Handling Subject Access Requests: Then and Now

Olivia Whitcroft, Solicitor and Principal of OBEP, takes us on a tour of subject access requests from 2001 to 2021, and discusses the most recent trends in how SARs are handled. Olivia is a Member of the Examination Board for the Practitioner Certificate in Data Protection (www.dataprotectionqualification.com)

Olivia leads the popular training session, 'Handling Subject Access Requests', which is available both live and on demand. For further information on the content and fees for this course, see www.pdptraining.com

Imagine it is the year 2001. The UK Data Protection Act 1998 ('DPA 1998') has been in force for a year, replacing the Data Protection Act 1984. Some of us are excited about data protection; most are not. Though the Information Commissioner's Office ('ICO') reports 12,000 calls over the year from individuals enquiring about their rights, subject access requests ('SARs') are relatively rare. My knowledge of SARs is therefore theoretical, rather than practical. The well-known *Durant* decision (*Durant v Financial Services Authority* [2003] EWCA Civ 1746) — which set limitations on the meaning of 'personal data' in the context of a SAR — would not be made for another two years.

Now, flash forward 10 years to 2011. There have been high profile data protection breaches in recent years including, in 2007, HMRC's loss of CDs containing child benefit data relating to 25 million people. Individuals are now much more aware of their rights. Subject access requests are common, and are the top reason for data protection complaints to the ICO (the ICO reported almost 6,000 SAR complaints from April 2011 to March 2012). There is also talk of a reform to EU data protection law, including new rights for individuals. The first draft of what was to become the GDPR was published in January 2012. Whilst *Durant* is still a leading UK case, both UK and EU guidance provide different ways to interpret 'personal data', expanding the recommended scope of searches for controllers to undertake when a SAR is received.

Meanwhile (still in 2011), my client has received a SAR from a former employee. The HR and IT teams have spent the last week combing through files and systems to try to find relevant personal data, including searching through 10 years of emails. They have photocopied the hard copy personnel file, and printed out other documents and communications in which the individual is named, or which refer to the individual or activities in which they were involved.

I arrive at my client's offices, and there is a big pile of papers sitting on the table in the data protection team's office. My client and I spend the day going through each document, and discussing the issues for each one. We need to wait until an HR colleague is back in the office in order to query the context of some records. Eventually, a large pack of paper is sent by courier to the data subject.

It is now 2021. The UK has left the EU, and has changed its data protection regime twice in the last 10 years, transitioning from the DPA 1998 to the EU GDPR (in 2018), and then on to the UK GDPR (in 2021).

SARs have consistently been the most common reason for data protection complaints to the ICO. Almost 18,000 SAR complaints were reported for April 2019 to March 2020 (though the ICO's Annual Report for 2020 to 2021 is less clear on this). There is comprehensive ICO guidance on the right of access, and there has been a significant amount of case law over the past decade. The legal regime, the use of SARs by individuals, and the approach taken by controllers all look substantially different to how they did 10 years ago.

I have a client who has received a SAR from one of its customers. Due to the Covid-19 pandemic, my client has been working from home, and accesses the relevant electronic documents remotely. There are no paper files and nothing has been printed out. I am sent background information electronically. We discuss some difficult issues over Microsoft Teams, and are able to add a colleague to the call to clarify some points. A response is prepared and records are uploaded to a cloud storage solution, from which the individual can download them for a fixed period of time.

Technology

As my examples demonstrate, there is now a lot more use of technology in addressing the right of access. Most controllers have fewer paper files, and make fewer print-outs of electronic records. We also communicate more online; there is less of a need to manage requests in a physical office; and less need to send out records or media in the post.

(Continued on page 4)

(Continued from page 3)

During a recent PDP 'Handling Subject Access Requests' training session in London, I asked for a show of hands as to who stored key records about individuals in paper files, and who regularly sent out responses to SARs in paper format. Though I asked my questions just before lunch and delegates may have been keen to get to the food, their responses were telling: only one raised their hand for paper files, and no one signalled that they sent out responses on paper. Although it was arguably a small sample, when leading this training session a few years ago, I recall that many delegates would raise issues about the use of paper records.

As well as advances in technology, there have been significant cultural developments affecting the way SARs are handled. Among these is, of course, the Covid-19 pandemic.

The law itself also has more of a focus on electronic solutions. For example, controllers have an obligation under Article 12(2) of the UK GDPR to facilitate the exercise of all rights, including the right of access. As many relationships are now conducted electronically, such facilitation often takes the form of online systems through which requests can be made.

In addition, where requests are electronic, Article 15(3) of the UK GDPR requires personal data to be sent in a 'commonly used electronic form'. Recital 63 provides that, where possible, the controller should provide a data subject with remote access to a secure system to access their data. And let's not forget that security rules require consideration of the 'state of the art', so up to date secure methods of sending data should be considered.

If you are reading this and worrying that you are not up to date with the latest technological innovations — don't panic! Other methods continue to be used, too. The ICO itself requests on its website that requests for access are made by good old email or telephone. And, if your relationship with individuals is primarily in person, or they prefer paper-based communications, providing access without using the latest technology may be preferable.

"An organisation may be considering an online facility to provide an individual with access to their data under the right of access. It can also consider expanding the facility to enable the dowload of data sets in the exercise of the right to data portability, which has stricter requirements for the format of data."

Technology can also assist with searches for personal data. Document management systems can ensure that records are stored and tagged in a way they can be located when needed, and deleted at the end of their retention period. Further, more sophisticated search tools and algorithms can help organisations to find particular data in response to a request.

On the flip side, technology has facilitated the creation and storage of larger and more complex sets of data, which can go hand-in-hand with more complex requests for access, as well as complications in the search for personal data within these sets.

