Fraunhofer ISST

Fraunhofer Institute for Software and Systems Engineering ISST

Data Management under European Regulations

Compliance challenges and solutions for organizations

Table of Contents

Introduction

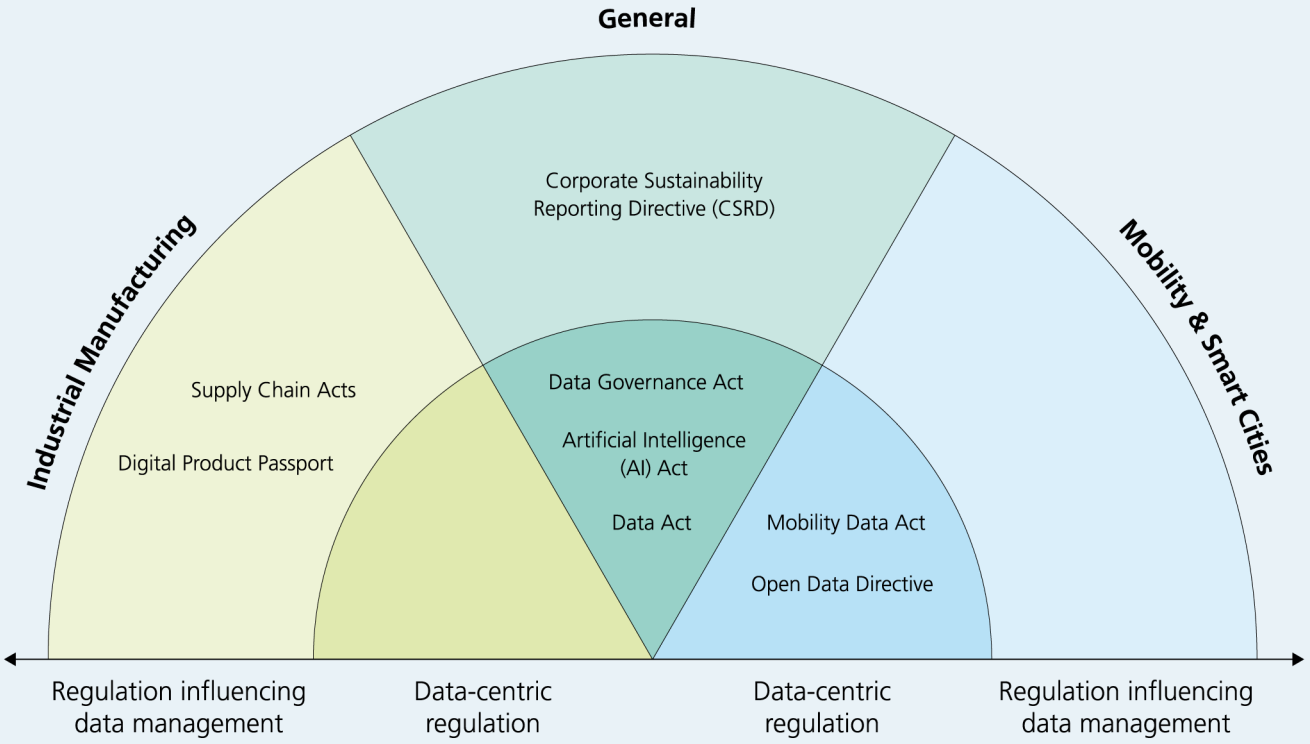

Figure 1. Regulation Radar

In terms of ensuring business continuity and business success, organizations face more demands than ever before. Rising raw material costs and energy prices, increasing customer demands, technological advancements and the competition for qualified employees pose challenges to maintaining a competitive advantage today. Additionally, the public now demands greater transparency, sustainability and fairness in business, which is increasingly being addressed by legislators. For example, the European Union (EU) recently introduced several novel regulations related to data law (including the Artificial Intelligence (AI) Act and the Data Act) and sustainability (such as the Corporate Sustainability Reporting Directive (CSRD) and Corporate Sustainability Due Diligence Directive (CSDDD)).

European organizations, as well as many international organizations operating in Europe, therefore need to pay particular attention to the legal classification of their activities and the implementation of the EU legal framework. On the other hand, the regulatory provisions also provide additional business opportunities, for example through the increased availability of data for data-driven business models or by offering novel digital services to facilitate compliance with regulatory requirements.

Data management is strongly impacted by regulation. For one, regulatory provisions result in direct requirements for the technical and/or organizational implementation of data management. Nowadays, this concerns the organization's internal data management as well as the data-based interaction between an organization and its business ecosystem. On the other hand, data management must ensure the secure, efficient, and timely provision of data that can be transformed into the information needed by regulators and other stakeholders, such as shareholders and investors. Excellence in data management is becoming a prerequisite for meeting regulatory requirements in many industries and a fundamental basis for taking advantage of the new opportunities presented by increased data availability.

This paper provides an overview of recent and upcoming regulations in the EU and Germany that have a significant impact on data management. It focuses on the laws and regulations that are most relevant for large and medium-sized organizations on their digital transformation journey. It describes the impact of emerging EU data regulations on the data management practices of affected organizations and provides recommendations on the use of data management approaches to facilitate regulatory compliance, including data strategies, data governance and metadata management.

First, this paper covers those regulations relevant to all industry sectors:

- The CSRD mandates increased transparency by requiring organizations to report on their sustainability activities, thus impacting how organizations manage and disclose environmental, social and governance (ESG) data, including data from the supply chain network.
- The AI Act aims to ensure safe and ethical development and usage of AI, which directly affects how AI systems and the underlying data are designed, collected and managed within organizations.
- The Data Act aims at fostering data availability and data sharing by enhancing access to data, which influences organizational data management strategies and practices, especially for organizations developing or using intelligent devices and services.
- The Data Governance Act establishes measures to foster trust in data sharing and the availability of high-quality data by establishing a governance framework that includes mechanisms such as data intermediation services and data altruism.

Second, this paper elaborates on the regulatory frameworks that cover enterprises involved in the industrial manufacturing of goods:

- Supply chain acts on European and national levels require organizations to identify, prevent, mitigate and account for human rights and environmental impacts within their supply chain networks, necessitating robust data management systems to integrate external supplier data and allow for sharing the needed information with their customers.
- The Digital Product Passport is a digital artifact that provides information about the origin, composition and life cycle of a product, and its implementation requires standardized data formats, a suitable IT infrastructure and the cooperation of all relevant stakeholders.

Third, this paper outlines data-related regulations aimed at fostering the establishment of smart cities and intelligent mobility services:

- The Mobility Data Act focuses on fostering access to and exchange of mobility-related data to enhance innovation and enable multimodal mobility services, which requires organizations in the mobility sector to provide certain types of data in high quality and via standardized interfaces.
- The Open Data Directive revises and strengthens the EU's approach to open data and the reuse of public sector information, requiring bodies in the public sector to make their data more accessible and usable, therefore impacting how these organizations manage and share their data.

Finally, this paper summarizes the effects of individual regulations on data management and provides actionable recommendations for executives and data professionals to ensure legal compliance, meet data provisioning requirements and systematically benefit from increased data availability.

Legal notice

Corporate Sustainability Reporting Directive

Entry into force: January 5, 2023

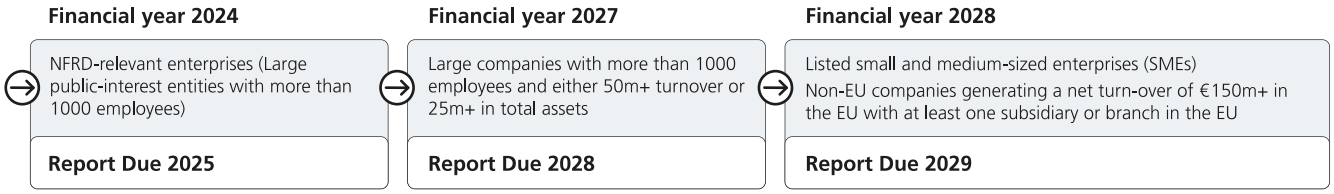

Figure 2. Timeline for the applicability of the CSRD

The CSRD adds ESG information to the reporting requirements of organizations operating in the EU. It replaces the previous Non-Financial Reporting Directive (NFRD). The increased availability of ESG information improves transparency with regard to the impact of an organization's operations and promotes informed decision-making by investors, consumers, policymakers and other stakeholders.

Scope and implementation timeline of the CSRD

The CSRD is implemented in a phased approach, starting with organizations that are already subject to the NFRD in 2025 (see Figure 2)[1]. The directive not only applies to European enterprises but also to non-European enterprises with more than 150 million euros turnover in the EU and at least one European subsidiary. Companies with up to 1,000 employees and a turnover of up to 50 million euros will not be covered by the CSRD. According to EU estimations, the CSRD will affect around 10,000 enterprises. The sustainability statement shall be created for the same reporting undertaking as the financial statement, meaning that a parent organization will generally report on behalf of its subsidiaries plus additional joint operations or joint ventures under its operational control. As with financial reporting, the organizations are independently audited and certified to ensure they provide reliable information. The depth of these audits will be increased over time, starting with 'limited assurance' and later with 'reasonable assurance'.

