

EU Data Act

& its impact on cloud services in the Life Sciences sector

2025

The EU Regulation 2023/2854 on fair access to and use of data (Data Act) aims, among other objectives, to address the issue of cloud service customer lock-in and foster a more competitive EU cloud market. The Data Act introduces comprehensive new obligations for cloud service providers, particularly by enabling customers to switch providers free of charge in the long term and to terminate (even fixed-term) contracts generally within two months.

What is the Data Act and why is it relevant for the life sciences sector?

The Data Act is a new cross-sectoral horizontal EU Regulation that forms part of the European strategy for data and is **directly applicable in all EU Member States**. In addition to its goal of making data generated by the Internet of Things (IoT) more accessible, the Data Act aims to promote a fair and competitive EU cloud market. The EU views the ability of customers of data processing services (**DPS**) to switch from one service to another without undue obstacles or transfer costs, as a key condition for fostering a more competitive market with lower entry barriers, and for ensuring greater resilience. The Data Act introduces the following **key obligations** and **implications for cloud service providers**:

Key obligations and implications

- 1. Switching obligations:** Cloud service providers must fulfil various obligations to enable their customers to switch to a cloud service covering the same service type offered by a different provider, to an on-premises ICT infrastructure, or, if applicable, to use several cloud service providers simultaneously.
 - **Impact on contractual agreements:** The Data Act **mandates specific contractual** content that must be included in cloud contracts. These provisions impose far-reaching obligations, particularly on providers, related to switching and other aspects of the customer relationship.
 - **Impact on business model (esp. revenue recognition):** Two aspects of the Data Act are particularly important here: firstly, customers have **the right to terminate any cloud contract** with as little as **two months' notice**; and secondly, providers may only impose reduced switching charges until 12 January 2027, after which **no switching charges will be allowed**.
 - **Impact on technical setup:** Different requirements apply depending on the type of cloud service, e.g. specific interoperability requirements.
- 2. Obligation to prevent unlawful international and third-country governmental access to non-personal data held in the EU**
 - **Impact on work processes:** The implementation of adequate technical, organisational and legal measures is required. Specific rules apply to the fulfilment or non-fulfilment of these obligations.

The Data Act’s provisions on cloud switching are particularly important for life sciences companies, who rely heavily on cloud infrastructure for the storage and processing of sensitive health data. These regulations require cloud service providers to ensure seamless data switching and to prevent vendor lock-in situations, which is critical for healthcare organisations that manage patient records, clinical trial data and research data sets. For pharmaceutical companies that run multi-year drug development programmes, the ability to switch cloud providers without losing access to data or facing prohibitive costs provides greater flexibility in their technology strategies.

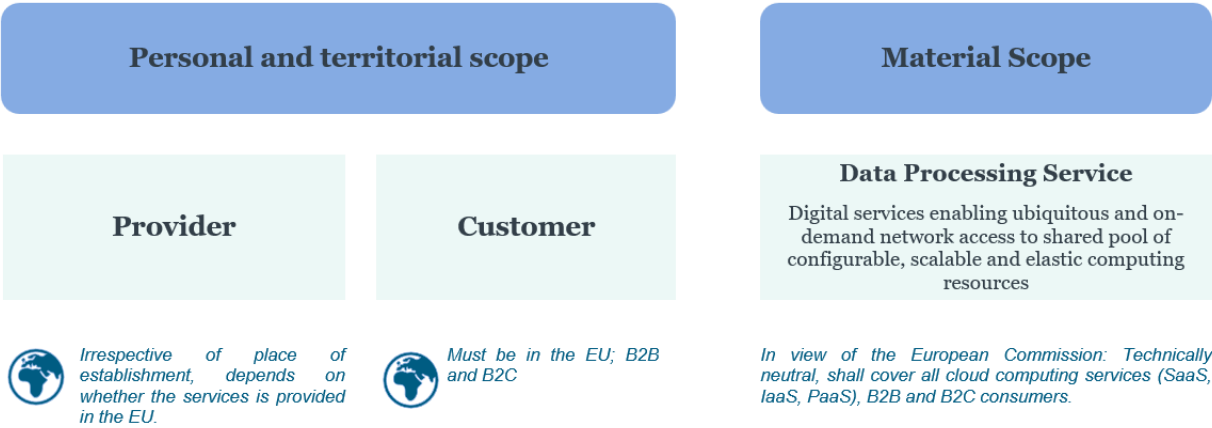
Health apps and digital therapy platforms benefit from improved data portability requirements, enabling them to more easily migrate users’ health data between different cloud environments while remaining compliant with healthcare regulations. The provisions also address unfair contract terms that have previously hindered life sciences companies from switching cloud providers. This is particularly important given the long-term nature of clinical research and patient monitoring programmes. For manufacturers of healthcare IoT solutions and medical devices, these regulations ensure that data generated by connected devices remains accessible even when switching cloud infrastructure providers.

