Employers now liable for rogue employee GDPR breaches

Both the Court of Appeal and High Court have confirmed that employers can be liable for data breaches perpetrated by rogue employees, even where the employer is not directly at fault.

This decision may be considered to be a significant blow to employers who had hoped for a reversal of the decision. The case involved a disgruntled employee of the supermarket chain Morrisons, who leaked the payroll data of around 100,000 fellow employees online and to newspapers. The High Court held that, although Morrisons was not primarily liable for the data breach, it was vicariously liable for the unlawful acts of its employee.

What the law currently states

An employer will be vicariously liable for the actions of its employee if that employee is acting 'in the course of the employment', even where those acts are unlawful. Whether the acts are sufficiently closely connected with employment to be 'in the course of the employment' will depend on the facts of the particular case.

In this case, the Court of Appeal and High Court agreed that they were sufficiently closely connected – the rogue employee's acts in sending the data to third parties were 'within the field of activities' assigned to him by Morrisons, and there was an unbroken thread that linked his work to the unlawful disclosure. So it was held that the employee was acting in the course of his employment, meaning that Morrisons were held to be vicariously liable for the losses suffered by those affected by the breach. This was the case despite the fact that the employee leaked the data specifically in pursuit of a grudge against his employer. Counsel for Morrisons argued that holding employers liable in such circumstances "might have a chilling effect on enterprise and efficiency".

What does this mean for employers?

The decision may be challenging as it demonstrates that businesses can be held liable for an unlawful data breach even where they are not at fault and could do little to prevent the wrongdoing. The judgments stated that there may be a danger that this decision could incentivise disaffected employees into abusing their access to data in order to harm their employer. The Court of Appeal's response to these objections is that employers should seek appropriate insurance cover. Lester Aldridge recommends that businesses consider whether their current policies properly protect them against this risk.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com

This was a case of an employee with authorised access to significant amounts of employee data behaving in a criminal way. This type of risk is probably the hardest for businesses to guard against. However, if businesses can be held liable in these circumstances, then – as well as insurance – Lester Aldridge recommends that businesses review how they manage 'authorised access'. They should also review how they assess individuals to be suitable for positions where they can access data and consider the extent to which they should make changes to existing data security procedures.

Morrisons is now appealing this decision to the UK Supreme Court in an effort to overturn this ruling. No date has yet been given for the appeal hearing.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com