This study explores the evolution of EU Data Regulations from the GDPR, through the DMA, DSA, DGA, Data Act and the upcoming AI Act. It addresses a research gap of a comprehensive evolutionary view of a significant regulatory expansion in the scope of data, the diversification of regulated entities, and the increasing complexity of data management activities. Through a comparative legal analysis, it highlights how the regulations responded to digital challenges, from the often obscure and anticompetitive data management practices of big tech companies to the emergence of new technologies such as IoT, smart contracts and generative AI, and created the expansion of regulatory reach to new entities, including gatekeepers, online intermediaries, data intermediaries, data altruism organizations, manufacturers of connected products, AI system developers and many more, and a broadening scope of data from personal to non-personal and business data. Our analysis critically assesses the alignment of this evolution with the European Data Strategy of creating a single market for data through fostering innovation and competition, and shaping a society empowered by data by safeguarding fundamental rights through ensuring data access, accountability and transparency. This paper contributes to understanding the EU’s evolving approach to data governance, fundamental rights and innovation.

I. Introduction

In the digital age, data governance stands as a pivotal element in the intersection of technology, law, and societal values. The European Union, in particular, has been at the forefront of shaping data governance policies, creating a comprehensive suite of regulations with an emphasis on protecting fundamental rights, ensuring fair and competitive digital markets, and maintaining fair and efficient digital services. The EU’s journey in data governance began with the landmark GDPR setting a precedent for personal data protection. The GDPR’s influence and even the issues with its implementation have been extensively explored in academic literature e.g. in a critique of consent-based models and sphere transgressions by big tech

1 Maitrayee Pathak, (Pathak, Maitrayee) Ph.D, LLM, LLB, is a legal and technology researcher with a combination of an international and interdisciplinary background in the academic field and a registered lawyer under Bar Council of India since 2011. She was awarded a doctorate degree in law (PhD) from the renowned University of Szeged (SZTE), Department of Private International Law, in Hungary. She has a unique view combining civil law (EU) and common law (India), and several research projects and publications in the field of Law and Technology. She is currently practicing as Legal Counsel in FintechX Technologies Zrt. in Budapest (Hungary) focusing on blockchain, international data privacy, GDPR and data governance regulations.

Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act.

companies. However, the GDPR was just the initial step. Subsequent regulations such as the Digital Markets Act (DMA), Digital Services Act (DSA), Data Governance Act (DGA), and the Data Act have been added to the EU’s data governance framework and the AI Act is set to expand it further. Each regulation was designed to regulate different areas of data governance, tackling challenges of the digital economy. Studies have highlighted some specific aspects of these regulations. Common values and approaches have been identified in the “Package Acts” (DMA, DSA, DGA). Potential conflicts were uncovered between the Data Act proposal and other regulations. The AI Act proposal was examined in a search for a so-called “trustworthy AI” highlighting trust as a major factor in data governance of AI technologies.

Despite this growing body of work, there is a noticeable gap in the comprehensive analysis of these regulations as a collective evolution from the GDPR. Existing literature often examines these regulations in isolation or focuses on specific dimensions, such as market power, personal data protection, or the rights of digital service users. There is a need for an integrated analysis that considers how the scope of data governance has expanded and its dimensions are interlinked across these regulations.

This research aims to bridge this gap by offering a comparative analysis of the GDPR, DMA, DSA, DGA, Data Act and the AI Act. By doing so, it aims to illuminate the EU’s strategic approach to data governance, exploring how it has adapted to protect fundamental rights, foster innovation, and ensure fairness in the digital market, aligning with the broader vision of the European Data Strategy and the development of common European data spaces, including common standards and practices to share or jointly process data for the development of new products and services (including artificial intelligence), scientific research or civil society initiatives in a collaborative way.

---

14 Data Governance Act, (27)
1. Definitions of Data Governance

DAMA International defines Data Governance as “the exercise of authority and control (planning, monitoring and enforcement) over the management of data assets”.15 The Data Governance Institute defines it as “a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods”.16 Another working definition is “the organization and implementation of policies, procedures, structure, roles, and responsibilities which outline and enforce rules of engagement, decision rights, and accountabilities for the effective management of information assets.”17

The DGA does not define the term data governance but highlights that the TFEU calls for the establishment of an internal market. It states that “The establishment of common rules and practices in the Member States relating to the development of a framework for data governance should contribute to the achievement of those objectives, while fully respecting fundamental rights.”18 Therefore it shows a dual focus on emphasizing fundamental rights and creating an efficient single market of data.

A common theme between the above definitions is the authority and control, accountability and informed decision-making over the management of data. In accordance with the protection of fundamental rights in the EU legal order, as well as the UN and OECD data governance approaches, said authority and control should reside with the primary right-holders over the data.

This paper defines Data Governance as follows:

*Data Governance is the strategic framework that ensures data is managed with accountability and transparency towards data rights holders, providing them with the authority and control necessary to protect their rights, and with fair, non-discriminatory, interoperable access to data to promote innovation and competition in digital markets, while safeguarding the fundamental and commercial rights of data rights holders.*

This definition fosters an environment of informed and active data rights holder engagement in the management of their data. It is in line with the authority and control aspect of the data governance definitions discussed above. At the same time, it balances the rights and interests of individuals and commercial entities, while emphasizing principles like transparency, accountability, and fair access, which are central to the EU’s data regulatory framework.

