Client Alert: Court of Appeal confirms Morrisons' vicarious liability for the actions of its rogue employee

Date : January 14, 2019

Introduction

In October 2018 the UK Court of Appeal upheld a UK High Court ruling 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 – our article and film about the High Court ruling can be found here: http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds/.

What's the case about?

This case concerns a "group action" (in some respects similar to a US class action) as regards whether an employer is liable, directly or vicariously, for the criminal actions of a rogue employee who has publicly disclosed personal data relating to fellow employees. The case was decided under the UK Data Protection Act 1998, i.e. it is a pre-GDPR regime case.

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 informed Morrisons. The file contained names, addresses, gender, date of birth, home and mobile phone numbers, National Insurance (social security) 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 (who had previously been subject to disciplinary action over an incident), was arrested, charged (with various offences), convicted and eventually (in 2015) sentenced to eight years in prison.

Over 5,000 of Morrisons' employees later brought civil legal proceedings against their employer for Skelton's (malicious) misuse of their personal data; potentially there is liability to all 100,000 employees. The judge decided that Morrisons was not primarily to blame, i.e. it had not breached the UK Data Protection Act 1998 because adequate security safeguards were in place to protect the data. But, instead, the judge ruled that Morrisons was vicariously liable – in simple terms Morrisons 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. Morrisons then appealed the vicarious liability issue arguing the following:

- The UK Data Protection Act 1998 excludes vicarious liability, and so the judge had in effect gone legally too far in his ruling; and,
- Skelton's wrongful actions were not sufficiently connected to his employment to allow for a finding of vicarious liability (he used his own computer at home on a Sunday several weeks after having downloaded the personal data), and his malicious motivation (to harm his employer and not to harm others or achieve some gain for himself) was also inconsistent with a finding of vicarious liability.

What did the appeal court rule?

The Court of Appeal ruled that Morrisons was legally vicariously liable for Skelton's actions in that:

- The UK Data Protection Act 1998 (the Act) does not exclude the vicarious liability of an employer for the misuse of private information and breach of confidence by an employee, and the absence of anything in the

Act addressing the situation of an employer where an employee (data controller) breaches the Act, meant "the Judge was correct to hold that the common law remedy of vicarious liability of the employer in such circumstances (if the common law requirements are otherwise satisfied) was not expressly or impliedly excluded by the [Act]"; and,

- Although Skelton's actions were not performed whilst he was at work it was his working practices which had allowed him to be in a position to perform them. To this end the Court of Appeal directly quoted the words of the High Court judge that "there was an unbroken thread that linked [Skelton's] work to the disclosure [of personal data]; what happened was a seamless and continuous sequence of events. […]. This was no sequence of random events, but an unbroken chain beginning even before, but including, the first unlawful act of downloading data from his personal work computer to a personal USB stick"; in addition, the motive for causing harm to a third party was irrelevant.

Although this ruling leaves organizations potentially very exposed for the wrong-doing of others, for the appeal court the solution is to be properly insured:

- "There have been many instances reported in the media in recent years of data breaches on a massive scale caused by either corporate system failures or negligence by individuals acting in the course of their employment. These might, depending on the facts, lead to a large number of claims against the relevant company for potentially ruinous amounts. The solution is to insure against such catastrophes; and employers can likewise insure against losses caused by dishonest or malicious employees."

Quite whether the cyber insurance market in the UK is mature enough and experienced enough to be able to address this type of issue remains to be seen.

No decisions have been made yet on the amount of compensation and it is understood that Morrisons were trying to appeal before the UK Supreme Court. The Court of Appeal's judgment can be found here: https://www.bailii.org/ew/cases/EWCA/Civ/2018/2339.html

What are the takeaways?

The outcome in this type of case for a business is negative in financial terms (compensation and share price if it is stock exchange listed), and is also likely to affect reputation. To avoid such outcomes businesses should therefore consider doing the following:

1. Check your existing insurance or take out new insurance to cover potential risks from "innocent" errors to the actions of a rogue employee; update your data protection risk assessments accordingly;
2. Take a close look at security measures and ensure that access rights etc. are policed;
3. Put in place appropriate policies and procedures to make sure that data protection principles like data security and data minimization are properly understood;
4. Do a Data Protection Impact Assessment for new processes;
5. Make 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;
6. Put in place and rehearse a data breach notification procedure, including detection and response capabilities;
7. Train staff on all of the above; and,
8. Set up and undertaking regular compliance audits or reviews in order to identify and rectify issues.

The Morrisons case was decided under the previous UK data protection rules, but in our view it is likely that the findings would be the same under GDPR. Also, 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. We have written about data protection breaches and compensation/litigation here http://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/. We recently also wrote about data protection litigation against Google here http://www.corderycompliance.com/google-class-action-claim-rejected/.

For more of our reporting about data protection issues see 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.

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 hard copy and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.
- For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

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