SQUIRE PATTON BOGGS

EU Data Act in Full Effect

EU – November 2025

The EU Data Act (Data Act) entered into full effect earlier this year, but case law is yet to emerge to provide authoritative interpretation on some of its key provisions.

Absent any case law on point, the chief compliance officer, chief digital officer and legal departments of companies falling within the scope of the act are at pains to devise workable compliance strategies. The primary pain points for compliance with the Data Act include significant legal uncertainty, contractual review burden, substantial technical and operational changes, as well as potential business model disruption. This client alert tries to assuage some of these pain points by providing an overview of the act (Section A), its key practical compliance challenges (Section B) and a correlation table between each of the provisions of the act and its recitals, the unofficial guidance provided by the European Commission in its FAQs document and other overlapping statutory instruments (Section C).

A. Summary of the Data Act

The Data Act is one of the cornerstones of the EU's digital strategy and a key instrument for building a fairer and more competitive data economy. Its main purpose is to ensure that the vast amount of data generated by connected products and related services can be accessed, shared and reused under fair conditions. Until now, such data often remained locked within the systems of manufacturers or service providers, limiting competition and slowing innovation. The regulation seeks to change that by giving users more control over the data they generate, creating obligations for data holders to make that data available and setting safeguards to protect competition, trade secrets, privacy and security. The ultimate aim is to rebalance relationships between the different actors in the digital ecosystem and encourage a more open, contestable and transparent use of data across the EU.

Status and Enforcement

After its formal adoption in June 2023, the Data Act entered into force on 11 January 2024. Most of its provisions started applying on 12 September 2025, giving organisations time to adapt their technical and contractual frameworks. As a regulation, it is directly applicable across all EU member states, ensuring a uniform legal framework for data access, sharing and use. It also interacts closely with other key instruments, such as the General Data Protection Regulation (GDPR), the ePrivacy Directive, the Digital Markets Act (DMA), the Trade Secrets Directive and EU competition law, forming part of a broader legislative ecosystem that governs the European data economy.

In terms of enforcement, the Data Act follows a decentralised model similar to that of the GDPR: member states are responsible for designating competent authorities and establishing effective, proportionate and dissuasive penalties for infringements. This approach allows flexibility at the national level, while maintaining a high and consistent standard of protection and compliance across the EU.

Access and Use of Data (Articles 3–6)

A key feature of the Data Act is the creation of a fair framework for accessing and using data generated by connected products and related services. It grants users the right to obtain and use the data they generate, ensuring that access and sharing take place under transparent and non-discriminatory conditions. This obligation mainly concerns raw and pre-processed data, and excludes enriched or inferred data derived from further analysis.

The Data Act seeks to balance users' rights with the legitimate interests of data holders. Users gain control over their data, but holders may protect competition, trade secrets, confidentiality and security. These provisions go beyond the portability right under Article 20 of the GDPR, as they also cover non-personal data and mixed datasets.

Users may also request that their data be shared with third parties of their choice. Such sharing must rely on a valid GDPR basis, respect trade secret protections and exclude gatekeepers under the DMA. Third parties may use the data only for agreed purposes, and are prohibited from developing competing products or disclosing the data further.

Fairness and Compensation (Articles 8–9)

The Data Act also lays down rules on the conditions for making data available, as well as on compensation for doing so. Access must be provided on fair, reasonable and non-discriminatory terms, ensuring equal treatment among comparable data recipients. Any differentiation must be objectively justified and discriminatory arrangements could, in some cases, breach EU competition law.

As for compensation, charges must be transparent and proportionate to the actual costs incurred. Profit margins are not permitted when the recipient is a small- or medium-sized enterprise (SME) or a non-profit organisation. These provisions aim to prevent excessive pricing practices and ensure economic fairness, following the competition law principle of fair, reasonable and non-discriminatory (FRAND) terms.

Cloud Switching and Contractual Terms (Articles 23–25)

Another major aspect of the framework concerns the removal of barriers to switching between cloud service providers. The rules aim to prevent customer lock-in and ensure that users can move their data, applications and digital assets between providers without undue obstacles, included elevated costs. Providers must allow switching under clear and fair conditions, with reasonable notice periods and transparent transition timelines.

Contractual clauses must also reflect this principle of fairness. Standard contractual clauses are being developed to harmonise practices across the EU and apply to all service models, including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). These provisions complement the Free Flow of Non-Personal Data Regulation, and align with competition law objectives, promoting genuine choice and interoperability in the European cloud market.

