Subject Access Requests and Investigations

Date : May 19, 2016

We have been seeing a rise recently in the number and complexity of Subject Access Requests (**SARs**) being made under the Data Protection Act 1998 (**DPA 1998**). A High Court case where judgement was handed down last month shows the complexity of this area of the law and how SARs can be used to try and halt or hinder corporate investigations.

What is an SAR?

The DPA 1998 gives individuals (called by the Act Data Subjects) the right (subject to exceptions) to access any information a Data Controller holds on them. There is a definition of Data Controller and Data Subject in our data protection glossary here (http://www.corderycompliance.com/eu-data-protection-regulation-glossary/)

In the UK, Data Controllers are entitled to ask for a small fee and they are entitled to ask the Data Subject to prove who they are but if they hold information they usually have to give the Data Subject a description of the personal data they hold, the purposes for that data being processed and the people they are likely to disclose data to. Section 7 gives Data Subjects various other rights and there are also more detailed provisions about redacting data. The Act also contains various exemptions which restrict the right to make an SAR.

What was this case about?

The case was brought by two Russian individuals Andrey Grigoryevich Guriev and Evgeniya Viktorovna Gurieva against a firm of private investigators, Community Safety Development (UK) Limited (**CSD**). Guriev and Gurieva made SARs under Section 7 of the DPA 1998 and they said that CSD did not reply. As a result Guriev and Gurieva issued proceedings under Section 7(9) of the DPA 1998.

It seems that the wider issue was an investigation and then a subsequent private prosecution brought by one of CSD's clients in Cyprus against Guriev and Gurieva. The larger dispute concerned a company called OJSC PhosAgro. Guriev was the Deputy Chairman of PhosAgro and he and his wife, together with their family were the main beneficial owners. PhosAgro was listed on the London Stock Exchange. CSD said that PhosAgro was founded by their client Alexander Gorbachev who fled Russia and was granted asylum in the UK in 2005. An Interpol arrest warrant was issued for Gorbachev but withdrawn in 2015. Gorbachev and a company called Marholm had instructed CSD "*in respect of claims issued and/or which may be issued*" against Guriev and Gurieva.

CSD wrote to Guriev in March 2015 saying that they had been instructed to "*conduct a criminal and regulatory investigation into the circumstances leading to the flotation of PhosAgro*". CSD's letter said that solicitors had been instructed but the letter came from CSD and not the solicitors involved. In the letter CSD asked Guriev for answers to various questions they posed. CSD's letter was unhelpfully written. It seemed to imply that Guriev had to answer questions asked by CSD "*under the provisions of the United Kingdom's Freedom of Information Act 2000*". It is hard to see why CSD thought the FOI legislation applied to either PhosAgro or Guriev. The Judge, Mr Justice Warby, described the letter as "*legally misconceived*". CSD later wrote a similarly ill-prepared letter to Mrs Guriev.

The SAR

Guriev and Gurieva issued an SAR in relatively standard form on 15 June 2015 through their solicitors. CSD responded within the statutory time limit saying that they had been instructed "*through*" their client's solicitors and "*as such, any relevant processing of personal data would be subject to legal privilege*". The firm of solicitors mentioned later wrote to Guriev and Gurieva's solicitors however to say that they did not act for CSD nor had they instructed CSD. They also said that they were not involved in the Cyprus proceedings that Gorbachev had started against Guriev and Gurieva.

In response to CSD's letter lawyers for Guriev and Gurieva asked CSD to confirm the basis of the privilege they asserted. CSD replied and said that the SAR had not been properly made. There was then somewhat extensive correspondence between the parties until proceedings were issued in October 2015.

What are applications under Section 7(9) of the DPA 1998?

If an individual makes an SAR which is not complied with they can essentially do one of two things:

1. Complain to the ICO who may investigate the failure to deal with the SAR; or
2. Issue court proceedings under Section 7(9).

The proceedings ask the court to order the Data Controller to comply.

It is important to remember that, for private companies at least, the courts have a discretion as to whether to grant a Section 7(9) request. There have been quite a few cases on Section 7(9) and the nature of that discretion - for full disclosure we have represented clients in litigation on s.7(9).

What was CSD's response?

CSD said that they held around 1500 documents which were responsive to the SAR. They sought to withhold some of the documents under s.29(a) of DPA 1998 which contains an exemption for personal data processed for the purposes of the prevention or the detection of crime or the apprehension or prosecution of offenders. They sought to resist the SAR for some of the documents because they claimed privilege. They also said that the court should refuse to grant the s.7(9) request using the general discretion it has. CSD also argued that it would be disproportionate to require it to seek legal advice on the privilege exemptions in respect of all 1500 pages.

