

Client Alert: UK Appeal Court Ruling on Spreadsheet Data Breach Damages Case

Date : July 25, 2018

What is this about?

Where data breaches have occurred those individuals affected by the breach may choose to bring claims for compensation/damages against the organisation that has committed the data breach.

In the UK cases are on the increase and notable cases include 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/>).

The recent appeal case of The Home Office and Secretary of State v TLU and TLV (2018) highlights the issue of compensation not only for those whose data was disclosed but also for people connected with them.

Some technical terms are used in this note which are explained in our glossary here <http://bit.ly/gdprwords>.

What is the background to the case?

In brief, in this case the UK's Home Office (the ministry dealing with interior matters) accidentally published online a spreadsheet which contained the sensitive personal details of individuals applying to the UK for asylum or permission to stay in the UK. The error was discovered after couple of weeks and the spreadsheet taken down. Several weeks later the UK's data protection authority, the ICO, was officially notified of the breach and later a statement was made in Parliament about the incident. The individuals named in the spreadsheet who were (still) in the UK were informed. The ICO did not take any regulatory action.

Individuals affected by this brought legal claims for damages for distress caused to them by the breach. They were awarded (by a court) sums ranging from £2,500 to £12,500. The wife and daughter of one of the claimants also succeeded in their claims – despite not being named on the spreadsheet, and the wife having a different surname to her claimant husband, they could be identified from the data of the claimant husband/father.

An appeal was brought concerning the issue of whether the Home Office etc. was liable to the family members of the main applicants and whether they could also claim compensation/damages.

What did the appeal court decide?

The UK Court of Appeal had no hesitation in upholding the lower court's judgement that the Home Office etc. was liable to the identifiable family members concerned along with the finding that the detailed personal information in question in the spreadsheet was enough to identify the family members in question.

What are the takeaways?

First, Article 82 of GDPR provides for a right to compensation from a data controller or data processor for anyone who has suffered "material or non-material damage" of a breach of GDPR (i.e. the right is not just limited to data breaches). Generally-speaking it is expected that compensation/damages claims will be brought in relation to GDPR and this Home Office case may serve as a precedent for this type of claim. Typically these claims will be for distress caused by e.g. a data breach and although in the past the amounts awarded have tended to be low in themselves, where a data breach affects many individuals the total amount claimed may be cumulatively significant.

Second, this judgement also shows how wide the definition of personal data can be.

Third, this case also highlights an all too common data breach which is caused through the disclosure to third parties of a spreadsheet containing personal data. The appeal judgment referred to the judgment of the lower court for the mechanics of what happened in the Home Office case as follows, stating that the second tab of the spreadsheet was accessible and:

“By error, the page on which this was displayed contained a further link to the spreadsheet. It contained details of 1,598 lead applicants for asylum or leave to remain. It is common ground that clicking onto that link would automatically download the spreadsheet onto the inquirer’s computer.”

The details were then downloaded and accessed by members of the public, one of whom uploaded the spreadsheet onto a US website, which was later taken down –although the relevant webpage was apparently accessed on 86 occasions the spreadsheet was not downloaded.

Our experience is that spreadsheets regularly feature in data breach cases and some DPAs have issued warnings on their use. To reduce risk organisations should consider limiting their use of spreadsheets, especially when sending them out as attachments to an email.

The case also highlights the need to act quickly when breaches do occur. To do this organisations must rehearse the handling of data breaches. There is more information on this here <http://www.corderycompliance.com/cordery-data-breach-academy/>. We know that in June 2018 alone the ICO received 1,792 data breach notifications. This shows that investment in a proper data breach handling process is also essential. There are more details of Cordery’s work in this area here <http://www.corderycompliance.com/dealing-with-a-breach/>.

We report about data protection issues, including damages, here: <http://www.corderycompliance.com/category/data-protection-privacy/>. For more information about GDPR please also see our GDPR FAQs which can be found here: <http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/>.

Cordery’s GDPR Navigator includes resources to help deal with data protection compliance including a specimen data breach reporting procedure and a short film outlining the security aspects of GDPR – for more on GDPR Navigator please see here: <http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/>.

The judgement in this case can be found here: <http://www.bailii.org/ew/cases/EWCA/Civ/2018/2217.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.

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com



[Jonathan Armstrong](#)

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

