WINSTON & STRAWN LLP

CLIENT ALERT

Morrisons Wins Supreme Court Appeal Over Vicarious Liability For Data Breach

APRIL 14, 2020

On 1 April 2020, the Supreme Court ruled that UK supermarket chain Morrisons was not required to pay compensation to staff following a data breach which affected approximately 100,000 employees. The appeal comes after the Court of Appeal upheld the High Court's decision to hold Morrisons vicariously liable after a disgruntled employee, Andrew Skelton, leaked sensitive payroll information online in 2014.

Although vicarious liability was not established in this instance, the Supreme Court judgment should be noted by all employers as it expressly confirms that the English law doctrine of vicarious liability applies in the context of the Data Protection Act 1998 (the "DPA"), and provides useful guidance on how the question of vicarious liability should be approached.

Background

Mr. Skelton's grievance with Morrisons stemmed from a disciplinary incident resulting from an investigation into white powder found in the company post-room. The powder was suspected to be cocaine but was later revealed to be slimming formula which Skelton had been selling via eBay and for which he had used Morrisons' post room to send packages. During the investigation, Morrisons suspended Skelton for a period of six weeks and upon his return he received a verbal warning.

Subsequently, as part of his role Skelton was provided with sensitive payroll data for almost 100,000 employees to pass on to external auditors. Skelton took this opportunity to launch his personal vendetta against Morrisons and saved the file to a personal USB stick. Skelton uploaded the payroll data onto a file sharing website and then in March 2014, to coincide with the publication of Morrisons' annual financial results, he sent CDs containing the data along with a link to the file sharing website to three newspapers. One of the newspapers notified Morrisons who immediately informed the police and had the personal data removed. Skelton was subsequently convicted of criminal offences under the Computer Misuse Act 1990, the Fraud Act 2006 and the DPA and sentenced to eight years' imprisonment.

Following the criminal proceedings, a group of approximately 9,000 Morrisons employees affected by the data breach brought a claim against the supermarket chain for breach of the statutory duty created by Section 4(4) of the

DPA (misuse of private information) and breach of confidence, arguing that Morrisons was both primarily and vicariously liable for Skelton's actions.

The High Court found that Morrisons was not primarily liable for the data breach caused by Skelton's conduct but did find that Morrisons was vicariously liable. The Court of Appeal upheld that decision.

Supreme Court judgment

Vicarious liability under the DPA

The Supreme Court considered whether the DPA excluded the imposition of vicarious liability for breaches of its own provisions, committed by an employee as a data controller, or for misuse of private information and breach of confidence.

Section 13(1) DPA provides that an "individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that damage"; it was also a data protection principle (Schedule 1, paragraph 10) that the "data controller must take reasonable steps to ensure the reliability of any employees of his who have access to personal data". In this case, it was argued by Morrisons that the DPA impliedly excluded liability of an employer on the grounds that the DPA provided that liability was to be imposed only on data controllers, and only where they had acted without reasonable care. It was common ground that Morrisons performed the obligations incumbent upon them as data controllers, and that Skelton was a data controller in his own right in relation to the data which he copied and disclosed. Accordingly, Morrisons argued that they could not be under a vicarious liability for Skelton's breach of his duties.

The Supreme Court rejected that argument, finding that the "imposition of a statutory liability upon a data controller is not inconsistent with the imposition of a common law vicarious liability upon his employer" and confirmed that "since the DPA neither expressly nor impliedly indicates otherwise, the principle of vicarious liability applies to the breach of obligations which it imposes, and to the breach of obligations arising at common law or in equity, committed by an employee who is a data controller in the course of his employment".

Vicarious liability of Morrisons

Although vicarious liability was not excluded by the DPA, the Supreme Court did not find that Morrisons was vicariously liable.

The Supreme Court applied the general principle applicable to vicarious liability arising out of a relationship of employment as set out in *Dubai Aluminium Co Ltd v Salaam* [2003] 2 AC 366, i.e. (in this case) "whether Skelton's disclosure of the data was so closely connected with acts he was authorised to do that, for the purposes of the liability of his employer to third parties, his wrongful disclosure may fairly and properly be regarded as done by him while acting in the ordinary course of his employment".

The Supreme Court found that publishing the personal data online was not a task that Skelton was authorised to do and therefore not part of his "field of activities". The Supreme Court outlined that actions of employees need to be "closely connected" with their work duties for employers to be held vicariously liable. The Supreme Court went on to observe that "although there was a close temporal link and an unbroken chain of causation linking the provision of the data to Skelton for the purpose of transmitting it to external auditors and his disclosing it on the internet, a temporal or causal connection does not in itself satisfy the close connection test". Lord Reed highlighted that "in the present case, it is abundantly clear that Skelton was not engaged in furthering his employer's business when he committed the wrongdoing in question. On the contrary, he was pursuing a personal vendetta". Lord Reed went on to make clear that "the mere fact that Skelton's employment gave him the opportunity to commit the wrongful act would not be sufficient to warrant the imposition of vicarious liability".

Implications for businesses

Employers should take note of the Supreme Court judgment as it confirms the application of vicarious liability to data protection. Although *Morrisons* involved a consideration of the provisions of the DPA, which has now been replaced by the GDPR and the Data Protection Act 2018, the case provides important guidance on how the courts should approach the question of vicarious liability under the new legislation.

Against this background data controllers should ensure that their data protection measures and policies are suitably robust and should:

1. Undertake regular compliance audits to review internal policies and procedures;
2. Risk assess all key employees to ensure only qualified and responsible personnel are handling personal data and monitor disgruntled employees and their responsibilities;
3. Limit access to personal data to only those employees who need access to it;
4. Ensure that appropriate technical and organisational measures are in place (as a lesson from this case, this may involve blocking the ability of employees to use personal USB sticks and only issuing USB sticks following reasoned justification);
5. Train employees on the company's policies and procedures, the impact of breaching data protection laws (including personal consequences) and consider incorporating indemnities into key personnel's employment contracts to discourage them from pursuing a personal vendetta like Skelton;
6. Ensure that data breach notification procedures are in place that allow for an efficient response to incidents; and
7. Ensure sufficient insurance policies are taken out to protect the company from minor errors as well as rogue employees like Skelton.

5 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | London | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

Antitrust Competition EU | Antitrust and Competition | competition EU | Supreme Court | Data Protection

Related Capabilities

Antitrust/Competition

Related Regions

North America | Europe

Related Professionals

Peter Crowther