CLIENT ALERT | 15 September 2025

EU Data Act – What Businesses Need to Know

The Act presents a significant overhaul of European data law, affecting most companies that handle digital products and connected services, and data processing services, in the EU.

Key Points:

- The new legislation will reshape how businesses manage data, presenting both compliance challenges and potentially significant new opportunities for companies across the consumer and industrial data markets.
- Users are granted extensive rights to access, control, and share the data generated by their use of connected products and related services. Businesses must enable this by design and through contract, and can no longer treat product or service data as their exclusive asset.
- Providers of cloud and other data processing services are subject to new service switching requirements and mandatory customer contract terms.
- The EU Data Act may trigger significant litigation, including class actions and regulatory investigations, particularly around the new user rights to data.

The EU Data Act, which took effect on September 12, 2025, is a sweeping new law that will affect any company offering connected products, related digital services, or cloud and other data processing services in the European Union (EU), even if they are based outside the EU. Until now, many companies seem to have underestimated the impact of the upcoming data regime. In particular, it gives users of digital products wide-ranging new rights regarding their data, be it personal or non-personal data, including far-reaching access rights. This type of information was previously largely unregulated. Now, providers of connected products and services, as well as other data holders, will need to amend existing contracts to grant device and service users extensive rights.

The EU Data Act also brings new information obligations and requires companies to give users access to data generated by their products and to share data with third parties on fair terms. Providers of cloud and other data processing services are subject to new service switching obligations, including mandatory terms in their customer contracts. Non-compliance can result in high fines, civil lawsuits, and regulatory investigations — similar to what many companies experience under the EU's privacy law. The EU's General Data Protection Regulation (GDPR), which also applies to many US companies, pursues a similar approach and is already known for its high fines and strict requirements.

Key Dates

- **Effective date:** September 12, 2025 for key obligations
- **Product design requirements:** Apply to connected products and related services offered in the EU after September 12, 2026
- **Cloud and data processing services switching rules:** Apply to new contracts from September 2025 and to some existing long-term contracts by 2027

Key Definitions and Scope

The following key definitions set a very broad and unspecific scope for applicable devices and services.

- **Connected products:** Any physical product that collects or transmits user or device data, such as smartphones, tablets, computers, smart vehicles, industrial equipment, home appliances, medical devices, and wearables.
- **Digital services:** Software, apps, or online platforms that interact with connected products or process data from those products or their users.
- **Data processing services:** Regulators and courts may take the view that the definition includes the three primary categories of computing services: Infrastructure-as-a-Service (IaaS), which involves infrastructure resources such as storage or rented servers; Platform-as-a-Service (PaaS), which provides infrastructure and core software that allows customers to build, deploy, and manage their applications; and Software-as-a-Service (SaaS), which refers to software applications that are fully provisioned and hosted by the service provider.

How Relevant Is the EU Data Act?

The EU Data Act is the most significant overhaul of European data law since the GDPR, with its impact being more disruptive than the EU AI Act. The EU Data Act will fundamentally reshape how businesses handle data from connected products and digital services, presenting potentially significant new opportunities for businesses across the consumer and industrial data markets. Unlike previous laws, it covers both personal data (about individuals) and non-personal data (such as technical or usage data), and it will impact nearly every business model involving digital products or services in the EU.

What Will Change?

- **Impactful new access rights to data:** Under Article 4 and Article 5 of the EU Data Act, users (including both consumers and business customers) are granted extensive rights to access, control, and share the data generated by their use of connected products and related services. Users can therefore demand access at any time (including requesting real-time data access if technically feasible), decide who else can access it (such as repair shops, aftermarket service providers, or competitors), and even restrict how businesses use the generated data.

Businesses must enable this by design and through contract, and can no longer treat product or service data as their exclusive asset.

