Subtle but helpful — changes to the right of access under DPDI 2

Olivia Whitcroft, Principal of OBEP, examines the 'tweaks' to the law in the current Data Protection and Digital Information (No. 2) Bill

In my last article for *Privacy & Data Protection* ('Handling Subject Access Requests: Then and Now', Volume 22 Issue 2, pages 3-5), I hinted that you may have to wait until 2031 before I wrote another update on subject access requests. Well, I have come back early to discuss the upcoming changes under the Data Protection and Digital Information (No. 2) Bill ('DPDI 2'). Some of these changes also impact the broader rights of data subjects.

Changes to UK data protection law that depart from the EU GDPR have been in the pipeline since Brexit. Government consultations on reforms in 2021 culminated in the Data Protection and Digital Information Bill ('DPDI 1') in 2022. Its stated aim was to "update and simplify the UK's data protection framework with a view to reducing burdens on organisations… while maintaining high data protection standards" (though question whether it is enough to keep the EU's adequacy decision for the UK). This Bill has been lingering now for well over a year. Technically, it was withdrawn in March 2023, and immediately replaced with the new and fresh DPDI 2. However, DPDI 2 was largely copied across from DPDI 1.

DPDI 2 stalled at the Report stage of the House of Commons, and at the time of writing, the latest published version is that produced following debate by the Public Bill Committee of the House of Commons. Standing at 220 pages long, one may assume that this a big overhaul of data protection law, reminiscent of the start of the GDPR in 2018. However, at least on the data protection (rather than digital information) side, a lot of the changes are more subtle; a few tweaks here and there to existing rules under the UK GDPR and Data Protection Act 2018. Nonetheless, some of the tweaks may have a significant impact on organisations which need to apply the relevant rules. In relation to rights of individuals, the changes may provide some helpful clarity for controllers.

Vexatious requests

In my previous article, I noted that the government was consulting on its proposal to lower the threshold required by the 'manifestly unfounded or excessive' exemption (under Article 12(5) UK GDPR). This exemption applies not just to the well-known and well-used right of access under Article 15 ('please send me a copy of all the data you hold about me'), but also to other rights of data subjects, such as the right to erasure, right to restriction of processing, and the right to object (among others). These all intend to protect important interests of individuals. However, they can be misused, creating disruption for an organisation or leading to excessive work which is disproportionate to the interests they are seeking to protect.

If an organisation can demonstrate that a request is manifestly unfounded or excessive, it may refuse to act on the request, or charge a reasonable fee for addressing it. In accordance with guidance from the Information Commissioner's Office ('ICO'), 'manifestly unfounded' means that the requestor has no intention to exercise their right, or the request is malicious and is just being used to cause disruption.

To give one example of where an organisation has sought to apply this exemption: an individual made a subject access request using aggressive language. The organisation considered that the request was being used to threaten the organisation rather than the individual genuinely wanting to access their data. The data subject's behaviour was consistent with this motive, but it was up to the organisation to demonstrate this. The individual does not need to specify or justify their reasoning for a request. The ICO considers that the word 'manifestly' means that there must be an obvious or clear quality to the unfoundedness, and use of strong language in itself is not sufficient.

There are concerns that the threshold is too vague or too high, and it can be a hurdle for organisations to back up an assertion that a request is unfounded. This is exacerbated by there being limited published examples or case law to assist with interpretation.

(Continued on page 8)

Olivia leads various training sessions for PDP, including 'Data Protection — Rights of Individuals', 'Data Protection by Design and Default' and 'How to Conduct a Data Protection Audit'. See the website for further information.

(Continued from page 7)

Section 8 of DPDI 2 changes the exemption to 'vexatious or excessive' requests (within a new section 12A UK GDPR). It provides examples of circumstances which should be taken into account to determine whether a request is vexatious or excessive, such as the nature of the request, the relationship between the parties, the resources available, and whether it is a repeat request. It also provides examples of when requests may be vexatious, such as those intending to cause distress, or those not made in good faith. In addition, the concept of a vexatious request is already well-known under UK freedom of information laws, and there are a wealth of published decisions which may assist in interpreting its meaning.

These changes may provide more clarity in applying the exemption. Readers should note that the changes also remove the 'manifestly' qualification for when a request is excessive. This also potentially makes it easier to demonstrate that a request is unreasonable or disproportionate in context.

If this makes it into the final version of DPDI 2, the change would of course mean that the wording is significantly different to the equivalent exemption under the EU GDPR. However, the ICO already interprets 'manifestly unfounded' more widely than the interpretation suggested by the European Data Protection Board (within its Guidelines 01/2022 on the Right of Access).

"It has always seemed strange to me that organisations would need to demonstrate that they hold a large quantity of data before having a legitimate reason to clarify a request. If more information is needed in order to find personal data, then surely more information is needed to find the data, regardless of how much data are held."

Time periods for responding to requests

Section 9 of DPDI 2 covers time periods for responding to requests from individuals to exercise their rights. In particular, it addresses the issue of when the one-month period starts (although one month is a maximum, and organisations must respond without undue delay).

ICO guidance currently assists organisations to determine this issue, which itself is partly based on equivalent rules under the Data Protection Act 1998.

DPDI 2 provides that the one-month period begins when the controller receives the request, or, if later, when it receives requested information to confirm the identity of the data subject, and any fee charged for a vexatious or excessive request.

In addition, if the controller asks the data subject for further information to clarify the request (see discussion on this below), the time between asking for the information and the information being provided does not count towards the one-month period. In other words, the clock is 'paused', which is consistent with the ICO's current guidance.

DPDI 2 also retains the ability to extend the time period by two months, where needed, due to the complexity or number of requests. In fact, it appears to duplicate this provision within the UK GDPR, which is potentially an oversight.

Charging fees for subject access requests

A proposed change within the government consultation document that did not make it through to the Bill was the introduction of a fee regime for responding to access requests, either by allowing a nominal charge for each request, or by having a 'cost ceiling' similar to the rules under freedom of information laws. The government's response to the consultation indicates that many respondents felt this could disadvantage more vulnerable people. Other respondents felt it may discourage vexatious requests, though the introduction of the 'vexatious requests' provisions described above (which allow for a fee to be charged), may assist with this concern.

Clarifying an access request

Section 9 of DPDI 2 makes a change to the rule currently found in Recital 63 of the UK GDPR, which allows a controller to clarify a request for access if it holds a large quantity of data. A controller may request that the data subject specify the information or processing activities to which the request relates.

In my experience, the first questions that always pop up in applying this rule are how much is a 'large quantity' of data, and where is the boundary between having a large quantity and a not-so-large quantity? The ICO's guidance indicates that the meaning of 'large' differs depending on the size of the organisation and the resources available to it. The intention of this guidance appears to be for organisations to consider how easy or difficult it is to find all personal data before seeking clarification. However, it could mean that individuals have a different right of access depending on whether their data are held by a large or small organisation.

It has also always seemed strange to me that organisations would need to demonstrate that they hold a large quantity of data before having a legitimate reason to clarify a request. If more information is needed in order to find personal data, then surely more information is needed to find the data, regardless of how much data

are held. One example of this issue is where an organisation has relationships with individuals in several different contexts, and it is unclear of the context(s) in which a request from a particular individual is being made. It may have identified the individual in one context (such as a customer of a particular department), but potentially hold personal data within other records, too. Without conducting overly-complex searches, the organisation may not know whether it holds any information in these other records, let alone large quantities.

Aside from the large quantities of data rule, I often suggest that organisations try to open up a dialogue with individuals to seek the clarity that they need. Case law and ICO guidance determine that the search conducted to find an individual's personal data must be 'reasonable'. What is reasonable in context may depend on what the organisation knows. If the individual provides additional clarity (such as they are looking for records of when they bought certain services between particular dates), this may lead to a different search approach to the situation where no clarity is provided.

Section 9 of DPDI 2 introduces section 12B(5) into the UK GDPR: "Where the controller reasonably requires further information in order to identify the information or processing activities to which a request… relates…the controller may ask the data subject to provide the further information…". It then goes on to refer to the processing of a large amount of information as an example of where further information may be reasonably required.

So rather than large quantities of data being the only reason that the law permits, other reasons may be okay, too. This is more similar to the previous rules under the Data Protection Act 1998, which allowed organisations to request more information needed to locate the personal data which the individual is looking for.

Organisations will still need to conduct a 'reasonable search', whether or not clarity is provided. However, one advantage of the change in DPDI 2 is more certainty over when it is acceptable to ask for clarity, and when the clock may be paused, as discussed above.

Confidence in applying the rules

We now await finalisation of DPDI 2, which is unlikely to be before 2024. As I raised at the beginning, the amendments to data protection law discussed in this article are more tweaks to the wording of existing rules, than a complete overhaul of data subject rights. However, they do make some significant changes to the practical application of the rules, and turn some ICO guidance into actual law. The changes may assist organisations to be more confident on when they are permitted to refuse an unreasonable request (or charge a fee), and when the rules allow them to ask more questions and pause the clock.

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.uk