Aven -v- Orbis UK High Court Ruling on Compensation for Distress caused by Inaccurate Processing of Personal Data

Date : August 11, 2020

Introduction

The High Court in London recently gave judgment in a data protection case linked to President Trump's involvement in Russia and the so-called 'Russia Dossier' or Steele Report.

In the case of Aven, Fridman & Khan -v- Orbis Business Intelligence Ltd, the High Court awarded £18,000 to two individuals of Russian or Ukrainian origin as compensation for breaches of data protection law for the distress caused to them by the processing of inaccurate data about them. This brief article highlights the issues in the case.

What's the case about?

The background is as follows:

- Messrs. Aven, Fridman and Khan ("the three individuals") were "businessmen of Russian or Ukrainian origin" and the beneficial owners of a Russian financial-investment conglomerate called the Alfa Group Consortium. Mr. Christopher Steele was (and still is) a director of the English insight, intelligence and investigative consultancy Orbis Business Intelligence Ltd ("Orbis");
- In 2016 Orbis was commissioned by a US organisation, via its US law firm, to investigate whether there were any links between Russia, Vladimir Putin and Donald Trump. As a result of its findings it produced a number of memoranda, including one in particular that was disputed by the three individuals. The memoranda included personal data in five propositions concerning the three individuals:

i. Putin and the three individuals doing significant favours for each other;
ii. Two of the three individuals giving informal foreign policy advice to Putin;
iii. One of the three individuals meeting directly with Putin shortly before 14 September 2016;
iv. Two of the three individuals using a particular individual to deliver large amounts of "illicit" cash to Putin when he was the Deputy Mayor of St Petersburg; and,
v. Two of the three individuals doing Putin's political bidding;

- The three individuals alleged that the processing of the personal data in question had been done in breach of both the fair and lawful principle and the accuracy principle under the UK Data Protection Act 1998 (DPA 1998) concerning the putting together and disclosure of material in the disputed memorandum in question to various third parties (government officials and organisations, politicians, a consultancy and a publication);
- Consequently, amongst other remedies sought (including rectification of alleged inaccuracies), they applied to the High Court for compensation.

What did Orbis say?

Orbis relied on both s.35(2) and s.28(1) of DPA 1998. Under s.35(2) it said that since the report was commissioned by an external law firm it was "for the purpose of obtaining legal advice". Under s.28(1) it said that the report was required for the purpose of safeguarding national security. It said more generally that the data protection principles were not breached and denied any remedies were due.

What did the court rule?

In a complex ruling, including about the scope and nature of the personal data in question along with the meaning of "illicit" in connection with what that suggested about two of the three individuals, the court decided that:

- The proposition about the alleged delivery of "illicit" cash was inaccurate and its disclosure by Orbis (which

had failed to take reasonable steps to verify this allegation) breached the accuracy principle. The judge said that "[…] the steps taken to verify that proposition fell short of what would have been reasonable. It is of a nature and gravity which are wholly distinct from and far more serious than the other four propositions. It relates to a period of time 15-20 years before the compilation of the memorandum. Mr. Steele knew that his source did not have direct personal knowledge of the underlying facts, but could only be relying on hearsay. He has failed to explain how that information would or could have come to the sub-source by virtue of his job. The allegation clearly called for closer attention, a more enquiring approach, and more energetic checking";

- No other breaches of the DPA 1998 were otherwise established – the other above-mentioned four propositions consisted of third-party information which Orbis had recorded accurately and had taken reasonable steps to verify; and,
- For this breach, two of the three individuals were each awarded £18,000 as compensation for the distress they suffered as a result; this appeared to also take account of reputational harm. Because the two individuals in question were (according to the judge) of "robust character, not given to undue self-pity" only "modest" damages for distress suffered as a result of the breach were seen as being appropriate. Although the judge granted a limited order for rectification of all the inaccurate data he declined to provide for the other remedies that the three individuals had also sought.

Data protection not defamation

It is interesting that this case was brought as a data protection case. Traditionally cases like this have been brought as defamation cases, in fact a defamation case was brought in the US in 2018 which involved similar litigants and similar portions of the Dossier. The DC Superior Court dismissed those proceedings. Additional litigation in the US seems to be still pending.

In the UK we have seen a rise in people trying to use data protection law when traditionally defamation law proceedings might have been threatened. Often the process starts with a subject access request and so organisations need to be on the alert and have proper processes in place to deal with these requests properly with an eye on possible future litigation.

What are the takeaways?

There are a number of takeaways from this case including:

1. Generally-speaking, the accuracy of personal data is not an issue that has received that much attention by courts or regulators – this case may therefore be a game-changer and shouldn't be seen as limited to the seemingly exotic facts.
2. Individuals are more willing to use their data protection rights. This includes individuals based outside the UK for example in Russia, Monaco or the Middle East. Organisations will need to be ready to deal with these complaints.
3. This case demonstrates that organisations must ensure that the personal data that they process (collect, use, disclose etc.) is accurate. Under Article 5(1)(d) of GDPR, personal data must be "accurate and, where necessary, kept up to date" and "every reasonable step must be taken to ensure that personal data that are inaccurate […] are erased or rectified without delay".
4. This case also shows that failing to check and keep personal data accurate can form the basis of a claim for compensation from aggrieved parties – we have written about compensation claims for breaches of data protection rules here https://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/. We also wrote about data protection damages in light of the Katie Price case here https://bit.ly/jordandp. This ruling also shows a certain benchmark for the level of compensation to be expected when infringements of data protection law causes distress. Organisations might also want to check their existing insurance policy (or consider taking one out) to see the extent of their cover for the full range of potential civil claims under GDPR.
5. Investigations into wrongdoing can be an especially tricky area. We've seen litigation on this previously in the Guriev case (see here https://bit.ly/guriev2) and we've written about these issues recently here https://bit.ly/gdprinvest.

6. Organisations should ensure that in their practices and documentation they are getting the message across about collecting and maintaining accurate personal data, and have in place procedures to quickly turn around the erasure or rectification of inaccurate personal data – a quick audit of this issue might reveal if action needs to be taken.

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.

For information about our Breach Navigator tool please see here: https://www.corderycompliance.com/solutions/breach-navigator/

We report about data protection issues 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 Data Protection Glossary which can be found here: http://www.corderycompliance.com/?s=glossary.

The court's judgement can be found here: http://www.bailii.org/ew/cases/EWHC/QB/2020/1812.html

For more information please contact André Bywater or Jonathan Armstrong 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