NOERR

Everything, everywhere all at once —
New approaches to data regulation in the EU

January 2025

New approaches to data regulation in the EU

Nowadays, data serves as the decisive foundation for innovation, economic growth and technological development. Much like oil in industrialisation, data drives all areas of the modern economy — from artificial intelligence and personalised services to advertising and smart cities. Companies and government institutions leverage data to make better decisions, optimise processes and develop new products. Looking ahead, the value of data is expected to increase exponentially with growing networking and digitalisation.

The EU too has recognised this development and is placing the previously untapped potential of the European data union at the top of its political agenda. Its aim is to create a "simplified, clear and coherent legal framework" that allows companies and government institutions to exchange and use data "seamlessly and on a large scale".[1] The EU is pursuing a holistic approach: not only will the handling of data be redefined, but data-driven markets will also be made fair and contestable, with the market power of large digital corporations being limited. At the same time, the fundamental rights and freedoms of citizens and core European values will be safe-guarded.[2]

This shows that the EU is pursuing what might initially seem like a paradoxical goal: removing existing barriers to data exchange through additional regulation while fostering a thriving European single market for data. However, as can be seen from the report published in September 2024 by former ECB President and former Italian Prime Minister Mario Draghi on the future of the EU's competitiveness, this approach has a clear and logi-cal rationale. To date, the single market has suffered not least from the fact that companies have high compliance costs due to varying national laws and the fragmented enforcement of EU regulations.[3]

The EU is therefore faced with the challenge of mastering the regulatory balancing act of fostering cross-industry data usage, innovation and competition, while at the same time upholding European values. A pivotal role in this effort will be played by Henna Virkkunen, the newly appointed Executive Vice-President of the European Commission for Technological Sovereignty, Security, and Democracy. Among other tasks, she has been requested by European Commission President Ursula von der Leyen in a "mission letter" to present a strategy for a European Data Union.[4]

Amid the interplay of all these factors, European data law is gradually taking shape step by step.

I. What goals is the EU pursuing with its data regulation?

The EU aims to establish itself as one of the most attractive, secure and dynamic data economies in the world. The Commission is aware of the complexity of the digital space, where numerous interests, risks and opportunities related to data usage must be balanced. Five key objectives are intended to help establish a secure, fair and future-proof digital space in the EU:

— **Creation of a single European market for data:**

  The EU aims to promote the free and secure exchange of data within Europe, thereby establishing a single European market for data.

1 See European Commission, Communication of 19 February 2020, COM(2020) 66 final, esp. p. 1 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52020DC0066, retrieved on 18 December 2024.

2 See European Commission, Communication of 19 February 2020, COM(2020) 66 final, esp. pp. 9 and 27 https://eur-lex.europa.eu/legal-content/DE/ TXT/?uri=CELEX:3A52020DC0066, retrieved on 18 December 2024.

3 See European Commission, The future of European competitiveness Part A, p. 30, https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en, retrieved on 18 December 2024.

4 See European Commission, mission letter to Henna Virkkunen dated 17 September 2024, https://commission.europa.eu/document/3b537594-9264-4249-a912-5b102b7b49a3_en, retrieved on 18 December 2024.

As a vital resource for innovation and economic growth, data should be made accessible and shareable across sectors and borders by citizens, companies, governments, and research organizations.

— **Opening up new data-driven markets:**

Data regulation is not only aimed at creating markets for the exchange of data itself. Instead, it seeks to enable the emergence of new *data-driven* markets whose unique capabilities are only made possible through the availability of data. In particular, these markets may include those where existing products or services are improved through the analysis and use of data, or where in fact entirely new products and services are offered.

— **Promote innovation and competition:**

In this context, the aim is also to create a dynamic digital environment where new ideas and technologies can flourish while ensuring fair and open competition. Both existing and newly emerging, data-driven markets should no longer be perpetually dominated by a few digital corporations, but should remain fair and contestable.

— **Strengthen data sovereignty:**

In addition to these primarily economic considerations, the EU also seeks to ensure the responsible handling of data in accordance with European values, including data protection, data security and transparency.

— **Guarantee the trustworthiness of technologies:**

This includes promoting secure, transparent and reliable digital systems that chiefly ensure the protection of data, user privacy and the integrity of digital communication.

