The new Guidelines on access requests — is the bar now too high?

Davinia Brennan, Partner with Matheson, examines the EDPB's draft Guidelines on access requests and asks an important question about their practical application

The European Data Protection Board ('EDPB') recently published draft Guidelines ('the Guidelines') on the right of access (www.pdp.ie/docs/11025), bringing some clarity to several operational aspects of responding to access requests. Whilst the Guidelines are informative, they raise the bar in regard to what is expected of controllers. In particular, the EDPB's rejection of any proportionality limit with regard to the efforts a controller has to take to comply with the data subject's request is surprising.

This article examines the new Guidelines and offers guidance on the steps that organisations should take in light of them.

Background

The right of access set out in Article 15 of the GDPR provides individuals with a right to:

- confirmation as to whether or not personal data relating to them are being processed;
- certain prescribed information about the processing of their data; and
- a copy of their personal data.

However, an individual's right of access is not absolute and is subject to certain statutory exemptions under the GDPR and Data Protection Act 2018 ('DPA 2018'). Whilst the Data Protection Commission ('DPC') has published general guidance on subject access requests including FAQs (www.pdp.ie/docs/11026), much uncertainty remains concerning about several operational aspects of responding to requests. The Guidelines have therefore been broadly welcomed.

Four key operational steps when handling access requests

Organisations generally take four key operational steps on receipt of an access request, including:

- assessing the validity of the access request;
- searching for personal data relating to the requester;
- considering whether any statutory exemptions apply; and
- responding to the request.

The Guidelines provide some helpful clarity in regard to these steps.

Step 1: Assessing the validity of the request

Form of the request: The GDPR does not require an access request to be in any particular form—a request can be made verbally or in writing, and does not need to refer to either the GDPR or the DPA 2018. Whilst controllers may request that individuals use standard or online forms in order to submit access requests, and Recital 59 GDPR even encourages this for electronic requests, the Guidelines warn that use of these forms should not be compulsory. Data subjects must also be permitted to make requests by other means, such as by post, email, or by telephone call.

Searching for personal data relating to the requester: Readers will be aware that under the GDPR, the scope of an access request for 'personal data' only covers personal data relating to the requester. Access by third parties to other people's data can only be requested subject to appropriate authorisation.

The GDPR definition of 'personal data' is very broad. It includes any information 'relating to' an identified or identifiable person. EU case-law and guidance from the Article 29 Working party (the predecessor to the EDPB) indicate that information will 'relate to' an individual where, by reason of its content, or purpose or effect, it is linked to a particular person. The Guidelines point out that the right of access extends not only to data provided by the data subject, but also data observed about the data subject by virtue of use of a service (e.g. transaction history), and data derived from other data (such as credit ratio). It also covers not just objective information about the requester, but also subjective information in the form of opinions and assessments.

'Undergoing processing': The right of access applies to any personal data 'undergoing processing' by controllers. The word 'processing' is defined broadly in the GDPR, and includes storage of personal data. It is not surprising therefore that the Guidelines assert that the right of access also applies in respect of archived and back up data where access to such data are 'technically feasible'.

Identity verification: Having a general policy of asking individuals for additional identity information when they exercise their data protection rights may result in GDPR violations due to the fact that the GDPR only permits proof of identity to be requested where there is 'reasonable doubt' about an individual's identity. Even where reasonable doubt exists, requesting a copy of official ID, such as a passport or driving licence, may be deemed to be excessive and in breach of the GDPR's data minimisation principle when there are other less intrusive authentication measures available, such as sending a verification email or code by text message.

The Guidelines emphasise that the method used for identity verification must be proportionate in light of the nature of the data being processed (for example, Special Category data), and the damage that could result from improper disclosure. Where an identity document is sought, the Guidelines recommend as good practice that the controller, after checking the ID document, makes a note that 'ID was checked', and avoids unnecessary copying or storage of copies of the ID.

In a case study in the DPC's Annual Report for 2021, the DPC warned that a request for official ID is only likely to be proportionate to validate identification where the data being processed are sensitive in nature, and where the information on the official ID, such as a photo, address, or date of birth, can be corroborated with the personal data already held by the controller.

We have seen Supervisory Authorities starting to take enforcement action against organisations for requesting excessive identity verification documentation, with the Spanish SA recently imposing a €240,000 fine, and the Dutch SA imposing a €525,000 fine.

Step 2: Searching for the personal data

Proportionality test: The most difficult part of responding to an access request is often deciding on the scope of the search for personal data. To date, there have been strong grounds to believe that a controller is only required to take reasonable and 'proportionate steps' to search for personal data, in line with the EU principle of proportionality. However, the Guidelines reject the application of any proportionality test with regard to access requests, adopting the view that as the doctrine of proportionality is not expressly referred to in Article 15 of the GDPR, it should not apply to access requests. If this view is endorsed in the finalised guidelines and enforced by Supervisory Authorities, it is likely that it will be subject to challenge in the courts.