2. State of Art: Data Governance, Fundamental Rights, and the EU Data Regulations

Post-GDPR, literature on data governance has identified several aspects beyond personal data protection. The MyData initiative has identified fundamental rights as a frame to understand citizen participation in the datafied economy. The initiative shows similarities to the goals of the Data Governance Act, particularly in regards to data altruism.19

Ruohonen and Mickelsson emphasize the inadequacies of the current consent-based European legal foundations of informational self-determination citing several previous studies. They mention the two extremes of

---

18 Data Governance Act, (1)
Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act.

information: thousands of pages of legal text virtually incomprehensible for the average reader, and the short click-through cookie consent banners that give barely any information about the data management activities. Experiments have also shown the high impact of consent positioning and framing on acceptance, suggesting often un-informed consent. Micheli and others identify four main governance models that emerged in our current platform society. They use a social science-informed conceptualisation of data governance that takes into account the power dynamics of the different actors. This approach brings to the forefront the power relations and economic and social interactions within data governance models emerging in an environment mainly dominated by quasi data monopolies of big tech platforms. The current platform models and these alternative data governance models provide a contrast to the individualistic view of data governance under the GDPR, and open the doors for more participatory and collaborative data management.

Rocher and others investigated AI-enabled de-anonymization methods which also emphasizes the need for a broader view of data governance than personally identifiable information under GDPR.

Sharon and Gellert have reviewed the EU Data Regulations and found that they are inadequate in addressing the risks of sphere transgressions by big tech companies, because they focus on data protection and fair markets, while neglecting socio-economic rights, the publicness of critical sectors, and the protection of societal spheres. They argue that fundamental rights safeguarded through data protection (but to some extent also through the AI Act and the DSA) may be too narrow to encompass the broader socio-economic rights, such as health, education and welfare.

Picht and Richter analyzed the DMA, DSA and DGA which together they call the “Package Acts” that aim to regulate the digital sector, especially the market power of gatekeepers and the use of data. They investigate data transactions, such as data access and use rights, data ranking conditions, and data intermediation services, and identify significant values that the regulations aim to uphold such as FRAND (fair, reasonable and non-discriminatory). They also argue that data intermediaries should be strengthened and developed into Data Intermediary Trustees, who can assist and monitor gatekeepers, facilitate data sharing, and act as data guides for consumers.

Holznagel and Freese analyzed the proposal of the Data Act and pointed out that while there is broad consensus on the goal of the proposal, there is significant criticism of the specifics. They point out potential conflicts with several of the EU Data Regulations. They identified a potential conflict with the GDPR around transfer of personal data to third parties or public authorities, with the DGA around data altruism mechanisms and data intermediaries, with the DMA around interoperability and portability requirements.

Díaz-Rodríguez and others analyzed the European Commission’s AI Act proposal with the goal of creating responsible AI systems called trustworthy AI using a comprehensive approach. They define data governance and privacy as one of the major requirements of a trustworthy AI system, using definitions that are very much in line with our data governance definition above. They define data governance as the ability to trace how data is used, and privacy as an ability to verify that protected information is not accessed during the life cycle phases.

20 Ruohonen and Mickelsson, ‘Reflections on the Data Governance Act’
21 Christine Utz and others, ‘(Un)Informed Consent: Studying GDPR Consent Notices in the Field ACM Reference Format’
24 Sharon and Gellert, Regulating Big Tech Expansionism?
25 Picht and Richter, EU Digital Regulation 2022
26 Holznagel and Freese, EU Data Act
of a trustworthy AI. They even emphasize that the need for such requirements stem from the fundamental rights such as the right to privacy, intimacy, dignity or the right to be forgotten.27 These authors recognize to varying degrees the importance of a data governance framework in the EU Data Regulations for the protection of fundamental rights, trust, and point out some commonalities such as underlying values. They also identify challenges and gaps in the current data governance requirements of the EU Data Regulations, such as the complexity of consent, the power imbalance between data controllers and data subjects, the inadequacy of data protection to address socio-economic rights, and the potential conflicts between different regulations.

However, even though these papers emphasize the need for full control over data and its usage, there is a clear research gap in identifying the trends in the evolution of the data governance obligations under all the EU Data Regulations, and thus understand the underlying regulatory approach in more detail, including how these regulations are intended to protect fundamental and commercial rights and interests in the EU and beyond.

II. Hypothesis Development

The main thesis of this paper is the following:

The data governance regulatory approach in the EU Data Regulations is showing an evolution towards a broader scope of governance which has increased data governance obligations in multiple dimensions, including the types of data rights holders and their data, and the types of regulated entities and their data management activities.

This main thesis can be broken down into several hypotheses that we can investigate individually:

- The scope of data under the data governance obligations of these regulations has increased from the GDPR to the new EU Data regulations,
- There are new natural and legal persons under the data governance obligations of the new EU Data regulations as compared to GDPR.
- The data management activities that the regulations aim to control have also increased in scope.