II. New approaches to data regulation

The legal anchoring of these key objectives is crucial for establishing a coherent and sustainable European data policy. The EU has demonstrated a clear willingness to act. It has already created a comprehensive legal framework for the protection of personal data through the General Data Protection Regulation (GDPR)[5]. However, given the rapid developments in the digital sector, the EU has also recognised that further regulatory adjustments are necessary to keep pace with the increasing complexity of the "data universe" and to remain competitive on a global scale, especially against the USA and China. It seeks to address this challenge through new approaches to data regulation. While previous data regulation primarily focussed on data protection and security, the EU is now moving in the opposite direction with its recent legislation. Many of these legislative measures govern the commercial usability of data. Notable examples include the *Data Act*, adopted as part of the European data strategy,[6] and the *Data Governance Act (DGA)*[7], both aimed at promoting data availability in Europe. Additionally, the *Digital Markets Act (DMA)* and the *AI Act*[8], while not primarily aimed at data regulation, are groundbreaking legislation that significantly impact Europe's economy in the digital space.

1. Data Act

The Data Act aims to improve access to and the use of data, particularly data generated by the use of networked products. Its objective is to remove the legal, economic and technical barriers that are responsible for the underutilisation of data so far, thereby encouraging greater use of data within the EU. The Data Act supports the creation of a single European market for data and facilitates the emergence of new data-driven markets. Specifically, the Data Act establishes new data access rights and governs legally permissible forms of data usage in the B2B and B2C sectors, as well as between private individuals.

At its core is the principle of user data sovereignty, granting users cross-sectoral rights to access data generated by their IoT products and associated services. At the same time, users, as data owners in the B2B relation-

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

6 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828.

7 Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724.

8 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 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.

ship, may request that providers of IoT products or product-related digital services (connected services) transfer this data to third parties on fair, reasonable and non-discriminatory terms. This is intended to enable third parties to develop additional services and/or products based on this data. This right of access to data is subject to limitations, including general competition law rules on unauthorised information sharing and regulations protecting trade secrets. In addition, large digital corporations designated as gatekeepers under the DMA are largely excluded from accessing data under the Data Act.

The concept of data sovereignty is reinforced by a consent requirement: in the future, data owners will only be able to use and process data generated by IoT products with the user's consent. This applies in particular to manufacturers of networked products, providers of connected services and data processing services (e.g. cloud computing services). In addition, the Data Act contains provisions on product design obligations, abuse controls in general terms and conditions for data usage contracts and the interoperability of data spaces and data services.

Failure to comply with these obligations can result in severe penalties. Depending on the type, severity, scope and duration of the infringement, fines of up to €20 million or up to 4% of worldwide turnover may be imposed. Previous offences and financial gains resulting from the infringement may also be considered when determining penalties.

The Data Act came into force on 11 January 2024. However, most provisions will only apply starting from 12 September 2025,[9] giving companies affected time to adjust their systems accordingly.

2. Data Governance Act

The DGA, on the other hand, establishes a legal framework for the shared use of data by ensuring neutral access to data, promoting interoperability and helping to avoid lock-in effects. The DGA is aimed in particular at public bodies. For example, it provides a framework for the (more secure) sharing and reuse of protected data held by public bodies, including a ban on exclusive agreements for such data and addi-tional obligations regarding the design of data licensing agreements between public bodies and private parties. In addition, the DGA governs the use and transfer of data by data intermediary services and altruistic organisations, which currently play a limited role in the data economy. Infringements of the DGA may also result in penalties. However, their nature is determined by individual EU Member States. The national authority responsible for enforcing the DGA is empowered, for example, to impose fines or suspend the provision of the data intermediation service.

3. Digital Markets Act

The DMA[10] aims to curb the market power of large digital corporations and ensure fair and contestable markets. Often referred to as a "quasi competition-law regulation"[11], the DMA essentially builds on the EU's experience over recent years and decades in enforcing competition law against digital companies, particularly those leveraging data-driven business models.

At the heart of the DMA are extensive behavioural obligations that apply to companies that have been designated as gatekeepers by the European Commission. Designation as a gatekeeper depends on the fulfilment of certain qualitative criteria by the core platform services operated by these companies. These criteria relate to the influence and importance of the services in digital markets within the EU and their stability. If certain threshold values are exceeded (with regard to turnover, market capitalisation and the number of commercial users and end users), there is a strong presumption in favour of gatekeeper status. The companies named so far are Alphabet, Amazon, Apple, Booking, ByteDance, Meta and Microsoft.