- **Product design requirements:** From 2026, new connected products and related services must be designed so users can access their data easily and free of charge, with direct user access required if technically feasible, requiring significant changes to product development and IT infrastructure.
- **Business model disruption:** These new rights will force many companies to rethink and adapt their data strategies, product designs, and customer contracts. In particular, businesses will need to build technical interfaces and processes to allow users to access and share data easily, and must update all relevant agreements to reflect these rights. Companies that previously relied on exclusive access to product or usage data for competitive advantage will now face new competition and potential loss of aftermarket revenue streams.
- **Fair data sharing:** Companies that hold user data must share it on fair, reasonable, and non-discriminatory terms (similar to patent licensing and US antitrust concepts). Unfair contract terms that block access or overcharge for data access are prohibited and will be unenforceable.
- **Cloud and data processing service switching:** The EU Data Act makes it much easier for businesses and individuals to switch between data processing service providers, requiring providers to allow customers to transfer their data within 30 days and banning excessive exit fees. These service switching requirements may have a significant impact on market dynamics in smaller-scale IT arrangements; practical implications may be more limited in multifaceted IT environments, where changing service providers and porting data is typically complex.
- **Mandatory data processing service contract terms:** The EU Data Act introduces mandatory contractual obligations and transparency requirements for customer contracts regarding data processing services, aimed at eliminating technical, commercial, and contractual barriers that create vendor lock-in. Contracts must allow customers to switch service providers at any time and on short notice (as referenced above), after which the contract is considered terminated, regardless of any minimum term the provider may otherwise impose. As a result, it is likely that fixed-term commitments may effectively become month-to-month arrangements, potentially affecting revenue predictability and discouraging providers from offering long-term discounts. Additionally, contracts need to include a comprehensive list of transferable data and digital assets, and require providers to assist customers and third parties in facilitating a smooth transition, including supporting the customer's exit strategy.
- **Government access:** Public authorities can require access to data in emergencies or for certain public-interest reasons.

- **Enforcement and litigation:** Each EU Member State will appoint authorities to enforce the EU Data Act and — if necessary — impose significant fines. If personal data is impacted, existing data protection authorities will also be involved. The EU Data Act also allows for collective civil lawsuits (similar to US class actions) against companies that violate these rules, increasing the risk of mass litigation. This will also be a likely playing field for EU data protection authorities, which are tasked to regulate the EU Data Act where personal data as defined in the GDPR are affected.

Who Is Affected?

The EU Data Act targets companies that manufacture or offer connected products in the EU. It will also impact providers of digital services that interact with connected products or process user generated data within the EU, as well as providers of data processing services, such as cloud and edge computing, on the EU market.

Businesses that rely on access to data from connected products in the EU for their own services, such as repair shops, insurance companies, logistics providers, or companies using AI and analytics, will benefit from new rights to request and receive data from product users or data holders.

Any business that could be asked by EU authorities to provide operational data, including those in energy, healthcare, transportation, or agriculture, must be prepared to comply with government data access requests.

What Products, Services, or Use Cases Does the EU Data Act Cover?

Any product that can connect to the internet or another network and send or receive data falls into the scope of the EU Data Act. This includes everything from smart thermostats and cars to industrial robots and medical equipment. If a product generates data during use, users now have the right to access and share that data. Furthermore, any digital service that interacts with these products, such as apps, online platforms, or software that collects or analyzes product data, must support user data access and sharing rights.

Both personal data (information about individuals) and non-personal data (such as machine performance data) are covered. If personal data is involved, the GDPR still takes priority, but the EU Data Act extends user rights to all data types.

Finally, all types of cloud and data processing services, no matter how they are delivered (including infrastructure, platforms, SaaS, or edge computing), must enable user-driven data portability and switching.

Does the EU Data Act Apply to Companies Outside the EU?

Yes. The EU Data Act has a wide scope and applies to manufacturers and providers of products and services placed on the EU market, regardless of where the manufacturer/provider is based.

Consequently, the EU Data Act applies to companies established or based outside the EU if they manufacture connected products sold in the EU and/or offer connected services or data processing services, such as cloud services, within the EU.

How Does the EU Data Act Affect M&A, PE, and Other Transactions?

