withersworldwide

Morrisons ruled not on the hook for a true 'rogue employee' stealing personal data

02 APRIL 2020

CATEGORY:
ARTICLE

In what is likely to be seen as a victory for common sense, businesses with troublesome employees who are intent on damaging an employer's business interests by the unauthorised theft of personal data should not now be held liable for their actions. The UK Supreme Court judgment in WM Morrison Supermarkets plc v Various Claimants was handed down yesterday and saw the supermarket finally triumph in a six-year legal ordeal.

The decision also means that the focus in rogue employee cases is likely to shift to the question of imposing primary liability for breaches under data protection legislation, in other words whether any affected business had solid data security measures in place. At trial, Morrisons was able to show that its systems and procedures were robust and only defeated by a determined individual acting wilfully against its policies. The level of forensic scrutiny that was placed on Morrisons' practices was intense and would have tripped up many a data controller.

The Supreme Court unanimously held that an ex-employee's 'wrongful use of the gun' i.e. his wrongful disclosure of payroll data, was not something done in the course of employment. The Court found Morrisons to not be vicariously liable at common law, stating it was 'abundantly clear' that the ex-employee, Mr Skelton, was not engaged in furthering his employer's business when he committed the wrongdoing in question.

On the facts, the Court held that Mr Skelton could not be said to have been engaged in furthering Morrisons' business when he unlawfully disclosed the payroll data online. On the contrary, he was pursuing a personal vendetta and seeking vengeance for the disciplinary proceedings some months earlier.

The judgment – which has far wider significance in the employment field generally – also re-affirms the importance of the distinction between cases where a disgruntled employee is engaged, misguidedly, in furthering his employer's business, and cases where the employee is engaged solely in pursuing his own interests and on a 'frolic of his own'.

The Court decided that data protection legislation, in principle, does not exclude an employer from having 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. However Morrisons was excused in this instance, given Skelton's data breaches were not closely connected with his authorised tasks.

It is a very welcome outcome for all data controllers to have this clarity. However, there remain many pitfalls for the unwary in ensuring that the primary obligation to maintain data securely is satisfied. Businesses fortunately should enjoy protection from the true rogue employee.

Perhaps another important point to remember is that Skelton sent his stolen personal data to newspapers on the day of publication of Morrisons' annual financial results, apparently aiming to cause maximum reputational damage. It didn't work and the newspapers did not publish. A disclosure to the media of unauthorised information does not automatically transform the sender into a 'whistleblower'; Skelton was convicted and sentenced to eight years imprisonment. The subsequent legal fight has cost Morrisons millions of pounds, but fortunately might spare some other businesses the same fate.

For more information on data risk and compliance, please contact any member of our Data and Cyber law team.

Authors

Jo Sanders

PARTNER | LONDON

Litigation and Arbitration

+44 20 7597 6009

jo.sanders@withersworldwide.com

Chloe Flascher

ASSOCIATE | LONDON

Litigation and Arbitration

+44 20 7597 6263

chloe.flascher@withersworldwide.com