Data breach and Morrisons: can a rogue employee leave you on the hook?

By Deborah Margolis - 20 November 2018

The UK supermarket chain Morrisons has been all over the press after it was held liable for a data breach by a rogue employee. This article analyses the judgment to set out what it means for employers.

The Background

The key question for the Court of Appeal here was whether an employer (in this case Morrisons) was liable where an employee committed a deliberate criminal act and disclosed personal data in breach of the Data Protection Act 1998. The High Court had previously held that the employer was not **directly** liable for the breach (except in respect of one small security point) but was **vicariously** liable to the 5,000 claimants that brought the claim.

(As a separate point, this case was decided under the old law, not under GDPR. Whilst this doesn't impact the substance of the case, it would affect the amount of the potential fine.)

The Facts

This was an unusual – perhaps even unique – case, so we have set out the facts below:

- Mr Skelton was an IT internal auditor at Morrisons. He was given a formal written warning in July 2013 and this incident left him with a grudge against his employer.
- On 1 November 2013, as part of his duties, Mr Skelton came into contact with some payroll data, which was saved on his desktop. A few weeks later, Mr Skelton copied the payroll data onto a personal USB with view to the subsequent commission of a crime.
- In January 2014, Mr Skelton copied the payroll data from his personal USB and posted a file (containing the names, addresses, gender, dates of birth, phone numbers, national insurance numbers, national insurance numbers, bank details etc) of 100,000 employees on the internet.

- A few months later, he anonymously sent a copy of the data to three newspapers and alerted them to the information on the internet.
- Not long afterwards, the activity was traced back to Mr Skelton and he was arrested and charged with criminal offences and sentenced to 8 years imprisonment.

The High Court

The High Court held that Morrisons was not the data controller in respect of the data at any time (i.e. Mr Skelton had become the data controller) and was therefore not directly liable to the claimants (except in respect of one small point on security). However, it held that Morrisons (as the employer) was vicariously liable for the data breach of the 5,000 employees that brought claims.

The Court of Appeal and Vicarious Liability

Morrisons appealed against the finding that they were vicariously liable for Mr Skelton's actions. In order to be successful, the individuals bringing the claims had to demonstrate that the act was within the "field of activities" that had been entrusted by Morrisons to Mr Skelton and that there was a sufficient connection between Mr Skelton's role and his wrongful conduct to make it right for Morrisons to be held liable.

Outcome

The Court of Appeal upheld the High Court's decision that Morrisons was vicariously liable for the actions for Mr Skelton.

On the first point, Morrisons had entrusted Mr Skelton with the payroll data as part of his role and as part of a task that had been assigned to him.

On the second point, the Court of Appeal upheld the High Court's decision that the close connection test was satisfied. We have drawn out a few notable points for employers:

- **It doesn't matter where or when the breach happened** - the High Court said that although the act that caused the harm was done at Mr Skelton's home on a Sunday, several weeks after he downloaded the data onto his own USB, there was an "unbroken thread that linked his work to the disclosure: what happened was a seamless and continuous sequence of events". The Court of Appeal said that it wasn't so much about the gap in time, but the change in the nature of relationship and the employee didn't need to be in the workplace or in working time for Morrisons to be vicariously liable.
- **No exception for motive** - there was no exception for Mr Skelton's motive (which was to damage the Company, and not to achieve some benefit for himself or to harm the individuals).
- **The solution is to insure** - the Court of Appeal said (in a slightly unusual comment) that the solution was for employers to insure against data breaches by employees.
- **Burden on employers was irrelevant** - in this case there was no harm, however in future cases if there was harm the individuals would be able to claim against the employer.
- **Data protection group litigation** - this is the first example of data protection group litigation the UK, might it be the start of things to come?

Morrisons have said that they will appeal this case to the Supreme Court – keep your eyes peeled for the next instalment!

To mark six months of GDPR, we are holding a webinar on 27 November 2018 which will include some discussion of breach notification. Please register here to sign up for it.