III. Research Methodology

To investigate the hypotheses, a multi-dimensional comparative study will be conducted on the data governance obligations established by the EU Data Regulations. In order to perform a systematic comparative study, we will first analyze the dimensions used for the comparison so we have consistent definitions when comparing the regulations.

1. Dimensions of Comparison

In order to put into context, the different data governance obligations in the regulations, we will start each analysis with summarizing the stated Regulatory Objectives of each regulation. This comparative dimension explains the primary goals or purposes of the regulation. It defines what the regulation aims to achieve in terms of data governance, such as enhancing data protection, ensuring fair use of data, or promoting data-driven innovation.

Secondly, we will investigate the Regulated Entities. This comparative dimension refers to the types of organizations, companies, or entities that the regulation directly targets and whose activities are subject to regulatory control. This could include individuals, private or public entities as well, who will be involved in the

27 Natalia Díaz-Rodríguez and others, Connecting the Dots in Trustworthy Artificial Intelligence
management of data in some capacity. We will not include the regulatory oversight organizations in this list, unless they have a direct role in the management of data according to the regulation. The indirect role of regulatory reporting, audits we will not consider in this comparative study. However, that may be an interesting research topic for a future study.

Thirdly, we will identify the Data Management Activities. This comparative dimension encompasses the specific actions, processes, or practices of the regulated entities that are regulated or mandated by the legislation in the realm of data management. It includes activities related to the handling, sharing, processing, protection, and even publishing details on the governance of data. The regulatory and compliance reporting, and audit procedure activities included in demonstrating the compliance with the regulations are not included in the list. Only the data management activities themselves.

Fourthly, we will identify the Data Rights Holders. This comparative dimension identifies those parties whose rights over the data the regulation aims to protect. It includes individuals and entities whose data is being governed, such as consumers, businesses, and other users of data-related services. More often than not, these actors are the generators of the data, but they may have acquired the data in other legitimate means as well (e.g. through acquiring intellectual property rights). Data Rights Holders are a broader category than data subjects that the GDPR defines. This broader definition is necessary given the extent of the protections of the EU Data Regulations, as we will examine.

Lastly, the Data Categories: This comparative dimension refers to the types of data that the regulation addresses. It includes various data classifications such as personal data, non-personal data, content data, business data, user data, and optionally others, depending on the regulation's scope. We will use these types of data to determine whether the EU Data Regulations have increased the scope of data under the data governance obligations.

2. Types of Data

The study uses the following data categories:

- Personal Data: This refers to any information relating to an identified or identifiable natural person ('data subject'). Personal data can include names, identification numbers, location data, online identifiers, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

- Content Data: This category includes data that is created, shared, processed, and managed via digital means. It can encompass text, images, videos, and other user-generated content. It may be created by end users or business users as well. It may contain data protected by intellectual property rights (e.g. copyrighted data).

- Business Data: Business data refers to information that is related to the operations, strategies, processes, and transactions of businesses. This could include commercially confidential information such as trade secrets, business plans, data about business activities on digital platforms, and analytics. Some business data may be protected by intellectual property rights.

- User Data: User data is a broader category that can include both personal and non-personal data generated by users of digital services. This may involve usage patterns, preferences, interaction data, and other metrics that are valuable for service optimization, targeted advertising, and personalization. Users may be end users or business users as well.

- Non-Personal Data: Non-personal data refers to any data that is not related to an identified or identifiable natural person. This can include aggregated datasets, anonymized data, and information
that is not linked to individuals. They may be used for market analysis, service improvements, regulatory compliance or research without infringing on individual privacy.

Although there are significant overlaps between some of these categories, due to covering the types of data the regulations are targeting, this categorization will serve its sole purpose of being able to draw a comparison between the regulations. Therefore the comparative study will identify the specific types of data the regulatory protection is targeting, but it will also attempt to categorize them into the above categories.

IV. Results

The table below shows a summary of the results of the comparative study which will be presented in detail later in this section.

<table>
<thead>
<tr>
<th>Regulated Entities</th>
<th>Regulatory Objectives</th>
<th>Data Management Activities</th>
<th>Data Rights Holders</th>
<th>Data Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GDPR</strong></td>
<td>Data controllers</td>
<td>Protection and free movement of personal data</td>
<td>Processing personal data, ensuring data subject rights, data security measures, data breach notifications</td>
<td>Data subjects who are natural persons in the EU</td>
</tr>
<tr>
<td></td>
<td>Data processors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>DMA</strong></td>
<td>Gatekeepers (large online platforms with significant impact on internal market)</td>
<td>Ensuring fair and open digital markets, regulating gatekeepers to prevent unfair practices and promote competition</td>
<td>Consent for data combination; providing access to services and data; advertising and ranking; data sharing with business users, portability for end users; search data sharing; consents for profiling</td>
<td>Users of gatekeeper services, including businesses and end consumers</td>
</tr>
<tr>
<td><strong>DSA</strong></td>
<td>Online intermediary service providers (e.g. online platforms, search engines)</td>
<td>Ensuring a transparent, safe, predictable and trustworthy online environment within the Union</td>
<td>Data Protection, content moderation, use of personal data, data sharing, advertising practices</td>
<td>Recipients of the service (business users, consumers, and other users)</td>
</tr>
<tr>
<td><strong>DGA</strong></td>
<td>Public sector bodies, data intermediation service providers, data altruism organizations, data users</td>
<td>Develop borderless digital internal market and a human-centric, trustworthy and secure data society and economy by creating a harmonised framework for data exchanges and laying down certain basic requirements for data governance</td>
<td>Data sharing of data subject to re-use; data intermediation services; data altruism activities; implementing safeguards for data protection and commercial confidentiality (e.g. anonymization, secure processing environments); publishing access conditions</td>
<td>Data subjects, data holders</td>
</tr>
</tbody>
</table>

Electronic copy available at: https://ssrn.com/abstract=4718891
Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act.