The crime exemption

CSD sought to resist the SAR in part because they said that s.29 of the DPA 1998 provided an exemption where personal data was being processed for the prevention or detection of crime or the apprehension or prosecution of offenders. It is important to remember however that s.29 has an additional condition – in essence the exemption only applies "*to the extent to which the application of [the subject access right] to the data would be likely to prejudice any of the matters mentioned in this sub-section"* in short then to rely on the s.29 exemption disclosure has to be likely to prevent the detection of crime or the apprehension or prosecution of offenders. Our experience is that this part of the section is often missed. The Judge in this case also reminded CSD that if they were relying on an exemption like that the burden of proof was on them. The Judge felt that they had not met that burden. He also felt that CSD had not shown that disclosure would have any effect on the ability to prevent or detect crime or apprehend or prosecute offenders. CSD seemed to be trying to argue that disclosure would cause serious prejudice "*more widely to CSD's business*" as it would "*wholly undermine the work which CSD, and other organisations, carry out*". Clearly the Judge was right to ignore these objections. S.29(1) was not put in place to support private investigators to go about their business unchallenged.

What were the applicants entitled to see?

CSD, in common with many people receiving SARs, seem to have confused their obligation to provide information under s.7 with an assumed obligation to provide all of the documents they had. The Judge helpfully referred to a recent CJEU ruling in YS v. Minister Voor Immigratie, Integratie En Asiel which served as a reminder that the EU Data Protection Directive "*does not establish a right of access to any or every document or file in which personal data are listed or used*". Whilst documents are commonly provided the s.7 obligation can be met by redacted copy documents, transcripts or summaries. The obligation is limited to personal data as well and there is quite a lot of case law, some of which the Judge referred to in this case, on the meaning of personal data in this context**.**

Privilege exemption

Again in this case the Judge reminded CSD that the onus was on them to prove that privilege applied. The Judge

effectively said that CSD had not met that burden since they had not analysed the documents to work out which were covered by privilege and which were not.

Litigation - abuse of process/improper purpose

In this case CSD tried to rely on the important ruling of 2015 also given by the High Court in the Dawson-Damer and others -v- Taylor Wessing LLP and others case where, although the High Court decided that the discretion did not arise for the particular reasons given in that case, it also said that it would not in any event have exercised discretion and order compliance with a SAR on the grounds that the SAR in that particular case was made for the sole purpose of getting information for use in litigation and so was "not a proper purpose".

CDS argued that the SAR in this case was an abuse of process and/or made for an improper purpose. But the Court rejected this because *"such purposes could and would be thwarted by properly reasoned reliance on the privilege and crime exemptions"*, and, the judge concluded that *"even assuming (without deciding) that the doctrine of abuse of process is capable of application to a SAR and/or to proceedings under s 7(9), I find it hard to see how it could apply on the facts of the present case."* The court also made the interesting comment that it had *"difficulty with the notion that the use of an SAR for the purpose of obtaining early access to information that might otherwise be obtained via disclosure in pending or contemplated litigation is inherently improper"*.

It is understood that the *Dawson-Damer case is* being appealed and may be heard this summer - if so it will be of interest to see what the appeal court says on this particular abuse of process/improper purpose issue.

What did the Judge decide?

The Judge decided that the SAR is and was valid. He said

> *there was never any proper basis for questioning its validity. CSD's failure to disclose any personal data at all represents a breach of the Claimant's rights. The personal data held by CSD that relates to the Claimants may include some that is protected by the crime exemption, and some that is protected by litigation privilege, but it has not been proved that all of it is so protected*".

Lessons learned

There are a number of lessons to be learned from the case including:

1. Lawyers and their clients when dealing with investigations will need to rein in the activities of investigators and other non- lawyers instructed to assist in the investigation. From our experience it is relatively common for investigators to assert that they have privilege protecting their investigations – that is rarely the case.
2. Those commissioning an investigation need to choose their advisors wisely. Bad behaviour by an investigator can taint the whole investigation and lead to ancillary litigation like in this case.
3. Data protection has an increasing role to play in investigations. We are seeing those under suspicion seek to assert their rights at a much earlier stage in an investigation. We've been involved in one case where defendants in criminal proceedings in the UK sought access to documents using s.7 alongside the disclosure they had received in criminal proceedings so they could 'contrast and compare' the evidence against them. Whilst this claim did not reach court we've seen an increased level of aggression from some when seeking to exercise data protection rights.

The future of SARs

It should be remembered that when the new General Data Protection Regulation comes in in 2018 the SAR regime will change. SARs will become free and the time to respond will be tighter (albeit with the possibility of extensions). There are more details on the new SAR procedure in our GDPR FAQs here (http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/).

We are already seeing a considerable increase in the number of SARs and in some respects an unwillingness on behalf of requestors to pay the statutory fee. Dealing with SARs in a complex process and companies need a proper procedure in place to handle them. That procedure will include:

1. Checking that the SAR has been properly made;
2. Making an early search for the documents involved – our experience is that the first search rarely finds all of the documents that are needed;
3. Carefully considering issues like exemptions, redaction and the rights of others who might be affected;
4. Maintaining a dialogue with the requestor; and
5. Making sure the SAR is responded to appropriately and if possible within the statutory time limit.

Those responding to SARs also need to have appropriate training.

Details of Cordery's data protection practice and some of the recent SAR projects we have worked on are here (http://www.corderycompliance.com/data-protection-privacy/).

For more information please contact Jonathan Armstrong or André Bywater who are experienced in data protection matters.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com