The European Sustainability Reporting Standards (ESRS) define the reporting content

The CSRD refers to the European Sustainability Reporting Standards (ESRS) [1] as authoritative source for the structuring and contents of a sustainability report. It defines 12 standards for ESG information that organizations must disclose to inform about their material impacts, risks and opportunities in relation to sustainability issues. This includes two overarching standards as well as standards in three categories: environment (e.g., climate change, energy consumption and mix), social (e.g., own workforce, working conditions, adequate wages) and governance (e.g., business conduct, corporate culture). The individual enterprise reporting requirements are determined based on a preceding materiality assessment. The European Financial Reporting Advisory Group (EFRAG) provides a comprehensive list of ESRS data points (metrics) as part of its implementation guidance [2]. It currently[2] describes 161 data points that need to be provided irrespective of the materiality assessment (and thus must always be included), while 622 additional data points are subject to the materiality assessment. This includes a total of 238 'numerical' data points, which often include aggregated or calculated measures. Figure 3 provides a high-level overview about the measures potentially required by the CSRD, including potential data suppliers within and beyond the organization as well as exemplary data categories based on the EFRAG implementation guidance. This overview highlights the challenges that large and diverse organizations face when producing their

[1] The first 'omnibus' package postponed the sustainability reporting requirements for companies that would have been affected in 2026 and 2027 (CSRD waves 2 and 3) by one year to 2027 and 2028, respectively.

[2] The EU announced that the number of data points will be reduced in the future.

first sustainability reports: a) Digital data from different sources and departments must be collected and made available, b) the quality and timeliness of the data must be ensured, and c) data from different sources, across departments and potentially across sites must be integrated in a potentially reusable manner.

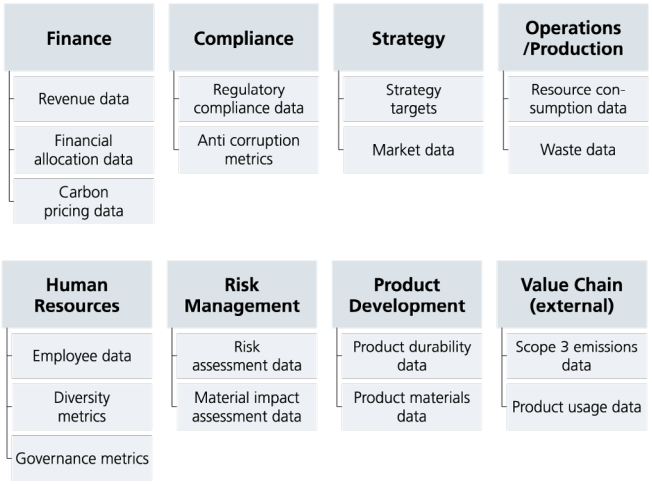

Figure 3. Overview of potential data points to be reported

Data management maturity equals ESG reporting maturity

Implementing efficient and robust sustainability data management systems is a key enabler and challenge when it comes to meeting ESRS requirements. Data must be collected from within the organization and from external partners in the supply chain (e.g., to calculate Scope 3 emissions), normalized and cleansed, aggregated, and presented to relevant business users and external auditors. However, a study conducted by PwC and the Ludwigshafen University of Business and Society shows that 73 percent of organizations surveyed struggle with collecting, processing, and analyzing the data needed for sustainability reporting [3]. Unlike financial reporting, sustainability reporting functions are usually not completely covered by standard enterprise information systems, leaving many organizations to rely on spreadsheets, which leads to limitations in data standardization, versioning, etc. ESG data is widely dispersed across different business units with their own data management approaches, resulting in ESG data silos. These silos can result in different ways of interpreting and calculating certain sustainability metrics, making it difficult to integrate sustainability data and produce sustainability reports at an organization-wide level. Leaders are often faced with insufficient and poor quality ESG data or delays in ESG data delivery due to limited data ownership, limited understanding of the data, or prioritization issues. This challenge is exacerbated in decentralized organizations with many independent organizations, investments, and joint operations that collectively implement their own data strategy, data governance and information systems architecture. Furthermore, data from the value chain, and thus outside of an organization's sphere of influence, may need to be collected. Vice-versa, environmental data need to be shared with customer companies.

Incorporating ESG reporting into the enterprise data strategy

With increasing regulatory pressure and costly audits, all these challenges require a more rigorous approach to ESG data management. From a technical perspective, organizations need to move from their collection of ESG spreadsheets to an integrated data architecture for ESG data. These architectures are typically based on a cloud data warehouse as a central component and include several layers, including data integration, data storage and modelling, and data provisioning to the relevant reporting systems. To define accountability, consolidate understanding of data and KPIs and consequently drive timely delivery of high-quality ESG data, corporate data governance must include structures and processes relevant to ESG data. To demonstrate the importance of ESG reporting to the organization, it should become an integral part of the corporate data strategy. In addition, data culture initiatives can raise awareness of the importance of ESG information for business continuity. In this sense, ESG reporting can serve as a key motivator to drive organization-wide data strategy, data architecture, or data governance initiatives. Federated approaches for these initiatives may be most suitable in large organizations as individual domains or enterprises retain autonomy with regard to their internal data processing while achieving a virtual global data layer.

Summary

The Corporate Sustainability Reporting Directive (CSRD) requires organizations to report detailed ESG information based on the European Sustainability Reporting Standards (ESRS), including environmental, social and governance (ESG) data. It requires independent verification and certification, with increasing levels of assurance over time. Organizations currently struggle to collect, process, and analyze ESG data due to disparate data sources, reliance on spreadsheets, and inconsistent data management practices. This leads to issues such as data silos, inconsistent KPI calculations, and low quality or outdated data.

To address these challenges, organizations need to move to integrated data architectures for ESG data and implement robust data governance frameworks. To underscore the strategic importance of ESG data to future business, ESG should be integrated into the corporate data strategy. ESG metrics as well as the underlying data should be governed to create a unified understanding across the organization and the relevant departments. In addition, a data culture initiative will raise awareness and prioritize the importance of high-quality ESG information for data providers.

Artificial Intelligence Act

Entry into force: August 1, 2024 (24-month transition period); notwithstanding unacceptable risk (February 2, 2025) and high risk (August 8, 2027)

The AI Act is the world's first law to regulate AI and aims to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI [4]. The AI Act is a regulation of the EU [5]. This form of legal act results in direct implementation in all EU member states without the need for conversion into national law. Member states can take additional measures to support the enforcement and application of the regulation [6]. The AI Act establishes general rules for placing on the market, putting into service, and using artificial intelligence systems. AI systems for research and development purposes are excluded from the AI Act. The regulation thus mainly targets providers and operators of AI systems. In the event of non-compliance with the regulation, organizations face fines of up to 35 million euros or 7 percent of their total annual turnover, whichever is higher. According to the EU classification, there are four risk classes of AI (Figure 4). The four risk classes are subject to different measures under the AI Act. The classes and measures are discussed in more detail below.

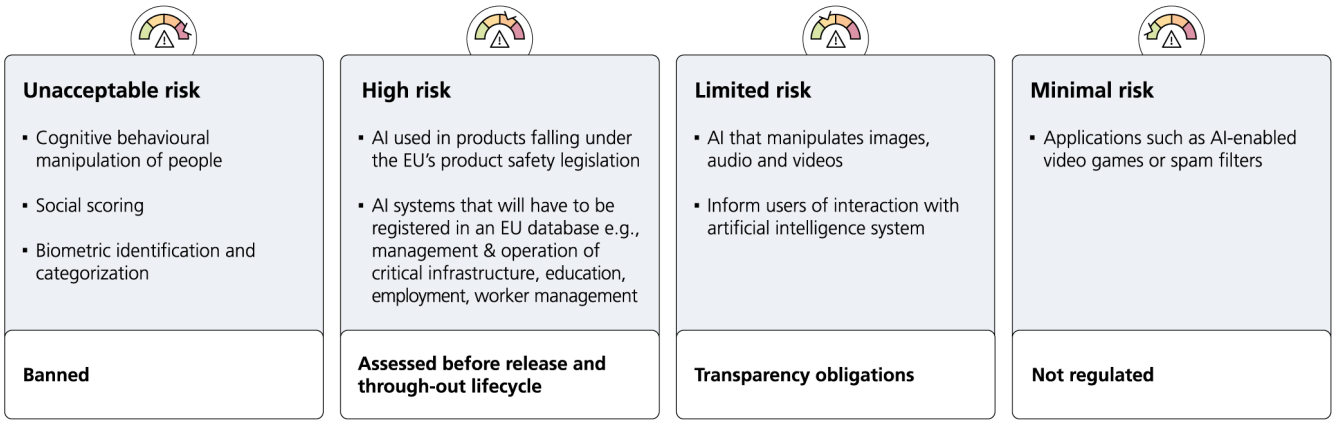

Figure 4. Overview levels of AI regulation

Banning the unacceptable AI risk class to ensure safety and rights

According to the AI Act, several types of AI systems that pose a clear threat to the safety, livelihoods, or rights of people fall under unacceptable risk. These include systems that employ subliminal, manipulative, or deceptive techniques, as well as those that exploit human vulnerabilities. The act bans biometric categorization systems and social scoring mechanisms. The assessment of the risk that an individual might commit a crime, along with the creation of facial recognition databases, is forbidden. Emotion detection in workplaces or educational settings is not allowed and the use of real-time biometric remote identification in publicly accessible spaces for law enforcement purposes is similarly prohibited. Nevertheless, the act specifies certain exceptions for these prohibitions, particularly for medical or public security reasons.

Continuous assessment of high-risk AI systems

Most of the regulation relates to high-risk AI systems. These systems include safety components that need third-party conformity assessment. They also encompass systems that perform critical tasks, except for narrow procedural tasks. Additionally, they enhance human activities, reveal decision patterns or support evaluations, but do not replace or influence human judgment. AI systems are deemed high risk if they create profiles by processing personal data to evaluate aspects like job performance, economic status, health, preferences, reliability, behavior, location or movements.

AI systems that fall into this risk category will be assessed before release and throughout the whole lifecycle. High-risk AI providers must fulfill the minimum transparency and security requirements for their AI systems. The minimum requirements encompass establishing a risk management system to ensure compliance with the requirements of the regulation by means of specifically designated procedures and instructions. This also includes ensuring data quality through quality requirements for training, validation, and test datasets. Additionally, providers are obligated to draw up technical documentation and instructions for use for downstream deployers.