### Data Act

| Data holders; data recipients; manufacturers of connected products, providers of related services; vendors of smart contracts; participants in European data spaces |
| Establish harmonized rules for fair access to and use of data within the EU. Promoting data-driven innovation, protecting trade secrets, and allowing data access in the public interest for emergency response |
| Data sharing, providing portability and interoperability between platforms and services; implementing data protection and confidentiality safeguards; use of smart contracts for data sharing; participation in common European data spaces |
| Individual and business users of connected products and services, of data processing services, and of data holders’ products or services |
| Personal and non-personal data; user data, business data (commercially confidential data), data protected by intellectual property rights (business data, content data) |

### AI Act

| AI system providers and deployers (so-called “users”) |
| Ensuring that AI technologies respect health, safety, fundamental rights, democracy, sustainability, while also promoting innovation. |
| AI training, validation, testing, development and deployment; providing transparency on copyrighted content used; tagging content generated by AI; technical documentation; risk assessments; prevention of illegal content; fundamental rights impact assessments; consents for real-world testing |
| Data subjects, business and individual rights holders, (and indirectly even society of the EU) |
| Personal and non-personal data used in training, testing, deployment and operations, including copyrighted data |

**Table 1: Comparative analysis of the EU Data Regulations**

1. **General Data Protection Regulation (GDPR)**

The GDPR, as a pioneering legislative framework, set a precedent in data governance within the EU. This section evaluates the GDPR as a baseline for subsequent comparisons.

**Regulatory Objectives:** The GDPR’s primary objective is the protection of personal data within the EU, alongside the facilitation of free movement of such data. These dual-purpose addresses both the safeguarding of fundamental rights (especially privacy and data protection) and the promotion of a seamless digital single market. The GDPR emphasizes individual control over personal data, reflecting a rights-based approach to data governance.

**Regulated Entities:** The GDPR identifies two main categories of regulated entities: data controllers and data processors. Data controllers are entities that determine the purposes and means of processing personal data, while data processors are entities that process data on behalf of the controller. This distinction underlines the GDPR’s effort to allocate responsibility and accountability in data processing activities across different stakeholders.

**Data Management Activities:** The GDPR’s governance activities encompass a broad spectrum, including the processing and handling of personal data, ensuring data subject rights (such as access, rectification, and erasure), implementing data security measures, and mandating data breach notifications. These activities reflect the GDPR's comprehensive approach to data management, emphasizing both proactive and reactive measures to protect data integrity and privacy.

**Data Rights Holders:** The primary rights holders under the GDPR are the data subjects, who are natural persons in the EU. The regulation's focus on data subjects underscores its commitment to individual rights, ensuring that personal data protection is centered around the individuals to whom the data belongs.

**Data Categories:** Under the GDPR, the primary category of data governed is personal data of data subjects. This includes any information related to an identified or identifiable natural person. The GDPR’s definition of
personal data is broad, encompassing a wide range of data types and contexts, thereby providing extensive coverage under its protective measures.

**Comparative Observations:** The GDPR, as the baseline of modern EU data governance, establishes a solid framework focused predominantly on the protection of personal data and the rights of individual data subjects. While its scope is primarily centered on personal data, the principles and mechanisms it introduces (such as consent, data subject rights, and accountability of data controllers and processors) have influenced broader regulatory approaches in the EU’s data governance landscape.

### 2. Digital Markets Act (DMA)

The DMA represents a significant evolution in the EU's approach to data governance, particularly in addressing the challenges posed by large online platforms known as gatekeepers.

**Regulatory Objectives:** The DMA's primary objective is to ensure fair and open digital markets within the EU. This involves regulating gatekeepers to prevent unfair practices and promote competition. Unlike the GDPR, which focuses on personal data protection, the DMA aims to address the power imbalance in digital markets, ensuring that gatekeepers do not abuse their dominant position. In terms of data governance, it strives for balancing their dominant position by mandating transparency over their data management and empowerment of their users. It also seeks to create an environment where innovation can thrive, smaller businesses can compete, and consumers have access to a wider range of services.

**Regulated Entities:** The DMA targets 'gatekeepers,' defined as large online platforms with a significant impact on the internal market. These gatekeepers are identified based on criteria such as the number of users, market turnover, and the entrenchment of their position in the market measured in the number of Member States they offer their services in. This focus marks a shift from the GDPR's broad application to all entities processing personal data, to a more targeted approach aimed at entities with substantial market power, since these are the organizations whose power the regulator is aiming to balance.

