BCLP. Client Intelligent

Insights

KEY IMPLICATIONS FOR CLOUD SERVICE PROVIDERS

Nov 05, 2025

WHAT IS THE DATA ACT ?

The EU Data Act (Regulation (EU) 2023/2854), applicable from September 12, 2025, introduces a comprehensive legal framework aimed at enhancing data portability, interoperability, and minimizing dependency on individual service providers throughout the digital economy. Among its most impactful provisions are the mandatory switching rights under Chapter VI, which regulate cloud switching and impose significant obligations on providers of “data processing services.”

While fixed-term contracts remain lawful, service providers, including IaaS, PaaS and SaaS, are now required to reassess the structure and content of these agreements in light of the Data Act’s new obligations. This regulation introduces harmonized rules that affect the way providers interact with their clients, compelling them to ensure that contractual terms reflect fair, reasonable, and non-discriminatory conditions. As a result, many existing agreements may need to be adapted to align with the regulation’s requirements and to maintain compliance in future renewals or amendments.

WHICH ENTITIES ARE WITHIN SCOPE ?

The Data Act applies to entities involved in the generation, processing, and use of data. Its scope includes:

1. **Manufacturers of connected products and Providers of related services:** Entities placing Internet of Things (IoT) devices and their associated digital services on the EU market.
2. **Data Holders:** This includes manufacturers, service providers, and platform operators who control access to data generated by connected products or services.
3. **Data Recipients:** Entities, whether public or private, who receive data from data holders for commercial or public interest purposes.
4. **Public Sector Bodies:** EU institutions and Member State authorities may request data from holders in cases of exceptional need, such as public emergencies.

5. **Providers of Data Processing Services:** according to Article 2(8) and Recital 81 of the Data Act, data processing services are digital services enabling on-demand network access to a shared pool of configurable computing resources. This includes:

   - Software-as-a-Service (SaaS)
   - Platform-as-a-Service (PaaS)
   - Infrastructure-as-a-Service (IaaS)

However, not all SaaS providers are automatically in scope. Only those whose services meet the definition of data processing services, i.e. those offering scalable, elastic, and configurable computing resources, are covered.

Nonetheless, the Act applies irrespective of where the provider is established, provided that the services are made available to customers within the EU.

KEY OBLIGATIONS OF CLOUD SERVICES PROVIDERS ?

Under Chapter VI, SaaS providers are subject to mandatory service switching obligations and contractual transparency requirements. From 12 September 2025, these include:

DATA PORTABILITY

(*Article 23*): Providers must remove barriers to switching by enabling clients to port their data, and where feasible, applications and other digital content, to another provider. This includes taking all necessary technical and contractual measures to support effective migration.

TECHNICAL OBLIGATIONS

(*Article 24*): While providers must offer reasonable assistance during the switching process, they are not required to rebuild the client's environment within the destination infrastructure. Their obligations are limited to their own services, contracts, and commercial practices.

SWITCHING CONTRACT REQUIREMENTS

(*Article 25*): Contracts must clearly define the client's rights and the provider's obligations in the event of switching or migration to on-premise infrastructure. Contracts must include a two-month cancellation period and a 30-day switching period during which the provider must support the transition.

INFORMATION OBLIGATIONS

(*Article 26*): Providers must inform clients about available switching procedures, formats, and known technical limitations. They must also maintain an online registry detailing data structures, formats, and relevant interoperability standards.

DUTY OF GOOD FAITH

(*Article 27*): All parties involved in the switching process must cooperate in good faith to ensure secure, timely, and disruption-free data transfers using open, machine-readable formats.

TRANSPARENCY ON INTERNATIONAL TRANSFERS

(*Article 28*): Providers must publicly disclose the jurisdictions of their ICT infrastructure and describe the safeguards in place to prevent unlawful international access to non-personal data. These disclosures must be referenced in service contracts.

ELIMINATION OF SWITCHING FEES

(*Article 29*): Between January 2024 and January 2027, providers may charge reduced fees limited to direct costs. From January 2027 onward, switching must be free of charge. Clients must be informed of all applicable fees before contract conclusion.

OPEN INTERFACES AND INTEROPERABILITY

(*Article 30*): Providers (excluding IaaS providers) must offer open interfaces free of charge to enable interoperability and data portability. They are not required to develop new technologies or disclose protected digital assets.

UNFAIR CONTRACTUAL TERMS

(Article 13): Providers may not impose unfair terms unilaterally in B2B contracts, particularly those affecting data access or use. Certain clauses are deemed null and others presumed abusive, requiring careful legal review.