A brief comparative digression: in the UK, the Competition and Markets Authority (CMA) has recently concluded its Cloud Market Investigation, looking in-depth at the same issues concerning the lack of switching and interoperability between cloud providers that led to the adoption of the Data Act. The CMA concluded that the UK cloud market is afflicted by an adverse effect on competition arising from certain features of the market, including the concentration of market power in the hands (or rather their data centres) of two main cloud providers. It recommended that the newly established CMA Digital Markets Unit considers using its newly acquired Digital Markets, Competition and Consumers Act (DMCCA) powers to impose regulatory obligations on those two providers, that would be aimed at creating a more contestable market and promoting switching and interoperability. It is expected that some of such new obligations, if any, might look like some of the provisions of the Data Act.

Interoperability and Standards (Article 33)

Interoperability is another cornerstone of the framework, ensuring that different data systems and services across the EU can communicate and work together effectively. The Data Act introduces essential requirements for interoperability within and between data spaces, allowing data to flow more easily across sectors and member states. Where harmonised standards are insufficient, the European Commission may adopt common specifications as a fallback to guarantee technical and organisational compatibility.

These measures are aligned with the Data Governance Act and the EU Standardisation Regulation, reinforcing the role of European standardisation organisations in developing trusted and interoperable data infrastructures. By promoting compatibility and common standards, the idea is that this framework will reduce market fragmentation and foster innovation across the European data economy.

B. Compliance Challenges

Legal and Contractual

- **Unclear legal terms** – The interpretation of key concepts like FRAND compensation is highly contentious, and likely to lead to significant litigation without clear guidance from the European Commission.
- **Contract review and renegotiation** – Article 13's "fairness test" for unilaterally imposed contract clauses in business-to-business (B2B) data-related agreements applies to new contracts from September 2025, and many existing long-term contracts from September 2027. This forces businesses to review and potentially renegotiate a vast number of agreements, creating a significant retroactive burden.
- **Interplay with other laws** – The Data Act's complex interaction with existing regulations like the GDPR, DMA, competition law and the NIS2 Directive creates a challenging web of obligations — see Section C below.
- **Protecting trade secrets** – While the Data Act provides some safeguards for trade secrets, companies face a difficult balancing act between their data-sharing obligations and the need to protect sensitive, proprietary information. This is expected to be a major area for future disputes.
- **Extraterritorial scope** – Non-EU companies offering products or services in the EU must comply and may need to appoint a legal representative within a member state, adding an administrative layer.

Technical and Operational Challenges

- **Product redesign** – For manufacturers, new connected products placed on the market after September 2026 must be designed to allow users easy, direct and free access to their data "by design," requiring significant changes to product development and IT infrastructure.
- **Data identification and accessibility** – Companies must develop technical solutions to identify, separate (from trade secrets) and provide data in a comprehensive, structured, commonly used and machine-readable format, which many lack the existing infrastructure to do.
- **Cloud switching implementation** – Providers of cloud and data processing services must remove technical, commercial and organisational barriers to switching, including facilitating data transfer within a short (30-day) transitional period. This requires significant technical assistance and can affect revenue predictability from long-term contracts.
- **Ensuring data continuity** – A practical challenge is ensuring data rights seamlessly transfer when a connected product is sold (e.g. from one owner to the next), often requiring complex contractual "hinge" mechanisms.

Business and Financial Challenges

- **Business model disruption** – Companies that previously relied on exclusive access to user data for competitive advantage or aftermarket services (like repairs) will need to fundamentally rethink and adapt their business models.
- **Cost and resources** – The costs associated with technical infrastructure investments, legal reviews and establishing new compliance processes (similar to the GDPR rollout) can be substantial, particularly for SMEs.
- **Litigation and enforcement risks** – The new user rights are expected to be a key driver of litigation, including class actions. Non-compliance can result in significant fines (similar to the GDPR) and legal action from regulators or competitors.

C. Interconnected Legal Framework

The following correlation table summarises the key provisions of the Data Act, highlighting the main obligations, relevant recitals and cross-references with the European Commission's unofficial FAQs document and other EU instruments. It shows that compliance with the Data Act cannot be achieved in isolation, as the regulation interacts closely with several complementary frameworks, including the GDPR, the Trade Secrets Directive, the DMA, the Data Governance Act and EU competition law. Together, these instruments form a coherent legal ecosystem that governs how data is accessed, shared and protected within the European single market. This cross-reference approach is essential for organisations to understand the practical overlaps and to design integrated compliance strategies.