Furthermore, providers must document assessments in the following cases if they believe their AI systems do not pose high risks before market release or operation:

Table 1. Overview of high-risk categories [7]

Category	Description
Biometric remote identification systems for identity verification	Security components in the management and operation of critical digital infrastructures
AI systems in education	e.g., for admission to an educational institution
Employment, employee management and access to self-employment	e.g., recruitment for targeted job advertisements, analysis and filtering of applications and assessment of candidates
Access to and use of essential public and private spaces	e.g., assessing eligibility for benefits and services
Law enforcement	e.g., assessment of a person's risk of becoming a criminal offender
Migration, asylum, and border control management	e.g., tracking, recognizing or identifying people
Administration of justice and democratic processes	e.g., influencing the results of elections and referendums

Enhancing transparency for limited-risk AI systems

Limited risks as defined in the AI Act involve the lack of transparency in AI usage. The AI Act mandates transparency to ensure people are informed and trust is built. For instance, users should know when they are interacting with AI, such as chatbots, to make informed decisions. AI-generated content must be identifiable, and any AI-generated text, audio or video aimed at informing the public must be labeled as such, including deepfakes. The limited risk class is thus mostly subject to transparency obligations.

Regulation of general-purpose AI as an exception in the minimal-risk class

Most AI systems are expected to fall into the minimal-risk class (e.g., spam filters and video games). Those are not regulated by the AI Act, but there is an exception: Even if general-purpose AI (GPAI) like ChatGPT is classified as minimal risk, it is still subject to transparency and documentation requirements. As in high-risk AI systems, GPAI providers must draw up technical documentation and information to supply to downstream providers. Furthermore, a detailed summary about the content used for training must be provided. High-impact GPAI could pose systemic risks and must therefore undergo a thorough evaluation process. Transparency requirements for GPAI include, for example, compliance with EU copyright law, detailed summaries of the content used for training, and additional requirements for high-risk AI.

Data management as enabler for AI quality and transparency

In the advent of novel security and transparency obligations, especially for high-risk AI, concise and well-documented input and output data management becomes crucial. For example, providers of high-risk AI systems need to conduct the necessary due diligence to ensure that training datasets are relevant, representative and free of errors. In general, organizations should therefore pay attention to the quality of the data used and reduce biases to a minimum. This includes having the skills and technical means to assess data quality and conduct data profiling to infer potential biases and, furthermore, making this information available for all relevant stakeholders. In addition, it should of course be ensured that the data used in training processes complies with data protection guidelines such as the GDPR. It must also be made transparent if content like images or texts were generated by (limited-risk) AI systems. If an organization or entity does not want to include this information in the content itself, the necessary transparency can be achieved by maintaining the corresponding metadata and making it available. While some implications can be inferred from the AI Act itself, the European Commission will develop additional guidelines for the practical implementation of the AI Act, which will certainly define more precise means and consider the individual requirements of start-ups and small and medium businesses.

Summary

The AI Act, effective as of the third quarter of 2026, is the EU's regulation to ensure the safe and responsible use of AI, classifying systems into four risk categories with corresponding obligations. It mandates transparency, documentation and assessment for high-risk AI while banning those posing unacceptable risks, ensuring user awareness and compliance with EU laws. Organizations developing AI should document the origin of data, the use of data and the algorithms used and establish an internal control mechanism to ensure ongoing compliance with the AI Act and other laws and the security of data from unauthorized access.

Data Act

Entry into force: January 11, 2024 (20-month transition period until September 2025)

The Data Act [8] regulates the ownership and utilization rights of data. The aim is to promote the data economy, support innovation, and ensure the protection of personal data by defining who, in addition to product manufacturers, may access data and under what conditions. The Data Act has four central aspects, as shown in Figure 5.

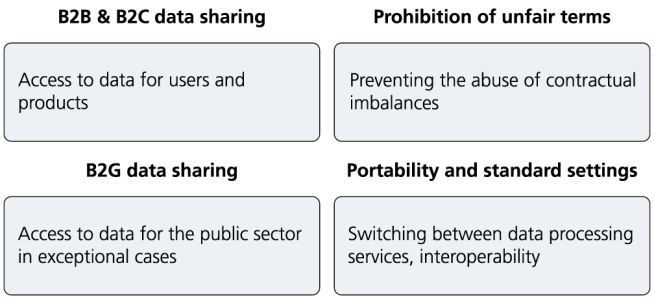

Figure 5. Overview of the topics in the Data Act

Core components of the Data Act

The first objective of the Data Act is to create legal certainty for organizations and consumers, which may or may not be a natural person, by defining who has which rights when handling data. This includes granting consumers access to the data generated by their use of 'connected devices' and related services. The aim is not only to protect consumers (who generate data), but also to encourage organizations (regardless of their size) to invest in high-quality data generation and participate in the data economy. Furthermore, the Data Act is intended to prevent the exploitation of power imbalances between contractual partners. At present, contract terms are sometimes deliberately drafted in a misleading way to give an advantage to one partner over the other. The Commission intends to address this situation by developing model clauses. The Data Act additionally formulates some rights of public authorities to access private sector data. For example, in the event of public emergencies, it should be possible to acquire data quickly to be able to respond to these emergencies, for example by making data-driven decisions for mitigation strategies. Finally, the Data Act is intended to enable customers to switch freely between different providers of data processing services. These regulations should contribute to a framework for data interoperability. Therefore, the Data Act defines requirements regarding interoperability specifically targeting providers of data spaces, data processing services, and smart contracts. In formulating the above requirements, the Data Act affects citizens as well as businesses of all sizes.

Enforcement of the Data Act

The enforcement of the Data Act will involve several key components to ensure its effective application and compliance. National regulatory authorities in each EU member state will oversee the enforcement, potentially coordinated at the EU level by existing bodies like the European Data Protection Board or a new specialized agency. The act is expected to provide mechanisms for individuals and businesses to file complaints if their rights are infringed and to include penalties and sanctions for non-compliance, which may range from fines to mandates to cease certain practices or modify data-related processes. Additionally, enforcement might feature both public and private channels, allowing for lawsuits by competitors or consumer associations against non-compliant organizations. Transparency and reporting requirements could compel organizations to regularly disclose their data practices, facilitating audits and compliance checks by authorities, complemented by awareness-raising and training programs to improve understanding and adherence to the regulations across all sectors.

Enhanced availability of data within the European Union

The Data Act focuses on a variety of data types, including data generated by connected devices and business operations as well as data used by government agencies in emergencies such as major fires or floods. This regulation aims to enhance the

availability of data within the EU by establishing clear rules for accessing and utilizing data, which is intended to support SMEs and promote a sustainable data economy. Furthermore, the Data Act seeks to foster innovation by enabling the development of new and improved products and services through enhanced data access, balancing negotiation power in data-sharing contracts, particularly to benefit SMEs that often face disadvantages when negotiating with larger organizations.

Simplified switching of cloud service providers

Additionally, the Data Act supplements the portability right under Article 20 of the GDPR by simplifying switching between cloud service providers. The aim is to promote data portability and interoperability, increase competition and reduce the risk of vendor lock-in. The Data Act ensures that users can transfer their data securely and efficiently from one cloud service to another without significant interruptions or costs. It considers the protection of trade secrets to ensure that organizations do not lose competitiveness through data disclosure. Technical standards and interfaces are developed to ensure compatibility between different providers. At the same time, data protection and data security are maintained, as all data transfers are carried out in strict compliance with data protection regulations such as the GDPR.

Impact on data management

The Data Act obliges organizations to organize product data and product usage data that customers gain access to. This requires appropriate organizational preparation. In addition, the Data Act opens the possibility of avoiding cloud lock-in effects and gaining access to public sector data. The increased portability requirements offer new opportunities for service usage and more cost-effective data management through greater competition between cloud providers. The Data Act covers data generated by connected devices, ensuring that data from such devices is accessible to both users and third parties. This requires robust data management systems to handle the large volumes of data generated by Internet of Things (IoT) devices and ensure it is properly shared and used. Organizations that rely on proprietary data for competitive advantage may need to rethink their business models, as the Data Act encourages more openness and sharing of data. This could lead to both challenges and opportunities as organizations adapt to a more collaborative data economy. The Data Act requires organizations to make extensive technical adjustments to their data management to fulfil the new requirements. One key measure is the development of data access and export mechanisms. Systems must be designed in such a way that users can easily view, export and forward data to third parties. This requires standardized formats such as CSV, JSON or XML. The development of application programming interfaces (APIs) enables users to access their data via interfaces, while user-friendly dashboards visualize data access and export. APIs are developed using programming languages such as Python, Java or JavaScript and frameworks such as Flask, Spring Boot or Express.js, utilizing common standards such as REST, GraphQL or gRPC. Tools such as Swagger, Postman and API gateways (e.g., Kong or Apigee) support documentation, administration and security, while JSON, XML and Protobuf serve as data formats. Security protocols such as OAuth 2.0 and JWT as well as container technologies such as Docker and Kubernetes enable the secure and scalable provision of APIs in modern cloud environments.

Data security is another key issue. Organizations must implement technical security measures, such as encrypting data during transmission and storage using technologies like TLS or AES. Identity and access management (IAM) systems ensure that access to data is controlled and monitored at a granular level. For example, a mobile service provider could introduce multi-factor authentication to ensure that only authorized persons access sensitive data. In addition to security measures, effective data governance is also required. Organizations must be able to document, monitor and report on the flow of data. Data catalogues can be used for this purpose, which list all available data records including their origin, intended use and access rights. Tools such as Splunk or the ELK stack can help to log access to data and monitor suspicious activities. It is also important to ensure the quality of the data. Data should be checked for consistency, completeness and timeliness before it is passed on. Data validation algorithms can recognize and correct errors or inconsistencies. Real-time monitoring systems, such as Apache Kafka, help to monitor large data streams and recognize anomalies.

