£6000 damages awarded for Council's misuse of private f inancial information and GDPR breaches (Bekoe v Mayor and Burgesses of the London Borough of Islington)

This analysis was first published on Lexis+® UK on 24/07/2023 and can be found here (subscription required):

Dispute Resolution analysis: The defendant council obtained private financial information about the claimant and his son during the course of a possession claim concerning property belonging to the claimant's neighbour, Ms Sobesto. The court rejected the defendant's argument that it obtained the information as part of its duties as Ms Sobesto's Deputy, or that it had done so as part of an enquiry under section 42 of the Care Act 2014. Rather, the accessing of the financial information was disproportionate and amounted to a misuse of the claimant's private information. Further, the court found that the defendant council breached Articles 5, 12 and 15 of the GDPR by: failing to adequately respond to the claimant's DSAR for over four years; deleting the claimant's data; and failing to locate and disclose various data, which demonstrated a 'slapdash' approach to data security. The claimant was awarded damages of £6000, including aggravated damages. Written by Lily Walker-Parr, barrister at 5RB.

Bekoe v Mayor and Burgesses of the London Borough of Islington [2023] EWHC 1668 (KB)

What are the practical implications of this case?

The judgment is to some extent confined to the unusual facts of this case, which include a significant (four-year) delay in responding to a DSAR, confusion as to whether data had been lost or destroyed, and intrusive actions taken by a council into the claimant's (and his son's) financial affairs which went far beyond the purpose for which the information was required.

However, the award of aggravated damages highlights the perils of attempting to minimise the seriousness of GDPR breaches/misuse of private information where the data is plainly sensitive (as here, where the information related to the claimant's financial affairs) and disclosure likely to cause distress.

The judgment also provides a helpful summary of the law in respect of adverse inferences which may be drawn where relevant evidence has been destroyed (paras [19]–[24]) and on the approach to calculating quantum in misuse of private information (MOPI) and (UK) GDPR claims where it is appropriate to award a single sum for various heads of loss (paras [65]–[73]).

What was the background?

Mrs Sobesto was taken into care in 2013, after which time her neighbour, C, maintained and let out her property (the 'Property') ostensibly on her behalf. In 2014, D obtained a deputyship order over Mrs Sobesto and reported suspicions of fraud against C to the Metropolitan Police (who later confirmed to C that no further action would be taken).

In 2015, D issued a claim for possession and damages against C in respect of the Property. During the course of that claim, D obtained private information about C's financial affairs, including information about his bank accounts, mortgage accounts and mortgage balances (the 'Private Information'). A County Court Order for possession and damages was made in July 2015 and the Private Information was then used by D to obtain orders for specific

disclosure against both C and banks with whom he held accounts. It was also discovered in the week before trial that one of D's employees may have conducted an Equifax credit agency search in respect of C.

On 10 December 2018, C made a Data Subject Access Request (the 'DSAR') which was acknowledged on 22 May 2019. There was a delay in responding and C complained twice about the quality of responses once received - for which D apologised.

In December 2020, D's legal officer left D's employ and the legal file relating to the possession claim was destroyed.

C subsequently issued claims for Misuse of Private Information and breach of the GDPR (under various heads, including delay in responding to the DSAR and destroying personal data related to ongoing proceedings).

What did the court decide?

Misuse of Private Information

The court held that D misused private information belonging to C (and others) by accessing the Private Information without lawful authority (para [56]).

The Private Information gave a comprehensive view of C's financial situation and was clearly information over which C had a reasonable expectation of privacy (paras [48]; [51]). D also accessed C's son's account, highlighting the disproportionate nature of the access to C's private information, which went far beyond financial information relating to the letting of the property (para [49]). There was nothing in D's argument that C's expectation of privacy was extinguished by the possession claim, as the information went far beyond what was relevant to that claim (para [50]).

The Private Information was accessed in July 2015 and shared within D's organisation and with the County Court in the possession claim. The court rejected D's argument (unsupported by evidence) that the access was based on D's duty as Mrs Sobesto's deputy and that it amounted to an enquiry under section 42 of the Care Act 2014 (CA 2014) ([52]–[53]).

Absent a clear legal basis for accessing the Private Information by D, a public authority, there was no requirement to conduct a balancing exercise between C's Article 8 rights and Mrs Sobesto's property rights under Article 1 Protocol 1. The interference with C's Article 8 rights was not a lawful or legitimate exercise (paras [54]–[55]).

GDPR

The court held that D was in breach of C's rights under Articles 5, 12 and 15 GDPR (para [60]).

D admitted that its delay in responding to the DSAR had breached the GDPR. The court found that the delay, which began on 19 June 2019, was not remedied until at least 8 June 2023 and amounted to a significant breach (para [57]).

It is likely that further personal data belonging to C had not been disclosed in breach of the GDPR, as documents containing personal data would have been created in respect of the police report and the credit reference enquiry (para [58]).

The legal file relating to the possession claim had either been deleted (contrary to D's six-year data retention period) or otherwise could not be found, which amounted to a failure to provide adequate security for C's personal data in breach of the GDPR (para [59]). Along with the likely existence of data regarding police reports and credit enquiry, this indicated a 'generally slapdash' approach to data security in respect of C's data (para [59]).

Quantum

Applying the principles in *Gulati v MGN Ltd* [2015] EWHC 1482 (Ch), the court awarded C £6000 (including aggravated damages for D's litigation conduct). A single damages award was appropriate due to the overlap of the two claims–including in respect of the distress caused (paras [67]–[73]).

The de minimis principle did not apply because this was a case which plainly crossed the 'threshold of seriousness' set out in *Lloyd v Google LLC* [2021] UKSC 50; [2022] AC 1217 at paras [153], [66].

Case details

- Court: King's Bench Division
- Judges: Susie Alegre (sitting as a deputy judge of the High Court)
- Date of judgment: 5 July 2023

Lily Walker-Parr, barrister at 5RB. If you have any questions about membership of LexisPSL's Case Analysis Expert Panels, please contact caseanalysiscommissioning@lexisnexis.co.uk.