You are liable for data breaches by rogue employees regardless of how much care you take

By Daniel Pollard - 21 December 2017

The case of *Wm Morrisons Supermarket PLC v Various Claimants (2017)* arises out of the well publicised data breach by supermarket Morrisons (the fourth largest in the UK). Personal data relating to 100,000 employees was posted on the internet by a former employee. The data included names, addresses, bank account information, national insurance numbers, salary and contact details.

The rogue employee was an internal auditor who was entrusted with transmitting the entire employee data set to external auditors. The employee concerned has been convicted of offences under the Computer Misuse Act 1990 and under the Data Protection Act 1998 and sentenced to a term of 8 years imprisonment.

This case concerned a claim for compensation by 5,000 impacted employee data subjects against Morrisons. It is the first case in the UK of its kind and addresses important issues of liablity by employers for the malicious acts of insiders.

The claim was brought on two alternative basis. First, as a breach by Morrisons of its obligations under the seventh data protection principle to adopt "*appropriate technical and organisational measures*" to protect the personal data controlled by it. Secondly, on the basis that the rogue employee was personally liable for common law breach of confidence and that Morrisons was variously liable for the actions of that employee under ordinary common law principles of vicarious liability.

The High Court found for the data subjects on the second but not the first basis. This is significant because – if this is right – it means that the common law effectively imposes **strict liability** for breaches of rogue employees. This is a far higher standard than imposed under data protection law which effectively imposes an obligation to take reasonable case. This aspect of the judgment is being appealed.

This is the first case in the UK where the courts have unpacked the data controller's duty under the seventh data protection principle and the following points are of interest:

1. The High Court held that when determining what security measures were *appropriate* the nature of the data and the quantity of it will be relevant. Thus the measures that a large employer with 100,000 records must take are significantly greater than those of a smaller employer. This is interesting but not surprising.

2. There was a detailed discussion about whether or not Morrisons was breach of the seventh data protection principle as a result of entrusting the data to this particular employee. This turned on whether Morrisons knew, or ought reasonably to have known, that he harboured a grudge against them as a result of disciplinary action that they had recently taken against him. On the facts Morrisons were held to be on the right side of the line but it illustrates that employers may have to justify why they entrusted data to certain individuals. Traditionally, whilst this might be a factor in selecting a data processor, little consideration will have been given to the fidelity of employees.

3. The vulnerability exploited by the employee was that the personal data was to be extracted from PeopleSoft and transmitted by an (encrypted) USB key via the rogue employee's personal computer. It was from this device that he likely copied the data. Morrisons was found to be in breach of the seventh data protection principle by failing to have a process to ensure that the data was deleted from the rogue employee's personal computer. Whilst Morrisons was in breach, no loss followed on these facts but in another case this could be significant and employers may need to consider taking steps to verify that data is deleted by trusted employees.

4. Morrisons was not criticised for the transfer process per se but employers should carefully consider how non-routine transfers such as this are managed. By extracting the dataset from Peoplesoft, Morrisons lost the audit trail that would otherwise have quickly identified the person responsible (and, with the right software, could have possibly prevented it. Employers might also consider disabling USB devices on personal computers all together.

The seventh data protection principle is, in practice, the most significant of the duties imposed by the Data Protection Act 1998. Effectively it imposes a statutory information security standard. Almost all of the large monetary penalty notices issued by the UK's Information Commissioner under the Data Protection Act 1998 are for breach of this principle. The General Data Protection Regulation, which will come into force in May of 2018, will also impose a data breach notification duty which will likely mean that more breaches will make it into the public domain.

The decision only considered liability and so a separate hearing will need to consider the important question of remedy.

Update Jan 2018: We understand that an appeal has now been lodged by Morrisons in relation to this controversial decision.