Whilst the Irish courts have not to date considered whether the EU principle of proportionality can be invoked by a controller to justify limiting its duty to respond to a costly or burdensome access request, there are good reasons to believe that it is a legally permissible approach. The concept of proportionality is a core doctrine of EU law, and is specifically recognised by Article 5(4) of the Treaty of the European Union, and by the Court of Justice of the EU. In addition, Recital 4 of the GDPR acknowledges in clear terms that the right to data protection is not absolute, and has to be balanced with other fundamental rights, in accordance with the principle of proportionality. Its arguable that this means the right of access should be balanced against a controller's right to conduct a business under Article 16 of the European Charter of Fundamental Rights.

Asking data subjects to specify scope of requests: Whilst clarity from the courts on the application of the proportionality test to access requests is awaited, there are certain steps controllers can take to assist with responding to requests. In particular, where a controller processes a large amount of data relating to the data subject, it can request that the data subject specifies the information or processing activities to which the request relates (as per Recital 63 GDPR). However, if the data subject refuses to specify the particular scope of their request, the controller is obliged to provide all personal data relating to the data subject. This will effectively require the controller to search throughout all electronic information, and structured manual filing systems for any personal data relating to the data subject.

Use of search terms: The Guidelines state that when searching for personal data, controllers can use search criteria that mirrors the way in which the information is structured. For example, if the information is organised in files according to customer name or number, the search can be limited to those two categories. However, if data are organised by additional categories, such as professional titles or any kind of direct or indirect identifiers, the search should be extended to include these.

It appears that the controller is free to determine the most appropriate search terms to use in order to search unstructured electronic data and structured manual files. There is no requirement or recommendation in the Guidelines to agree these search terms in advance with the data subject. However, the Guidelines assert that the controller should always be able to demonstrate that its handling of an access request aims to give the broadest effect to the right of access.

Time reference point for reviewing data: Helpfully, the Guidelines confirm that the time reference point for reviewing data, in order to respond to an access request, is the point in time at which the request is received. However, where the controller is aware of additional processing or modifications to data between the time of receipt of the access request and the time of re-

(Continued on page 6)

(Continued from page 5)

sponse by the controller, then it is recommended that the controller includes information about these changes when responding to the request.

Once the controller has carried out a review of all documents containing personal data relating to the requester, the controller may consider whether any statutory exemptions apply.

Step 3: Exemptions

The Guidelines discuss two exemptions to the right of access that are set out in the GDPR, including that: the request is manifestly unfounded or excessive; and the request concerns third party data. Further exemptions are set out in Member States' national laws.

'Manifestly unfounded' or 'excessive': Article 12(5) of the GDPR allows controllers to refuse 'manifestly unfounded' or 'excessive' requests, or to charge a reasonable fee for such requests. Prior to the publication of the Guidelines, there was much uncertainty in terms of the scope of this exemption.

The Guidelines point out that as there are very few prerequisites regarding access requests, the scope of considering a request as 'manifestly unfounded' is rather limited. They also warn that the fact that a request requires a vast amount of time and effort, does not make it 'excessive'. The main reason that requests will be deemed to be excessive will be their repetitive character. However, the Guidelines highlight that a request may be deemed to be excessive in other circumstances, including where it is made only with 'the intent of causing damage or harm or disruption to the controller'.

Whilst a controller should not question the motivation of a data subject in making an access request, it appears that the controller is (to a certain extent) entitled to consider the motives behind a request, in order to ascertain if it can be refused on the basis that it is 'excessive'.

"The Guidelines assert that information in the privacy notice needs to be 'updated and tailored' to reflect the processing operations actually carried out with regard to the data subject making the request. If this approach is endorsed in the finalised guidelines, it will make responding to access requests an even more burdensome and time-consuming task."

Third party information

According to Article 15(4) of the GDPR, the data subject's right to obtain a copy of their personal data must not adversely affect the rights and freedoms of 'others'. This exemption effectively enables controllers to redact any personal data relating to third parties, where such disclosure would have a negative effect on them.

The Guidelines note that in principle, any right or freedom based on EU or Member State law, such as the right to confidentiality of correspondence with regard to private email correspondence in an employment context, may be considered to involve the limitation of Article 15(4) GDPR.

The Guidelines note that 'others' includes any person or entity other than the data subject, including the rights and freedoms of the controller or processor. However, not every interest amounts to 'rights and freedoms'. The Guidelines cite the example of the economical interests of a company, stating that as long as they are not trade secrets, intellectual property or other protected rights, these are not to be taken into account. The Guidelines warn that a general concern that the rights and freedoms of others 'might be affected' by complying with the access request is not enough to rely on Article 15(4) of the GDPR. Rather, the controller must be able to demonstrate concretely that in the specific situation, the rights or freedoms of others 'would factually be impacted'.

When a controller considers that complying with the request would have an adverse effect on others, it will need to carry out a balancing test, weighing the conflicting interests of the parties and taking into account the likely risks to their rights and freedoms. Where their rights cannot be reconciled, the controller will have to decide which of the conflicting rights prevail. This balancing test should be documented by the controller in line with the GDPR's accountability principle, and in order to be able to demonstrate to the competent Supervisory Authority on request that it carefully considered the conflicting rights of the parties.

Step 4: Responding

Time Limit: Organisations are required to respond to access requests without undue delay, and in any event within one month of receipt of the request. Helpfully, the Guidelines clarify that when a controller requires more information from a data subject in relation to the scope of a request or proof of their identity, there is a suspension in time until the controller receives the additional information.

Extension of time due to complexity or number of requests: Controllers can extend the response time by two further months where necessary, taking into account the 'complexity of the request' or 'number of the requests'. However, such extensions should be the exception rather than the rule.

Helpfully again, the Guidelines provide a non-exhaustive list of factors that are relevant in determining whether a request is sufficiently 'complex' to warrant an extension of time for responding. These include,

for example:

- the amount of data processed by the controller;
- how the information is stored, especially when it is difficult to retrieve it, for example when data are processed by different units of the organisation;
- the need to redact information due to exemptions applying (e.g. third party data); and
- whether the information requires further work in order to be intelligible.

The Guidelines assert that the mere fact that complying with the request would require 'a great effort' does not make a request 'complex'. Neither does the fact that a large organisation receives a large number of requests. However, when a controller temporarily receives a large amount of requests, for example due to an 'extraordinary publicity' regarding its activities, the Guidelines state that this could be regarded as a legitimate reason for prolonging the time of the response.

Its noteworthy that the DPC's guidance on access requests indicates that the response time can only be extended where the organisation receives a large number of requests from the same individual, however the draft EDPB guidelines do not provide such a restrictive interpretation.

Format of response: A controller is obliged to provide the personal data in an 'intelligible and easily accessible' form, in line with Article 12 (1) of the GDPR. In addition, Articles 12(3) and 15(3) of the GDPR provide that in the event of a request by electronic means, information should be provided in a commonly used electronic form, unless otherwise requested by the data subject.

The DPC's guidance on access requests goes further, and recommends that — as a general rule — controllers should respond to an individual's access request in the same way the request was made, or in the way in which the requester specifically asked for a response.

The Guidelines highlight the importance of the controller deploying appropriate security measures when responding to access requests, particularly when the response contains Special Category data, for example, by using registered post, or applying encryption, or password protection. In accordance with the GDPR's accountability principle, controllers should document their approach to responding to access requests, and be able to demonstrate how the means chosen to provide the necessary information under Article 15 are appropriate in the circumstances at hand.

Copy not original: According to the Guidelines, the controller has an obligation under Article 15(3) of the GDPR to provide a copy of the personal data undergoing processing, rather than reproduction of the original documents. The CJEU decided in the case of *YS* (C-141/12 and C-373/12), that the right of access under the former Data Protection Directive (95/46/EC) could be complied with by providing the data subject with a 'full summary' of the data in an intelligible form.

The Guidelines indicate that the CJEU's ruling remains relevant in terms of the scope of the right of access under the GDPR. However, they warn that the word 'summary' should not be misinterpreted as meaning that the compilation would not encompass all data covered by the right of access. Rather, it is a way to present all the data without systematically providing access to the actual documents.

Making some kind of compilation and extraction of the data that renders the information easy to comprehend is also a way of complying with the requirement to provide the information in a way that is both 'intelligible and easily accessible.'

Supplementary information: In addition to providing a data subject with a copy of their personal data, a controller is obliged to provide data subjects with a list of prescribed information about how their data are processed, such as information on the purposes of the processing and recipients of the data. This prescribed information is set out in Article 15(1) (a)-(h) and 15(2) of the GDPR, and largely reflects the information which must be included in privacy notices. As a result, it is common practice for controllers to discharge this obligation by including a link to, or a copy of, their privacy notice, or copying out relevant sections of a privacy notice when responding to an access request.

However, the Guidelines assert that information in the privacy notice needs to be 'updated and tailored' to reflect the processing operations actually carried out with regard to the data subject making the request. If this approach is endorsed in the finalised guidelines, it will make responding to access requests an even more burdensome and time-consuming task.

Conclusion

Although the Guidelines (once finalised) will not be legally binding on organisations subject to the GDPR, they do reflect the views of the EU Supervisory Authorities in terms of what is expected of controllers when responding to access requests. It would therefore be prudent for organisations to familiarise themselves with the finalised version of the guidelines in due course, and ensure their policies and procedures for handling requests are in line with the EDPB's expectations.

It will be interesting to see whether the finalised guidelines continue to reject the application of any proportionality test in relation to the effort a controller must expend on searching for personal data. It seems likely that it will ultimately take a court challenge in order to obtain legal certainty on this issue. In the interim, controllers should ensure they can demonstrate that their handling of a request aims to give the broadest effect to the right of access.

Davinia Brennan
Matheson
davinia.brennan@matheson.com