The Data Act strengthens users' rights by giving them more control over their data and enabling easy access and sharing with third-party providers. This allows consumers and organizations to use data-based services such as analyses or optimization more efficiently and benefit from innovative offers. The Data Act also ensures greater transparency and fairness with regard to the handling of data, which reduces barriers to competition and creates new opportunities in the digital economy. The extensive technical measures enable organizations to meet the requirements of the Data Act, ensure compliance and modernize their data infrastructure at the same time. This not only strengthens legal certainty but also offers long-term competitive advantages through more efficient and secure data utilization.

Summary

The Data Act ensures fair access to data and strengthens the rights of the users. In the context of data management, the Data Act mandates organizations to organize data accessibly for customers and offers opportunities to avoid cloud lock-in, access public sector data and enhance services and cost-effectiveness through increased cloud provider competition. It aims at ensuring the privacy of the creators (for example European citizens) while allowing organizations and other big players to use data to create new possibilities by forming a clear legal framework for the ownership and use of data.

Data Governance Act

Entry into force: June 23, 2022 (15-month transition period until September 2023)

The Data Governance Act (DGA) [9,10] provides a framework for establishing common data governance in the EU and promoting cross-border data flows. Data is at the root of social and economic change, thus an inclusive framework for the free and secure flow of data within the EU and with third countries needs to be established that offers benefits for the common good. Data should flow according to the 'FAIR' principles (findable, accessible, interoperable, re-usable) in a common European data space. The intended principles create neutrality, transparency and trust in the data economy, with the interoperability of data and prevention of lock-in effects in compliance with all applicable laws (including the General Data Protection Regulation) creating further conditions for the shared use of data in the internal market.

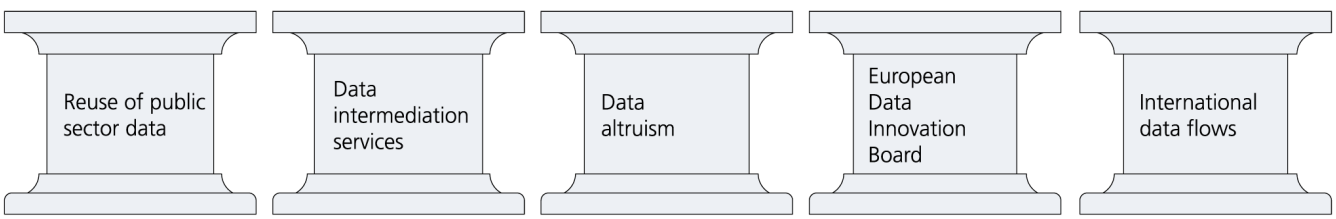

Figure 6. Framework conditions of the Data Governance Act (DGA)

Enhancing access to generated, protected data in the public sector

Public sector bodies should provide easier access to their generated protected data (e.g., personal data) for use and reuse. Techniques, mechanisms and processes such as anonymization or the provision of a secure processing environment should be established to facilitate the privacy-friendly processing of data for public sector bodies. Public sector bodies should comply with competition law and the open market economy and establish harmonized conditions and procedures for use and further processing that are non-discriminatory, transparent, proportionate and objectively justified. Scientific research, start-ups and SMEs need to be supported, and the interests and needs of reusers should be addressed. A fee may be charged for the approval of further use, but this fee aligns with and covers the arising costs. Public sector bodies should ensure that organizations and data subjects, their rights and interests are protected and that additional protective mechanisms are implemented, especially if further use occurs outside the public sector, for example if data is to be transferred to third countries. Further support structures are required, such as a supervisory authority and a central information point.

Data intermediation services are expected to play key role in the data economy

The responsibilities of data intermediaries include the efficient pooling of data and the facilitation of bilateral exchange through the networking of affected parties, data owners and data users so that data can be shared while maintaining neutrality. Data intermediaries can charge fees for mediation services, but they cannot use the mediated data themselves, e.g., for developing their own product. Richter (2023) explains that a data intermediary has a fiduciary duty and an obligation to act in the best interests of the data provider, but these are not clearly defined. [11] However, acting in a fiduciary function does not necessarily exclude the data intermediary from acting in its own interest. Data intermediaries play a supporting role in the creation of ecosystems and in ensuring non-discriminatory access to the data economy, including for SMEs and start-ups. Data intermediation services are responsible for setting up platforms, suitable special infrastructure, and databases to enable networking and sharing between the parties involved.

Data altruistic organizations gain more trust because their purpose is both altruistic and in the common interest

As a regulation, the DGA was intended to pursue the objective of making large datasets available through data altruism. Data altruism should be facilitated by organizational and/or technical mechanisms, such as awareness campaigns. In addition, a European consent form for data altruism should be developed, which is modular to adapt to different purposes and sectors and to facilitate altruistic data sharing.

Both approved data intermediaries and approved data altruism organizations should be identified with a common logo throughout the Union, and authorities and supervisory mechanisms should be set up to ensure that the services are monitored. The EU certification enables organizations offering similar services to differentiate themselves and use the logo, for example as part of their brand marketing.

The European Data Innovation Board as an authority for the implementation of a data governance framework

To successfully implement the data governance framework, a European Data Innovation Board consisting of expert groups and involving all relevant stakeholders and representatives should be elected. The Data Innovation Council deals with standardization work that supports the development of a functioning data economy. This requires sanctions that can be enforced in the context of non-compliance and that are effective, proportionate and dissuasive but do not create excessive discrepancies or distort competition in the digital single market.

Impact on Data Management

The DGA regulations specify, for instance, that business data should be shared. However, if the data formats are not standardized, data availability is limited and the interoperability of data access and data quality are not suitable, thus business data cannot be usefully shared. The DGA aims to create trust in the data economy and in the data, with reliable, correct data being especially useful for applying analysis techniques. The regulatory instruments are designed to especially integrate small and medium-sized organizations as core players. Most of these organizations do not have adequate data management.

Summary

The Data Governance Act (DGA) is a legislative framework that regulates the cross-sectoral reuse of certain categories of publicly available data and promotes, regulates, and determines the sharing and reuse of data for both altruistic purposes and through data intermediaries. Promoting effective data management in organizations can create a foundation for the successful implementation of data sharing and data intermediation services offering organizations potential for new business models and products.

Supply Chain Acts

Entry into force: January 1, 2023 (German Supply Chain Act), July 25, 2024 (European Supply Chain Act, transition period until July 2027)

The Corporate Sustainability Due Diligence Directive (CSDDD) is an EU directive that aims to make human rights and environmental due diligence mandatory for organizations. The aim is to ensure that European organizations, as well as certain non-European organizations with significant sales in the EU, identify, prevent and mitigate adverse impacts of their business activities and global supply chains on the environment and human rights. The CSDDD was adopted in June 2024 and is to come into force in stages from 2028 until 2029 [12]. It will require regular assessments every five years.

Scope of application and affected organizations

The original plan was for the CSDDD to apply to organizations with more than 250 employees or an annual turnover of over 50 million euros. However, after intensive discussions and political debates, the scope of application was adjusted. The version that has now been adopted applies to organizations with more than 1,000 employees and an annual turnover of over 450 million euros. This represents a significant restriction compared to the original plans, which were aimed at a much broader corporate landscape. Nevertheless, the directive remains an important step towards mandatory due diligence at the EU level.

The directive also applies to organizations based outside the EU that generate a significant turnover within the EU. Specifically, this means that international corporations with an annual turnover of over 450 million euros in the EU will also be required to address human rights and environmental risks in their global supply chains.

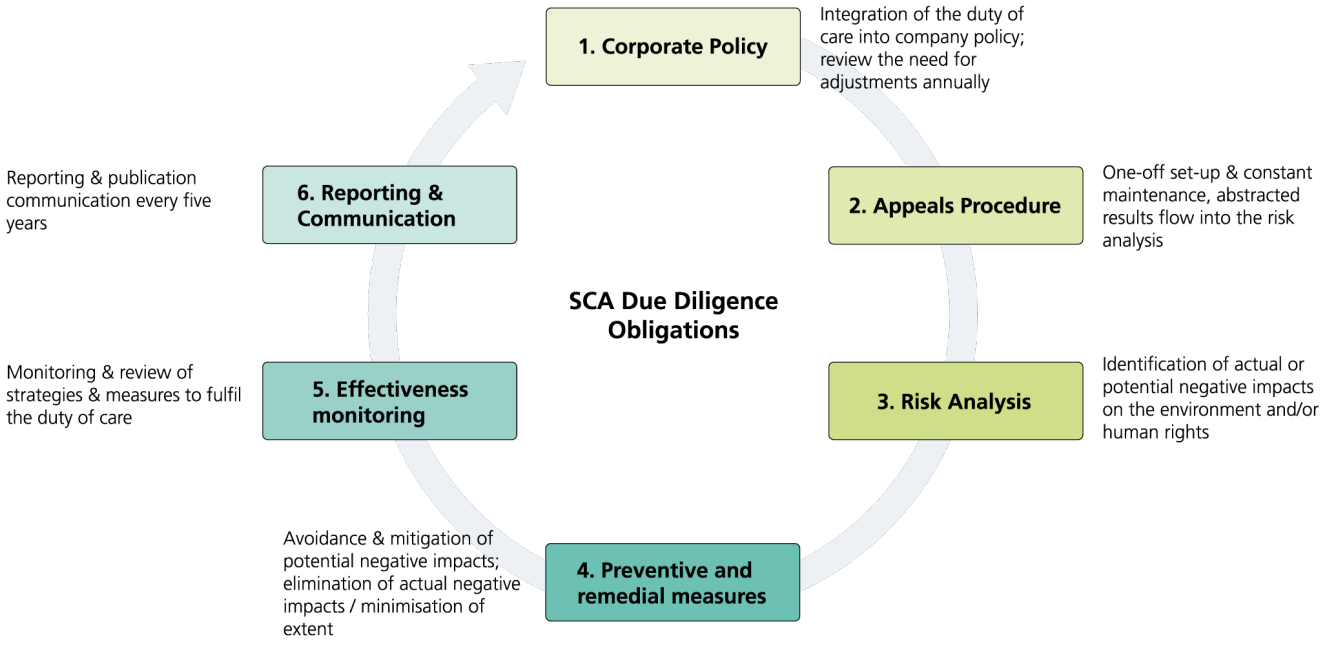

Figure 7. Supply chain act: due diligence obligations [13]

