

Bld. Brand Whitlock 114 B-1200 Brussels
hello@applia-europe.eu | www.applia-europe.eu
APPLiA Home Appliance Europe AISBL
Transparency number: 04201463642-88
VAT BE 0460 033 584

APPLiA's recommendations and amendments proposal for the Digital Omnibus: Data Act and GDPR



1. Data Act

While APPLiA supports the Data Act's goal of fostering a fair and innovation-friendly data economy, the regulation, as adopted, raises serious concerns over the protection of trade secrets and confidential business information. Mandatory sharing of potentially sensitive data with users and third parties lacks sufficient safeguards, creating legal uncertainty and competitive risks for the European industry.

1. Inadequate protection of trade secrets

The current "handbrake," requiring an agreement on technical-organisational measures (TOMs) with the user, is inadequate and practically unworkable, as it risks trade secrets being widely shared or aggregated to reveal confidential information through multiple data requests.

1. **Reversal of trade secret protection:** The Data Act shifts ultimate protection to the (often unknown) data recipient, making enforcement nearly impossible and increasing the risk of data leakage or reverse engineering by third-party competitors. Art. 4(6)-(12) and Art. 5(9)(12) Data Act allows users to request access to data generated by connected products and services, even if such data is protected as trade secrets.
2. **Ineffective TOMs:** Legal uncertainty surrounds what constitutes adequate TOMs. Measures like encryption, digital rights, or hashing do not reliably prevent malicious disclosure, and breaches of non-disclosure agreements are often undetectable. Unlike GDPR, where processors protect data in their possession, releasing sensitive data to multiple actors cannot realistically ensure protection after disclosure.
3. **High threshold for refusal and proof:** Under Recital 31, Art. 4(8), and Art. 5(11), demonstrating "serious economic damage" or "irreparable loss" ex-ante is extremely difficult. The potential financial risk, even with TOMs in place, may not be evident to the data holder before disclosure.



Data Act (EU 2023/2854)

Article 4 (1)

Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. This shall be done on the basis of a simple request through electronic means where technically feasible.

Article 4 (6)

Trade secrets shall be preserved and shall be disclosed only where the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding third parties. The data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata, and shall agree with the user proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.

APPLiA proposed amendments

Article 4 (1)

Where data cannot be directly accessed by the user from the connected product or related service, data holders shall make readily available data, as well as the relevant metadata necessary to interpret and use those data, accessible to the user without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge, in a comprehensive, structured, commonly used and machine-readable format ~~and, where relevant and technically feasible, continuously and in real-time.~~ This shall be done on the basis of a simple request through electronic means where technically feasible.

Article 4 (6)

Trade secrets shall be preserved ***in line with Directive (EU) 2016/943*** ~~and shall be disclosed only where the data holder and the user all necessary measures prior to the disclosure to preserve their confidentiality in particular regarding third parties.~~ The data holder or, where they are not the same person, the trade secret holder shall identify the data which are protected as trade secrets, including in the relevant metadata. ***The data holder, or where they are not the same person, the trade secrets holder may*** ~~and shall~~ agree ***voluntarily*** with the user proportionate technical and organisational measures necessary to preserve the confidentiality of the shared data, in particular in relation to third parties, ~~such as model contractual terms, confidentiality agreements, strict access protocols, technical standards and the application of codes of conduct.~~



Article 4 (7)

Where there is no agreement on the necessary measures referred to in paragraph 6, or if the user fails to implement the measures agreed pursuant to paragraph 6 or undermines the confidentiality of the trade secrets, the data holder may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay. [...]

Article 4 (8)

In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, that data holder may refuse on a case- by-case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product, and shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.

Article 4 (7)

Where there is no agreement on the necessary measures referred to in paragraph 6, ~~or if the user fails to implement the measures agreed pursuant to paragraph 6 or undermines the confidentiality of the trade secrets,~~ the data holder **can** may withhold or, as the case may be, suspend the sharing of data identified as trade secrets. The decision of the data holder shall be duly substantiated and provided in writing to the user without undue delay.

