WINSTON & STRAWN LLP

BLOG

UK Supreme Court Rules on Data Breach Vicarious Liability

APRIL 8, 2020

On 1 April 2020, the United Kingdom's Supreme Court ruled that supermarket chain Morrisons was not required to pay compensation to staff following a data breach, which affected approximately 100,000 employees. The Court reversed the appellate court's decision upholding 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 expressly confirms that vicarious liability applies in the context of the Data Protection Act 1998 (the "DPA"), and provides useful guidance on how vicarious liability should be approached going forward.

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, sent in packages out of Morrisons' post room . Subsequently, as part of his role Skelton was provided with sensitive payroll data for almost 100,000 employees to pass onto KPMG. Skelton saved the file to a personal USB stick and uploaded the payroll data onto a file sharing website. In March 2014, he sent CDs containing the data along with a link to the file sharing website to three newspapers. A newspaper notified Morrisons, who immediately informed the police and had the personal data removed. Skelton was convicted of violating 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 sued 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 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". Morrisons

argued that they could not be under a vicarious liability for Skelton's breach of his duties because 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.

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".

The Supreme Court then declined to find that Morrisons was vicariously liable under these facts. The Supreme Court applied the general principle applicable to vicarious liability that actions of employees need to be "closely connected" with their work duties for employers to be held vicariously liable. Here, 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 observed 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

Tip: Data controllers should ensure that their data protection measures and policies are suitably robust to protect against rogue employees mishandling or leaking data.

1. Risk assess all key employees to ensure only qualified and responsible personnel are handling personal data and monitor disgruntled employees and their responsibilities;
2. Limit access to personal data to only those employees who need access to it;
3. 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);
4. 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;
5. Ensure sufficient insurance policies are taken out to protect the company from minor errors as well as rogue employees like Skelton.

3 Min Read

Author

Peter Crowther

Related Locations

Houston | London

Related Topics

Data Privacy | Data Breach

Related Capabilities

Litigation/Trials

Related Professionals

Peter Crowther

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.