Once designated as a gatekeeper, companies must comply with a detailed catalogue of obligations, which may be expanded by the European Commission in the future. The catalogue also includes several data-related obligations and prohibitions. For example, it prohibits merging data from different services without the consent of end users, using data to compete with business users and also imposes various data access requirements in favour of users of core platform services. Overall, the EU's aim

9 vgl. Art. 50 S. 2 Data Act.

10 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amend-ing Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

11 See European Commission, press release of 15 December 2020, https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2347, retrieved on 18 December 2024.

with the DMA, particularly in relation to data, is to limit the competitive advantage of large digital companies in data-driven markets and to open these markets to other companies, thereby making the markets more contestable.

Infringements of the DMA can also be penalised with severe fines of up to 10% of annual worldwide turnover. In cases of systematic non-compliance, the DMA even allows for the possibility of imposing structural remedies on gatekeepers. In addition, the DMA aims to enable affected users to enforce behavioural obligations in court through private enforcement (e.g. by suing for access to data).

4. AI Act

The AI Act likewise does not primarily regulate data processing. However, the use of AI presents potential systemic risks to fundamental freedoms and the protection of personal data, which the EU aims to address through this regulation.

Accordingly, the AI Act functions as a preventive, cross-sectoral prohibition law by banning the use of AI in certain application scenarios outright or making its use conditional on meeting specific technical, organisational, and legal requirements. For example, certain AI systems that process sensitive personal data are categorically prohibited. This includes social scoring systems, profiling in law enforcement and database AI systems for facial recognition.

When using other AI systems, however, providers and operators must comply with numerous obligations based on the type of AI system. For example, providers must inform natural persons when they are interacting with an AI system. Moreover, operators of an AI system that generates or manipulates image, sound or video content (deep fakes) must disclose that the content has been artificially generated or manipulated.

Infringements of the ban on certain AI practices can result in fines of up to €35 million or up to 7% of annual worldwide turnover. In the case of general-purpose AI models, however, fines of up to €15 million or 3% of annual worldwide turnover may be imposed.

III. What does this mean for companies?

The new European regulations on data and AI present companies with complex tasks. They face the challenge of not only adapting their business models to technological developments but also navigating an increasingly complex and dense network of regulatory requirements, thereby ensuring compliance with extensive obligations. The goal is to understand the impact of the new regulations on one's own company and to efficiently adapt existing compliance and governance structures, as necessary, to the EU's new data-centric frameworks — across interfaces and legal domains.

This increases the organisational obligations and liability risks for management. The new regulations introduce a large number of new and complex obligations, some of which overlap with other laws and, in certain cases, may even conflict. The density of data regulation is particularly high in regulated industries such as banking and insurance, healthcare and telecommunications.

If companies violate the new regulations, they face the risk of increasingly severe fines and significant reputational damage. Moreover, experience from data protection law and competition law shows that private enforcement, i.e. mass actions by customers, consumer protection authorities or competitors is gaining increasing practical importance in the EU.

In addition to compliance requirements and their impact on products and commercial projects, it is also essential to consider a strategic element, i.e. what is referred to as "holistic data strategy". On the one hand, this in-volves determining how a company can utilise its data as profitably as possible in line with its strategic business objectives. On the other hand, it raises the question of whether the new EU regulations may provide opportunities for obtaining and using data from other companies. The new

statutory requirements for a company’s compliance and governance structures will largely depend on the specifics of its data strategy.

There is no time to lose. The obligations will begin to take effect in stages starting in 2025. Given the complexity of these legislative changes and the potential costs involved in their implementation, it is crucial to evaluate existing compliance structures early. This will ensure timely adaptation to the new legal requirements and allow for necessary adjustments to products, services and business processes. This process should not be viewed as a burden but rather as an opportunity. A well-crafted data strategy not only safeguards against liability and reputational damage but also serves as a foundation for future business success. Our lawyers are mindful of both aspects and specialise in guiding companies safely through European data regulations.

Authors

Sarah Blazek
Lawyer, Partner
Brienner Straße 28, 80333 München
sarah.blazek@noerr.com
T +49 89 28628121

Pascal Schumacher
Lawyer, Partner
Charlottenstraße 57, 10117 Berlin
pascal.schumacher@noerr.com
T +49 30 20942030