LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Things To Know About The European Data Act

By **Susan Kempe-Mueller, Elisabetta Righini and Thies Deike** (August 1, 2023, 3:24 PM BST)

The European Parliament and the Council of the European Union adopted the European Data Act on June 28 after lengthy negotiations.


Susan Kempe-Mueller

The Data Act creates a legal framework for a single European data market, and its key target is to facilitate the commercial exploitation of data generated by connected products, which was previously accessible only to the manufacturers of those products.

The act aims to regulate a complex and economically highly significant area. It raises many complex legal and technical questions, which also became apparent from the controversies around several core aspects of the act.


Elisabetta Righini

Here are the five things you need to know at this stage.

1. The act is about unlocking the economic potential of data.

The Data Act focuses on smart connected products in the Internet of Things. They produce large amounts of data with high economic value.

The act addresses data arising from a broad range of applications including, for example, industrial and agricultural machinery as well as private use like home automation, personal devices or medical products.


Thies Deike

The Data Act has extraterritorial application and applies to manufacturers who put their products on the market in the EU as well as data holders who make their data available in the EU.

Until now, due to technical barriers and the absence of a clear legal framework, access to the data generated by connected products has rested solely with the product manufacturers.

The European legislator has recognized that lack of access to this data may not only concentrate digital market power among a few large companies but could also hinder the development of new data-based business models or even preclude the business of entire economic sectors, like maintenance services.

The Data Act is part of the European data strategy and aims to enable a single market for data. It is designed to release the economic potential of this data and make it more widely usable by compelling data holders to make the data accessible.

Users of connected products and related services have to be given free and, if possible, direct access to data generated by their use in a structured, commonly used and machine-readable format.

If direct access is not feasible, data holders should make the data available to the users without undue delay and, if possible, continuously and in real time. The data also should be available to third parties that the users designate.

2. The new rules cover a range of issues, including data access for public authorities and interoperability.

Data of connected products must also be available to public authorities at national and EU level in the event of an exceptional need, such as a public emergency.

The act also requires that customers of data processing services, and especially cloud services, are able to switch to another service or an on-premise solution easily, among other things by specifying a maximum permissible notice period for termination by customers.

Providers of data processing services must take appropriate steps to prevent international data transfers and access by government agencies that would be unlawful under EU law, or the law of the member state concerned.

Last, framework conditions and standards for data interoperability are to be created based on the act to enable data exchange and joint data processing, for product development and research purposes, for example. This framework includes requirements for providers of smart contract applications for contracts on the provision of data.

After assessing existing standards, the European Commission may request European standardization organizations to draft new harmonized standards to ensure interoperability.

If that is not possible because the standardization process is blocked, the commission may adopt common specifications itself.

3. The data access remit is complex.

Applying the concept of connected products, determining the scope of the data covered and implementing third-party data access may be challenging in practice.

The Data Act excludes items whose primary function is to store, process or transmit data for third parties and mentions servers or cloud infrastructure as examples in this context.

The act covers raw data generated by the connected product, like sensor data and related metadata, but it does not cover information derived from that data through additional investment, in particular proprietary complex algorithms, or content that the user records, displays or transmits with the connected product.

Data use by third parties is likely more economically meaningful in practice than data access by the product user, but it also involves additional complexity.

In practical terms, the relationship between data holder, user and third-party data recipient with respective contractual agreements will likely generate issues when short-term access is needed, in the case of urgent repairs, for example. Further complexity arises if the user is not the owner but is renting the connected product.

At the user's request, the data holder must grant access to third parties and agree contractual terms and conditions with them to permit data provision. The data holder can demand appropriate compensation if the data recipient is a company, which must be nondiscriminatory and reasonable. If the recipient is a small to medium enterprise or a nonprofit organization, they data holder may not charge more than the costs of providing the data.

One of the biggest hurdles facing the Data Act's implementation lies in finding the right balance between free access to data and protection of the trade secrets of manufacturers or data holders — an issue highlighted during negotiations.

The act subjects the disclosure of trade secrets to the condition that the data holder and user take all necessary measures to protect and maintain their confidentiality, especially in regard to third parties.

If no agreement is reached on the necessary measures, or the user fails to implement agreed measures, the data holder can refuse or suspend the provision of the data classified as a trade secret. It must, however, inform the supervisory authority responsible for implementing the Data Act.

The Data Act will require manufacturers to technically ensure users of their products have direct data access and the use of common data formats during the development and production of connected products. If direct data access is not possible, data holders, who in many cases will also be the product manufacturers, will need to create a system for making product data and metadata available, if possible in real time.

The act requires nondiscrimination in providing data and prohibits the use of abusive contractual terms and conditions. It also instructs the commission to draw up nonbinding model contractual terms and conditions for data use.

4. The interplay with data protection laws and the digital markets act is challenging.

The act applies to both nonpersonal and personal data, but data protection laws including the General Data Protection Regulation also apply to personal data. The GDPR requires a legal basis for the processing of personal data, but these are not satisfied by the requirement under the Data Act.

This interplay may present challenges if the data to be made accessible under the Data Act is personal data of a third party who is not the user of the connected product given there is no interface to provide notices and/or user controls.

Data holders should assess carefully if the data they need to make accessible according to the Data Act would comprise personal data to avoid violating either the Data Act or the GDPR. The Data Act hardly provides any guidance on how the combined requirements of the GDPR and the Data Act can be practically fulfilled.

Violations of the Data Act or the GDPR will result in fines of up to €20 million ($22 million) or up to 4% of a company's annual global turnover, whichever is greater.

The Data Act also interplays with other regulations targeting the digital space, in particular the Digital Markets Act. The portability requirements of the DMA are expected to be applicable from March 2024. Under the DMA, companies designated as gatekeepers shall ensure portability of the data generated by the users of their core platform services.

This obligation overlaps with the data portability obligations under the Data Act. Hence, the gatekeepers likely will have already made data generated on their core platform services accessible before the Data Act becomes applicable.

The Data Act prevents gatekeepers from being granted access to data generated by the connected products. However, since the Data Act cannot limit the rights derived from other regulations, gatekeepers will still be able to access and use data made available under the DMA.

5. The next steps for practitioners.

The Data Act is a European regulation that does not require implementation by national legislators and will be applied directly in the member states 20 months after its entry into force, which is likely to occur in the next few months.

Manufacturers of connected products should begin preparing their devices to meet the requirements of the Data Act, drafting the necessary terms and conditions for agreements with users and third parties later on and diving deeper into the complex legal and technical issues raised by the act.

Susan Kempe-Mueller and Elisabetta Righini are partners, and Thies Deike is counsel at Latham & Watkins LLP.