Cooley

PaaS, IaaS or SaaS – Be Aware: New Switching Rules Will Become Applicable in EU

September 8, 2025

Key takeaways for cloud, SaaS, edge and other digital service providers

Introduction

On September 12, 2025, sweeping new rules under the EU Data Act (Regulation (EU) 2023/2854) will become applicable, introducing significant new obligations for cloud service providers in the European Union (EU), particularly around interoperability, termination rights and switching between providers. These rules are designed to make it significantly easier for customers of data processing services to switch between providers, thereby reducing vendor lock-in and fostering a more competitive, innovative digital market. The new regime draws inspiration from existing EU rules on phone number portability and personal data portability, aiming to empower customers with greater control and flexibility over their digital assets and services.

This alert provides a concise overview of the new requirements, the definition of "data processing service" under the Data Act, the practical consequences for in-scope providers and key steps to ensure compliance.

What is a 'data processing service' under the EU Data Act?

The Data Act introduces a broad, technology-neutral definition of "data processing service" (DPS) in Article 2(8):

> A digital service that is provided to a customer and that enables ubiquitous and on-demand network access to a shared pool of configurable, scalable and elastic computing resources of a centralised, distributed or highly distributed nature that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Key criteria for a DPS include:

- **Digital service provision:** The service is delivered electronically, typically over the internet or a dedicated network.
- **On-demand network access:** Customers can access resources whenever needed, from any location, without requiring manual intervention from the provider.
- **Shared pool of resources:** The service offers access to virtualized or pooled compute, storage, network, platform or application resources.
- **Configurable, scalable and elastic:** Customers can adjust capacity up or down, and the service automatically adapts to workload changes.
- **Rapid provisioning and release:** Resources can be provisioned or de-provisioned quickly, with minimal management effort.

Examples of services that typically qualify as a DPS:

- **Infrastructure as a service (IaaS):** virtual machines, storage, networking
- **Platform as a service (PaaS):** application hosting, development platforms
- **Software as a service (SaaS):** cloud-based productivity suites, customer relationship management (CRM) platforms
- **Edge and distributed computing services**

Also applicable to companies not established in the EU

Consistent with other EU legislation on digital services, the scope of the Data Act is extraterritorial and covers providers of data processing services, irrespective of their country of establishment, if they provide services to customers in the EU. Consequently, numerous service providers located outside the EU will fall under the provisions of the Data Act.

Types of data to be switched over

The switching rules apply to input and output data, including metadata, generated through the customer's use of the service. However, these rules do not extend to data protected by intellectual property rights or to information specific to the internal functioning of the service where disclosure would risk revealing the provider's trade secrets. This approach is designed to secure effective portability for customers while safeguarding providers' proprietary assets.

It will therefore be important to map these categories to determine what qualifies as "exportable data" and what may be legitimately excluded.

New obligations for service providers

If your service qualifies as a DPS under the Data Act, you will be subject to a range of new legal obligations from September 12, 2025. In particular, Chapter VI introduces detailed rules on:

Switching facilitation

- Customers must be able to switch to another provider or to on-premises infrastructure with minimal friction. This includes a maximum two months' notice.
- Providers must enable the transfer ("porting") of all exportable data and digital assets within a maximum 30-day transition period (extendable only in cases of technical unfeasibility).
- From January 12, 2027, all switching and data egress charges must be eliminated (with limited exceptions for parallel use scenarios).

Interoperability and open interfaces

- Providers must offer open, well-documented interfaces (APIs) to enable interoperability and portability and support export in structured, commonly used, machine-readable formats.
- Compliance with harmonized standards and specifications published in the forthcoming EU repository will be mandatory.

Functional equivalence (IaaS)

- When a customer switches to another IaaS provider of the same type, the destination service must ensure functional equivalence. In other words, the destination service should, using the customer's exported data and digital assets, provide a comparable level of functionality and deliver materially similar outcomes for the shared features under the contract.

Safeguards against foreign government access

- Providers must implement technical, organizational and contractual measures to prevent unlawful access to nonpersonal data by non-EU authorities, including a judicial review test for disclosure orders.

Contractual and compliance measures

- Providers must update contracts to reflect mandatory switching rights and phase out egress fees.
- Updated contracts shall, among other obligations, enable customers to terminate contracts after the maximum notice period once switching is complete; conclude new contracts with alternative providers of the same service type; port their exportable data and digital assets to another provider or on-premises infrastructure; and achieve functional equivalence with the new service.
- Noncompliance may result in injunctions, damages claims and significant administrative penalties.

Specific regime for certain data processing services

- These rules do not apply where the service is custom-built for a single customer. This means when most features or all components are developed specifically for that customer, and the service is not offered at commercial scale via the service provider's catalogue.
- Similarly, nonproduction test or evaluation services offered for a limited period are exempt.
- Importantly, providers must inform prospective customers in advance if any of the Chapter VI obligations will not apply because the service falls within one of these exceptions.

Key actionable takeaways for legal and compliance teams

To prepare for the new EU Data Act requirements, you should:

1. Assess service portfolio
    - Conduct a detailed review of all products and services to determine which qualify as "data processing services" under the Data Act.
    - Pay special attention to multi-tenant SaaS, PaaS, IaaS and edge computing offerings.
2. Create a data inventory
    - To comply with the Data Act, providers of data processing services will need to establish and maintain a clear inventory of the data and digital assets processed through their services.
    - This inventory should distinguish between:
        - Customer-provided data
        - Metadata and system-generated data
        - Derived or processed datasets
3. Update contracts and policies
    - Revise customer agreements, data processing agreements (DPAs) and service-level agreements (SLAs) to include mandatory switching rights and timelines, and to phase out egress fees.
    - Consider including in the contracts with your customers the European Commission's forthcoming nonbinding model contractual terms on data access and standard contractual clauses for cloud computing, which address issues such as data access and use, reasonable compensation, and protection of trade secrets.
    - Coordinate with finance and auditors when updating contracts to assess how new termination rights and switching obligations may affect revenue recognition and overall business models.
4. Implement technical solutions
    - Develop or enhance self-service data export tools, and ensure APIs will be compatible with forthcoming EU standards.
    - Monitor the EU standardization work under the Data Act, particularly the development of interoperability standards and reference architectures for cloud and edge services.
    - Assess the impact of the upcoming standards on your services, and proactively plan for implementation, as early alignment can reduce compliance risks and enhance market trust.
5. Strengthen compliance and training
    - Establish internal processes for handling switching requests and foreign government data access demands.
    - Train relevant staff on new obligations, compliance procedures and contractual terms.
6. Monitor regulatory developments
    - Track the European Commission's interoperability repository, forthcoming model contractual clauses, FAQs and guidelines from the European Commission.

Early action is critical; it will not only mitigate compliance risks but also position businesses to take advantage of new opportunities in a more open and competitive data ecosystem.

At Cooley, our cross-disciplinary team is actively monitoring the Data Act implementation and standardization process, and we stand ready to help you anticipate obligations, update contracts and design practical compliance strategies tailored to your business models.

Key Contacts

Patrick Van Eecke Brussels	pvaneecke@cooley.com +32 2 486 7501
Enrique Gallego Capdevila Brussels	ecapdevila@cooley.com +32 2 486 7534
Bartholomäus Regenhardt Brussels	bregenhardt@cooley.com +32 2 486 7542