LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

EU Act Establishes Data Sharing Rules, But Hurdles Remain

By **Aadam Sattar and Andrea Otaola** (October 23, 2025, 3:08 PM BST)


Aadam Sattar


Andrea Otaola

Most of the European Union Data Act's provisions took effect from Sept. 12, 2025, although the legislation entered into force on Jan. 11, 2024.[1]

For any organization that designs, manufactures or uses connected products, provides related services or utilizes or provides cloud platform services within the EU, the act is a strategic game-changer.

It transforms static data owners into data holders, giving users and others access to data that was, so far, unknown or unavailable to them and hence unexploited. This shift brought about by the act tests business models and affects product design and governance, requiring board-level attention.

This article examines the act's main obligations, then provides key practical considerations for organizations preparing for compliance. It also demonstrates how stimulating the sharing of connected product data is not only an EU priority, but is also critical for the U.K.'s economic objectives, meaning that organizations will need to navigate cross-border compliance requirements.

Backdrop to EU Data Act

While Europe has championed the protection of personal data through the General Data Protection Regulation, when it comes to nonpersonal data, this regulation is different: The act seeks to liberalize rather than restrict data sharing.[2]

This landmark, cross-sectoral regulation deals primarily with Internet of Things-generated data by establishing harmonized rules on who can access and use data generated within the European single market. Its purpose is to unlock connected product data to stimulate competition and growth across the EU.[3]

EU Data Act Rollout

All obligations kicked in on Sept. 12, except for the following:

- Obligations on design and manufacturing of connected products and related services for accessibility of data, with statutory data sharing obligations applying from Sept. 12, 2026; and

- Provisions concerning unfair contractual terms apply immediately to contracts concluded from Sept. 12, 2025, and will apply from Sept. 12, 2027, to contracts concluded on or before Sept. 12, 2025, that have an indefinite duration or are due to expire in at least 10 years from Jan. 11, 2024.

Unlocking Industrial Data Potential

A summary of the key provisions of the act is set out here, as well as, importantly, how the act interplays with European competition law.

Data Sharing for Internet of Things

Users — consumers and businesses — of connected products and services, from smart home devices to industrial equipment, must be able to access the data generated by these products.

If direct access is impossible, data holders must provide the data promptly, securely and in a machine-readable format. This is to stimulate competition in after-market services, e.g., maintenance.

Fairness in Data Sharing

Mandatory data sharing terms must be fair, reasonable and nondiscriminatory. This is to prevent data-driven market concentration and ensure a level playing field.

Data holders can request reasonable compensation from data recipients, which can cover the costs of making the data available. However, charges to small and midsize enterprises and nonprofits are capped at the direct costs incurred, aiming to lower barriers to entry across the digital economy.

These safeguards are intended to complement EU competition law by promoting data accessibility without distorting market dynamics.

Unfair Contractual Terms

To support SMEs, the act introduces a so-called unfairness test for nonnegotiable contractual clauses on data access. It lists terms that are always considered unfair or presumptively unfair, and shifts the burden of proof for fairness onto the party that imposed the term.

Business-to-Government Sharing

In certain situations, such as public emergencies or for public interest tasks, public bodies can request access to data held by private companies, subject to proportionality and trade secrets safeguards.

Unlocking the Cloud Market

The act sets new rules to make switching between cloud service providers free, fast and seamless, banning switching charges entirely after a three-year transitional period.

Foreign Government Access

Any transfer of nonpersonal data to a third country requires companies to assess whether such requests

are valid under applicable EU and member state law. This is another consideration for global organizations in an already prescriptive international data transfer ecosystem.

Promoting Interoperability

The act lays down essential requirements for participants in common European data spaces and to ensure the interoperability of data processing services.

Enforcement

Member states are responsible for enforcement in their respective jurisdictions by setting the level of national administrative fines.

While fine levels must be "effective, proportionate, and dissuasive" according to Article 40 of the EU Data Act, and reflect the recommendations of the European Data Innovation Board, they could vary significantly between countries for identical offenses,[4] potentially reaching the level of fines under GDPR, up to €20 million ($23.2 million) or 4% of global annual turnover.

Complementing Competition Law

The act constitutes an important complement to EU competition law for fostering innovation and a competitive data market in Europe. Its mandatory sharing requirements, intended to prevent data-driven foreclosure, align with the principles of fair, reasonable and nondiscriminatory access under Article 102 of the Treaty on the Functioning of the EU.

However, the act also places limits on with whom and how data is shared, e.g., to protect trade secrets, cybersecurity or consumer privacy.

If these are applied selectively or strategically, dominant firms could use them to deny access to rivals or impose disproportionate technical and contractual hurdles, raising concerns of discriminatory treatment or exclusionary conduct.

Conversely, overly broad sharing obligations could also risk facilitating collusion under Article 101 of the TFEU if competitors use access to coordinate commercially sensitive information. Therefore, applying the act's obligations in a proportionate and transparent way is essential to avoid antitrust risks and to safeguard the pro-competition objectives of the act.

Practical Challenges

Translating Principles Into Practice

Some of the act's requirements, such as enabling access by design, are technically complex to implement. The lack of binding standards or best practices at this stage leaves organizations to their own devices in interpreting the act.

The job of in-house legal teams is challenging, as operationalization of the act cannot be approached using the GDPR as a reference point. Unlike the GDPR, which centers on protecting individual privacy, the act is about unlocking economic value and ensuring fairness in business-to-business, business-to-consumer and business-to-government data sharing. Data is seen by policymakers as a shared asset.

