Neutral Citation Number: [2023] EWHC 1668 (KB)

Case No: QB-2019-000780

IN THE HIGH COURT OF JUSTICE
KING'S BENCH DIVISION
MEDIA AND COMMUNICATIONS LIST

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 05/07/2023

Before :

SUSIE ALEGRE SITTING AS A DEPUTY HIGH COURT JUDGE

- -

Between :

YAO BEKOE	**Claimant**
- and –	
THE MAYOR AND BURGESSES OF THE LONDON BOROUGH OF ISLINGTON	**Defendant**

- -
- -

Gervase de Wilde (instructed by **Direct Access Claimant**
Alex Cunliffe (instructed by London Borough of Islington Legal Services**Defendant**

Hearing dates: 13-14 June 2023

- -

Approved Judgment

This judgment was handed down remotely at 10.30am on 5th July 2023 by circulation to the parties or their representatives by e-mail and by release to the National Archives.

.....

DEPUTY HIGH COURT JUDGE SUSIE ALEGRE :

Introduction

1. This is a claim for misuse of private information and breach of rights under the General Data Protection Regulation ("GDPR"). The Defendant, the Mayor and Burgesses of the London Borough of Islington ("LBI") is the London Borough where the Claimant, Mr Yao Bekoe has lived since 1962, and owns property.

2. The factual background to the claim is complex. I will not set out all the details here, rather I will summarise the essential points to the extent necessary for this judgment. The claim arises out of litigation brought during 2015 and 2016 ("the Possession Claim") by the Defendant, LBI, for possession of property ("the Property") belonging to Mrs Sobesto (now deceased), an elderly neighbour of Mr. Yao Bekoe. The Possession Claim followed on from proceedings in the Court of Protection in 2014 and 2015 ("the Court of Protection Proceedings") in which LBI was appointed as Deputy for Mrs Sobesto who had been taken into a care home in 2013 as her health declined. Mr Bekoe challenged the deputyship appointment but was unsuccessful. Prior to these legal proceedings, Mr Bekoe says he had an informal arrangement with Mrs Sobesto and her family whereby he managed and let out flats in the Property on her behalf with the income being intended to help pay for her care.

3. The first claim in these proceedings is that the Defendant misused private and confidential information relating to Mr Bekoe's finances ("the Private Information") by accessing it and sharing it during the Possession Claim. The Private Information included the account number and sort code of several of the Claimant's bank accounts, mortgage accounts and mortgage balances providing a snapshot of his general financial affairs at the time. That private information was provided by the Defendant to the County Court in the Possession Proceedings. The Claimant says that the Defendant obtained the private information without a legal basis.

4. The second claim is about the Defendant's conduct in relation to a Data Subject Access Request ("DSAR") which the Claimant says was originally sent to the Defendant on 10 December 2018. There was some dispute between the parties as to the date when the DSAR was first sent and received by the Defendant. However, it was accepted by both parties that, for the purposes of these proceedings, the DSAR was acknowledged by the Defendant on 22 May 2019, and breach of the DSAR started from 19 June 2019. This was admitted by the Defendant.

5. In addition to the alleged delay in responding to the DSAR, the Claimant claims that the Defendant was responsible for a series of further infringements of his rights under the General Data Protection Regulation (GDPR), including failing to disclose further data and destroying his personal data in the form of the legal file which related to ongoing proceedings.

The facts

Witness Evidence

6. The Claimant provided a witness statement and gave evidence in the trial including evidence in response to late disclosure from the Defendant which had been received after his witness statement dated 4 August 2022. There was no need to call the Claimant's other witness, Lucilda Stewart, who gave evidence about the sending of the DSAR in December 2018, as it was accepted that the claim for breach of GDPR related to delays from 19 June 2019 only.

7. The Defendant put forward two witnesses, Karen Mitchell, a Senior Litigation Lawyer within the Resources Department of LBI and Leila Ridley, Head of Information Governance and DPO within the Resources Department of LBI. Neither witness had any personal knowledge of the facts underlying the two claims.

Chronology

8. There is a complex history to this claim and I will set out a brief summary of key dates and elements here.

Misuse of Private Information

9. Mrs Sobesto, an elderly neighbour who lived next door to the Claimant for many years, was taken into care in 2013. The Claimant, Mr. Bekoe continued to let out flats in the Property and organised for maintenance work on it after she was taken into care.

