Browne Jacobson

More good news for data controllers: High Court finds local authority not vicariously liable for the actions of social worker who went off on a "frolic of her own"

09 February 2022

Further to the welcome relief that followed the Supreme Court's judgment in Lloyd v Google LLC [2021] UKSC 50 and the decisions of the High Court in both Warren v DSG Retail Ltd [2021] EWHC 2168 and Rolfe & Ors v Veale Wasbrough Vizards LLP [2021] EWHC 2809 (QB) (see our update here for a discussion of how these decisions will help to stem the tide of data breach claims), public bodies will be pleased to hear that another significant court decision has been made that is favourable to data controllers.

In Ali v Luton Borough Council [2022] EWHC 132 (QB) ("Ali"), a claim was brought against a local authority on the basis that one of its social workers had accessed a social care database to obtain sensitive information about the claimant which was then disclosed to the claimant's estranged husband with whom the social worker had been in a relationship. The High Court, applying Various Claimants v Wm Morrison Supermarkets plc [2020] AC 989, held that whilst the social worker had gained the opportunity to access the data on an unrestricted basis during the course of her employment, it should not be held liable when the employee went off on a *"frolic of her own"* by accessing these records for reasons that were unconnected with her role.

The scenario dealt with in Ali is unfortunately not uncommon. Public bodies often have to deal with security breaches that arise as a result of employees accessing records without the proper authority or business reason to do so. The good news is that if the actions of the employee were in no way part of the work in the ordinary course of their employment or to further the interests of the employer and adequate security measures are in place (such as appropriate data protection policies and training for staff, and any restrictions to access that information are necessary), then the employer should be able to avoid liability (either directly or vicariously) for a breach of the data protection legislation.

Robust employment policies and procedures should also be in place to ensure that the unacceptable nature of such conduct is clear and that appropriate consequences will follow. Data protection training for staff and security measures should be kept under regular review.

If this is all done then it will be very difficult for a claimant to obtain damages from a public body for a data breach that occurs as a result of the actions of a rogue employee. Public bodies should therefore thoroughly investigate the cause of any such breach before deciding whether to settle a claim.

Contact

Matthew Alderton

Partner

matthew.alderton@brownejacobson.com

+44 (0)330 045 2747

Related expertise

Cyber liability and data security insurance

Data protection and privacy

Information law