Article 4 (8)

The obligation to share product data and related service data in paragraphs 1 and 2 does not apply to data identified by the data holder or where they are not the same person, the trade secrets holder, as trade secrets within the meaning of Directive (EU) 2016/943. The data holder, or where they are not the same person, the trade secrets holder, may refuse a request for access to trade secrets relevant data. ~~In exceptional circumstances, where the data holder who is a trade secret holder is able to demonstrate that it is highly likely to suffer serious economic damage from the disclosure of trade secrets, despite the technical and organisational measures taken by the user pursuant to paragraph 6 of this Article, that data holder may refuse on a case- by case basis a request for access to the specific data in question. That demonstration shall be duly substantiated on the basis of objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, and the uniqueness and novelty of the connected product, and shall be provided in writing to the user without undue delay. Where the data holder refuses to share data pursuant to this paragraph, it shall notify the competent authority designated pursuant to Article 37.~~



Article 5 (1)

Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in real-time. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9.

Article 5 (1)

Upon request by a user, or by a party acting on behalf of a user, the data holder shall make available readily available data, as well as the relevant metadata necessary to interpret and use those data, to a third party without undue delay, of the same quality as is available to the data holder, easily, securely, free of charge to the user, in a comprehensive, structured, commonly used and machine-readable format and, where relevant and technically feasible, continuously and in realtime. The data shall be made available by the data holder to the third party in accordance with Articles 8 and 9. **This obligation does not apply to data identified by the data holder as trade secrets within the meaning of Directive (EU) 2016/943.**

Equivalent amendments to Art. 4 (6-8) to be made with regards to third-party access and trade secrets protection in Art. 5 (11).

2. Excessive temporal scope of application

Some obligations of the Data Act will apply retroactively to products and services placed on the market before September 2025, including the right to data access, the data-sharing obligation, and the requirement for the data holder to secure a right to use the data (Art. 4(13)). This poses significant challenges:

1. **Legacy data governance:** Older products were not designed with data management processes in place, making it difficult to identify, collect, process, and render data understandable. Technical systems for data access and transfer are often lacking.
2. **Identifying users:** Contacting data users for legacy products can be difficult or impossible.
3. **Obtaining data licenses:** Updating contractual terms with existing customers may be costly and complex, and refusal could prevent data holders from using essential data for diagnostics, product optimisation, or development of related services.



Data Act (EU 2023/2854)

Article 50 - Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 12 September 2025.

The obligation resulting from Article 3(1) shall apply to connected products and the services related to them placed on the market after 12 September 2026.

Chapter III shall apply in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which enters into force after 12 September 2025.

Chapter IV shall apply to contracts concluded after 12 September 2025.

Chapter IV shall apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are:

- (a) of indefinite duration; or
- (b) due to expire at least 10 years from 11 January 2024.

APPLiA proposed amendments

Article 50 - Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

It shall apply from 12 September 2025.

The obligation resulting from Article 3(1) shall apply to connected products and the services related to them placed on the market after 12 September 2026.

Chapter II shall apply to data generated, collected or in any other process during the use of a connected product or related service on or after 12 September 2025, unless otherwise contractually agreed between the parties.

Chapter III shall apply in relation to obligations to make data available under Union law or national legislation adopted in accordance with Union law, which enters into force after 12 September 2025.

Chapter IV shall apply to contracts concluded after 12 September 2025.

Chapter IV shall apply from 12 September 2027 to contracts concluded on or before 12 September 2025 provided that they are:

- (a) of indefinite duration; or
- (b) due to expire at least 10 years from 11 January 2024.



2. GDPR

APPLiA **opposes the introduction of Article 88a into the GDPR**, which seeks to transpose and 'modernize' the access rules currently found in Article 5(3) of the ePrivacy Directive. While intended to simplify the 'cookie' regime, this amendment creates a legal overlap for the home appliance sector. By shifting these rules into the GDPR, the Commission subjects physical terminal equipment, such as connected household appliances, to a rigid, browser-centric consent framework that was never designed for the Internet of Things (IoT).

APPLiA proposed amendment:

Removal of Article 88a from GDPR

Reference contact

Michał Zakrzewski *Senior Policy Director,*
Digital & Competitiveness
michal.zakrzewski@applia-europe.eu

Reference contact

Iulia Florea *Junior Policy Officer,*
Digital & Competitiveness
iulia.florea@applia-europe.eu