10. The Defendant applied for deputyship for Mrs Sobesto on 11 June 2014 and an order was made by the Court of Protection for deputyship on 23 August 2014. Meanwhile, in June 2014, the Claimant had found tenants for the Property and on 15 August 2014 he had entered into Shorthold Tenancy Agreements for the property, he says acting on behalf of Mrs Sobesto. On 19 September 2014, the Claimant received a letter addressed to one of the tenants by the Defendant, which is when the Claimant says he first learned of the deputyship.

11. On 21 November 2014, the Defendant reported suspicions of fraud against the Claimant to the Metropolitan Police. The Claimant met with Mr Micklewright, an employee of LBI, on 25 November 2014. When the Claimant later contacted the police for more information about the resulting police report, he says he was told that the police had sent a report to the Defendant saying there was no evidence of criminality and declining to pursue the matter.

12. The Defendant started the Possession Claim against the Claimant for the property on 23 April 2015. A County Court Order for possession and damages was made on 13 July 2015. It appears that the inquiries made about the Claimant's financial affairs by the Defendant that are the subject of the misuse of private information claim took place in July 2015 against the background of the Possession Claim. On 15 July 2015, Radha Pillai, a Legal Services Officer at the Defendant sent an email to Chris Lobb, an employee at the Defendant. This email, for which the full surrounding chain was only disclosed immediately prior to the trial on 8 June 2023 read:

> *"We have evidence of fraud by Mr Yao Bekoe. He rented a property (….) belonging to a neighbour (service user) who is in care and he*

> *has received the rental income of approximately £40,000-£50,000…*
>
> *We need evidence of his bank accounts to verify if he received the rental income in his bank accounts…*
>
> *Please confirm if you can carry out checks on Mr Bekoe. We need evidence if he owns [.....], bank accounts, records of previous criminal offences. i.e. fraud/theft, and if he owns other properties."*

13. On 20 July 2015, Lotte Wentworth, a Legal Officer at the Defendant, emailed Bob Knightley, a Local Government Officer at the Defendant asking for the Claimant's account numbers. The Private Information was then put before the County Court on an application for disclosure. By an order dated 20 August 2015, the Claimant was ordered to give specific disclosure to the Defendant in relation to the seven bank and building society accounts which had been identified in what the Defendant called the "Basic Investigation".

14. On 28 September 2015 Lotte Wentworth sent a further email to Bob Knightley asking for branch details. He responded on 29 September 2015 and by application notice dated 30 September 2015, the Defendant made an application for an order for disclosure against the banks responsible for those seven accounts. LBI exhibited to Mr Micklewright's Witness Statement in support of the application a letter to Barclays Bank PLC which said *"we are currently working with Islington Police concerning suspected financial abuse perpetrated against Mrs Sobesto"*. The order for disclosure was made on this basis on 24 November 2015.

GDPR

15. The Claimant sent the Defendant a letter of claim on 10 December 2018 and went on to issue a Claim Form in a Part 8 Claim on 6 March 2019. The Defendant acknowledged service for the Part 8 claim on 21 March 2019 and acknowledged receipt of a DSAR from the Claimant on 22 May 2019. While the Claimant said that a Data Subject Access Request had been sent along with the letter of claim, this was not pursued and therefore 22 May 2019 was the effective date from which timing related to the GDPR claim started to run. The Part 8 Claim was stayed by Order of Master Gidden on 23 May 2019.

16. The Defendant issued its first response to the DSAR on 24 June 2019. The Claimant wrote to the Defendant on 17 September 2019 to complain about that response and the Defendant replied, to apologise, on 17 October 2019. On 21 January 2020 the Claimant made a second complaint about the DSAR response and the Defendant replied on 30 January 2020.

17. According to Karen Mitchell, witness for the Defendant, Lotte Wentworth left LBI on 15 December 2020 and the legal file relating to the Possession Claim was destroyed around that time.

18. Proceedings in this Claim continued through 2021 with an exchange of witness statements on 4 August 2022. During the week prior to the trial before me, the

Defendant provided further disclosure material including additional emails and documents that the Claimant had not seen previously. In particular, this included (1) a Witness Statement made by Mr Micklewright in the Court of Protection Proceedings in 2015, (2) the full surrounding chain of emails relating to the request made by Ms Pillai on 15 July 2015, (3) internal emails relating to the DSAR of June 2019, which referred to and discussed the possibility of Mr Knightley having undertaken "an Equifax search in respect of Mr Bekoe", and (4) an account of November 2019 by Ms Wentworth of the content of her legal file and the likelihood of other departments involved having "disclosable records".

Law

Evidence and Inferences

19. The general rule concerning the evidence of witnesses is set out at CPR r.32.2.

> "32.2—(1) The general rule is that any fact which needs to be proved by the evidence of witnesses is to be proved—
>
> (a) at trial, by their oral evidence given in public; and
>
> (b) at any other hearing, by their evidence in writing."