Aims and obligations of the CSDDD

The core obligations of the CSDDD include several due diligence requirements that organizations must fulfill along their value chains. These include:

- **Identification and risk assessment:** Organizations must systematically analyze potential human rights and environmental risks along their supply chains. This includes both direct and indirect suppliers.
- **Prevention and remedial measures:** Organizations are obliged to take measures to minimize or prevent identified risks. These include, for example, working with suppliers, introducing sustainable production standards or adapting business models.
- **Reporting requirements and transparency:** Organizations must regularly publish reports outlining the measures they have taken to fulfill their due diligence obligations. These reports should be made available to the public and the supervisory authorities.
- **Sanctions and liability:** Organizations that fail to meet their obligations can be subject to heavy fines. In addition, the CSDDD introduces civil liability, enabling affected parties to claim damages in European courts if organizations have demonstrably violated the due diligence obligations.

The German Act on Corporate Due Diligence Obligations in Supply Chains

The CSDDD builds on existing national legislation, such as the French Duty of Vigilance Law (Loi de Vigilance), the German Act on Corporate Due Diligence Obligations in Supply Chains (LkSG) and similar initiatives in the Netherlands and other EU states. The creation of a unified regulation at the European level is intended to produce a competition-neutral solution that ensures that organizations in all EU member states are subject to the same standards. The LkSG applies to all organizations in Germany with at least 1,000 employees and includes six due diligence obligations [14]:

1. Establishing a risk management system
2. Designating a responsible person or persons within the company
3. Conducting regular risk analyses and issuing a policy statement
4. Laying down preventive measures
5. Taking remedial action and establishing a complaints procedure
6. Documenting and reporting

The rules are enforced and monitored by the German Federal Office for Economic Affairs and Export Control (BAFA). In case of violations, organizations can be fined up to 8 million euros (regardless of the organization's annual revenue) or up to 2% of their global annual revenue (if the organization's annual revenue exceeds €400 million). It is also possible to be excluded from public procurement contracts for up to three years [15]. In Germany, the Federal Ministry of Labour and Social Affairs (BMAS) is responsible for translating the CSDDD into German law [16,17].

Impact on data management

Both the European and the German supply chain acts have one thing in common: a huge impact on data management. While this may seem like a burden on corporate legal departments, none of the obligations can be met without proper data management. Organizations must ensure that they have or acquire these following capabilities:

- Functioning data governance to identify responsible employees.
- Deep data architecture management and data quality management to be able to collect, analyze and use the right data to document and report on processes.
- Data platform & data space management expertise for efficient data sharing and the ability to provide transparency across the organization's whole supply chain.
- Ensure that data compliance is a part of the corporate compliance board in order to avoid potential fines.

The Corporate Sustainability Due Diligence Directive will profoundly impact data management practices within organizations, driving the need for more comprehensive, accurate, and transparent data across supply chains. Organizations will need to invest in advanced data management systems, ensure data accuracy and security and develop robust reporting and transparency mechanisms. The directive also emphasizes the importance of continuous monitoring, data-driven decision-making and collaboration across supply chains, presenting both challenges and opportunities for businesses as they adapt to these new requirements. Acquiring these capabilities will also help organizations to meet the requirements of the Digital Product Passport, Corporate Sustainability Reporting Directive and the Data Act.

Summary

Both the European and the German supply chain acts have one thing in common: a huge impact on data management. While this may seem like a burden on corporate legal departments, none of the obligations can be met without proper data management. The laws increase the requirements for data provision across the entire product and supply chain, and the industry needs to gain expertise in data governance, data sharing and many more data-related capabilities to ensure compliance with the supply chain acts. Acquiring these skills will also help organizations to meet the requirements of the Digital Product Passport, the Corporate Sustainability Reporting Directive, and the Data Act.

Digital Product Passport

Entry into force: planned for 2027

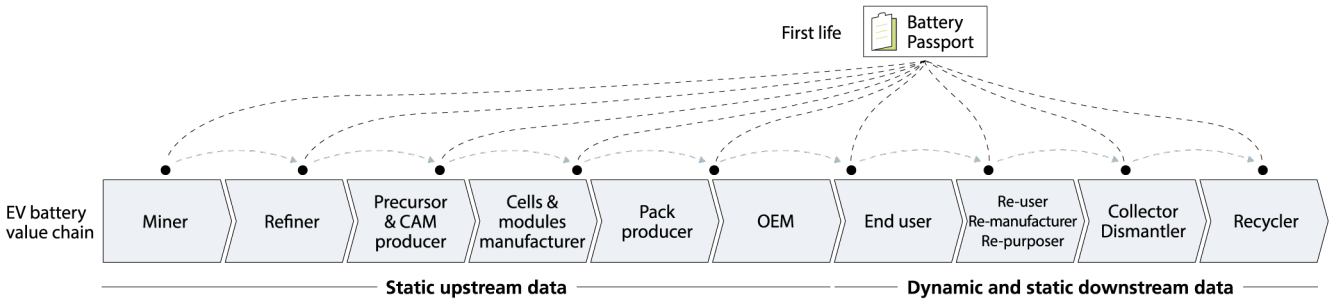

Figure 8. Data flow in the Battery Passport of the Catena-X Automotive Network Initiative

The relevance of harmonizing economic activity with an environmentally compatible approach requires increasing consideration of the life cycle data of produced goods. Within the EU, the Green Deal and the EU Circular Economy Strategy are pursuing new ways of aligning solutions for the harmonization of environmental requirements and economic activities.

As part of the EU Circular Economy Strategy, the Ecodesign for Sustainable Products Regulation ESPR is a central building block aiming to 'significantly improve the circularity, energy performance and other environmental sustainability aspects of products'. The ESPR replaces the current Ecodesign Directive 2009/125/EC and aims to establish a 'framework for setting ecodesign requirements on specific product groups', including the Digital Product Passport (DPP). The DPP is a central element for promoting the circular economy and sustainability, as it is intended to provide comprehensive transparency about the materials, origin, and manufacturing processes of a product. According to European legislation, the DPP is a 'tool for making information available to actors along the entire value chain and the availability of a digital product passport is expected to significantly enhance end-to-end traceability of a product throughout its value chain' [18].

The DPP is a central element of the CIRPASS project. CIRPASS is working on developing and implementing the foundations and standards for Digital Product Passports. These passports should contain comprehensive information about products, such as their origin, composition, environmental impact, and disposal options. By establishing these standards, CIRPASS supports the implementation of the Digital Product Passport and thus promotes the circular economy and sustainability in the EU [19].

The Battery Passport is a first instantiation of the Digital Product Passport within the Catena-X Automotive Network initiative

Currently, many general aspects of the DPP are still open, especially those related to the technical implementation of this concept. How can it be ensured that all relevant data is collected and maintained throughout the entire life cycle of an asset? An initial instantiation of the DPP for tracking automotive batteries already exists as part of the Catena-X Automotive Network automotive initiative. The Battery Passport serves to provide holistic traceability of all relevant life cycle data of a battery, from production to recycling, and thus forms a first use case-specific instantiation of the DPP. Figure 8 shows the data flow starting from the request to the Battery Passport to the final transmission of the required data. The access process itself utilizes a user interface and an EDC Connector that enforces data sovereignty policies, with the Catena-X Automotive Network acting as the verification and authentication entity. As part of Catena-X Automotive Network, BMW reports a comprehensive database to its suppliers, comprising a total of 107 data points. Of these data points, 52 are classified as primary data,

containing both sensitive and verified information. This structured data transfer enables efficient collaboration and transparency within the supply chain (see Figure 8). The battery passport acts as a key instrument between the original equipment manufacturer (OEM) and the end user. It enables the traceability and documentation of all relevant data along the entire supply chain. This includes all players, from raw material miners to manufacturers and recycling companies. The collection and storage of this data in the battery passport ensures that all information about the origin, use and recycling of the battery is transparent and traceable.

Initial proposals focus on the collection of data like product modification, usage and maintenance, material composition and others [20]. There are major conceptual similarities between the DPP and the concept of the digital twin, which provides a useful abstraction of the implications for data management. According to Glaessgen and Stargel (2012), a digital twin is 'an integrated multiphysics, multiscale, probabilistic simulation of an as-built vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its corresponding flying twin. The Digital Twin is ultra-realistic […] integrates sensor data […] maintenance history and all available historical and fleet data obtained' [21].