**Data Management Activities:** The DMA describes a range of data governance activities under the regulatory umbrella that are more diverse and extensive than those under the GDPR. These include practices around consent and data combination, interoperability with and access to services and data, transparency and fairness in advertising and ranking, data sharing with business users, portability for end users, search data sharing, consent requirements around profiling. These activities reflect a more nuanced, practical understanding of the complex digital markets, many years after the implementation of the GDPR. They are extending beyond the traditional scope of data protection to intersect with aspects of market fairness, transparency, and user empowerment.

**Data Rights Holders:** The DMA expands the scope of data rights holders beyond the GDPR’s focus on individual data subjects. It includes users of gatekeeper services, encompassing both businesses and end consumers. This broader range of stakeholders indicates a recognition of the interests of businesses in digital ecosystems as well, particularly European small and medium-sized enterprises (SMEs), and the need to protect and empower all participants in these environments.

**Data Categories:** In contrast to the GDPR's focus on personal data, the DMA governs a wider array of data categories. These include personal data, content data, business data, user data, and non-personal data. This expansion reflects the DMA's attempt to address the complexities of data use in large digital platforms, where various data types are intertwined and have significant implications for data protection, competition and consumer choice.
Comparative Observations: The DMA represents a strategic evolution in the EU's data governance framework, shifting from a singular focus on personal data protection to addressing the broader challenges of digital markets. It reflects many of the lessons of the implementation of the GDPR, as we discussed in the State-of-the-Art chapter, such as the awareness and literacy of users about the terms and conditions and the actual data processing activities performed by organizations. Its targeted approach towards gatekeepers is geared towards a risk-based regulatory strategy to manage the unique challenges presented by large online platforms. This regulation, with its comprehensive range of data management activities and inclusion of various data categories, signifies an advancement in the data governance obligations in the EU. The DMA's focus on the gatekeepers’ possible anti-competitive and opaque data management practices also highlights an extended approach to regulation, one that is not solely about protecting fundamental rights, but also about ensuring fair market practices and fostering a competitive digital economy.

The DMA’s emphasis on market fairness and competition, while still incorporating data protection elements, illustrates an integrative approach to data governance. This approach acknowledges that the management of data on digital platforms has far-reaching implications beyond personal privacy, impacting market dynamics and consumer rights. It shows an evolution in the EU's regulatory vision as described in the European data strategy. Moreover, the DMA’s introduction of specific data governance activities, such as data sharing and interoperability requirements, shows a proactive stance in promoting competitive fairness by mandating data management to be more open and transparent. This is a departure from the GDPR’s rights-based approach and more reactive measures, such as breach notifications and data subject rights enforcement. The DMA’s proactive measures aim to pre-emptively shape the digital markets, ensuring that gatekeepers do not misuse their dominant position to the detriment of other market players.

Therefore, the DMA builds upon the foundations laid by the GDPR, extending the scope of governance to address the challenges of digital markets dominated by big tech companies. The DMA’s targeted approach to gatekeepers, expansive range of regulated data activities, and inclusion of diverse data categories, and businesses as a new data rights holder category are strong steps towards the EU Data Strategy.

3. Digital Services Act (DSA)

The DSA is focusing on the regulation of online intermediary service providers. This section analyzes the DSA and compares it with the GDPR and DMA.

Regulatory Objectives: The DSA is primarily aimed at ensuring a transparent, safe, predictable, and trustworthy online environment within the EU. The DSA expands the EU’s regulatory scope to online services. Its objectives include safeguarding users’ rights online, establishing a liability framework for digital services, and ensuring that these platforms operate transparently and responsibly.

Regulated Entities: The DSA applies to a wide range of online intermediary service providers, including online platforms and search engines. This includes entities both within and outside the EU, provided they offer services to EU users.

Data Management Activities: The DSA governs activities related to data protection, content moderation, personal data usage, data sharing, and advertising practices. It introduces obligations for transparent and accountable content moderation, clear and understandable terms of service, and mechanisms for users to challenge content decisions, and transparency around advertising and profiling practices.

Data Rights Holders: The data rights holders identified by the DSA include recipients of the service, encompassing business users, consumers, and other users. This expands the concept of data stakeholders from
Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act.

the GDPR's data subjects and the DMA’s focus on users of gatekeeper services, to include a broader range of participants in the online ecosystem.

**Data Categories:** Like the DMA, the DSA governs a variety of data categories, including personal data, content data, business data, user data, and non-personal data.

**Comparative Observations:** The DSA, while sharing some similarities with the GDPR and DMA, introduces unique elements to the EU’s data governance framework. While the GDPR is centered on personal data protection and individual rights, and the DMA focuses on market fairness and gatekeeper regulation, the DSA extends the scope to the broader context of online services and their impact on the broader society and thus aims to protect a wider range of fundamental rights as well. For example, through its focus on fair and transparent content moderation practices it aims to protect the freedom of expression and information and the freedom and pluralism of media.

The DSA introduces a differentiation within online service providers, imposing additional obligations on very large platforms and search engines, recognizing their significant societal and market impact. This targeted approach aligns with the EU's strategy of proportionate regulation, tailoring obligations to the scale and nature of the services provided.

