Client Alert | Data, Privacy & Cyber Security / Technology

English court compels investigators to disclose information on data protection grounds

May 2016

Authors: Jonathan Pickworth, Tim Hickman, Joanna Dimmock

The High Court has ruled that a company conducting an investigation may be compelled to give effect to requests for information made under data protection legislation. The case serves as a stark reminder that data protection law is increasingly being used as a weapon by individuals affected by corporate investigations.

On 6 April 2016, the High Court of England and Wales issued its judgment in *Gurieva v CSD* [2016] EWHC 643 (QB), in which two individuals (the claimants), who were being investigated by a company (the defendant), asked the defendant to disclose the information it held about them, in accordance with the Data Protection Act 1998 (the "**Act**"). The court held that defendant was obliged to disclose the requested information even though it was clear that this disclosure might adversely affect the defendant and its client in future litigation. The potential impact of this case on corporate investigations is significant.

The key facts

The case relates to a dispute over a Russian company that is listed on the London Stock Exchange. The claimants are a married couple who, together with their family, are the main beneficial owners of that company. The defendant is a private company that conducts investigations and is run by several former police officers. The defendant was hired by a previous owner of the company to investigate the claimants for purposes including civil litigation and potential criminal proceedings.

Upon discovering that they were being investigated, the claimants issued a Subject Access Request ("**SAR**") under section 7 of the Act to the defendant. In the SAR, the claimants asked the defendant to provide information about the personal data about them that was being processed by the defendant.

The defendant rejected the SAR on a number of grounds. In particular, the defendant argued that:

- the requested information was protected by the exemption for the detection and prevention of crime (under section 29 of the Act);
- the requested information was subject to an exemption for legal professional privilege (under paragraph 10 of Schedule 7 to the Act); and
- the claimants were making the request for the purposes of discovering information to use in future legal proceedings between the parties which, according to the defendant, made the SAR an abuse of process.

The claimants challenged the defendant's decision to reject the SAR.

The decision

The court held that:

- **The defendant was not protected by the exemption for the detection or prevention of crime.** On the facts, the court found that although at least some of the personal data held by the defendant were being processed for these purposes, the defendant was also processing those data for other purposes, including civil litigation. Consequently, this exemption did not apply to the data processing activities performed by the defendant in the course of its investigation.

  In addition, in order to fall within this exemption, the defendant would have to show that the disclosure of the data requested in the SAR would be likely to prejudice the detection or prevention of crime. The defendant claimed that if it was forced to disclose this information to the claimants its work would be "wholly undermined". However, the judge dismissed this as "a clear exaggeration".

- **The defendant was not protected by the exemption for legal professional privilege.** The defendant had obtained a number of documents from solicitors instructed by their ultimate client. The defendant sought to argue that legal professional privilege applied to those documents. The court rejected this argument, pointing out that where investigators obtain copies of pre-existing documents, those documents do not thereby become privileged. It appears possible that the final investigation report could be protected by privilege, although the court did not comment on this point.

  The defendant also argued that it should not be required to review the 1,500 documents in its possession in order to work out which of them might attract privilege. The judge rejected that proposition, holding that "litigation solicitors are quite used to dealing with" reviews on this scale.

- **The claimants' reasons for requesting the information did not make the SAR an abuse of process.** The defendant sought to rely on a 2015 case, in which the High Court had refused to order compliance with a SAR on the grounds that the SAR in that case was solely made for the purpose of obtaining information for use in litigation. In the present case, the judge acknowledged that the claimants may have issued the SAR, in part, to see what the defendant's client "had on them". However, the judge held that because the claimants had not conceded that litigation was the dominant purpose of the SAR, and because the evidence did not show that that was their main purpose, there was no abuse of process.

Impact on corporate investigations

This case has potentially significant implications for corporate investigations, and could place significant additional burdens on companies. First, it is becoming ever-easier for individuals to use SARs as quick and inexpensive alternative to pre-action disclosure. Provided that such individuals do not admit that their primary motive is to obtain documents for the purposes of litigation, such SARs are often difficult for companies to resist. Secondly, the cost and administrative burden of complying with SARs can be significant, especially where there are large numbers of documents involved.

Thirdly, in the course of conducting an investigation, companies often gather together collections of information for review, including information obtained from third parties. All personal data under the company's control (including personal data about which the company might not have known, save for the investigation) are potentially subject to a SAR.

Fourthly, and perhaps most significant, where an investigation is conducted for a mix of purposes including, but not limited to, the detection or prevention of crime, the exemption in section 29 of the Act does not apply to all of the data that are processed. This point raises an anomaly for corporate investigations conducted by entities in the regulated sector. Where a corporate investigation is conducted by, say, a financial institution, the scope of the investigation will ordinarily encompass a number of outcomes including detecting the prevention of crime in relation to criminal wrongdoing, possible systems and controls failings within the organisation, together with disciplinary and employment issues. Under *Gurieva*, such an investigation would be deemed to have been conducted for a mixed purpose. However, it would be illogical to conclude that the section 29 exemption would fail to apply to a financial institution in circumstances where the provision of the personal data requested in the SAR would constitute a tipping off offence under s.333 Proceeds of Crime Act 2002 ("**POCA**") in respect of an individual or entity suspected of a money laundering offence. In these

circumstances, acceding to the SAR and breaching the tipping off provisions under POCA would constitute a criminal offence for those conducting the corporate investigation. This is a point which will need to be clarified in subsequent authority.

Meanwhile, companies conducting an internal investigation should, wherever possible, set out a clear statement of purpose at the start of such an investigation, specifying which activities are carried out for the purposes of the detection and prevention of crime, and those which are not. To the extent practicable, companies should avoid conducting investigations with mixed purposes. Where this is not practicable, companies should be aware that personal data processed in the context of an investigation, for purposes other than the detection and prevention of crime, may be subject to disclosure in response to a SAR.

It should, however, be noted that *Gurieva* does provide a few positives for companies conducting corporate investigations. First, the court confirmed that the exemption for the detection or prevention of crime is available to private organisations (albeit not on the facts of *Gurieva*). Second, as recently confirmed by the European Court of Justice, a company in receipt of a SAR is not obliged to disclose all documents that are responsive to the SAR. The disclosure of the requested personal data (extracted from documents that may contain other information) would be sufficient.

Going forward, it is important for any company that is conducting corporate investigations, and that receives a SAR, to carefully consider whether it is obliged to comply with the SAR, in light of *Gurieva*. Where it is necessary to comply with a SAR, organisations should ensure that they provide the requested information within the 40-day deadline specified in the Act.

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000