As an EU regulation, the Data Act is directly applicable across Member States, but enforcement is delegated to national authorities. Each Member State must designate one or more competent authorities responsible for monitoring compliance and handling enforcement actions. Non-

compliance may result in significant fines, civil liability, and regulatory investigations, especially where personal data is involved, triggering parallel enforcement under the GDPR.

ADAPTING AGREEMENTS WITH SCCS AND MCTS?

Under Article 41 of the Data Act, the European Commission convened an expert group tasked with developing non-binding model contractual terms (MCTs) and standard contractual clauses (SCCs). These instruments are designed to facilitate the drafting of fair, reasonable, and non-discriminatory cloud service contracts, including SaaS agreements.

The expert group's final report clarifies that the SCCs are voluntary and non-binding, but they are structured to be adaptable by the parties and relevant across all cloud service models (IaaS, PaaS, SaaS). Rather than prescribing mandatory elements, the SCCs offer a baseline framework that promotes compliance with the Data Act and encourages contractual best practices. They address key areas such as:

- Switching and termination procedures,
- Service continuity and security,
- Allocation of liability,
- Transparency and change management.

These clauses are designed to be integrated into Data Processing Agreements and other contractual instruments to help providers and customers anticipate and align with the Data Act's requirements, particularly in the context of data access, portability, and interoperability.

COMPLIANCE TIMELINES ?

Pursuant to Article 50 of the Data Act, the regulation becomes applicable from **12 September 2025** to all entities within its scope. However, the Data Act also introduces a transitional regime specifically for contracts concluded before 12 September 2025, delaying the application of the obligations related to unfair contractual terms set out in Article 13:

- For contracts signed on or after 12 September 2025, Article 13 applies immediately.
- For contracts concluded prior to that date, Article 13 will only apply from 12 September 2027 if one of the following conditions is met:
  - the contract is of indefinite duration, or
  - it is set to expire at least ten years after 11 January 2024, meaning on or after 11 January 2034.

This phased approach ensures that long-term or open-ended contracts are gradually brought into compliance, while shorter-term agreements may remain unaffected unless they are renewed or amended.

In accordance with French contract law and consistent with EU legal interpretation, the renewal of a fixed-term contract after 12 September 2025 is treated as the conclusion of a new contract, thereby subjecting it to the Data Act from the date of renewal. Similarly, an automatic renewal (tacit reconduction) may also trigger the application of the regulation if it results in a contract of indefinite duration. In such cases, the contract falls within the scope of the transitional clause under Article 50, and Article 13 may apply from 12 September 2027.

WHAT STEPS SHOULD YOU TAKE NOW?

With the Data Act now in force, SaaS providers must act swiftly to align their operations, contracts, and technical infrastructure. The following steps are essential to ensure compliance and mitigate legal and commercial risks:

Contract audit and redrafting:

- Review existing SaaS agreements to identify clauses that conflict with the Data Act and especially Chapter VI, such as restrictive termination terms or opaque switching procedures.
- Update standard terms and templates to include mandatory dispositions, such as a two-month cancellation period, a 30-day switching window with defined support obligations, and clear descriptions of transferable data and digital assets.

Technical readiness assessment:

- Evaluate platform capabilities for data export, portability, and interoperability.
- Develop or enhance APIs and secure transfer protocols to support user-driven migration.

Governance and documentation:

- Establish internal policies and procedures for switching, data access, and user rights and maintain technical documentation, and a public registry of data formats and standards.
- Prepare for regulatory audits and enforcement actions, including cross-border data access reviews.

Customer Communication:

- Provide clear guidance on switching rights, procedures, and limitations.

- Ensure transparency on fees, jurisdictions, and safeguards related to data transfers.

Training and Monitoring

- Train legal and technical staff on the Data Act's requirements and implications.
- Monitor regulatory developments and enforcement trends across EU Member States.

HOW CAN WE ASSIST YOU?

BCLP's team is equipped to support your organization in navigating the compliance landscape introduced by the Data Act. We help identify services and contractual arrangements impacted by the regulation through targeted gap analyses, and assist in drafting or revising contract templates to ensure alignment with the new legal framework. Our guidance extends to the technical implementation of compliance measures, ensuring that operational strategies reflect the regulation's requirements.

To support long-term compliance, we offer ongoing legal monitoring and deliver tailored training sessions to in-house teams, ensuring they remain informed and prepared.

By proactively addressing these obligations, SaaS providers not only mitigate legal risk but also strengthen their position in a competitive, data-driven market.

RELATED CAPABILITIES

- Data Privacy & Security
- General Data Protection Regulation

MEET THE TEAM

Pierre-Emmanuel Froge

Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