What cloud services are covered by the Data Act, and who is subject to its cloud service obligations?

The Data Act defines a DPS as

“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”.

According to the EU Commission and the Data Act’s recitals, **all types of cloud computing services** - such as **SaaS, IaaS and PaaS** – are included. The marketplace principle applies, meaning the Data Act applies to providers offering **their services to customers in the EU**, regardless of the provider’s place of establishment. Furthermore, any service can qualify as a DPS regardless of whether it is intended for use by consumers and/or businesses (B2B and B2C). The Data Act only very restrictively excludes certain services from the applicability of specific obligations.



What are the main implications of the switching obligations?

The upcoming **switching obligations** are expected to have a significant impact on the cloud services market. Cloud service providers should proactively understand the new requirements and associated challenges, adapt their offerings and processes accordingly, and develop practical solutions. Providers must comply with a broad range of **switching obligations** and eliminate relevant (pre)-commercial, technical, contractual, and organisational obstacles to switching. This includes:

- **Technical obligations:** These depend on the type of service with differences in interoperability requirements between IaaS and other services, for example.
- Extensive requirements for **mandatory contractual content** in cloud contracts with customers:
 - Providers are obligated to include clauses such as reasonable assistance and due care to maintain business continuity.
 - According to the EU Commission, these **contractual requirements also apply to legacy contracts**, i.e. contracts that were concluded before the Data Act becomes applicable.
 - In the EU Commission's view, this means that once the Data Act applies, **any cloud contract, including fixed-term contracts, can generally be terminated within a two-month period**, regardless of whether the termination right is stipulated in the contract).
 - The resulting **problem with revenue recognition** are amplified by the fact that only reduced switching charges may be imposed temporarily and **no switching charges at all in the long term**.
 - The EU Commission will issue **non-binding standard contractual clauses (SCCs)**. While the exact publication date is unclear, time is of the essence, as customers are already requesting contract adjustments.

Based on our participation in webinars organised by the EU Commission on the draft SCCs, we believe that the SCCs should be adapted to the specific business needs of cloud service providers and not used 'as is' (e.g. some of the draft SCCs go beyond the obligations of the Data Act).

- The switching obligations cover **digital assets** ("elements in digital form, including applications, for which the customer has the right of use, independently from the contractual relationship with the data processing service it intends to switch from") and **exportable data** ("input and output data, including metadata, directly or indirectly generated, or cogenerated, by the customer's use of the data processing service, excluding any assets or data protected by intellectual property rights, or constituting a trade secret, of providers of data processing services or third parties").

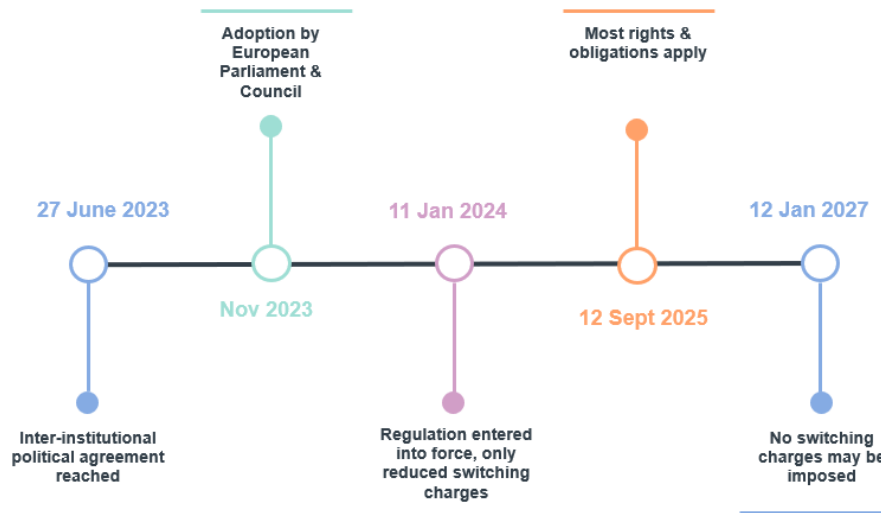
How we can support your business

To ensure compliance with the Data Act, we can support you in:

- **Getting an overview** about the existing legal landscape, upcoming legislation, developments and the market practice
- **Undertaking a scoping exercise** to determine the applicability of the Data Act to your services and data
- **Conducting an impact analysis** to identify which (new) rules apply to your organisation and what it means for your business
- **Implementing the Data Act** including:
 - Advising on **changes to technical setup and information requirements** to comply with data processing service obligations
 - Advising on **compliance with existing obligations** (esp. GDPR, NIS2 Directive) when implementing the Data Act
 - **Designing processes and procedures** for handling the switching process
 - **Drafting and revising your contracts, template agreements and additional documentation**, including notices providing users with transparent information and advice on how to implement the SCCs
 - **Advising on approaches** as to how **problems with revenue recognition** in connection with the Data Act (esp. termination right, no switching charges may be imposed in the long term) can be compensated, e.g. by adopting a different pricing policy
 - Advising and representing you in **potential conflicts with contractual partners and toward authorities**
 - Advising on the **potential benefits of the Data Act** (e.g. switching as a customer)

What is most urgent?

The Data Act has been in force since **11 January 2024**. Most rights and obligations will apply from **12 September 2025**. Regarding the ban of switching charges, a staggered approach has been adopted: From **11 January 2024**, only reduced switching charges may be imposed and from **12 January 2027**, no switching charges at all.



Enforcement

Member States are required to designate the competent authorities and establish effective, proportionate and dissuasive penalties in their local law. If personal data is involved, such fines may align with Regulation (EU) 2016/679 (GDPR) up to **20,000,000 EUR** or **4 % of the total worldwide annual turnover** of the preceding financial year, whichever is higher. It is currently unclear how the competence of the authorities and the number of fines will be defined in detail.



More information



Sign up for our [Connected newsletter](#) for a monthly round-up from our Regulatory & Public Affairs team.

Band 1 for Europe-
wide Information
Technology, IP,
Telecoms & Data
Protection

Chambers Europe 2025

Band 1 for
Global Multi-
jurisdictional
TMT & IP

Chambers Global 2025

Tier 1 for Artificial
Intelligence -
Germany & UK

Legal 500 2025

Tier 1 for TMT in
12 Jurisdictions

Legal 500 2024



twobirds.com

Abu Dhabi • Amsterdam • Beijing • Bratislava • Brussels • Budapest • Casablanca • Copenhagen • Dubai
• Dublin • Dusseldorf • Frankfurt • The Hague • Hamburg • Helsinki • Hong Kong • London • Lyon
• Madrid • Milan • Munich • Paris • Prague • Rome • San Francisco • Shanghai • Shenzhen • Singapore
• Stockholm • Sydney • Tokyo • Warsaw

The information given in this document concerning technical legal or professional subject matter is for guidance only and does not constitute legal or professional advice. Always consult a suitably qualified lawyer on any specific legal problem or matter. Bird & Bird assumes no responsibility for such information contained in this document and disclaims all liability in respect of such information.

This document is confidential. Bird & Bird is, unless otherwise stated, the owner of copyright of this document and its contents. No part of this document may be published, distributed, extracted, re-utilised, or reproduced in any material form.

Bird & Bird is an international legal practice comprising Bird & Bird LLP and its affiliated and associated businesses.

Bird & Bird LLP is a limited liability partnership, registered in England and Wales with registered number OC340318 and is authorised and regulated by the Solicitors Regulation Authority (SRA) with SRA ID497264. Its registered office and principal place of business is at 12 New Fetter Lane, London EC4A 1JP. A list of members of Bird & Bird LLP and of any non-members who are designated as partners, and of their respective professional qualifications, is open to inspection at that address.

Admin\64018932.1