Lack of Clarity

The act, while comprehensive, is often vague and open-ended, especially in relation to scope and definitions. These practical challenges led the European Commission to publish a set of FAQs, last updated in September,[5] though these still leave many questions unanswered. This requires businesses to take a stance, which is not easy, considering the magnitude of the paradigm shift the act demands.

The commission is also developing nonbinding model contractual terms for data sharing agreements, and standard contractual clauses for cloud contracts to help organizations draft fair and balanced data sharing contracts, including terms on reasonable compensation and trade secret protection.

The commission's expert group on B2B data sharing and cloud computing contracts published its final report, dated April 2, with templates for various data sharing scenarios. This is expected to be formally recommended to the commission by autumn 2025.

While nonbinding, these templates can prove as a useful benchmark. Whether they will be widely endorsed remains to be seen. As many stakeholders still face uncertainty, further guidance will likely be needed.

Overlapping Regulatory Regimes

Compliance with the act often overlaps with product safety, cybersecurity and industry-specific regulation.[6] This is relevant for manufacturers of connected industrial products, where requirements relating to access by design may clash with existing product regulatory obligations.

As the threshold for what constitutes personal data under the GDPR is relatively low, the act's intersection with EU privacy law should not be forgotten. The challenges raised by the act are not unique on that front, but overlapping requirements always lead to obstacles for global businesses. Taking a reasonable approach that still mitigates regulatory risk often means walking a tightrope.

M&A Due Diligence

In mergers and acquisitions, due diligence on a target's preparedness for compliance with the act is increasingly common, e.g., evidence of data access policies, governance and contractual arrangements.

The absence of a clear road map for compliance risks has heightened buyer scrutiny, leading to negotiations for valuation discounts and delayed closings.

Complex Enforcement Ecosystem

Compliance with the act will be monitored by competent authorities designated by each member state, with a data coordinator acting as a single point of contact in countries with multiple authorities. As designations face delays, member states' ability to enforce the act will be delayed.

The European Data Innovation Board is tasked to help ensure consistent application of the act and cooperation across the EU, although it remains to be seen whether a consistent approach will be developed.

U.K. Landscape

For global data-driven organizations, the act creates yet another regime for data management beyond the GDPR. It overlaps and could conflict with some other approaches taken regionally, such as the upcoming U.K. regime highlighted here.

In the U.K., rules on the sharing of data and particularly nonpersonal and industrial data remain in development. While processing of personal data is governed primarily by the U.K. GDPR and Data Protection Act 2018, each amended by the Data (Use and Access) Act 2025, the legal framework for nonpersonal data is less defined and, for now, relies on a patchwork of intellectual property and competition rules and contract law principles.

Nonetheless, rooted in the success of the U.K.'s open banking scheme, which allows for financial data to be shared between banks and third-party service providers, the Data (Use and Access) Act has established powers for the U.K. government to create a framework for so-called smart data schemes — part of the U.K. government's industrial strategy, published in June, to establish the U.K. as a leader in data-based innovation.

These schemes are designed to enable consumers and organizations to share data securely with authorized third parties to foster innovation and competition in various industries.

Further regulations are necessary to formalize these schemes, and the U.K. government recently ran a public call for evidence until Sept. 15 to obtain stakeholders' feedback on how to set up smart data schemes and address key questions, such as, what key design features a smart data scheme would need to support intended use cases.

Practical Takeaways

A proactive global approach to compliance is recommended and below are some practical steps for compliance readiness:

- Data mapping: Organizations should identify and classify the data generated by their products and services to determine what falls under the scope of the act, including territoriality.

- Review and redesign: Assessment of the products and services against the access by design principle is needed before planning any technical changes to facilitate data portability.

- Contract update: Organizations should review all data-related contracts for unfair terms and ensure any data shared under the act is carefully scoped and the appropriate licensing terms or contractual restrictions are in place. The forthcoming model clauses from the commission should be used for benchmarking.

- Governance and procedures: Processes for managing and responding to data access and portability requests from users and third parties should be developed to ensure requests are actioned in a timely manner.

- Trade secret safeguard: Organizations should implement robust technical and contractual measures to protect their trade secrets before entering into data sharing agreements.

- Transparency: It is key to prepare clear and comprehensive information for users about the data generated by the relevant products, how it can be accessed, and users' rights under the act — and for cloud services, any switching charges.

- Training: Organizations must educate, at a minimum, their legal, compliance, IT and product development teams on the requirements of the act to ensure awareness and readiness.

To conclude, the act is intended to help the EU economy capitalize on a data-driven world. It represents a strategic opportunity for users to gain access to data, tests existing business models, and will have knock-on effects for manufacturers of connected devices and cloud services businesses in the coming months and years by redefining data value chains.

Aadam Sattar and Andrea Otaola are associates at King & Spalding LLP.

[1] https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.

[2] This is sometimes referred to as 'D-regulation' in some EU circles to (1) illustrate the 'de-regulation' of data introduced by the Act, and (2) as an abbreviation of digital regulation.

[3] IoT refers to any product that has software, sensors or other connectivity technologies embedded in it capable of collecting and exchanging with other products or systems.

[4] By way of example, the initial draft bill of the German implementing legislation (Data Act-Durchführungsgesetz-Entwurf – draft DA-DG) sets fines for certain violations at the higher of €5 million or 4% of global annual turnover.

[5] https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act.

[6] In relation to cybersecurity, the interactions and intersections between the Act and, amongst others, the Cybersecurity Resilience Act, i.e., a horizontal minimum cybersecurity requirements regulation, for products with a digital element, that follows a staggered implementation timeline through to December 2027, must be closely monitored.