20. The commentary on the rule in White Book 2023, 32.2.1 at pg. 1017 says:

> "Traditionally, the law applicable in England and Wales has placed greatest weight on evidence given by witnesses in open court on oath or affirmation under examination by the parties. Rule 32.2(1)(a) restates the general principle in relation to the most important part of the civil process, the trial. The rule applies only to evidence as to matters of fact."

21. In ***Active Media Services Inc v Burmester Duncker & Joly GmbH & Co KG*** [2021] EWHC 232 (Comm) (Calver J), at [299]-[311], the Court summarised the applicable principles regarding a court's ability to draw adverse inferences from the absence of evidence before the court. In relation to the claimant company's failure to call relevant witnesses Calver J referred to the observations of Brooke LJ in ***Wisniewski v Central Manchester Health Authority*** [1998] P.I.Q.R P324, including that *"(1) In certain circumstances a court may be entitled to draw adverse inferences from the absence or silence of a witness who might be expected to have material evidence to give on an issue in an action."*

22. In relation to the destruction of evidence, Calver J referred to the observations of HHJ Simon Brown QC in ***Earles v Barclays Bank*** [2009] EWHC 2500, at [31]: *"In cases where there is a deliberate void of evidence, such negativity can be used as a weapon in adversarial litigation to fill the evidential gap and so establish a positive case."*

23. In summarising the application of the principles in ***Active Media Services Inc*** at [311], Calver J held:

> "that the court is entitled in such a case, depending upon the particular facts, to draw adverse inferences as to (i) what the destroyed documents are likely to have shown on the issue on question, and (ii) the evidence that the witnesses are likely to have given on the issue in question but which was withheld, without the need for some other supporting evidence being adduced by the innocent party on that issue."

24. In ***Vardy v Rooney*** [2022] EWHC 2017 (QB); [2023] E.M.L.R. 1, the Court held that it could draw adverse inferences on the basis that the wrongdoer has *"parted with relevant evidence"*, under the principle in ***Armorie v Delamirie***.

Misuse of Private Information

25. Misuse of private information is a tort under common law. Information is private for the purposes of this tort if the person in question has a reasonable expectation of privacy in respect of it. If so, the question is whether that expectation is outweighed by a countervailing interest: ***ZXC v Bloomberg LP*** [2022] UKSC 5, [2022] AC 1158, [43]-[62]

26. *ECHR Article 8: Right to privacy*

> Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> There shall be no interference by a public authority with the exercise of this right except such as 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.

27. *Care Act 2014 - S. 42 Enquiry by local authority*

(1) This section applies where a local authority has reasonable cause to suspect that an adult in its area (whether or not ordinarily resident there)—

(a) has needs for care and support (whether or not the authority is meeting any of those needs),

(b) is experiencing, or is at risk of, abuse or neglect, and

(c) as a result of those needs is unable to protect himself or herself against the abuse or neglect or the risk of it.

(2) The local authority must make (or cause to be made) whatever enquiries it thinks necessary to enable it to decide whether any action should be taken in the adult's case (whether under this Part or otherwise) and, if so, what and by whom.

The GDPR

28. Regulation (EU) 2016/679 ("the General Data Protection Regulation" or "GDPR") governed the processing and movement of personal data until 31 December 2020, when it was amended and became the "UK GDPR" following the UK's departure from the EU. For these proceedings, GDPR was the relevant applicable legislation.

29. Article 5(1) provides:

> *"Personal data shall be:*
>
> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
>
> *....*
>
> *(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."*

30. Article 12(3) provides

> *"The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request."*

31. Article 15(1) provides:

> *"*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
>
> *(a) the purposes of the processing;*
>
> *(b) the categories of personal data concerned;*
>
> *…*"

32. Article 15(3) provides:

> *"The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the*

> *data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form."*

33. Article 23 provides:

> *"Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:*
>
> …
>
> *(j) the enforcement of civil law claims."*

34. The Data Protection Act 2018 establishes an exemption for legal professional privilege. Paragraph 18 of Schedule 2, Part 4 provides:

> "In this Part of this Schedule, "the listed GDPR provisions" means the following provisions of the GDPR (the rights and obligations in which may be restricted by virtue of Article 23(1) of the GDPR)—
>
> (a) Article 13(1) to (3) (personal data collected from data subject: information to be provided);
>
> (b) Article 14(1) to (4) (personal data collected other than from data subject: information to be provided);
>
> (c) Article 15(1) to (3) (confirmation of processing, access to data and safeguards for third country transfers);
>
> (d) Article 5 (general principles) so far as its provisions correspond to the rights and obligations provided for in the provisions mentioned in sub-paragraphs (a) to (c).

