

**Alert | Technology Transactions/
Manufacturing & Supply Chain Industry**



July 2026

EU Digital Omnibus Package Proposes Amendments to Data Act

[Read in German.](#)

The European Commission has proposed substantial amendments to Regulation (EU) 2023/2854 – better known as the “Data Act” – as part of its Digital Omnibus legislative package. For now, the EU Council’s consolidated compromise text, which remains subject to further negotiation and may yet change in the course of the legislative process, touches on some of the most commercially sensitive areas of the Data Act: data sharing between private parties and with public authorities, cloud switching, and the re-use of public sector data. That said, on several points where businesses and stakeholders had called for amendments, or at least clarification, the Digital Omnibus leaves the Data Act’s underlying uncertainties unaddressed.

Five developments stand out as particularly significant:

1. Cloud service providers who are subject to the cloud switching obligations would gain express statutory clarity on the permissibility of early termination penalties in fixed-term contracts.
2. SME and small mid-cap providers of cloud services would benefit from meaningful grandfathering protections for contracts concluded before 12 September 2025, offering transitional relief from the cloud switching obligations.

3. Manufacturers and other persons receiving data from connected devices (data holders) would gain stronger (and more readily available) rights to refuse data access requests where disclosure risks exposing trade secrets to entities connected to third countries with insufficient legal protection.
4. The regime on access by public sector bodies to data from connected devices is restructured: the broad “exceptional need” framework would be replaced by a narrower regime tied almost exclusively to genuine public emergencies, potentially considerably reducing the risk of unsolicited governmental data requests.
5. Provisions closely related to those of the Data Governance Act (including rules on data intermediation services, data altruism organizations, data localization, and the re-use of public sector data) would be integrated into the Data Act, creating a more consolidated regulatory framework.

Cloud Switching: Limited Transitional Exemptions for Existing Contracts

Two new – and rather narrow – exemptions supplement the existing carve-out for fully bespoke services, offering transitional relief from the cloud switching obligations for contracts concluded on or before 12 September 2025.

- The first new exemption would apply to adapted standard services: where a provider has adapted the majority of a service’s features and functionalities to a particular customer’s needs, the full suite of switching obligations does not apply for the lifetime of any pre-12 September 2025 contract.
- The second exemption applies to all SME and “small mid-cap” providers of non-infrastructure data processing services. These providers are similarly exempt from the switching obligations for pre-12 September 2025 contracts.
- Both exemptions provide that the respective provider “shall not be required to renegotiate or amend a contract for the provision of those services before its expiry.” This may relate to Art. 29, which is still applicable for both exemptions and simply means that pre-12 September 2025 contracts that provide for switching charges or anything that is contrary to Art. 29 do not need to be amended. Compliance with Art. 29, or at least with its first three paragraphs, is still ensured as any terms in such legacy contract that contradicts Art. 29(1)–(3) would be null and void. It is unclear though where this leaves paragraphs (4) to (6) of Art. 29 and whether these provisions are enforceable for pre-12 September 2025 contracts.
- There are certain limitations to both exemptions – for example, infrastructure providers pursuant to Art. 30(1) do not benefit from them, and the Art. 29 switching-fee regime continues to apply as noted above.

Welcome as this transitional relief may be, its reach is limited. By introducing such limited exemptions rather than revising the regime itself, the Council left untouched the logically prior – and more fundamental – question of which services qualify as “data processing services” at all. That definition has been criticized as unclear, indeterminate, and broad, and its scope remains genuinely contested: whether it is read by reference to the underlying infrastructure or to the service actually provided to the customer may decide whether entire categories of providers – resellers and many software-as-a-service offerings in particular – fall within the switching regime at all. Neither the Commission nor the Council have clarified the rather confusing regime on the core of the switching obligations – i.e. whether a customer of a cloud service can require premature termination of any contract (even fixed-term contracts), or whether the customer can only require that the data that is subject to such contract, be transferred to a new provider or the customer.

Until guidance or the courts settle these points, providers must continue to self-assess against an uncertain standard, and the new exemptions would not relieve them of that burden. Ancillary operational questions also remain open, including which switching-related charges may still be levied once the charge ban takes full effect on 12 January 2027, and when a provider's measures suffice to deliver the "functional equivalence" the Data Act requires.

Clarity on Early Termination Penalties

The amended text introduces an express provision permitting all providers of data processing services to include proportionate early termination penalties in fixed-term contracts. While Recital 89 of the current Data Act already acknowledged this in passing, elevating the principle into the operative text of the Regulation may provide a materially stronger foundation for enforcement and remove any residual doubt as to compatibility with the broader switching framework. The substantive constraint would remain proportionality, and providers may wish to ensure their standard terms are drafted accordingly. The amendment does not, however, address how such penalties interact with the remuneration otherwise owed when a switch itself brings the contract to an end – a point on which the Regulation remains silent.

Stronger Trade Secret Defenses

Under the Data Act as currently in force, a data holder may refuse data access or data sharing requests by users only in exceptional circumstances and only where it can demonstrate that disclosure is highly likely to cause serious economic damage.

The proposed draft would significantly lower the threshold for refusing data access requests on trade secret grounds. The amendments remove the "exceptional circumstances" qualifier entirely, making refusal a more readily available tool rather than a last resort. The likelihood standard is also reduced from "highly likely" to "likely," and the factors by reference to which serious economic damage must be demonstrated are reframed as illustrative examples rather than mandatory criteria.