Number and complexity of requests

Since the GDPR has applied, some organisations have faced an increase in the number and complexity of subject access requests. This may stem from a variety of causes, including: greater awareness of individuals; the removal of the £10 fee (which may previously have been a disincentive); the increase in complexity and scope of data processing activities; and companies setting themselves up to encourage individuals to make SARs to other organisations, and to make 'bulk requests'. The UK GDPR provides some assistance to organisations faced with burdensome requests: clarification can be requested where 'large quantities' of data are held, and the timescale for responding can be extended for complex requests. In the context of bulk requests, the ICO has also indicated that, in considering complaints, it will have regard to the volume of requests received and the steps taken to ensure they are handled appropriately. Despite all of this, organisations still face significant resources and costs in handling complex requests.

Another interesting provision to consider for SARs is the 'manifestly unfounded or excessive' exemption brought in by the GDPR, which allows controllers to refuse a request for access to personal data (or charge a reasonable fee to respond). When the GDPR was completely new, there was very little guidance on the circumstances in which this exemption could be used, and organisations needed to tread carefully in how widely they could interpret it. Now we have some more detailed guidance from the ICO (see my previous article 'Clarifying the right of access', published in Volume 21 Issue 2, of *Privacy and Data Protection*).

I was surprised to read the government's report that the ICO has indicated that organisations do not commonly rely on this exemption (see further below, under 'What do the next 10 years hold?'). This has cropped up a lot in my discussions with organisations! Where requests go beyond the purpose of the right of access and are used to cause disruption, or where they cause a disproportionate or unreasonable burden on a controller, the 'manifestly unfounded or excessive' exemption is a useful one to consider.

As most leading cases on SARs are still those decided under the DPA 1998, the scope of the exemption may not yet have been fully tested in the courts. However, it is interesting

to compare it to pre-GDPR decisions where courts were deciding whether to exercise their discretion to order a controller to comply with a SAR. Such decisions have determined that controllers should take 'reasonable' and 'proportionate' steps to respond to a SAR, taking into account the intended purpose of the right of access. For example, in the recent case of *Lees v Lloyds Bank plc* [2020] EWHC 2249 (Ch), the Court decided not to exercise its discretion against the controller on several grounds, including in consideration of the purpose of the SARs which had been made, and that the data subject's approach was abusive.

Now, if a request is manifestly unfounded or excessive, controllers can refuse the request by directly applying the exemption set out in the GDPR. However, its use must still be justified, and it is up to the controller to demonstrate the manifestly unfounded or excessive character of a request. The ICO and the courts can challenge a controller's decision to use the exemption if it is not used appropriately.

Exercise of other rights

The GDPR introduced a wide range of specific rights for individuals, including the right to data portability, the right to erasure, the right to rectification, as well as the already well-established right of access. The ICO's Annual Reports and related publications have, to date, provided limited information on ICO cases involving rights other than the right of access. Nevertheless, data subjects have been testing out these new rights, particularly the right to erasure. Individuals may combine their requests to exercise different rights, or they may follow on from each other (such as in the case of an objection or request for erasure following a subject access request).

Why is this relevant to an article about subject access requests? In order to handle requests consistently and efficiently, it can be helpful for organisations to consider their procedures for addressing rights together, as part of data protection by design. For example, an organisation may be considering an online facility to provide an individual with access to their data under the right of access. It can also consider expanding the facility to enable the dowload of data sets in the exercise of the right to data portability, which has stricter requirements for the format of data. Or, where appropriate, the organisation can give data subjects the ability to correct or erase data by means of the system. Information management procedures, identification procedures and measures designed to mitigate the risks of discrimination can also be designed with the full range of rights in mind.

What do the next 10 years hold?

On 10th September 2021, the UK government published a document called 'Data: A new direction', to consult on some proposals to update UK data protection law (and to depart from the EU GDPR). Chapter 2 contains proposals relating to the right of access. The government starts with: "The right of access is one of the fundamental rights in data protection legislation and the government will protect it". So it looks like the right is here to stay!

However, the government wants to help to ensure that controllers are "not overburdened by wide-ranging, speculative subject access requests". One proposal is to re-introduce a fee regime for responding to SARs, either by allowing a nominal charge for each request (similar to under the DPA 1998), or by having a 'cost ceiling' similar to the rules under the Freedom of Information Act 2000 ('FOIA'). If the costs of complying with a request would exceed this ceiling, controllers could then refuse the request or charge a fee for addressing it.

Another proposal is to lower the threshold required by the 'manifestly unfounded or excessive' exemption in order to refuse a request on that basis. The paper states: "the ICO has indicated that organisations do not commonly rely on this provision in order to justify a refusal to comply with a request or to charge a fee for compliance". Currently, controllers may find it difficult to demonstrate (for example) that the request has no real purpose and is being used to harass an organisation, particularly as a data subject is not required to provide specific reasons for their request. One suggestion is to introduce the concept of 'vexatious' requests (again similar to the FOIA regime).

The proposed changes appear to be favourable towards organisations, giving them greater scope to refuse requests, or to create additional obligations for data subjects. There is therefore a concern that the proposals may limit the right of access for those who genuinely wish to exercise their rights. Indeed, in its response to the government's report (on 7th October 2021), the ICO raised the importance of not undermining the right of access, and stressed that additional assessment of the benefits and risks of the proposals was required. The ICO highlighted equality issues, and the need to avoid disproportionate outcomes for vulnerable individuals.

The consultation was open for 10 weeks and closed on 19th November 2021. The government plans to publish its response in due course.

Perhaps see you in 2031 for the next instalment of this article?

Olivia Whitcroft
OBEP
olivia.whitcroft@obep.uk