Paragraph 19 provides:

> "The listed GDPR provisions do not apply to personal data that consists of—
>
> (a) information in respect of which a claim to legal professional privilege or, in Scotland, confidentiality of communications, could be maintained in legal proceedings, or
>
> (b) information in respect of which a duty of confidentiality is owed by a professional legal adviser to a client of the adviser."

35. Article 82(1) GDPR and s.168 of the Data Protection Act 2018 provide for Compensation for breaches of the GDPR, including for *"non-material damage"*, including distress.

Submissions on Liability

Misuse of Private Information

36. Mr. de Wilde for the Claimant argued that there was a reasonable expectation of privacy in relation to Mr Bekoe's financial information citing the test for establishing a reasonable expectation of privacy recently summarised by the Supreme Court in ***ZXC v Bloomberg LP*** [2022] UKSC 5; [2022] A.C. 1158 at [49]-[50] (Lord Hamblen and Lord Stephens JJSC)

> " (ii) Stage one
>
> …
>
> 49. Whether there is a reasonable expectation of privacy is an objective question. The expectation is that of a reasonable person of ordinary sensibilities placed in the same position as the claimant and faced with the *1192 same publicity—see Campbell [2004] 2 AC 457, para 99 per Lord Hope of Craighead; Murray [2009] Ch 481, para 35 .
>
> 50. As stated in Murray at para 36, "the question whether there is a reasonable expectation of privacy is a broad one, which takes account of all the circumstances of the case". Such circumstances are likely to include, but are not limited to, the circumstances identified at para 36 in Murray —the so-called " Murray factors". These are: (1) the attributes of the claimant; (2) the nature of the activity in which the claimant was engaged; (3) the place at which it was happening; (4) the nature and purpose of the intrusion; (5) the absence of consent and whether it was known or could be inferred; (6) the effect on the claimant; and (7) the circumstances in which and the purposes for which the information came into the hands of the publisher."

37. He noted that, at [52] the Court approved a list set out in **Gatley on Libel and Slander**, 12th ed (2013) at **22.5** of *"certain types of information which will normally, but not invariably, be regarded as giving rise to a reasonable expectation of privacy so as to be characterised as being private in character"*, which includes *"personal financial and tax related information"*.

38. Further, he drew the Court's attention to **The Law of Privacy and the Media**, 3rd Edition, at 5.80, which says that *"a reasonable expectation of privacy may exist in relation to information about a person's financial or professional affairs*"

39. Mr. Cunliffe for the Defendant cross-examined Mr Bekoe on the fact that he had shared some bank account information with EON for the purpose of direct debits. But in his submissions, he clarified that he did not mean to suggest that the information ceased to be private because it was shared with someone. He submitted however, that, in the specific circumstances, there could not be an expectation of privacy. This, he said, was because, in July 2015, Mr Bekoe would have been aware in the context of the ongoing Possession Claim that his financial information would be required to show what he had been paid, by whom and what he had paid out in relation to the Property. He pointed to the fact that, following the Court Order of 18 August 2015 with the list of bank statements, Mr. Bekoe was under a duty of disclosure to the court.

Breach of the GDPR

40. The Defendant accepts it breached the Claimant's rights under the GDPR in relation to inadequate and delayed responses to the DSAR dating from 19 June 2019.

41. The Claimant's submissions on breach of GDPR rights included the admitted 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. Although it was accepted that some of the information in the late disclosure would not be considered as a breach of GDPR rights as it related to emails about the DSAR itself, it was submitted that some of the email chains and other material in the late disclosure, in particular that dating back to 2015, did contain personal data and revealed significant delays in disclosing that data.

42. The Claimant also argued an inferential case that there was further data which has still not been disclosed and that the Defendant was liable for its failure to disclose this further data. The Claimant's case was that there were several categories of data likely to be controlled or processed by the Defendant. Through his submissions on late disclosure and the cross-examination of the Defendant's witnesses, Mr Gervase invited the Court to make inferences about the following types of further data:

    1. Reports made by Mr Micklewright to the Police about the Claimant which were not part of the legal file but in relation to which no details were retained or disclosed to the Claimant.

    2. Mr Micklewright and Mr Salter, an employee of the Defendant likely had further personal data concerning the Claimant in the form of internal notes.

