UK Supreme Court's decision on vicarious liability for employee's data breach highlights importance of robust organisational privacy policy, security and training for remote workers

Source: https://www.supremecourt.uk/cases/uksc-2018-0213.html

Date: 14 May 2020

Abstract:

The UK Supreme Court's recent decision in *WM Morrison Supermarkets plc v Various Claimants* [2020] UKSC 12 recognises an organisation may be held vicariously liable for data breaches committed by an employee, but that there are certain limitations to this liability. Despite the favourable decision by the court which found Morrisons' not to be vicariously liable, the supermarket giant spent more than £2.26m in dealing with the immediate aftermath of the former employee's breach. Therefore the importance of data security and financial implications of the failure to have adequate policies and security in place to ensure that such incidents do not occur, cannot be underestimated.

In 2014, an employee of the UK chain supermarket store Morrisons, posted the personal details, including names, addresses, gender, dates of birth, bank details and salary of almost 100,000 Morrisons' employees on a file sharing website. The employee, Mr Skelton also sent the data to three newspapers which did not publish the information but instead reported his action to Morrisons. Mr Skelton was arrested, charged and found guilty of offences under the *Data Protection Act 1998* ('the DPA 1998'), and sentenced to eight years in prison.

Nearly 10,000 employees or former employees of Morrisons brought proceedings against the supermarket giant for breach of s 4(4) of the DPA 1998, misuse of private information and breach of confidence. The claims were also brought on the basis that Morrisons was vicariously liable for Skelton's wrongful conduct.

By allowing the appeal from the Court of Appeal, the Supreme Court considered whether Mr Skelton's wrongful conduct was "so closely connected" with acts that he was authorised to undertake by Morrisons that the conduct may be fairly and properly be regarded as done by him in the course of his employment. Despite acknowledging that Mr Skelton would not have carried out the unlawful disclosure had he not been entrusted with the data, the court found that disclosure of that information on the filesharing website was not part of his functions or field of activities, nor was it an act he was authorised to undertake. Further, the court found that Mr Skelton's motive for the disclosure was relevant and that Mr Skelton had disclosed the data because of an "irrational grudge" against Morrisons for a previously recorded disciplinary action.

Importantly, the court held that since the DPA 1998 didn't indicate otherwise, vicarious liability applies to the data protection legislation and breach of duties under common law (including misuse of private information and breach of confidence), committed by an employee who is a data controller. While the DPA 1998 has been superseded by the Data Protection Act 2018 in the UK, which supplements the EU General Data Protection Regulation ('GDPR'), the responsibilities of data controllers (as defined in Article 4 of the GDPR) continue to be of significance.

See our guidance on the GDPR and when it applies to Australian organisations for detailed direction about compliance obligations under the GDPR.

While this judgment has clear implications for Australian organisations that are subject to the GDPR. it also serves as a reminder for all organisations regardless of their connection to the EU, to ensure that their organisational privacy policies and procedures as well as systems and physical security are robust, especially as they pertain to remote workers.Taking such steps will mitigate the risk of an employee engaging in similar unlawful conduct and a court making an adverse finding about the organisation's liability due to deficient policies and practices. It is also important that employees receive training on privacy and data-handling practices, and that organisations consider whether their they have adequate insurance in place if such incidents occur.

Our new checklist for remote working provides a list of recommendations and tips to help guide organisations and staff through the challenges of remote working, especially during the COVID-19 pandemic.