Client Alert: Morrisons Data Breach Litigation Succeeds

Date : December 4, 2017

https://youtu.be/Uwp0iI6KLIM?t=2

On Friday judgement was handed down in one of the biggest pieces of data protection litigation in the UK so far - Various Claimants v. WM Morrisons Supermarket plc. The case established that employees of WM Morrisons Supermarket plc (a retail chain usually known as Morrisons) could succeed in getting financial compensation after a data breach caused by one of Morrisons' employees.

What was this case about?

The case was a group action (in some respects similar to a US class action) on the question of whether an employer is liable, directly or vicariously, for the criminal actions of a rogue employee in disclosing personal data relating to fellow employees on the internet. There were a number of aspects to the claim but in this alert we'll just concentrate on the aspects of the case which relate to the UK Data Protection Act 1998 (DPA 1998).

What was the data breach?

The data concerned a file with employee data on it which was prepared for Morrisons' auditors, KPMG. On 12 January 2014 a file containing personal details of 99,998 of Morrisons' employees was posted on a file sharing website. Shortly after that links to the file were put on the internet. On 13 March 2014 a CD containing a copy of the data was received by three newspapers in the UK. The person who sent the CD did so anonymously and said that they had discovered the payroll data on the internet and gave a link to the file sharing site.

The newspapers concerned did not publish the story, but instead one of them told Morrisons. The file contained names, addresses, gender, date of birth, home and mobile phone numbers, National Insurance numbers, bank sort codes, bank account numbers and salary details.

Morrisons' management was told immediately and within a few hours the file had been removed from the file sharing website. Morrisons called in the police. The investigation soon identified the source of the file as Morrisons' PeopleSoft HR Database and subsequently Andrew Skelton, a senior IT auditor at Morrisons, was arrested, charged and convicted. He was sentenced to eight years in prison in 2015.

Who brought the proceedings?

The proceedings were brought on behalf of 5,518 Morrisons' employees who brought various claims, including a claim for compensation under section 4(4) of DPA 1998. Their case was that Morrisons had primary liability for their own breaches of DPA 1998 and secondary (vicarious) liability for Skelton's actions.

Why did Skelton do this?

The court heard that as well as working for Morrisons, Skelton operated his own business dealing with the supply of slimming drugs. He used Morrisons' post room sometimes to post packages on behalf of this business. In May 2013 there had been an incident in Morrisons' post room which caused alarm and the police were called. Since the police suspected that another drug was involved, Skelton was arrested and escorted from the premises. He was suspended from work pending laboratory analysis but allowed to return to work in July 2013. He then faced a disciplinary hearing and was given a formal verbal warning. Skelton appealed internally but his appeal was rejected.

Why was Morrisons liable?

Perhaps surprisingly there was no expert evidence in this case. Whilst the court did not seem to hear expert evidence as to whether better systems or software could have prevented the breach – like DLP or data loss

prevention software or FTP or file transfer protocol software – the judge decided that Morrisons was not primarily to blame. The judge decided, however, that Morrisons were vicariously liable – in simple terms that they had to underwrite Skelton's actions as an employee. This was in part because they had selected Skelton for the trusted position of being the middle man in transferring the PeopleSoft data to KPMG. As the judge said:

"…I find that Morrisons deliberately entrusted Skelton with the payroll data. It was not merely something to which work gave him access; dealing with the data was a task specifically assigned to him. Associated with this, I find that in his role with Morrisons, day in and day out, he was in receipt of information which was confidential or to have a limited circulation only; and he was appointed on the basis that this would happen, and he could be trusted to deal with it safely. Morrisons took the risk they might be wrong in placing the trust in him."

Insurance

Another factor in the judge's reasoning seems to be the possibility of Morrisons being able to insure their risk:

"Morrisons are more likely to have the means to compensate the victim than Skelton and can be expected to have insured against that liability, even if breaches of data security may not historically have been a mainstream risk."

What happens next?

The trial was concerned just with whether Morrisons could be liable rather than in setting out the amount of compensation they had to pay. The judge gave Morrisons leave to appeal, and Morrisons has indicated that it will appeal.

In addition the UK's Data Protection Bill is still going through Parliament and this may make changes to the law in this area. There's an update and film on some of the proposed new UK law here http://www.corderycompliance.com/client-alert-uk-data-protection-bill/.

What does this tell us about civil actions under GDPR?

It is wrong to suggest that this is the first group action to be brought in the UK for data protection breaches. We have commented before about the rising number of data protection civil actions, for example in our summaries of the Google v. Vidal-Hall case here http://www.corderycompliance.com/vidal-hall-data-protection-class-action-appeal-settled/.

The solicitors who are handling the Morrisons case are currently advertising for more employees or former employees to join the litigation. In addition, they seem to be planning a number of similar actions including against a bank and an insurer. More litigation against other companies is likely.

Additionally, we are currently waiting on judgment from the ECJ in a class action brought by Max Schrems against Facebook. An opinion from the court's Advocate General on the 14 November suggests restricting the ability of claimants to bring proceedings on behalf of claimants across Europe, although that opinion is not binding on the court. The Schrems action has approximately 25,000 claimants. Final judgment in this case is expected by the beginning of 2018.

The issue of compensation is also important under GDPR. Under GDPR, as a general principle, any person who has suffered "*material or non-material damage*" due to an infringement of GDPR has a right to compensation from the data controller or processor concerned for the damage suffered. There are some defences, as set out in GDPR. Our FAQs and video on the GDPR can be found here www.bit.ly/gdprfaq.

What should businesses do now?

For most organisations continuing their GDPR planning is a good way of reducing the risk of civil actions like this one. In particular organisations will want to consider:

1. Taking a close look at security measures and ensuring that access rights etc. are policed;
2. Putting in place appropriate policies and procedures to make sure that data protection principles like data security and data minimization are properly understood;
3. Doing a DPIA for new processes – for example in this case would a DPIA have indicated that the request for data from the auditors was too wide?
4. Making sure that employees in trusted roles are reliable and that their access rights are reviewed if there are concerns – implement monitoring of employees as the business thinks necessary, in compliance with data protection and employee monitoring rules and guidance (see our article here about employee monitoring, data protection and human rights here http://www.corderycompliance.com/?s=barbelescu);
5. Putting in place a data breach notification procedure, including detection and response capabilities;
6. Training staff on all of the above; and,
7. Setting up and undertaking regular compliance audits or reviews in order to identify and rectify issues.

There is more information about this and other data protection topics in Cordery's GDPR Navigator subscription service. GDPR Navigator includes short films, straightforward guidance, checklists and regular conference calls to help you comply. More details are at www.bit.ly/gdprnav.

You can read a transcript of the case here www.bit.ly/2zLWG2l.

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