The DSA's emphasis on transparency, particularly in advertising and profiling practices, complements the GDPR’s and DMA’s objectives. While the GDPR ensures transparency in personal data processing and the DMA mandates transparency in market operations, the DSA extends this principle to the operational practices of online services. This includes not just how data is processed (including profiling and advertisements), but also how content is moderated and presented to users, therefore signifying an enhanced focus on user empowerment and transparency in data governance of online services.

In summary, the DSA complements the GDPR and DMA by extending the EU’s data governance obligations even more. It addresses the societal and individual implications of online services, emphasizing the need for responsible, transparent, and accountable digital environments and safeguarding not only personal data and market fairness but also the societal and fundamental rights impacted by digital services.

### 4. Data Governance Act (DGA)

The DGA is focusing on creating a framework for data exchange and establishing basic requirements for data governance. This section examines the DGA in relation to the GDPR, DMA, and DSA.

**Regulatory Objectives:** The DGA aims to develop a borderless digital internal market and establish a human-centric, trustworthy, and secure data society and economy. It seeks to create a harmonized framework for data exchanges and lay down fundamental requirements for data governance. Unlike the previous regulations, the DGA specifically concentrates on facilitating data sharing and ensuring data governance standards across various sectors.

**Regulated Entities:** The DGA targets a range of entities, including public sector bodies, data intermediation service providers, data altruism organizations, and data users. This scope is a further shift towards a broader array of participants in the data economy. It encompasses alternative data management and representation models such as data pooling, data cooperatives, to the current individualized and gatekeeper dominated data economies.

**Data Management Activities:** The DGA oversees activities such as data sharing of data subject to reuse, provision of data intermediation services, data altruism activities, and implementing safeguards for data protection and commercial confidentiality. These activities extend beyond the typical data protection and market fairness scope of the GDPR, DMA, and DSA, focusing on the broader aspects of data governance, such
as data sharing even through intermediaries and altruism, supporting the vision of common European data spaces.

**Data Rights Holders:** The DGA recognizes data subjects and data holders as the data rights holders under its protection. Data holders in the DGA’s definition are any natural or legal persons (including businesses and public sector bodies) who are not data subjects, but have a right to grant access to or share personal or non-personal data. This approach builds upon the GDPR's focus on individual data subjects and expands it to include any other entities that hold or manage data subject to reuse.

**Data Categories:** The DGA governs both personal and non-personal data, including commercially confidential data (business data) and data protected by intellectual property rights (business data, content data). This further broadens the scope of data by explicitly including commercial confidentiality and intellectual property rights in the data to be shared while providing safeguards for their protection.

**Comparative Observations:** The DGA is a complementary piece in the EU’s data governance landscape, alongside the GDPR, DMA, and DSA. It uniquely focuses on enabling and regulating data sharing and intermediation across the single market for data.

The DGA extends the concept of data rights holders to include a broader array of entities, compared to previous regulations. This includes public sector bodies, data intermediation service providers, and data altruism organizations. Its regulatory approach emphasizes both personal and non-personal data in the data economy.

In contrast to the DMA's focus on just balancing the market power of digital gatekeepers, the DGA promotes a more collaborative data economy. It encourages models such as data pooling and data cooperatives. This shift is indicative of the EU’s broader strategy to foster innovation and growth in the digital economy through shared data resources, and with its emphasis on data sharing, including through intermediaries and for altruistic purposes, aligns with the EU's vision of common European data spaces, while safeguarding data rights and commercial interests.

5. Data Act

As the newest official regulation that went into force in January 2024, the Data Act focuses on fair access to and use of data. This section analyzes the Data Act in relation to the GDPR, DMA, DSA, and DGA.

**Regulatory Objectives:** The Data Act's primary objective is to establish harmonized rules for fair access to and use of data within the EU. It aims at promoting data-driven innovation, protecting trade secrets, and allowing data access in the public interest for emergency response. The Data Act concentrates on balancing the interests of data holders and users to foster an equitable data economy.

**Regulated Entities:** The Act regulates data holders, data recipients, manufacturers of connected products, providers of related services, vendors of smart contracts, and participants in European data spaces. The approach to data holders is slightly different in the Data Act compared to the DGA, because they may be considered a regulated entity with obligations in the Data Act, rather than data rights holders whose rights the regulation is aiming to protect. This scope is even broader and more varied than its predecessors, especially when considering the vendors of smart contracts and participants in European data spaces.

**Data Management Activities:** The Data Act governs activities related to data sharing, portability, interoperability between platforms and services, and implementing data protection and confidentiality safeguards. It also addresses the use of smart contracts for data sharing and participation in common European data spaces.
Data Rights Holders: The Data Act expands to a wide range of data rights holders, such as individual and business users of connected products and services, of data processing services, and of data holders’ products or services.

Data Categories: The Act governs personal data, non-personal data, user data (especially for connected devices and related services), and while not explicitly stated in the Act, it also governs business and content data (especially under commercially confidentiality or protected by intellectual property rights). It establishes explicit obligations of data access and portability on connected product and services data and on data used by data processing services e.g. cloud service providers.