Article	Recitals	FAQs	Cross-reference and/or related legal instruments
Article 3 – Obligation to make product and related service data accessible	16, 17, 20–25, 35	Q4:Scope covers raw/pre-processed data, metadata; not enriched/inferred data. Q7–13: Definitions of connected product, related service, use abroad, resale, anonymisation via PETs, etc.	GDPR – Personal data within scope requires compliance with the GDPR, including a valid lawful basis for processing and safeguards when users are not data subjects. ePrivacy Directive – Governs data stored on/collected from terminal equipment. Trade Secrets Directive – Protects confidential know-how; Article 3 obligations cannot undermine trade secret safeguards.
Article 4 – Rights and obligations of users and data holders (access/use)	23, 25–29, 33–36	Q14–20: Definition of "user"; only EU users covered; multiple users possible. Q18: Complements GDPR portability by extending beyond personal data. Q23: Balances access with trade secret protection. Q25: Access can be denied if safety/security risks.	GDPR – The Data Act complements the GDPR but goes beyond data subject portability rights (Article 20 GDPR). Trade Secrets Directive – Data holders may require confidentiality agreements and withhold disclosure if serious harm is likely. ePrivacy Directive – Applies if data involves storage on user device.
Article 5 – User right to share data with third parties	26–31, 33–36, 40	Q24: Protections can apply to direct access. Q25a: Data holder must rely on valid GDPR basis. Q31: Obligation to share remains, even if user has direct access. Q36: Users cannot force sharing with DMA gatekeepers.	GDPR – Sharing personal data with third parties requires valid basis (consent, contract). ePrivacy – Governs access to data on devices. DMA – Gatekeepers excluded as "third parties" who can benefit from this provision. Trade Secrets Directive – Safeguards still apply; disclosure limited if risk of serious economic harm. Consumer law – Ensures users' rights are not undermined in contracts.
Article 6 – Obligations of third parties receiving data	32, 33, 37–40	Q35: Third parties may use data only for agreed purposes; no competing product development or onward sharing with gatekeepers. Q37: Recipients must be EU-based; no obligation to share outside EU.	GDPR – Third parties become controllers/processors with full obligations (purpose limitation, minimisation and deletion). DMA – Prohibits onward sharing with gatekeepers. Trade Secrets Directive – Third parties must maintain confidentiality. Consumer law – Ensures fair practices when services offered to consumers using accessed data. Competition law – The use of shared data for the development of a competing connected product (which is considered to be interchangeable or substitutable within the meaning of competition law) is prohibited.

Article	Recitals	FAQs	Cross-reference and/or related legal instruments
Article 8 – Conditions for making data available	28, 42–45	Q38: No discrimination between comparable data recipients. Q40: All parties can use dispute settlement mechanism.	Competition law – Discrimination regarding the arrangements for making data available between comparable categories of data recipients could in certain circumstances also constitute a breach of competition law. GDPR – Equal treatment of personal vs. non-personal data requires safeguards. Data Governance Act – Dispute resolution mechanisms aligned with data-sharing frameworks.
Article 9 – Compensation for making data available	46–51	Q39: No fixed limit; compensation must be transparent and based on objective costs; SMEs/non-profits excluded from profit margin.	Competition law – Prevents excessive pricing or hidden margins in certain circumstances. In addition, competition law cases around FRAND terms could provide a useful benchmark for determining the compensation for making data available. Consumer law – Fairness obligations in pricing. GDPR – If personal data is involved; charging cannot undermine fundamental rights.
Article 23 – Removing obstacles to effective cloud switching	78, 79, 83–86, 93, 94, 96	Q55: Free-tier offerings covered. Q56: Clarifies timing of notice and transition periods.	Regulation 2018/1807 (Free flow of non-personal data) – Supports portability. GDPR – Imposes portability rights for personal data. Competition law – Prevents lock-in in certain circumstances and could be used as a complementary tool to promote switching. Standards Regulation 1025/2012 – Ensures interoperability in switching.
Article 25 – Contractual terms concerning switching	82, 85, 87–89, 94, 96	Q58: SCCs being developed for cloud contracts; obligations apply to SaaS as well as IaaS/PaaS.	Contract law/consumer law – Fairness of standard clauses. GDPR – This still governs data categories. Standards Regulation – Standard Contractual Clauses (SCCs) promote legal/technical harmonisation across cloud providers.
Article 33 – Essential requirements on interoperability	99, 100, 103		Standards Regulation 1025/2012 – EU standardisation imposed on organisations Data Governance Act – Promotes interoperability across data spaces. GDPR – Ensures personal data remains protected in cross-space sharing. Competition law – The lack of interoperability could be a breach of competition law in certain circumstances, and so competition law could be used as a complementary tool to promote interoperability.

If you have any questions on the contents of this client alert, or wish to discuss in confidence your Data Act compliance strategy, please contact your Squire Patton Boggs lawyer or any of the authors listed below:

Contacts

Francesco Liberatore
Partner, Competition – Antitrust
London, Brussels and Milan
T +44 207 655 1505
E francesco.liberatore@squirepb.com

Gorka Navea
Partner, Competition – Antitrust
Madrid
T +34 91 426 4805
E gorka.navea@squirepb.com

Bartolome Martin
Partner, Data Privacy, Cybersecurity and Digital Assets
Madrid
T +34 91 426 4867
E bartolome.martin@squirepb.com

The authors wish to thank Lucia Hartnett and Eva Díaz for their help in drafting this client alert.

69765/11/25