Client Alert: ICO Secures Criminal Convictions in Cambridge Analytica Subject Access Case

Date : January 10, 2019

Introduction

Yesterday's criminal conviction of SCL Elections, the parent company of Cambridge Analytica, shows the importance of dealing with data subject rights properly.

What is the background to the case?

The case concerns the investigation by the Data Protection Authority (DPA) in the UK, the Information Commissioner's Office (ICO) into Cambridge Analytica and its role in electioneering. The ICO investigation has involved 40 staff and 20 additional members of the investigatory team and has been wide-ranging. This investigation previously led in addition to what is thought to be the first enforcement action under GDPR in the UK against Canadian company AggregateIQ.

In this case the ICO were investigating a Subject Access Request (SAR) made by a US citizen, David Carroll. Professor Carroll had made a SAR to the company in January 2017. Since this was pre-GDPR he made the request under the old law, the Data Protection Act 1998 (DPA 1998).

In March 2017 he was provided with basic information, as well as a document containing predictions about him and his political opinions. He was dissatisfied with the disclosures made to him. He asked for further information from SCL, including the basis on which the predictions had been formulated, the source of information used to create the predictions, and the details of any parties with whom his data had been shared. He then asked the ICO to investigate. They wrote to SCL in September 2017.

SCL responded by claiming that as a non-UK citizen Carroll had no more right to submit a SAR "than a member of the Taliban sitting in a cave in Afghanistan". When the ICO informed the company that that was not their view the company replied, denying that the ICO had any jurisdiction or that Professor Carroll was legally entitled to his data, adding that SCL did "not expect to be further harassed with this sort of correspondence".

The ICO issued an Enforcement Notice ordering the company to comply in May 2018, shortly before GDPR came in. The ICO gave the company an additional 30 days to comply with the SAR. The company did not do as instructed and the ICO brought criminal proceedings to enforce its Notice.

What happened in court?

SCL Elections appeared before Hendon Magistrates Court yesterday. They pleaded guilty to an offence under s47(1) DPA 1998 of failing to comply with an Enforcement Notice from the ICO. This may be something of a pyrrhic victory for Professor Carroll and the ICO however as SCL Elections went into administration last May.

Counsel for the company's administrators told the court that the company's computer servers had been seized by the ICO following a raid on the company's premises in March 2018, but acknowledged that the company had still failed to respond to the Notice.

The District Judge fined the company £15,000 for failing to comply with an Enforcement Notice, and ordered it to pay a contribution of £6,000 to the ICO's legal costs, as well as a victim surcharge of £170.

What did the ICO say?

Commenting after the guilty plea the Information Commissioner, Elizabeth Denham, said:

"This prosecution, the first against Cambridge Analytica, is a warning that there are consequences for ignoring the law. Wherever you live in the world, if your data is being processed by a UK company, UK data protection laws apply. Organisations that handle personal data must respect people's legal privacy rights. Where that does not happen and companies ignore ICO enforcement notices, we will take action."

The ICO has also referred the company and its directors to the Insolvency Service. This could lead to an investigation into the company's activities despite its insolvency. Any investigation could also look at whether the directors had properly discharged their duties when running the company.

What did SCL say?

In a statement SCL Elections' administrators, Crowe LLP, said:

"At Hendon magistrates court today the administrators, as agents of SCL Elections Limited, represented the company in an action brought by the ICO against the company in connection with its failure to comply with a section 40 enforcement notice. The company pleaded guilty to the failure to comply with the enforcement notice whilst raising mitigating circumstances. The administrators confirmed that there are ongoing investigative matters, and have and will continue to fully co-operate with the ICO regarding the company."

What are the takeaways?

This case was decided under prior data protection law which has now been replaced by the General Data Protection Regulation (GDPR) and in the UK by the Data Protection Act 2018 (DPA 2018).

Lessons to be learnt from this case for compliance with the new regime include:

1. Regulators deserve respect – we have seen a few companies try and play hard and fast with DPAs. That's not likely to be a wise tactic. Occasionally you might disagree with a DPA and courts have been known to overrule a DPA's interpretation of the law but regulators deserve respect. Writing in the style the company did here is likely to exacerbate an already difficult situation.
2. Data subjects have rights and DPAs will help them enforce them. Data subject rights were extended under GDPR with new rights and an extension of the existing SAR regime. Our GDPR FAQs explain more about these changes – www.bit.ly/gdprfaqs
3. GDPR has wide extra-territorial reach. We've talked before about US corporations for example being subject to GDPR in most circumstances when they have dealings with the EU. The AggregateIQ case has shown the ability of DPAs to take action against non-EU companies. This case shows a further extension of GDPR by potentially permitting a non-EU resident to use GDPR to enforce data subject rights.
4. Under GDPR data subjects have a right to complain to a DPA (like the ICO) and/or bring their grievance to a court. A data subject can ask the court to enforce their data subject rights and can also claim compensation. Professor Carroll has already been admitted as a party in some litigation dealing with the company's administration when he said that his claim might be worth between £5,000 and £20,000. It may be that compensation claims will follow for any distress that may have been caused. In the UK civil actions like this are on the increase and notable cases include the Home Office spreadsheet case (see here for our article about it: http://www.corderycompliance.com/uk-appeal-court-ruling-on-spreadsheet-data-breach-damages-case-2/), the Morrisons supermarket case (see here for our article and film about it: http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds), and the Vidal-Hall/Google case (see here for our article about it: http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/).

We report about data protection issues, including data subject rights here: http://www.corderycompliance.com/category/data-protection-privacy/. For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our EU Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance – for more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact Jonathan Armstrong or André Bywater who are lawyers with Cordery in London where their focus is on compliance issues.

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 Farringd
Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com