Comparative Observations: The Data Act, as the newest addition to the EU’s data governance suite, complements and extends the regulatory landscape shaped by the GDPR, DMA, DSA, and DGA. One of the main contributions of the Data Act is that it further refines this framework with its focus on equitable data access and usage. It is opening the data vaults of data holders further, by establishing obligations of data access and portability on connected products and data processing services. It addresses the challenges of data monopolization and seeks to democratize data access, particularly in relation to IoT and connected devices. The Data Act's regulatory scope is broader than its predecessors, encompassing not only data holders and recipients, but it explicitly includes manufacturers of connected products, vendors of smart contracts, and participants in European data spaces.

The Data Act’s approach diverges from the DGA's emphasis on data holders as primarily rights holders, positioning them instead as entities with specific obligations under the Data Act. This is a further evolution in the EU data regulation, where the same participants may be rights holders and obligation bearers as well in the digital data economy.

The Data Act identification of data rights holders aligns with the previous EU data governance regulations in protecting both individual and business users' data. However, it goes further by specifically addressing the rights of users of connected products and services, adapting to the emerging realities of the IoT and smart technology era.

While the Data Act only defines personal and non-personal data in its scope, it is implicitly including business data and commercially confidential data as well, thus it is in line with previous regulations.

Unlike the other regulations, the Data Act specifically targets the emerging issues in the digital economy, such as the rights related to data generated by connected devices and the use of smart contracts for data sharing.

6. Artificial Intelligence Act (AI Act)

The AI Act is another major piece of legislation that will introduce crucial regulations on data governance in the EU. Even though the final text of the AI Act is not available as of the writing of this study, after a long and intensive debate process, finally a political agreement was achieved among the representatives of Member States in December 2023.28

The debate over the EU's AI Act was challenging due to major disagreements on key aspects like facial recognition and the regulation of General-Purpose AI Systems (GPAI), such as OpenAI's GPT models. Contentious issues included the categorization of GPAI systems, balancing innovation with strict regulatory measures, and the use of AI in surveillance, particularly biometric recognition. This was compounded by...

---

differing priorities of member states like France, Germany, and Italy, who were concerned about stifling innovation. GPAI transparency obligations (tagging content generated by AI, design to prevent illegal content generation, transparency of copyrighted content in training) were left as they were in the proposal by the Parliament, with a risk-based approach for high-impact GPAI systems with more stringent obligations. Therefore, this section analyzes the EU Press Release on the political consensus on the AI Act and the final draft published, in relation to the previous regulations.

**Regulatory Objectives:** The AI Act is aimed at ensuring that AI technologies protect health, safety and fundamental rights, democracy, rule of law and environmental sustainability, while promoting innovation. The AI Act uniquely targets the risks and impacts of AI technologies, the safe and transparent development of AI within (and even outside of) the EU.

**Regulated Entities:** The AI Act targets a wide range of entities, including providers and deployers (so-called “users”) of AI systems, including their manufacturers, operators and importers. Special attention is given to providers of high-risk AI systems and general-purpose AI models, particularly those posing systemic risks.

**Data Management Activities:** The Act will govern activities around AI development and deployment, including conducting data quality assessments, data management safeguards during training, validation, testing, providing transparency on copyrighted content used for training, on content generated by AI, prevention of illegal content and fundamental rights impact assessments. It introduces stringent measures for high-risk AI systems, such as record keeping, adversarial testing, technical documentation, complaint management, explaining of AI decisions, participating in AI sandboxes, and informed consent for real-world testing, particularly for high-impact GPAI systems.

**Data Rights Holders:** The AI Act considers the rights and protections of various data rights holders, including natural persons, businesses, like many of the new EU Data Regulations.

**Data Categories:** The Act implicitly governs a wide range of data categories through its regulation of AI systems, covering personal and non-personal data, and specifically including a vast array of content (content data) used in the training of these systems, which even include copyrighted data. This approach indicates an understanding of the broad range of data in AI applications.

**Comparative Observations:** The AI Act's primary objective of ensuring AI technologies respect health, safety, fundamental rights, democracy, and environmental sustainability, while fostering innovation, distinctly positions it in the EU’s regulatory landscape. It introduces new concerns into the regulatory objectives around the functioning of democracy, further emphasizing transparency, and recognizing the possible effects of AI technologies on many aspects of a well-functioning society in the EU. This strategic orientation may signify a shift towards a more technology-specific and impact-oriented regulatory approach from the data-focused perspectives of the earlier regulations.

The AI Act extends its reach to a wide array of regulated entities involved in AI, including providers, and deployers of AI technology, including manufacturers, operators, importers, which is following a similar trend than the other EU Data Regulations. The Act’s governance of AI-specific activities, including risk assessments, transparency requirements regarding training data, tagging of generated data, and fundamental rights impact

---


31 Yakimova and Ojamo, Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI

32 Bertuzzi, Caroli and Nechita (eds), Final Draft (2024): AI Act

Electronic copy available at: https://ssrn.com/abstract=4718891
assessments, reflects a deepened focus on AI’s unique challenges. This is a significant expansion from earlier regulations, which primarily concentrated on data protection, market operations, and service provisions. The AI Act encompasses an extensive set of data rights holders. This approach is in line with expectations of AI’s pervasiveness, thus extending protections to include not only individual rights holders of personal or non-personal data, but also businesses and their copyrighted data, and even EU society at large through its risk-based approach. By implicitly governing a vast array of data categories, including both personal and non-personal data involved in AI training and operations, the AI Act aims to address the unique challenge AI technology brings in data governance, from its use in training sophisticated models to its generation involving human cooperation, all the way to completely automated means.

