Council Liable to Pay £6,000 for Aggravated Distress Caused by Data Privacy Failings

Alexander Dittel
PARTNER IN TECHNOLOGY, WEDLAKE BELL LLP

Aggravated damages; Bank accounts; Data subjects' rights; Local authorities' powers and duties; Measure of damages; Misuse of private information; Personal data

In *Bekoe v Islington LBC*,[1] the claimant successfully sued the council for misuse of private information (MPI) and breach of rights under the General Data Protection Regulation (GDPR).[2]

The MPI claim related to the council's accessing of a collection of bank accounts and mortgage accounts associated with the claimant in pursuance of the council's possession claim. Under the possession claim, the council wanted to reclaim from the claimant the properties of an elderly landlady who was taken to a care home in 2013 and for whom the council acted as Deputy appointed by the Court of Protection in 2014. In 2013, she agreed with the claimant that he would let those properties for her and pay her the rental income to fund her healthcare. Seemingly unaware of this, the council suspected that, in letting the properties, the claimant was fraudulently profiting from someone else's assets and the council started the possession claim in 2015. The council reported its suspicion to the Police but, after speaking to the claimant, the Police decided not to pursue the matter further.

The GDPR claim concerned the council's failure to respond to the claimant's personal data access request made in late 2018, the improper destruction of information in 2020, and the withholding of information until 2023.

MPI claim

Under the common law tort of misuse of private information, information is private if the person has a reasonable expectation of privacy in respect of it, unless that expectation is outweighed by a countervailing interest.

The expectation is measured against that of a hypothetical reasonable person of ordinary sensibilities placed in the same position as the claimant and faced with the same interference in privacy. Under the *Murray* factors,[3] this depended on the person, their activity, location, nature and purpose of the intrusion, the absence of consent, effect on the person and facts leading to publication. Referring to *Gulati*,[4] the court accepted that a reasonable person would have a reasonable expectation that "a comprehensive snapshot of their general financial information would be kept private".

According to the European Convention of Human Rights (ECHR), any interference with the right to privacy must be limited to what:

> "is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

The council alleged that in accessing the claimant's financial information, it was acting in pursuance of its duty to safeguard the elderly landlady under the Care Act 2014 s.42 and that it was right to report its suspicions about the claimant to the Police. However, no evidence was adduced to support this defence as the people involved in those activities had left the council. The council even failed to provide an explanation as to how Care Act matters were normally handled.

The financial information accessed by the council went far beyond that which would have been necessary to demonstrate payments made or received in relation to the properties. The disproportionate nature of the council's access to data was revealed in cross-examination when it transpired that financial information relating to the claimant's son was also accessed.

The council failed to evidence that its interference with the claimant's privacy was a lawful and legitimate exercise in the balance of rights.

[1] *Bekoe v Islington LBC* [2023] EWHC 1668 (KB).
[2] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 [2016] OJ L119/1.
[3] *Murray v Express Newspapers Plc* [2008] EWCA Civ 446; [2009] Ch. 481.
[4] *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch); [2016] F.S.R. 12.

GDPR claims

The council admitted its failure to disclose personal data from 19 June 2019 through partial disclosure on 24 June 2019 and 30 January 2020 and finally the late disclosure on 8 June 2023. The council failed to rely on any exemptions which would allow it to withhold personal data from the claimant. The court established that the council failed to respond for almost four years to the claimant's personal data access request.

The claimant invited the court to infer from the evidence, or the lack of it, and the court agreed, that various other documents likely existed but were not disclosed. The council's witness described the usual practice which suggested that a record would have been made about reporting fraud to the Police, yet no such record was provided. Furthermore, the council's evidence referred to various missing documents. Finally, the council failed to adduce evidence to deny the inferential case.

The destruction of personal data in the form of the legal file which related to ongoing proceedings was alleged to constitute a breach of the GDPR's security principle and was a clear violation of the council's policies. The court observed that the council's handling of data around reporting a matter to the Police and accessing data through Equifax indicated a "generally slapdash approach" to providing adequate security for personal data.

The court was satisfied that the council has breached the GDPR arts 5, 12 and 15.

Adverse inferences

The court recalled that it may draw inferences from the "absence or silence of a witness who might be expected to have material evidence" or from a "deliberate void of evidence" or if a litigant "parted with relevant evidence". The court can do so without "the need for some other supporting evidence being adduced by the innocent party on that issue". The court proceeded to make such inferences in respect of the MPI claim as well as the GDPR claim.

Quantum

Satisfied that the de minimis threshold had been surpassed, the court struggled to "identify an exact comparator to this case for the purposes of assessing quantum". The court referred to the range of £3,000 to £10,000 in *Gulati* reflecting the range of intrusion and stated that the authorities give overall guidance as to damages taking account of the seriousness and extent of the misuse of private information and its likely impact.

The court was also guided by the analysis of aggravated damages for MPI in *Commissioner of Police for the Metropolis v Shaw*.[5] Under this authority, damages must not be punitive but greater hurt caused increases the damages. The defendant's conduct including manner of wrongful act, motive and subsequent conduct, such as how the litigation is conducted, are also relevant. Aggravated damages can be wrapped in one overall figure.

In particular, the council's lack of respect for legal requirements related to privacy and data protection, repeated failure to disclose key information, disclosure at the final hour, and the "absolute failure to evidence" or substantiate its defence submissions relating to alleged fraud and the frequent changes in the defence, were held to have clearly aggravated the distress caused to the claimant.

The court awarded an overall figure of £6,000 which was much closer to the claimant's claim of £7,500 than the council's counter-submission that £1,250 would be appropriate if *de minimis* did not apply.

Conclusion

The case highlights the damage that can flow from a badly run defence in litigation. The council's defence revealed a lack of proper processes, a slapdash approach to information security and a general disregard for data protection rights.

The lack of evidence on the council's part was likely the key reason for its defeat, and the resulting silence or evidential void allowed the court to draw adverse inferences. This is a helpful reminder of the rules for similar cases where the defendant withholds information about a breach of the GDPR or a personal data breach and fails to provide evidence to support its defence. If the relevant individuals are no longer there to explain the process at the time which gave rise to the claim, explaining the current typical process concerning the same subject matter might help establish a defence.

It seems that the council acted under an assumption which turned out to be incorrect. It is likely that this could have been avoided had the council communicated better. Blanket approaches to background checking on a party in litigation without a positive data protection assessment could result in a claim in MPI.

Many public authorities ignore personal data access requests unless they are sent to a designated channel. One can appreciate that need for public authorities to streamline its processes, but this practice has been criticised by the Information Commissioner's Office and is not considered compliant. If a request is missed, this is a breach of the GDPR which could result in a claim.

[5] *Commissioner of Police for the Metropolis v Shaw* [2012] I.C.R. 464; [2012] I.R.L.R. 291.