Impact on data management

On closer observation of the DPP, these requirements are certainly excessive, so that the DPP can rather be understood as a conceptual submodel of a digital twin that contains all data that is relevant for compliance with European legislation. Another important aspect is the decentralized approach of the DPP: 'To ensure that the digital product passport is flexible, agile and market-driven and evolves in line with business models, markets and innovation, it should be based on a decentralized data system and be set up and managed by economic operators' [22]. Accordingly, the DPP is part of a distributed system, characterized by the design goals of data sharing, transparency, openness, and scalability [23]. The resulting analogies to shared digital twins allow for the initial derivation of implications of the DPP for enterprise data management, which are explained below using the design principles for shared digital twins [24]:

1. **Interoperability:** Within the legislation, the DPP should have interfaces that are based on accepted standards. Those responsible should deal with this at an early stage and check to what extent the possible interface standard can be supported.
2. **Data Security:** The DPP should always have the option of restricting access. It should be ensured that unauthorized access is not possible. The implications for organizations remain open at present, including the question of possible legal liability.
3. **Data Acquisition:** It is not specified in more detail how data should be uploaded to the DPP. It probably depends on the technical circumstances of the organization in terms of whether data is entered automatically or manually.
4. **Data Input:** Users must ensure that only relevant data for the respective use case is uploaded to the DPP. Manufacturers must ensure that the required data is gathered and kept up to date in the required quality and scope.
5. **Synchronization:** According to the legislation, the DPP must be kept up to date. This does not primarily require real-time updating, but rather synchronization on demand.
6. **Interface:** According to the regulation, the use of the DPP should be 'user-friendly' for stakeholders. The access to the DPP should be as barrier-free and accessible as possible.
7. **Purpose:** The DPP is not intended to be used for processing data. Rather, it should be regarded as a repository, which in turn differs from the concept of the digital twin. It must be ensured that the data is of sufficient quality before it is uploaded. This results in a certain amount of work for the actors involved. In addition, according to the regulation, a back-up copy of the DPP should be created for security reasons.
8. **Data Link:** The DPP enables a bidirectional data flow. The extent to which this has an impact on data management depends on how the access and data retrieval are technically implemented.

Summary

The impact of the DPP on corporate data management is extensive, as the DPP specifies which data must be provided and shared with whom and in usable quality. The DPP requires a decentralized infrastructure as well as the integration of all actors involved in the life cycle design of a product and poses a particular challenge for organizations that bring a product to market and are therefore responsible for operating the DPP. However, it is not only the organizations that finally bring a finished product to market that are affected, but also suppliers that provide individual subcomponents for the final product, for example. So far, it remains unclear in what form data must be provided, what constitutes sufficient data quality and whether there should be specific semantic standards to ensure a certain degree of interoperability.

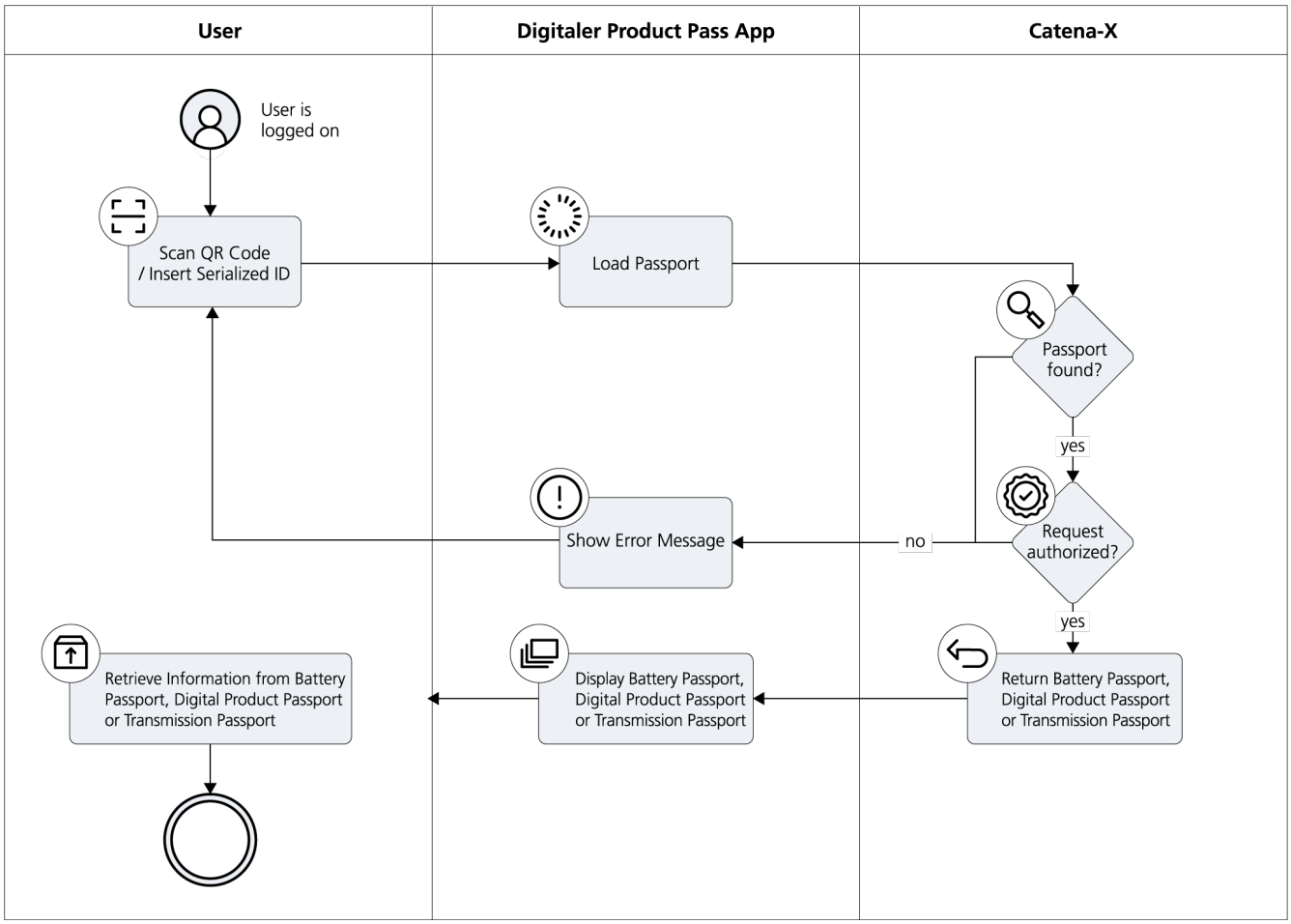

Figure 9. Battery Passport data extraction

Intelligent Transport Systems (Mobility Data Act)

Entry into force: since 2010 (last change: December 20, 2023)

The EU Directive 2010/40, which mandates the provision of publicly relevant mobility data, serves as the foundation for the 'Mobility Data Act'. It is mandatory for member states of the EU to make public mobility data accessible via the national access point (NAP); they are not required to gather additional data. This NAP is embodied as the 'Mobilithek' [25] in Germany. The objective of the Mobility Data Act is to create a digital, multimodally linked transport data network (digital twin) and enable:

a) (Transnational) seamless multimodal mobility
b) Development of innovative products, services, and business models

Duty of Public Mobility Data Provisioning

The German Mobility Data Act (Mobilitätsdatengesetz, or MDG for short) [26] carries out the EU directive for a NAP. The free accessibility of mobility data is guaranteed by the MDG. Real-time data from transportation businesses and mobility providers must be made available to the public under fair conditions. This applies to both static data (e.g., schedules, e-charging stations, bicycle parking facilities) and dynamic data (delays and cancellations, notifications about roadwork, closures and traffic jams, availability of charging points, etc.). A data supervisory authority may apply penalties for breaches of provision requirements or obligations to collaborate to improve data quality if firms refuse to deliver this data. Although the MDG increases legal certainty by establishing consistent requirements, a new draft of the MDG is being developed with significant extensions, such as for financial penalties and provision in machine-readable format [27, 28].

Private mobility data provisioning

The NAP gives priority to data that is publicly available or must be made available by law. This opens a gap in the mobility data ecosystem for private data. The Mobility Data Space [29] (MDS) fills this gap, as it is an infrastructure for sharing and trading data that is not publicly available. It is privately operated and builds on data space technology, which is a core technology in the European Data Strategy. Organizations willing to participate in the MDS need a connector to provide and use data. Usage policies attached to the data allow the sovereign sharing of data beyond organizational borders. The MDS as a marketplace enables an additional revenue stream for organizations. Present use cases are AI-based optimization of current mobility offers, finding profitable sites for electronic vehicle charging and pay-as-you-drive car insurance. The provisioning of data from the Mobilithek for MDS users is planned for 2025.

Impact on Data Management

Organizations within the EU member states are obliged to deliver their public mobility data assets (public transportation, delays, capacity utilization, etc.) into a NAP. In Germany, the NAP is embodied in the Mobilithek. It is particularly important to comply with the obligation to provide data in the NAPs, as penalties may be imposed in the future. For sharing non-public mobility data, organizations may seek revenue streams via marketplaces such as the MDS. Overall, organizations must be aware of their role in the mobility data ecosystem and, if they generate public mobility data, share their data via a NAP.

Summary

EU Directive 2010/40 for intelligent transport systems enables the free accessibility of mobility data. For seamless mobility, transport companies and mobility providers should make their real-time data available under fair conditions. The EU directive is enforced in the member states through their own national access points (NAP). Non-public data can be shared via marketplaces, such as the Mobility Data Space.

