The EU Data Act — what does it mean for controllers?

Sarah O'Brien, Managing Associate, and Alison Llewellyn, Senior Knowledge Lawyer, Stephenson Harwood, explain the practical implications of the EU Data Act for controllers

The European Union's new Data Act ('the Act') is a significant legislative development designed to foster a fair, competitive, and innovative digital environment.

The Act entered into force on 11th January 2024 and became legally effective on 12th September 2025. One of its main aims is to ensure that data generated by connected products (such as smart devices, vehicles, and industrial equipment) and related services (such as mobile apps the control the connected products) is shared more effectively, while also protecting the rights of individuals and businesses. Although it is not the focus of this article, the Act also includes provisions on switching and porting data between providers of data processing services (such as cloud providers).

Many organisations are already familiar with the GDPR. However, the Act introduces a separate set of requirements that, while overlapping with the GDPR in some areas, are distinct in their scope and application.

This article explains the practical implications of the Act for controllers. It outlines the roles of the various parties involved, explores the relationship between the Act and the GDPR, and provides guidance on steps controllers should take to ensure compliance.

Understanding the EU Data Act

The Act's main objective is to balance the interests of data holders, users, and data recipients by establishing clear rules on data sharing, particularly for connected products and related services. The principle underpinning the Act is that data generated by the use of such products should not be locked away by manufacturers or service providers. Instead, users should have meaningful access to this data, and, where appropriate, be able to share it with third parties.

The scope of the Act is intentionally broad. It covers both personal and non-personal data generated by connected products and related services. The Act applies to a wide range of stakeholders, including:

- data holders: entities with the right or ability to make data from connected products and related services accessible. This is often, but not always, the manufacturer or service provider;
- users: individuals or businesses that own or use the connected product, or receive the related service; and
- data recipients: third parties to whom data are made available at the request of the user.

The Act will apply to manufacturers of connected products and providers of related services placed on the market in the European Union.

Rights and obligations under the EU Data Act

At its core, the Act introduces new rights and obligations to facilitate access to and sharing of data generated by connected products and related services.

One of the most significant requirements is that connected products must be designed and manufactured so that data generated by their use is directly accessible to users. If direct access is not possible, the data must be made available upon request without undue delay. These obligations primarily fall on data holders.

This marks a shift from the traditional model where manufacturers and service providers had exclusive control over data. Now, users have explicit rights to access and use the data they generate.

The Act also requires data holders to make data available to third parties (data recipients) following a user's request. This is intended to promote innovation and competition, for example by enabling users to share

(Continued on page 10)

(Continued from page 9)

data with repair services or analytics providers. In exceptional circumstances, such as public emergencies, data must also be made available to public sector bodies and certain EU institutions.

Compared to the GDPR, the rights under the Act expand the concepts of access and portability. Notably, the Act applies to all data generated by the product or service, not just personal data, and is not dependent on the lawful basis for processing as required under the GDPR.

> ***"Compared to the GDPR, the rights under the Act expand the concepts of access and portability. Notably, the Act applies to all data generated by the product or service, not just personal data, and is not dependent on the lawful basis for processing as required under the GDPR."***

Practical scenarios for controllers

1. Controllers as data holders

Take the following example: a manufacturer of a smart watch sold to a consumer. The manufacturer is likely to be both the data holder and the controller, while the consumer is likely to be both the user and the data subject.

In this scenario, when responding to an access or portability request, the controller/data holder must:

- provide all data generated by the connected product and related service, not just personal data; and
- no longer assess the lawful basis for processing personal data to determine if the portability right applies; the right applies to all data generated, regardless of lawful basis.

If a third party provides the software for the watch and hosts the data, the third party is likely a processor on behalf of the manufacturer (the controller). Whether the third party also becomes a data holder is unclear under the Act, but it is generally more practical for the manufacturer to remain the data holder, given their relationship with the user.

If the user is a business rather than a consumer, the business still has access and portability rights under the Act, but not under the GDPR (since it is not a data subject). In such cases, the data holder/controller must still provide all relevant data but must also consider whether there is a lawful basis for sharing any personal data with the business user or a data recipient. The Act does not itself provide a lawful basis for sharing personal data, so this assessment remains necessary and fact specific.

2. Controllers as users

Some controllers will also be users of connected products. For example, a business that installs third-party telematics boxes in its company vehicles is a user under the Act and a controller under the GDPR, while the telematics provider is likely the data holder and a processor.

As a user, the business gains access and portability rights under the Act, even though it does not have these rights under the GDPR (since it is not the data subject). However, any personal data accessed or shared must still be processed in compliance with the GDPR. This includes identifying a lawful basis for processing, providing transparency to affected individuals (such as employees), and respecting data subject rights. This was the case prior to the Act.

The main impact of the Act for controllers who are also users is the new statutory right to access data that may not have been available under contract previously.

Additional considerations for controllers as data holders

1. Pre-contract information

Although not explicit in the Act, European Commission guidance suggests that a contract must be in place between the data holder and the user (such as a sales, rental, or service contract). Before concluding such a contract, data holders must provide users with a clear, comprehensive, and accessible description of the data generated and the user's rights to access and port this data.

Data holders should also be aware that they cannot use non-personal data generated by the product without the user's agreement. It is advisable to update terms and conditions to include a right for data holders to use such data for their own purposes.

2. Data sharing terms

The Act requires that the terms under which data is made available to data recipients must be fair, reasonable, and non-discriminatory. Data holders cannot impose unfair conditions or excessive fees. This is especially important in business-to-business contexts, where power imbalances could otherwise stifle competition.

3. Transparency to data subjects

Where the user is not the data subject, data holders should update their privacy notices to inform data subjects about any users or data recipients who may have rights to access their personal data.

Conclusion and next steps

Controllers subject to the Act should carefully assess and document their own roles and those of others under both the GDPR and the Act.

Once roles are clear, controllers should:

- update rights response proce-

dures and transparency documentation;

- prepare pre-contract information for users;
- develop template data sharing agreements with data recipients;
- review and update terms and conditions to reflect new rights and obligations; and
- conduct a lawful basis assessment for any personal data subject to an access or portability request, where the user or data recipient is not the data subject.

While the Act does not currently require controllers to redesign products to provide direct access to data, organisations experiencing an increase in rights requests may wish to consider future product redesigns to streamline compliance. Experience from the GDPR shows that responding to access requests can be time-consuming and costly.

By taking these steps, controllers will be better equipped to navigate the overlapping but distinct requirements of the Act and the GDPR. The key to successful compliance is to treat the Act as a complementary framework —distinct from, but closely linked to, the GDPR.

Sarah O'Brien and Alison Llewellyn
Stephenson Harwood LLP
alison.llewellyn@stephensonharwood.com
sarah.obrien@stephensonharwood.com