In conclusion, the AI Act complements the foundations laid by previous regulations, adapting to the rapid advancements of AI technologies. This Act solidifies the EU’s commitment to ensuring a responsible, but competitive digital future, driven by AI innovation while protecting fundamental rights.

V. Discussion

Based on the comparative analysis of the EU Data Regulations – GDPR, DMA, DSA, DGA, Data Act and AI Act – we can evaluate the three hypotheses:

The scope of data under the data governance obligations of these regulations has increased from the GDPR to the new EU Data regulations.

- The scope of data under governance has indeed broadened from the GDPR to subsequent regulations. The GDPR primarily focuses on personal data protection. In contrast, the DMA, DSA, DGA, Data Act and AI Act encompass a wider array of data categories, including non-personal data, business data, commercially confidential data, data protected by intellectual property rights, and user and content data. This expansion reflects a more comprehensive approach to data governance, addressing multiple types of data in the digital economy.

There are new natural and legal persons under the data governance obligations of the new EU Data Regulations as compared to GDPR.

- The subsequent EU Data regulations have extended data governance obligations to a wider range of natural and legal persons compared to the GDPR. The GDPR’s main focus was on data controllers and processors, primarily protecting individual data subjects. However, regulations like the DMA target gatekeepers, the DSA includes online intermediaries like online platforms and search engines, the DGA brings in public sector bodies, data intermediation service providers, and data altruism organizations, the Data Act expands this to include manufacturers of connected products, data processing services (e.g. cloud providers) and vendors of smart contracts, and the AI Act includes the developers and deployers of AI systems. This range of regulated entities covers more entities with data governance obligations in the data ecosystem.

The data management activities that the regulations aim to control have also increased in scope.

- The data management activities aimed to be controlled by these regulations have also seen a substantial increase in scope. While the GDPR focused on processing and handling of personal data, later regulations introduced more diverse activities. For example, the DMA addresses data sharing with business users and interoperability requirements, the DSA emphasizes content moderation and further transparency in online
services (consents, advertising), the DGA focuses on data sharing for re-use and data altruism, the Data Act covers data portability and access in the context of connected devices and cloud services, as well as the development of smart contracts for data sharing, while the AI Act addresses AI-specific activities such as transparency of training and tagging of AI-generated content.

VI. Conclusion

The evolution of EU Data Regulations from the GDPR, through the DMA, DSA, DGA, Data Act to the AI Act demonstrates a significant expansion in the scope of regulated data, the range of regulated entities, and the breadth of data management activities. This progression aligns with the European Data Strategy to create a single market for data and to make the EU a role model for a society empowered by data. It also aligns with the vision of common European data spaces, including common standards and practices to share or jointly process data for the development of new products and services (including artificial intelligence), scientific research or civil society initiatives in a collaborative way. Therefore, while it established many additional obligations on several entities involved in data governance, the framework may adapt to the complexities and demands of the digital age, aiming to protect fundamental rights, promote innovation, and ensure fair and competitive digital markets and a digital society.

VII. Limitations

While this comparative study provides a comprehensive analysis of the evolution of EU Data Regulations from the GDPR to the AI Act, there are inherent limitations and areas for further research. The study primarily relies on existing legal texts, but in the case of the AI Act only on political agreement, press releases and draft regulation. The final text of the AI Act was not available at the time of this study, which may have limited the depth of analysis regarding its specific provisions and implications. Future research could revisit the AI Act upon the release of its full text to provide a more detailed analysis. The field of data governance is rapidly evolving, with continuous technological advancements. Many of the regulations described in this study have only partly been adopted in practice with some regulated entities having compliance deadlines well into the future at the writing of this paper. Further research may be needed when the regulations are implemented in practice by these entities as well, and their effectiveness studied in addressing data governance challenges. The practical impact of these regulations on businesses, consumers, and the broader digital ecosystem remains an area for empirical research. Future studies could explore the enforcement challenges, the compliance burden on entities, and the actual effectiveness of these regulations in protecting fundamental rights and promoting innovation and fair digital markets.

This study primarily approaches the topic of data governance from a legal and regulatory perspective. Interdisciplinary research possibly involving computer science and organizational development may uncover insights on the effectiveness of the regulatory bodies in achieving their wide data governance oversight mandates.

Finally, apart from focusing on transparency and accountability towards the data rights holders, data governance may be viewed from another perspective: that of the national and international bodies responsible for ensuring compliance with the regulations. Any regulation may be only as effective as its enforcement. Thus, analyzing the EU Data Regulations from this viewpoint may also be an important topic for future studies, especially regarding the compliance transparency obligations, and their possible effects on the protection of fundamental and commercial rights in the EU.