

DA.056 Right of user access

Authors: Winfried Veil

Last update: 2023-08-02 22:48:04 | By: Winfried Veil

Created at: 2022-02-22 09:25:45

Art. 4 Data Act - Triologue Agreement

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 metadata** that is necessary to interpret and use that data, **accessible to the user** without undue delay, easily, securely and in a comprehensive, structured, commonly used and machine-readable format, free of charge and, where relevant and technically feasible, of the same quality as is available to the data holder, continuously and in real-time. This shall be done on the basis of a **simple request** through electronic means where technically feasible.

1a. Users and data holders **may agree contractually on restricting or prohibiting the access, use or further sharing of data**, if such processing could undermine security requirements of the product, as laid down by Union or national law, resulting in serious adverse effect on the health, safety or security of human beings. Sectoral competent authorities may provide technical expertise in this context. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.

1b. Without prejudice to the user's right to seek redress at any stage before a court or a tribunal of a Member State, the user may, in relation to any dispute with the data holder concerning the contractual restrictions or prohibitions referred to in paragraph 1a:

(a) **lodge** in accordance with Article 31(3), point (b), a **complaint** with the national competent authority ;
or

(b) agree with the data holder to **refer the matter to a dispute settlement body** in accordance with Article 10(1a).

1c. **Data holders shall not make** the exercise of the choices or rights under this Article of the user **unduly difficult**, including by offering choices to the users in a non-neutral manner or by subverting or impairing the autonomy, decision-making or choices of the user via the structure, design, function or manner of operation of a user interface or a part thereof.

2. In order to verify the quality as a user pursuant to paragraph 1, a **data holder shall not require** the user to provide **any information beyond what is necessary**. A data holder shall not keep any

information, in particular log data, on the user's access to the data requested beyond what is necessary for the sound execution of the user's access request and for the security and the maintenance of the data infrastructure.

3. **Trade secrets shall be preserved** and shall only be disclosed provided that the data holder and the user take all necessary measures prior to the disclosure to preserve their confidentiality in particular with respect to third parties. The data holder or the trade secret holder when it is not the data 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.

3a. Where there is no agreement on the necessary measures or if the user fails to implement the agreed measures 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 without undue delay to the user. In such cases, the data holder shall notify the national competent authority designated in accordance with Article 31 that it has withheld or suspended the sharing of data and identify which measures have not been agreed or implemented and, where relevant, which trade secrets have had their confidentiality compromised.

3b. In exceptional circumstances, when the data holder who is a trade secret holder can 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, that **data holder may refuse on a case-by-case basis the request for access to the specific data in question**. Such demonstration shall be duly substantiated, based on objective elements, in particular the enforceability of trade secrets protection in third countries, the nature and level of confidentiality of the data requested, the uniqueness and novelty of the product, and provided in writing and without undue delay. When the data holder refuses to share data pursuant to this Article, it shall notify the national competent authority designated in accordance with Article 31.

3c. Without prejudice to the user's right to seek redress at any stage before a court or a tribunal of a Member State, the user wishing to challenge the data holder's decision to refuse, withhold or suspend the sharing of data in accordance with paragraphs 3a and 3b within this Article may:

(a) **lodge** in accordance with Article 31(3), point (b), **a complaint** with the national competent authority, which shall, without undue delay, decide whether and under which conditions the data sharing shall start or resume; or

(b) agree with the data holder to refer the matter to a dispute settlement body in accordance with Article 10(1b).

4. The **user shall not use the data** obtained pursuant to a request referred to in paragraph 1 **to develop a product that competes** with the product from which the data originate, nor share the data with another third party with that intent and shall not use such data to derive insights about the economic situation, assets and production methods of the manufacturer or, where applicable the data holder.

4a. The **user shall not deploy coercive means or abuse evident gaps** in the technical infrastructure of a data holder designed to protect the data in order to obtain access to data.

5. Where the user is not the data subject whose personal data is requested, any personal data generated by the use of a product or related service shall only be made available by the data holder to the user where there is a **valid legal basis under Article 6 of Regulation (EU) 2016/679** and, where relevant, the conditions of Article 9 of Regulation (EU) 2016/679 and Article 5(3) of Directive (EU) 2002/58 are fulfilled.

6. A **data holder shall only use any readily available data that is non-personal on the basis of a contractual agreement with the user**. A **data holder shall not use such data to derive insights** about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active.

6a. Data holders shall not make available non-personal product data, referred to in point (a) of Article 3(2), to third parties for commercial or non-commercial purposes other than the fulfilment of their contract with the user. Where relevant, data holders shall contractually bind third parties not to further share data received from them.