In addition, the proposal introduces a new ground for refusal where disclosure poses a high risk of trade secrets being unlawfully acquired, used, or disclosed by third-country entities (or EU-established entities under third-country control) in jurisdictions that do not offer equivalent protection to EU law. Together, these changes would provide data holders with a materially stronger and more flexible basis to decline access requests, particularly from counterparties with ties to higher-risk jurisdictions. Conversely, businesses relying on data access may anticipate greater resistance to requests with any cross-border element. The Commission is tasked with issuing guidelines on the practical application of these provisions; until those guidelines are published, businesses would need to exercise their own judgement.

What Was Not Changed?

The data sharing obligations imposed on "data holders" by the Data Act may still be burdensome for European device manufacturers and deployers. They still require a data license from the user, and any use of data generated by the connected device without that license would be illegal. The user may share the data with any third party for any purpose, but manufacturers and other data holders may share it with third parties only for "the fulfilment of their contract with the user." Also, neither the Commission nor the Council took the opportunity to amend and clarify the criticized "circular" definition of "data holder" (which still is defined as the person that "has the right or obligation (...) to use or make available data"). More broadly, several definitional and drafting ambiguities identified since the Data Act took effect remain unaddressed by the Digital Omnibus, including those addressed herein.

A Narrower Public Access Regime

The draft replaces the existing dual-track system in Chapter V, which permitted data requests both in genuine emergencies and where a public body could demonstrate an “exceptional need” for a specific statutory task, with a regime tied almost exclusively to genuine public emergencies such as public health crises, natural disasters, and major cybersecurity incidents. This also includes a need for data to support the recovery from a public emergency (post-emergency recovery). The previously available “exceptional need” basis for general public interest tasks, including routine statistical production, is removed entirely.

Personal data may only be requested in pseudonymized form and only where non-personal data is insufficient. Microenterprises and small enterprises are excluded from the requirement to provide data for post-emergency recovery purposes entirely and would gain an express right to claim compensation in the emergency response context – a right previously denied to them. The previously fragmented complaint mechanisms are consolidated into a single procedural route before the competent national authority.

Integration of Data Governance Act Elements

In Chapters VIIa to VIIc, the draft incorporates provisions closely related to those of the Data Governance Act (Regulation (EU) 2022/868) into the Data Act, creating a more consolidated regulatory framework. This includes a voluntary registration regime for data intermediation services and data altruism organizations, backed by a public register and a common EU label; a general prohibition on data localization requirements for non-personal data within the EU; and a comprehensive regime governing the re-use of data and documents held by public sector bodies – covering open public sector data, high-value datasets, research data, and certain categories of protected data. Businesses and public sector bodies active in these areas may wish to assess the implications of this consolidation for their existing compliance frameworks.

BEREC’s New Role

The Body of European Regulators for Electronic Communications (BEREC) would have a formal, coordinating role in the enforcement of the cloud switching provisions, facilitating exchanges between national competent authorities and disseminating best practices. This signals a closer alignment between cloud regulation and the telecommunications regulatory framework.

Next Steps

The amendments described above represent the Council’s current compromise position and are not yet final – further changes remain possible as the text progresses through the legislative process. That said, the direction of travel is clear, and businesses may wish to begin preparing now.

- Data holders should consider reviewing and strengthening their trade secret documentation and classification processes (since the new refusal rights would only be as strong as the evidence base supporting them) and assessing whether existing data access agreements adequately address the risk of onward disclosure to third-country entities.

- Data processing service providers should consider including proportionate early termination penalty clauses in their fixed-term contracts. Infrastructure data processing providers, particularly SMEs and small mid-caps, might want to test whether their services are subject to Art. 30(1) Data Act as this would have even more significance under the newly proposed regime.
- Businesses relying on data access may anticipate a more challenging environment, particularly where cross-border elements are involved, and may wish to review data access terms and build appropriate contingencies into their service models.
- Public sector bodies should consider reassessing their data acquisition strategies in light of the narrower public access regime, and identifying alternative legal bases or voluntary arrangements for tasks that no longer qualify.

Authors

This GT Alert was prepared by:

- **Viola Bensinger** | +49 30.700.171.150 | Viola.Bensinger@gtlaw.com
- **Jannis P. Dietrich-Webb** | +49 30.700.171.214 | Jannis.Dietrich-Webb@gtlaw.com

Abu Dhabi[†]. Albany. Amsterdam. Aspen. Atlanta. Austin. Berlin[~]. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Dubai[†]. Fort Lauderdale. Houston. Las Vegas. London^{*}. Long Island. Los Angeles. Mexico City⁺. Miami. Milan^{*}. Minneapolis. Munich[~]. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Riyadh^{*}. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo[»]. Seoul[»]. Shanghai. Silicon Valley. Singapore[°]. Tallahassee. Tampa. Tel Aviv[^]. Tokyo[°]. Warsaw[~]. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. †Greenberg Traurig's Abu Dhabi office is a branch of Greenberg Traurig, P.A., which is registered with the Abu Dhabi Global Market Registration Authority (Registration No. 29906) and licensed to carry out legal services and regulated as a DNFBP by the ADGM Financial Services Regulatory Authority. ~Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ‹Greenberg Traurig's Dubai office is operated by Greenberg Traurig Limited, a company registered in the Dubai International Financial Centre (Registration No. CL7238), regulated as a DNFBP by the Dubai Financial Services Authority and licensed by The Government of Dubai Legal Affairs Department. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legal Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. «Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. ›Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. °Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. °Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¢Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-Zimoch Wysockiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysockiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2026 Greenberg Traurig, LLP. All rights reserved.*