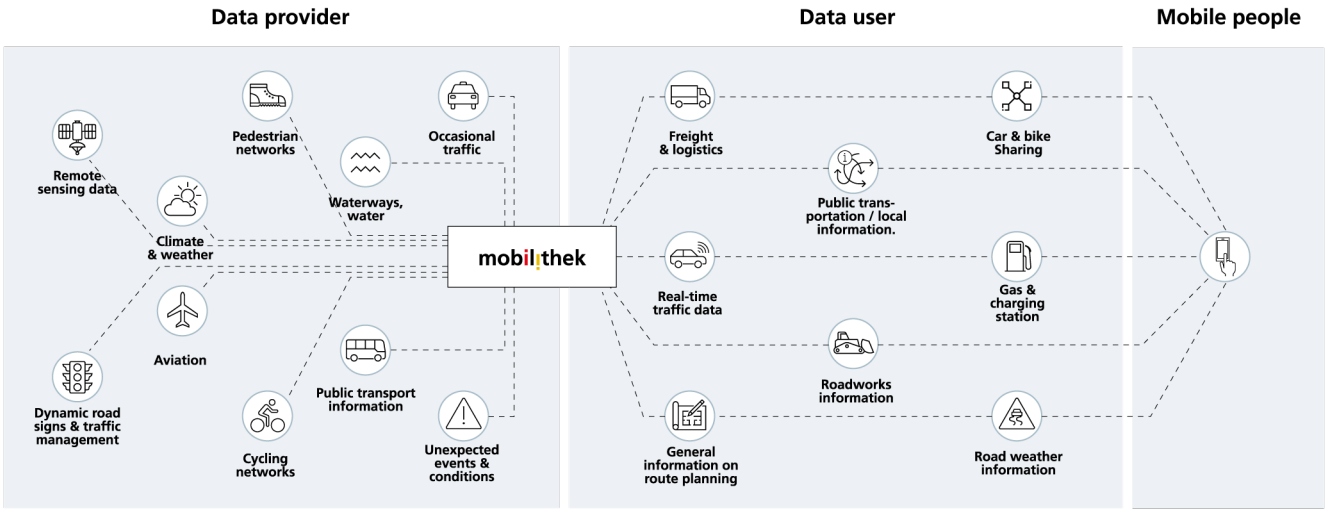

Figure 10. Illustration of the Mobilithek [25]

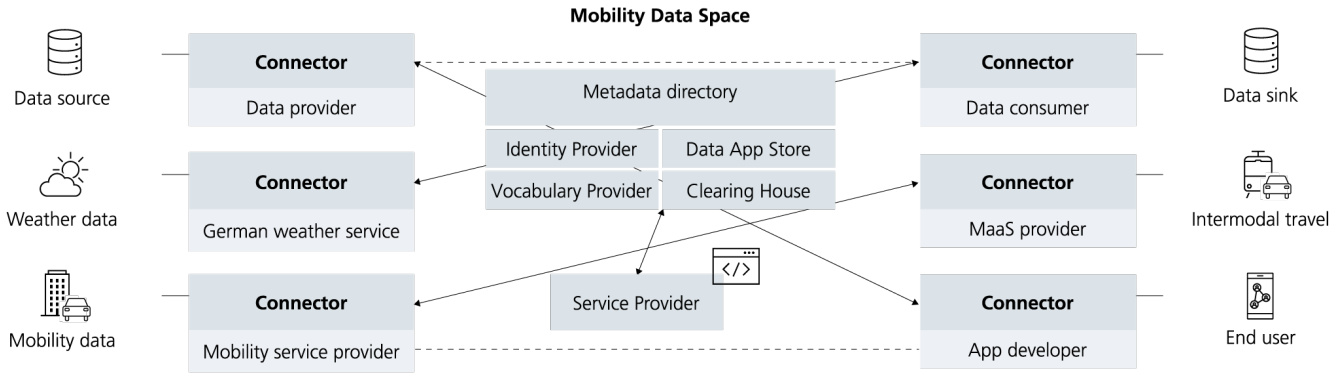

Figure 11. Data sharing in the Mobility Data Space

Open Data Directive

Entry into force: July 16, 2019

The 'Directive on open data and the re-use of public sector information', [30] also known as Open Data Directive, establishes a common legal framework for a European market for state-owned data and is intended to drive the publication of data in the public domain [31]. The Open Data Directive is the latest major upgrade to the Public Sector Information (PSI) Directive and replaces it [32].

Open data is defined as data in an open format which is freely accessible to everyone and can be re-used and shared under open and non-discriminatory licenses, gaining global significance as a crucial economic factor and a component of modern infrastructure [33].

Unlocking the economic potential of public data sources

The Open Data Directive focuses on the economic potential of the reuse of information. Through the directive, EU member states are encouraged to drive the availability of data from public administrations and data published under European open access mandates for commercial and non-commercial purposes. This is to be done at minimal or no cost and without exclusive agreements, with exceptions for certain personal data, confidential business information, statistically confidential information, third-party intellectual property, and other cases. It addresses data held by public sector bodies in EU countries at national, regional, and local levels. This includes material held by ministries, state agencies, municipalities and organizations funded primarily by or under the control of public authorities, such as meteorological institutes, water and energy services.

Maximizing benefits for businesses and organizations through high-quality datasets

Furthermore, the Commission has defined a catalog of high-quality datasets. To count as a high-quality dataset, the datasets must either be associated with important socioeconomic and environmental benefits, bring great use to many users (especially SMEs) or used to generate revenue. Datasets that have been defined as high-quality must be made available via an application programming interface (API), free of charge and in a machine-readable format, with exceptions, for example, if provision of the datasets leads to a distortion of competition. Currently, the directive defines six categories for high-value datasets, but these areas can be expanded on an ongoing basis (Figure 12). An example of such high-quality datasets is the 'list of navigation aids and traffic signs' in the mobility domain [34].

Impact on data management

As the directive addresses public or publicly funded organizations, there is no need for private companies to act. Private companies can benefit from various aspects, e.g., developing new products and services, improving market analyses and reducing research and development costs. In contrast, several data management measures can be derived for public or publicly funded organizations. One strategic aspect that emerges from the directive is the inclusion of open data in the data strategy of organizations. First, these organizations should have a holistic overview of their data ecosystem. This will ensure that the greatest potential can be utilized. It is important to know where the available data comes from and what license restrictions may

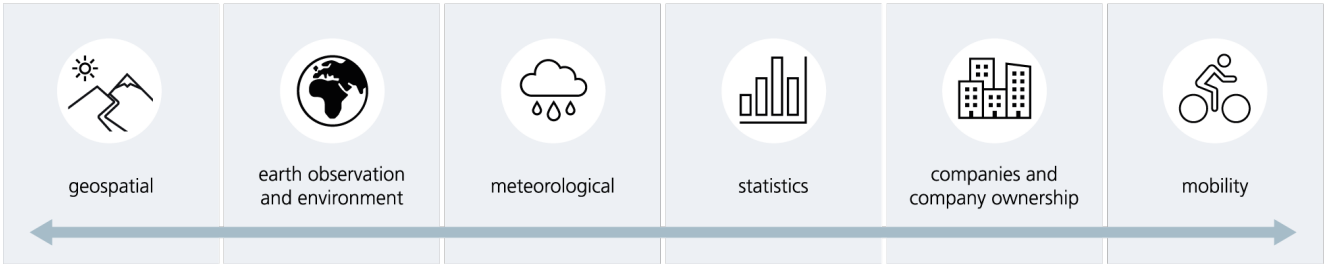

Figure 12. Categories for high-quality datasets

apply. In addition, there should be specialist knowledge about the datasets and care should be taken during data collection to ensure that the datasets are labeled with appropriate metadata. Furthermore, the FAIR principles should be observed during data collection to ensure high data quality. Finally, it is mandatory to make sure that no personal data is provided.

Summary

The Open Data Directive establishes a common legal framework for a European market for state-owned data. The goal of the directive is to drive the publication of data in the public domain with a focus on the economic potential. Private companies, especially SMEs, can benefit from freely available high-quality datasets.

Public or publicly funded organizations should incorporate open data into their data strategy, maintain a holistic overview of their data ecosystem, and understand the origins of their data. They should also use appropriate metadata and follow the FAIR principles to ensure high data quality.

Impact of regulatory requirements on data management in organizations

The question remains as to whether these regulations can be seen as a burden on data management or rather as an opportunity to bring data management systems up to date. A closer look at the individual regulations reveals that the upcoming tasks and challenges organizations are facing can essentially be summarized in 3 key aspects that represent a traditional data lifecycle, starting with data acquisition and data processing through to data sharing.

Data acquisition

The enhanced availability of usage data through the Data Act offers novel opportunities for the users of connected devices and related services. On the other hand, sustainability regulations demand greater availability of data that has possibly not been collected before. In any case, to leverage the benefits of the enhanced data availability, modern data infrastructures for the storage and management of the available data must be

in place. As sustainability data are currently handled as rather static and structured data objects collected for a specific reporting period, cloud-based data warehouse architectures offer promising benefits. This is especially true for mid-tier enterprises with limited data literacy. The use of a data warehouse involves moving data from different source systems, which generally represent heterogeneous platforms and data structures, [35] to a centralized location. The advantages of data warehouses thus lie in easier information retrieval and information consolidation. However, data retrieved from connected devices may come in high volume, velocity and variety. As a result, the transfer of these data to the cloud may not be feasible due to bandwidth limitations or high costs. Appropriate data management capabilities thus need to be built at the edge or on-premises in order to manage the data obtained from connected devices. Standardized interfaces and data models support companies in integrating data from different source systems.

Data processing

The forthcoming regulations will require organizations to handle data in a more targeted manner. This refers to the fact that data must be available in a certain quality and must be semantically interpretable. In this context, there are various established concepts for improving data quality within an organization, in particular. This includes, for example, a TDQM framework that enables holistic implementation in four phases, starting from the definition of criteria to the introduction of key indicators and analysis options through to the continuous improvement of data quality activities [36].

Managing data 'as a product' adapts product management principles to the management of data. Dedicated data product managers become responsible for providing data in a way they can easily be consumed by the data users for data-driven use cases. Data products adhere to jointly defined data quality metrics, semantics, interfaces and possibly even data models manifested in machine-readable data contracts. Access and usage conditions are also defined. Once created, data products accelerate data-driven value creation while ensuring regulatory-compliant data usage. With data product management, data ownership 'shifts left' along the data value chain, meaning that data-creating domains become responsible for their data rather than relying on centralized data units for data ownership. Thus, changes in data governance structures may be imminent in organizations seeking to establish regulatory compliance or seeking benefits from the novel possibilities offered by the regulation.

