Access rights: GDPR vs the EU Data Act

Katie Hewson, Partner, and Sarah O'Brien, Managing Associate, Stephenson Harwood LLP, ***compare and contrast the access rights under the EU Data Act and the GDPR, and provide some practical guidance on how to navigate the differences***

The EU Data Act (the 'Act') is a law that aims to foster a fair and competitive digital economy within the EU by enhancing data sharing practices and safeguarding certain rights of individuals and businesses. The Act introduces rules on access to and use of data generated by connected products and related services placed on the market in the European Union (referred to collectively in this article as 'connected products'). These are products that can communicate product data via an electronic communications service, physical connection or on-device access. The Act applies to various stakeholders, such as manufacturers, providers, users, and third parties, who are involved in the data value chain of connected products and grants rights to access certain data generated by connected products. The Act applies to connected products placed on the market in the EU irrespective of the place of establishment of the organisation responsible for such placement. This means, like the GDPR, the Act has extra-territorial effect and will apply to UK-businesses that sell connected products or provide related services in the EU.

The GDPR on the other hand protects the rights and freedoms of individuals with regard to the processing of their personal data. It grants individuals (referred to as data subjects) a right of access to their personal data held by controllers, who are entities that determine the purposes and means of the processing.

Given the different objectives and scopes of the Act and the GDPR, the access rights under these two laws differ in terms of who can exercise them, who must comply with them, and what data must be provided. This article compares and contrasts the access rights under the Act and the GDPR, and provides some practical guidance on how to navigate the differences.

What are the rights of access?

Under the GDPR, a controller must provide a copy of all its personal data relating to the data subject requesting it without undue delay and in any event within one month.

Under the Act, the entity that has the duty to provide data is referred to as the data holder. The legal definition of a data holder under the Act is unclear and circular, but we understand from the recitals to the Act and from guidance from the European Commission that this could include the designer and/or manufacturer of the connected product and the provider of the related service. Data holders' access duties are, to the extent a connected product is not designed in a such a way to allow users to access data generated by the connected product, make such data available to the user on request without undue delay. In addition, data holders must make such data available to third parties nominated by the user ('data recipients') on request without undue delay.

Who is entitled to exercise the access right?

Under the GDPR, the right of access is granted to data subjects, who are natural persons whose personal data are processed by controllers or processors.

Under the Act, the right of access is granted to users, who are natural or legal persons who generate data by using connected products. Users can be individuals or businesses, and they can generate data that are personal or non-personal.

This means that the access right under the Act is broader and covers both individuals and businesses, and both personal and non-personal data.

Who must comply with the access right?

Under the GDPR, the obligation to comply with the access right lies with the controller, who must provide a copy of the personal data concerning the data subject. If the request is received by a processor, the processor must inform the controller, but the processor does not have to pro-

vide the data to the data subject unless otherwise agreed with the controller (such as via a Data Processing Agreement).

Under the Act, the obligation to comply with the access right lies with the data holder, who must make available both the data generated by the user's use of the connected product, plus the metadata to interpret the data, without undue delay. The data holder must also make such data available to third parties nominated by the user (data recipients).

As stated above, the obligation to comply with the access right under the GDPR is based on the role of the entity as a controller or a processor, whereas the obligation to comply with the access right under the Act is based on the role of the entity as a data holder.

> ***"However, the unclarity of the definition of a data holder may create some confusion as to whether a processor under the GDPR can also be a data holder under the Act."***

However, the unclarity of the definition of a data holder may create some confusion as to whether a processor under the GDPR can also be a data holder under the Act. This is true particularly given that the recitals of the Act suggest that processors are not considered data holders unless they are specially tasked with making data available by the controller — a concept that is not explicitly set out in the Act. This confusion, unless clarified, could cause issues with users obtaining data under the Act, where they request it from an entity that is also acting as a processor under the GDPR.

