
Data Access Requests – More of the Same?



Data access requests are a well-known and often onerous aspect of GDPR. With the European Data Protection Board recently publishing draft new guidelines on Data Subject Access Rights, and the Health Access Modification Regulations also being updated, Sean O'Donnell and John Anthony Devlin ask has anything changed for controllers?

2022 has already seen important developments in the right of access: the European Data Protection Board (the EDPB) have published Guidelines 01/2022 on data subject rights - Right of access (the Draft EDPB Guidelines) and the Data Protection Act 2018 (Access Modification) (Health) Regulations 2022 (the 2022 Regulations) have been signed into law. This article highlights the key takeaways for controllers.

When are Data Controllers Obligated to Respond to Requests for Information?

The Draft EDPB Guidelines confirms that controllers have the obligation to respond to data subjects request for information without data subjects' giving data controllers a reason for submitting an access request. In other words, controllers should not assess "why" the data subject is requesting access, but only "what" is being sought. Neither is it up to the controller to analyse whether the request will actually help the data subject to verify the lawfulness of the relevant processing or exercise other rights. The EDPB considers it good practice for controllers to confirm receipt of requests in writing and confirming that the one month period runs from day X to day Y.

What are the Three Components of the Right of Access?

The EDPB explains the three components as follows:

1. Confirmation as to whether data about the person is processed
2. Access to the data, which does not depend on the type or source of the data
3. Access to information about the processing, such as purpose, categories of data and recipients, duration of the processing, data subjects' rights and appropriate safeguards in case of third country transfers.

What Personal Data can be Requested?

- Aside from basic personal data like name, address or phone number, a broad variety of data may fall within this definition like medical findings, history of purchases, creditworthiness indicators, activity logs or search activities.
- Pseudonymised data is still personal data as opposed to anonymised data.
- Personal data in the context of right of access should not be interpreted overly restrictively and may include data that could concern other persons too, for example communication history involving incoming and outgoing messages.

The guidance stipulates that the request must be fulfilled as soon as possible and in any event within one month of receipt of the request. This can be extended by two further months where necessary, taking into account the complexity and number of the requests. The data subject has to be informed about the reason for the delay.

What About Transparency Requirements?

- Controllers must ensure that information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Where the amount of data is very vast and it would be difficult for the data subject to comprehend the information if given in bulk – especially in the online context – the Draft EDPB Guidelines recommend making use of a layered approach.
- Controllers should consider what information the data subject would find most relevant when deciding what information to give, considering the different layers. In line with the fairness principle, the first layer should contain information on the processing which has the most impact on the data subject.
- Where a controller processes a large quantity of information they may request the data subject to specify the information or processing to which the request relates. This must not aim to limit the reply to the access request nor to hide any information.

When can Data Controllers Refuse to Give Access to Requested Data?

- Where the controller is not able to identify data that refers to the data subject, they must inform the data subject and they may refuse to give access unless the data subject provides additional information to enable identification.
- The controller is not obliged to acquire additional information to identify the data subject to comply with the request. However, controllers should not refuse to take that information. Any request for additional information must be proportionate to the type of data processed and factor in the damage that could occur through excessive data collection.
- The right to obtain data shall not adversely affect the rights and freedoms of others, whatever the means of access. The controller must be able to demonstrate the adverse effect on rights or freedoms.

Restrictions on the right of access may also exist in Member States' national law, and the 2022 Regulations are an important example of those restrictions. As with the 1989 Regulations (now revoked), the new 2022 Regulations limit the right of access under Article 15 GDPR where the information would be likely to cause serious harm to the physical or mental health of the data subject.


So What has Changed?

Much of what is set out above will be familiar to controllers. Nonetheless, there has to date been limited guidance on what the aim, scope and requirements of data access requests mean in practice. Controllers may find these obligations onerous;



for instance where the Draft EDPB Guidelines recommend controllers to give the broadest possible effect to the right of access, and to give “complete access” to the requested information, unless explicitly limited by the requesting data subject.

- Controllers must also have regard to the implications of the 2022 Regulations, in particular:
 - Under the 1989 Regulations, a controller was prohibited from supplying the information in question. Under the 2022 Regulations, the controller “may decide” not to provide the information. In practice, the distinction will require careful consideration.
 - Under the 1989 Regulations, a controller who was not a health professional was prohibited from supplying health data without consulting a health practitioner. Under the 2022 Regulations, a controller “may” consult with a health practitioner. The principle of data minimisation and the application of pseudonymisation also now explicitly apply when consulting with that health practitioner. The health practitioner must provide written advice when recommending withholding data, and this will also be subject to GDPR (and possible access requests).
 - Under the 2022 Regulations, access may be offered to a health practitioner on behalf of the data subject, similar to the mechanism under Section 37 of the Freedom of Information Act 2014.

The Draft EDPB Guidelines have been published for consultation and are subject to change, however controllers should begin to prepare now for their eventual adoption. Although not legally binding, the guidance is based on current case law and is indicative of the EDPB's position and understanding of GDPR. 



Under the 1989 Regulations, a controller was prohibited from supplying the information in question. Under the 2022 Regulations, the controller “may decide” not to provide the information