Data sharing

In the context of novel regulations, the collaborative utilization of data is of crucial importance. The regulations require a new approach to data, which is essentially characterized by the need to share data in a collaborative ecosystem consisting of a large variety of different organizations. A key aspect is to ensure the traceability of product information data along the entire product life cycle. The goal of these objectives is strongly related to overarching initiatives including the International Data Spaces (IDS) and GAIA-X from a technical perspective. In addition, similar approaches for designing data spaces within various industrial sectors, such as the Manufacturing-X and Catena-X Automotive Network and the Mobility Data Space are taken into consideration.

Overall, there is a lack of an overarching data architecture to build and run such an ecosystem that enables the necessary joint data management but at the same time considers the protection of the interests of individual persons or organizations. The challenges being faced arise from two main issues: first, the lack of governance for the ecosystem that spans across individual organizations and second, the lack of common standards relating to frameworks, structure, models, and processes regarding data management, exchange and utilization.

Additionally, some organizations may be reluctant to join these data sharing initiatives due to the costs and organizational overhead. International standards such as the data spaces protocol [37] and the W3C Verifiable Credentials [38] allow for technical interoperability in data sharing without the need to map data into the standards defined by the data sharing initiatives. These standards are implemented by the Eclipse Data Space Components (EDC) [39] which can be configured as a central endpoint for all of an organization's data sharing activities. The EDC will manage access to data based on the consuming organization's attributes and monitor the status of B2B data sharing. Furthermore, it allows for the definition of usage rules, which is crucial to ensure that the data provider's rights are not diminished by the data to be shared. One potential use case would be to prohibit the use of data made available on the basis of the Data Act for the development of competing products and services.

Clearly structured data management to meet the requirements

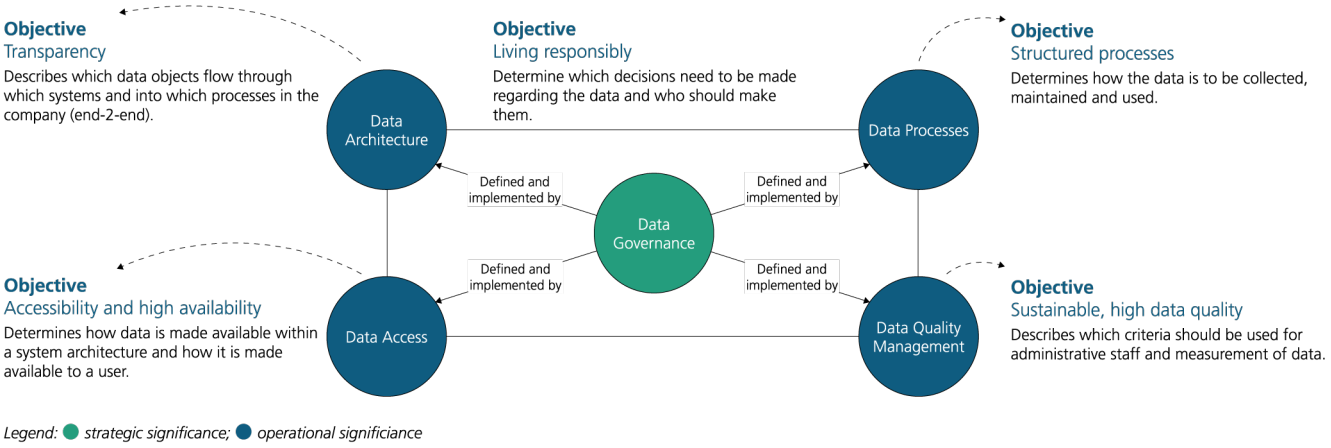

Figure 13. Maturity model of a data governance

In terms of data management, the solutions required are completely fundamental and initially do not differ substantially from the requirements that were already valid ten or more years ago. However, many organizations still do not fulfill these essential requirements, including an implemented data governance structure, a data strategy or even basic rules for data quality. The basis for everything is that organizations must have efficient data management. And as a first step, this means knowing where the organization stands in terms of its own data management. To understand what stage an organization's data management is at, the organization needs to understand the maturity level of previous activities in this context. Maturity models describe the development status of an organization by evaluating its current performance. Data maturity models are therefore a suitable means of determining the current state of data management within an organization.

To obtain an uncomplicated initial evaluation of the maturity level of a data management system, Fraunhofer ISST developed an easy-to-use self-assessment tool. The maturity measurement entails only twelve questions and provides a simple outline of the current state. No registration is required, and the results are provided in a pdf file.

https://datama.isst.fraunhofer.de/intro

References

[1] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32023R2772

[2] https://www.efrag.org/en/projects/esrs-implementation-guidance-documents

[3] https://www.pwc.de/de/mittelstand/esg-strategie-und-reporting-im-mittelstand.html

[4] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[5] European Parliament & Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence and amending; Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. Official Journal of the European Union.

[6] https://www.bundesregierung.de/breg-de/themen/digitalisierung/kuenstliche-intelligenz/ai-act-2285944

[7] https://artificialintelligenceact.eu/high-level-summary/www.fraunhofer.de

[8] https://digital-strategy.ec.europa.eu/en/policies/data-act

[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

[10] hhttps://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained

[11] Richter, H. 2023. Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing. GRUR International 72, 5, 458–470.

[12] https://ec.europa.eu/commission/presscorner/detail/de/qanda_25_615

[13] https://www.horn-company.de/publikationen/aus-der-beratungspraxis/corporate-sustainability-due-diligence-directive-csddd/

[14] https://www.bafa.de/DE/Lieferketten/Multilinguales_Angebot/multilinguales_angebot_node.html#:~:text=The%20Act%20on%20Corporate%20Due,diligence%20in%20their%20supply%20chains

[15] https://www.csr-in-deutschland.de/DE/Wirtschaft-Menschenrechte/Gesetz-ueber-die-unternehmerischen-Sorgfaltspflichten-in-Lieferketten/FAQ/faq.html#doc977f9a9d-bfdd-4d31-9e31-efab307ceee6bodyText14

[16] https://www.bmuv.de/themen/nachhaltigkeit/wirtschaft/lieferketten/europaeische-lieferkettenrichtlinie-csddd

[17] https://www.bmas.de/EN/Europe-and-the-World/International/Supply-Chain-Act/supply-chain-act.html

[18] European Union. (2024). Regulation (EU) 2024/1781. EUR-Lex. Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1781/oj/eng

[19] https://publica.fraunhofer.de/bitstreams/771a840f-dea6-4457-8c51-f52005c881bf/download

[20] Jensen, S. F., Kristensen, J. H., Adamsen, S., Christensen, A., & Waehrens, B. V. (2023). Digital product passports for a circular economy: Data needs for product life cycle decision-making. Sustainable Production and Consumption, 37, 242-255.

[21] Glaessgen, E. & Stargel, D. (2012, April). The Digital Twin Paradigm for Future NASA and U.S. Air Force Vehicles. In 53rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics and Materials Conference; 20th AIAA/ASME/AHS Adaptive Structures Conference 14th AIAA (p. 1818).

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0142

[23] Tanenbaum, A. S. & Van Steen, M. (2003). Verteilte Systeme: Grundlagen und Paradigmen (Vol. 1). Pearson Studium.

[24] Haße, H., van der Valk, H., Möller, F., & Otto, B. (2022). Design Principles for Shared Digital Twins in Distributed Systems. Business & Information Systems Engineering, 64(6), 751-772.

[25] https://mobilithek.info/

[26] https://www.bmv.de/SharedDocs/DE/Artikel/K/eckpunkte-mobilitaets-datengesetz.html

[27] Bundesministerium für Digitales und Verkehr. (2024). Referentenentwurf zur Bereitstellung und Nutzung von Mobilitätsdaten (April 19, 2024).

[28] https://bmdv.bund.de/SharedDocs/EN/Articles/DG/mobilithek.html

[29] https://mobility-dataspace.eu/

[30] https://digital-strategy.ec.europa.eu/en/policies/legislation-open-data

[31] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024

[32] https://www.openaire.eu/open-data-and-the-re-use-of-public-sector-information

[33] https://www.bmi.bund.de/DE/themen/moderne-verwaltung/open-government/open-data/open-data-node.html

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2023.019.01.0043.01.ENG

[35] Watson, H. J. & Wixom, B. H. (2007). The Current State of Business Intelligence. Computer, 40(9), 96-99.

[36] Batini, C. & Scannapieco, M. (2016). Data and Information Quality. Cham, Switzerland: Springer International Publishing, 63.

[37] https://projects.eclipse.org/projects/technology.dataspace-protocol-base

[38] https://www.w3.org/TR/vc-overview/

[39] https://eclipse-edc.github.io/

Imprint

Authors

Sebastian Emons
Daniel Grafen
Inan Gür
Dr. Hendrik Haße
Christoph Hoppe
Marius Hupperz
Nils Jahnke
Ilka Jussen-Lengersdorf
Anzelika Lipovetskaja
Maik Mannsfeld
Alexander Westphal

Contact

Dr. Hendrik Haße
Industrial Manufacturing
Tel. +49 231 97677-423
Send e-mail

Nils Frederic Jahnke
Mobility & Smart Cities
Tel. +49 231 97677-467
Send e-mail

Fraunhofer Institute for Software and System Engineering ISST
Speicherstraße 6
44147 Dortmund, Germany
www.isst.fraunhofer.de

Editor

Image Source

Cover: gorodenkoff – stock.adobe.com