- In mergers, acquisitions, or joint ventures, due diligence must now include a review of EU Data Act compliance, the technical and contractual ability to provide user data access, and the risk of litigation or regulatory action. Failure to comply can result in significant liabilities and reduce deal value.
- Commercial contracts must be updated to reflect user data rights, fair data sharing, cloud switching, and liability for non-compliance. Contract terms that try to circumvent user rights or the EU Data Act's requirements will be void and unenforceable.
- Lenders, investors, and business partners may require evidence of EU Data Act compliance as part of their risk and environmental, social, and governance (ESG) assessments. Non-compliance may increase financing costs or block deals.
- Technology deals will increasingly require standard interfaces (APIs), secure data transfer solutions, and clear records of data access and sharing to support user rights and regulatory requirements.
- In addition to assessing regulatory risk, deal teams should consider whether the relevant company's business model may be vulnerable to shifting data market dynamics resulting from the EU Data Act.

Litigation and Regulatory Risks

The EU Data Act is technology-neutral. It applies to all types of connected products and digital services, regardless of the technology used. The new user rights to data will be a key driver of litigation and regulatory action.

Due to its wide-spread impact, the EU Data Act is expected to trigger significant litigation, including class actions and regulatory investigations, especially if companies fail to provide user data access or fair terms. Companies should focus on where they are most vulnerable to lawsuits or regulatory action, particularly in areas where they have previously restricted user access to data.

EU GDPR-style fines can be imposed in addition to the retrieval of any profits gained from non-compliance, and both regulators and courts can order corrective actions, including forced data sharing or contract changes. If a violation involves personal data, companies may face penalty risks under both the EU Data Act and EU GDPR.

Another key risk is that competitors may use the provisions of the EU Data Act strategically to challenge a company's business practices or gain access to valuable data via lawsuits.

Next Steps and Opportunities for Companies

In order to ensure compliance and transform the impact of the EU Data Act into a strategic advantage, companies can engage in various steps:

- **Scoping and gap analysis:** Identify which products, services, and contracts are affected, and clarify the company's roles (manufacturer, data holder, cloud provider, user). Map where user data rights will require changes to the business.
- **Compliance program design:** Assist in identifying and building practical processes and technical solutions for user data access, data separation, and data export, ensuring compliance with both the EU Data Act and other relevant laws (such as privacy and trade secrets).
- **Contract review and updates:** Draft and update contract templates to include required EU Data Act terms for user data rights, fair pricing, cloud switching, and other aspects, and update existing agreements to avoid unenforceable terms.
- **Governance and documentation:** Set up clear policies, user notices, access logs, and documentation to defend against enforcement actions or lawsuits, and to demonstrate compliance to partners and regulators.
- **Litigation and enforcement readiness:** Prepare responses to regulatory requests, defense against class actions, and preserve evidence for potential disputes. Focus on building defensible processes and documentation.
- **Training and monitoring:** Provide training for in-house teams and monitor ongoing legal developments in key EU markets, in order to stay ahead of new requirements and risks.
- **Strategic opportunities:** Consider new business models, such as offering data-driven services, negotiate data partnerships, and participate in industry standard-setting, turning compliance into a strategic benefit.

Latham & Watkins actively monitors data regime developments and is well positioned to advise on the legal and practical impacts of the EU Data Act, including any of the above steps.

Conclusion

The EU Data Act is a game-changer for any business dealing with connected products, related services, or data processing and cloud services in the EU. It creates new risks of lawsuits and regulatory fines, but also new opportunities. Companies that proactively address these changes and adopt a strategic approach can transform compliance obligations into a source of competitive advantage.

Contacts

Sophie Goossens
sophie.goossens@lw.com
+44.20.7710.3080
London / Paris

Jean-Luc Juhan
jean-luc.juhan@lw.com
+33.1.4062.2000
Paris

Susan Kempe-Müller
susan.kempe-mueller@lw.com
+49.69.6062.6580
Frankfurt

Alfonso Lamadrid
alfonso.lamadrid@lw.com
+32.2.788.6310
Brussels

Myria Saarinen
myria.saarinen@lw.com
+33.1.4062.2000
Paris

Tim Wybitul
tim.wybitul@lw.com
+49.69.6062.6560
Frankfurt / Brussels

Gail E. Crawford
gail.crawford@lw.com
+44.20.7710.3001
London

James Lloyd
james.lloyd@lw.com
+44.20.7866.2668
London

Fiona M. Maclean
fiona.maclean@lw.com
+44.20.7710.1822
London