Client Alert: UK Supreme Court ruling in Morrisons vicarious liability case

Date : April 1, 2020

Introduction

Today the UK's Supreme Court gave an important ruling in the Morrisons case concerning whether employees could succeed in getting financial compensation after a data breach caused by one of Morrisons' employees.

Whilst the Supreme Court ruled that an employer can be legally responsible (under the principle of 'vicarious liability') for data breaches caused by their employees it also ruled that in the particular situation at hand Morrisons was not vicariously liable for the actions of their rogue employee in this case.

We previously wrote about the Court of Appeal judgment here: https://www.corderycompliance.com/client-alert-court-of-appeal-confirms-morrisons-vicarious-liability-for-actions-of-rogue-employees/ and about the High Court ruling here which we also made a film about here: http://www.corderycompliance.com/client-alert-morrisons-data-breach-litigation-succeeds/.

What's the case about?

The salient background facts of this case are as follows:

- This is a "group action" (in some respects similar to a US class action) to decide whether an employer is liable for the criminal actions of a rogue employee who publicly disclosed personal data relating to fellow employees;
- The data concerned a file with employee data on it which was prepared for Morrisons' auditors. In January 2014 a file containing personal details of 99,998 of Morrisons' employees was posted on a file sharing website, after which links to the file were put on the internet, and then in 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 also 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 in 2015 he was 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 (this was pre-GDPR) 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;
- The case then went to the Court of Appeal which ruled that Morrisons was legally vicariously liable for Skelton's actions; and,
- The case then went to the Supreme Court, the primary issue being whether Morrisons is vicariously liable for Skelton's conduct.

What did the court rule?

The court ruled that:

- The Court of Appeal had misunderstood the principles governing vicarious liability in a number of respects. The online disclosure of the data was not part of Skelton's 'field of activities' as it was not an act which he was authorised to do. Skelton had been authorised to transmit payroll data to the auditors. His wrongful disclosure of the data was not so closely connected with that task that it could be regarded as made by Skelton while acting in the so-called 'ordinary course of his employment'. The fact that Skelton's employment gave him the opportunity to commit the wrongful act was not sufficient to warrant the imposition of vicarious liability. An employer is not normally vicariously liable where the employee was not engaged in furthering his employer's business, but instead is pursuing a personal vendetta;
- However, the Data Protection Act 1998 (the relevant legislation at the time of the breach) did not exclude the imposition of vicarious liability for either statutory or common law wrongs; the 1998 Act says nothing about a data controller's employer.

What are the takeaways?

Although this was a victory for this particular employer due to the given facts of the case, on the core legal issue of vicarious liability this ruling still leaves employers potentially exposed for the wrong-doing of others. In the Court of Appeal ruling it was declared that the solution was for organizations to be properly insured (albeit in the context of that court's decision that Morrisons was vicariously liable for Skelton's actions), but this is easier said than done.

In addition – and as pure speculation - the case could have gone differently on the issue of *primary* liability. Under GDPR there is a very strong emphasis on organisations having 'technical and organisational measures' (TOMs) in place to ensure GDPR compliance, including with regard to keeping data secure. Whilst the law was similar pre-GDPR it could be argued that employers should be more conscious of TOMs like access rights and data loss prevention now that GDPR is in force. With this in mind, had the Morrisons case been decided under GDPR might there have been a different outcome as regards *primary* liability and the personal data that left Morrisons' systems? Even in pre-GDPR cases data protection regulators have been keen to emphasise the importance of TOMs, such as the recent ICO Cathay Pacific case, which we have written about here: https://www.corderycompliance.com/ico-fines-cathay-pacific-for-data-security-breach/ and in the DSG case here https://www.corderycompliance.com/pc-world-owner-fined-after-data-breach/

Businesses should therefore consider doing the following:

1. Take a close look at security measures and ensure that access rights etc. are policed. Data loss prevention systems should also be in place to check for large data files leaving the organisation;
2. Put in place appropriate policies and procedures to make sure that data protection principles like data security and data minimization are properly understood. For example in this case should a more appropriate system have been put in place with the company's auditors?;
3. Do a Data Protection Impact Assessment for new processes;
4. 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;
5. Put in place and rehearse a data breach notification procedure, including detection and response capabilities;
6. Train staff on all of the above;
7. Set up and undertaking regular compliance audits or reviews in order to identify and rectify issues; and,
8. Last but not least, either check your existing insurance or take out new insurance to cover the range of potential risks from "innocent" errors to the actions of a rogue employee.

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 Supreme Court's Morrisons judgement can be found here: https://www.supremecourt.uk/cases/docs/uksc-2018-0213-judgment.pdf

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