protect sustainable competitive advantages in turbulent times. She earned her PhD at the University of St. Gallen (HSG), has professional experience in advertising, and gained international academic experience through various scholarships, including a Swiss National Science Foundation fellowship for a research year at the University of California, Berkeley.

FHV Vorarlberg University of Applied Sciences



Martin Dobler has implemented over 20 national, Interreg, and EU-funded (research) projects at the Business Informatics Research Center of the University of Applied Sciences Vorarlberg (FHV). After studying computer science, he initially worked as a software developer and later in the simulation and modeling of digital, automated supply chain ecosystems. In addition to teaching at FHV and Schloss Hofen, his research focuses on information security, autonomous systems, and digital innovation management.

Interreg Alpenrhein-Bodensee-Hochrhein
Kofinanziert von der Europäischen Union
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra