VedderPrice

A Rise in DSARs: Why Can Data Subject Access Requests Be Such a Burden to Deal With?

By Rachel Easton

September 5, 2023

Under UK data protection legislation, individuals, also called "data subjects", have the right to make a data subject access request (DSAR) to organisations that "process" their personal data. Similar rights are required by both the EU's General Data Protection Regulation and the California Consumer Privacy Act. Amongst other things, as part of a DSAR, data subjects can expect to receive a copy of their personal data.

Results from the 2023 EY Law survey highlight that employers may see the number of DSARs increase, with 60% of those surveyed reporting an increase in DSARs over the past year. According to the survey, a contributory factor to this upwards trend is the UK's Information Commissioner's Office (ICO) campaign to raise awareness of access rights.

While DSARs are not a new right, they continue to be a challenge for organisations, quickly draining resources needed to deal with them. This begs the question of why they are such a burden to deal with. We explore this in more detail below.

The Initial Request

Many DSARs are presented as broad requests for "all personal data" held about an individual. This is often a huge undertaking for employers, who may find themselves processing a significant amount of personal data and storing that data in a variety of internal places. For employees, this data often goes back many years. Without further clarification on the scope of the request (or where clarification of the request does not prove helpful), a wide search involving a number of people may be necessary.

"Personal Information" and Locating It

"Personal information" broadly means information relating to a data subject. Given that definition, organisations will find such information in a variety of places, such as HR and payroll systems, social media platforms used for business purposes, personal data in emails and minutes, to name just a few. This puts a vast amount of data (located in a number of places) potentially within scope of the access request.

How an organisation finds the relevant personal information depends on the nature of the data itself, how/where it is stored as well as the organisation's approach to information management. While information stored electronically may be found and sorted easily, the potential volume of such data (and the usually unstructured nature of it) can make it a difficult task to tackle. Electronic information also may be held in harder to reach places, such as archived files or backups, which can add to the time and costs of accessing the information.

Testing Policies and Procedures

Access requests test an organisation's ability to locate personal data and can create internal conflict in situations where there is a risk of exposing limitations in the process or policies or procedures that are not working.

The ICO guidance states that organisations "should make reasonable efforts to find and retrieve the requested information". This might mean, for example, using targeted searches. Your organisation may well have a policy or protocol in place for locating information.

After locating the information, the next step would be to review and possibly redact (or look to rely on some other exemption). Such a step may require a variety of people within the organisation (and possibly external to it) and places demands on the business and those involved that go above and beyond "normal" day-to-day work. While technology can be used to assist, without a tested system in place to review and redact information, the ability to locate, review and analyse information within the timeframe remains a concern.

Timeframe

The organisation must respond to a DSAR without undue delay and in any event within one month of receipt of the request. Breaking down the one-month timeframe means that, on average, the organisation will only have between 20-22 working days to complete the request and respond to the data subject. When broken down to that timeframe, the efficiency needed to complete an access request on time is evident. Even a fine-tuned system, once overrun with bulk requests and high volumes of unstructured data, will be difficult to deal with within one (or even three) months of the request.

An organisation also will need to consider any period of leave for employees integral to the process or whether to consult with professionals concerning any required technical or legal assistance in order to complete the request.

Note that there is the possibility of extending the time limit for responding by up to two months if, for example, the DSAR is "complex". However, not every DSAR will be "complex". The ICO expressly states that "a request is not complex solely because the individual requests a large amount of information". The time also can be "paused", but organisations should only use this where it is genuinely required and the organisation processes a large amount of information on that individual. Neither method for extending the time should be used as a default reaction on receipt of a DSAR.

DSARs Being Used Alongside Tribunal Proceedings

It has long been the position of the ICO that it will not look at the motivation behind a DSAR when considering complaints by data subjects. Therefore, the time-consuming job of managing and dealing with tribunal proceedings alongside processing a DSAR can be resource heavy.

Preparation Will Be Key to Managing Any Challenges

The ICO reported over 15,000 subject access complaints last year. If organisations fail to respond to a DSAR within the time limit, they will likely be in breach of their obligations under Article 15 of the UK General Data Protection Regulation. This may lead to more than a fine or a reprimand from the ICO. The individual making the request is likely to be quite unhappy, and depending on the circumstances such individual may bring a subsequent claim against the organisation, and/or the ICO may wish to delve deeper into the organisation's data protection practices.

Whether or not your organisation receives a DSAR on a regular basis, the ICO states that it will be important to prepare and take a proactive approach to compliance. Consider your internal processes and whether they can be improved in light of the challenges noted here or the ones your organisation may have already come across. With the right tools and expertise, organisations can manage DSARs effectively and efficiently.

If you have any questions about this article, please contact Rachel Easton at reaston@vedderprice.com or any other Vedder Price attorney with whom you have worked.