Digital Omnibus on the EU Data Act

This position paper presents the views of Swedish Enterprise on the Omnibus proposal amending the EU Data Act.

Summary

1. New definitions in article 2(4a), 2(4b), 2(13) and 2(58) require clarification.

2. Guidance on trade secret protection under the Data Act is needed. In addition, a revision of the Trade Secrets Directive should be carried out to improve the protection of trade secrets.

3. While Article 15a appropriately limits mandatory B2G data sharing, further clarification is needed to ensure that public bodies first attempt to purchase data and that emergency-shared data is excluded from reuse rules. Clear guidance on purpose limitation and compensation is essential, including coverage of actual costs and extending compensation rights.

4. New rules on contract modification obligations limit retroactive application for certain cloud and data processing services, though clearer criteria are needed to ensure predictable assessments across service types and contract structures.

5. The Omnibus maintains existing restrictions on third-country access to non-personal data, but further guidance is necessary given the broadened scope of affected actors.

Comments

The Digital Omnibus introduces a comprehensive revision of the Data Act by consolidating definitions and rules from related digital legislation.

The Confederation of Swedish Enterprise's analysis highlights opportunities for improved legal certainty but also identifies several areas requiring clarification to avoid legal and operational challenges for businesses.

1. New Definitions

Article 2(4a) "consent"

The introduction of this definition risks creating confusion and misinterpretation in relation to the Swedish Data Act, in which "consent" as used in Article 11 refers to civil law consent that does not concern personal data. Article 11 of the Swedish Data Act should therefore be amended to replace the term consent with a neutral civil law expression, such as *authorisation* or *approval*.

Article 2(4b) "permission"

The term permission appears in Article 5.6 of the Data Act and refers to situations where a third party approves the use of data that could otherwise affect their commercial position.

The incorporation of the Data Governance Act (DGA) definition gives "permission" a new and significantly narrower meaning that does not align with how the term is used in Article 5.6 of the Data Act.

To avoid misinterpretation, this term should be replaced, for example by *authorisation* or *approval*.

Article 2(13) "data holder"

The Digital Omnibus broadens the definition of a data holder to include actors who have the right or obligation to either use data or make data available. The definition risks becoming too broad and may include actors without actual access to relevant data, creating legal uncertainty. A clearer definition is needed, limiting the term to those who have genuine and lawful access to readily available data. This would prevent organisations with limited access from facing disproportionate risks or administrative burdens.

Article 2(58) "machine-readable format"

The definition drawn from the Open Data Directive (ODD) has practical consequences beyond Chapter VIIc, as it pertains to accessibility requirements in Chapter II of the Data Act. However, the definition does not reflect the technical realities covered by the Data Act. The ODD

SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

focuses on file formats, while the Data Act concerns product and service data transferred via machine-to-machine communication. This causes confusion, particularly regarding connected products such as vehicles.

The proposal to include a definition of "machine-readable data" should be rejected.

Alternatively, the definition should be amended by removing all references to "files" or by explicitly ensuring that it also covers data transmitted via any communication interface—whether located in a device or on a remote server.

2. Strengthened Protection of Trade Secrets

Protection of trade secrets is strengthened by allowing data holders to refuse disclosure if there is a "high risk of unlawful dissemination" to actors in third countries with weaker or non-equivalent protections compared with the EU. The purpose is to prevent trade secrets from being exposed in jurisdictions where legal protection and enforcement are inadequate, which could otherwise erode competitiveness and innovation.

While the proposal is important for Europe's competitiveness, companies may incur costs because they must assess the level of protection for trade secrets in foreign jurisdictions and demonstrate the risk of unlawful exposure. The Commission should therefore urgently issue guidance on trade secret protection under the Data Act, as previously promised. Such guidance would support companies in carrying out the required assessments.

Trade secrets are fundamental to data-driven products and services and play a crucial role in ensuring economic security and resilience and maintaining global competitiveness. From a competition perspective, it is equally damaging if information ends up with domestic competitors or with others abroad. Therefore, the revision of the Trade Secrets Directive, announced in the 2020 data strategy, must be implemented to further strengthen the protection of trade secrets.

3. Emergency Access to Data

The Omnibus proposal (new Article 15a) significantly limits emergency access to data to situations constituting a formally designated public emergency, while also tightening and clarifying the rules for compensation in cases of mandatory data sharing. Limiting mandatory B2G data sharing is welcome. It should, however, be clarified that public bodies must first attempt to purchase data before requesting access under Chapter V of the Data Act. Mandatory measures should not be used where commercial solutions suffice.

The broader definition of "data holder" under the Digital Omnibus means more entities may be required to share data during emergencies, which requires clear purpose limitation. Recital 70 underscores that such sharing must be strictly limited, as the data is often sensitive. It should therefore be clarified that data provided under Chapter V should not fall under reuse rules in the DGA or ODD, nor be treated as open data, except for official statistics at an aggregated level.

Article 20 clarifies that data sharing must be free of charge in acute emergencies for larger entities, although compensation may be available depending on company size or the type of request.

The Confederation of Swedish Enterprise considers that the compensation principle must be clarified so that compensation at least covers actual technical and organisational costs incurred when sharing data under Article 15a. Recital 75 should be adjusted to ensure consistency with the articles.

The right to compensation should also be extended at least to SMCs.

4. Contract Modification Obligations (New Provisions)

Article 31(1a) stipulates that obligations in Chapter VI do not apply retroactively to certain older contracts for data processing services. The Confederation of Swedish Enterprise supports this limitation.

To qualify for the exemption: (i) the service must fall outside Article 30.1 of the Data Act, (ii) the majority of the service's functions must be customised to the

customer's needs, and (iii) the contract must have been concluded by 12 September 2025.

It must be clarified what constitutes "the majority" of customised functions. Recital 98 provides limited guidance, and current guidance does not explain how Article 31 applies when a contract covers several different data processing services. It is unclear whether the assessment should apply at the service level, per provider, or at contract level.

Clearer criteria are necessary to avoid legal uncertainty and arbitrary decisions.

5. Protection Against Transfers Outside the EU (Revised Article)

Article 32x does not introduce any fundamental changes to the restrictions on transfers of or access to non-personal data in third countries. Nor does the amendment address administrative burdens for the purpose of compliance with the current overlapping regimes on data transfers.

If Article 32x is retained, further guidance is needed on its practical application (although some guidance is provided in the FAQs)—particularly considering the expanded group of affected actors.