One option is for organisations to treat themselves as processors under the GDPR only in terms of the personal data they process on behalf of controllers, not the non-personal data they process. This would mean that, in response to an access request under the Act, a processor would be exempt from having to provide any personal data but would need to provide the user with non-personal data. If the request came from a user that is the data subject, the processor would need to notify the controller, an obligation that is typically included within a Data Processing Agreement, and the processor would need to provide its assistance to the controller to respond to the request. If the request did not come from a user that is the data subject, the processor would be under no obligation to provide the personal data.

Another option is for organisations to treat themselves as GDPR processors in respect of all data they process on behalf of a controller, despite the fact that the GDPR only applies to personal data. This approach would mean that, in response to an access request under the Act, the processor could be exempt from complying with the access right in its entirety. If the request came from a user that is the data subject, the processor would still need to notify the controller.

Neither of the above scenarios provide a satisfactory way for a user to exercise their right to access data under the Act and both would require the involvement of the GDPR controller in responding to an access request under the Act. This would mean that the controller would also need to be a data holder. But what if the controller does not have access to the data (for example, because its processor actually holds the data)?

Moreover, despite not being set out in the Act, the European Commission's guidance states that a data holder is typically the company that makes the connected product or that provides a related service, and that a data holder must have a contract with the user. However, this may not always be the case, especially when the connected product is manufactured by a third party on a white label basis, or when the related service is provided by a subcontractor or a licensee. In such scenarios, it may be difficult to determine who is the data holder and who is the processor, and whether the processor has to comply with the access right under the Act. This is where a clearer definition of a data holder would be helpful.

What data need to be provided?

Under the GDPR, only personal data related to the data subject requesting them need to be provided in response to an access request. This is limited in comparison to the Act, under which the data holder must make available the data generated by the user's use of the connected product and the metadata to interpret those data, regardless of whether the data are personal or non-personal.

Taking a connected activity watch as an example, under the GDPR access right, a data subject would be in entitled to information about their interactions with the manufacturer such as communications with the support team. However, they would not be entitled to this under the Act, as it wouldn't be data generated by their use of the connected product. To take an opposite example, the data subject could be entitled to information about the average battery life of the activity watch under the Act, whereas this wouldn't be likely to be available under the GDPR because it is not information relating to the data subject (it is about the watch).

What about where the user is not the data subject? For example, enterprise users of connected products.

An enterprise user does not have a right of access under the GDPR, but it does under the Act. However, where the data forming part of a request under the Act includes personal data, the personal data may only be made available where there is a legal basis for sharing such data under Article 6 GDPR (and Article 9 in cases of special category personal data). The Act clarifies that it does not provide a legal basis for personal data to be made

(Continued on page 12)

(Continued from page 11)

available.

How to navigate the access right under the GDPR and the Act

Mapping: As with everything that collects data, data mapping will be the key. Understanding what data the organisation holds, what data they control, where the data come from, who hosts them, and whether they are subject to the GDPR and/or the Act will be a good first step.

Procedures: Once there is a map of the data landscape, organisations can consider what procedures they need to implement to handle access requests without undue delay. If they are already controllers of personal data generated from connected products, they likely already have in place a procedure to deal with access requests. Organisations can consider updating this to include access requests under the Act. If they are manufacturers of connected products that do not collect personal data, organisations may not have any procedures in place to deal with GDPR access requests, and so will need to think about putting some in place to cover requests under the Act.

Organisations may even want to consider having separate procedures for dealing with rights requests from individual users and from business users, as the latter will require there to be a legal basis for sharing the data with a business user. Depending on whether they are processors, organisations should consider undertaking legal basis assessments to document their justification for sharing the data.

Contract terms: Under the Act, there are a number of prohibitions about what users can and can't do with the data they have access to from the data holder. For example, they cannot develop directly or indirectly a product that competes with the connected product from which the data originated. Data holders are only permitted to use non-personal data generated from the user's use of its connected product on the basis of a contract with the user.

Data holders should consider creating a data sharing template that includes the prohibitions on users' use of the data, and a consent from users for the data holder's use of the data. Data holders are also permitted to charge compensation for providing the data in most circumstances, so the obligation to pay and the payment terms could be added to these template.

Katie Hewson and Sarah O'Brien
Stephenson Harwood LLP
katie.hewson@shlegal.com
sarah.o'brien@shlegal.com