3. Information relating to Mr Knightley's accessing of the Private Information. Despite the highly intrusive nature of access to the private information which the Defendant carried out, no record was retained of the means of this access by Mr Knightley or the person instructed on his behalf.

4. Disclosable records that may have been held by other Client departments involved.

43. Mr de Wilde submitted that the Court could find that further data that had not been disclosed was held by the Defendant based on (i) the inferential case as the existence of the further data, (ii) the void of evidence on the part of the Defendant in response to that case, and (iii) the references to missing documents and the likelihood that further personal data concerning the Claimant was being processed by individual departments within the Defendant.

44. The third aspect of the GDPR claim focused on the Defendant's failures to ensure appropriate security of his personal data, in particular relating to the apparent destruction of the legal file. In the Claimant's submission, there was no exemption under paragraphs 18 and 19 of Schedule 2, Part 4 of the Data Protection Act 2018 removing the Defendant's obligation to maintain appropriate security of the Claimant's personal data.

45. In addition to being a clear breach of the Claimant's GDPR rights, the Claimant submitted that it was a clear violation of the Defendant's own policies (which are consistent with the general approach to keeping records in relation to litigation). This was confirmed in evidence by Karen Mitchell and Leila Ridley from the Defendant.

46. Following the Late Disclosure, the Claimant submitted that further personal data, in particular relating to queries Mr Knightley apparently made to Equifax, had either been accidentally lost or destroyed by the Defendant. In evidence, Leila Ridley indicated that, where such information was accessed, there would normally be a record kept of it.

47. Mr Cunliffe sought to minimise the importance of the alleged breaches of the GDPR, but the Defendant provided no concrete evidence to rebut the Claims.

Conclusions on Liability

Misuse of Private Information

48. There is ample authority that financial information can be categorised as "private information" for the purposes of the tort of misuse of private information [see e.g. ***Gulati; The Law of Privacy and the Media***]. There is therefore a reasonable expectation that this kind of information would be kept private. A reasonable person with ordinary sensibilities placed in the same position as the Claimant would expect that a comprehensive snapshot of their general financial information would be kept private.

49. The scale of the misuse of private information became clear in cross-examination which revealed that at least one of the accounts accessed related also to Mr. Bekoe's son. This highlighted the disproportionate nature of the access to private information that went well beyond financial information directly related to the letting of the Property.

50. The argument that the Claimant could not have had a reasonable expectation that his financial information would be kept private because of the Possession Claim that was ongoing in July 2015 is not persuasive. This is because the financial information accessed by LBI went far beyond that which would have been necessary to demonstrate payments made or received in relation to the Property. The Court Order of 20 August 2015 for disclosure in relation to Mr Bekoe's accounts alerted him to the fact that his private information had been accessed by the Defendant. But, as it came after the access by LBI took place, it could not have affected the reasonable expectation of privacy in July 2015.

51. In this case, the combination of financial information relating to several bank accounts and mortgage accounts including balances with the comprehensive view it gave of Mr Bekoe's financial situation is clearly private information. In addition, from the evidence before me, it would appear that it is not only Mr Bekoe's private information that has been compromised but also that of his son.

Adverse Inferences

52. There is no dispute that the Defendant accessed the private information sometime in July 2015 and shared it, both within the organisation and with the County Court in the Possession Claim. Mr. Cunliffe repeatedly put forward the argument that the access was based on LBI's duty to Mrs Sobesto and was an enquiry under Section 42 of the Care Act 2014, but no evidence was adduced by the Defendant to back up these submissions. Nor was any evidence adduced to back up submissions related to contact with the police beyond the reporting in November 2014 which resulted in no action by Islington Police.

53. The Defendant said that the officers involved in the Possession Claim and in earlier engagements with Mr Bekoe in relation to the Property and the Court of Protection proceedings have all left the Council. But in their absence, no evidence was brought to show how an enquiry under Section 42 of the Care Act would normally be carried out; and there was no evidence as to what actually happened on this occasion. Indeed, the only evidence of contact with the police was reference to the report in November 2014 which resulted in Islington Police taking no action. In light of the observations of Brooke LJ in ***Wisniewski v Central Manchester Health Authority*** [1998] P.I.Q.R P324, I conclude from the absence of witnesses from the relevant departments who might have material evidence on the process for making an enquiry under Section 42 of the Care Act, that there was no evidence to support this defence.

54. The argument that Mr Bekoe's privacy rights under Article 8 ECHR must be balanced against the late Mrs Sobesto's property rights under Article 1 Protocol 1 ECHR must also fail in the absence of evidence for a clear legal basis for accessing the information.

55. Article 8(2) of the ECHR states that: *"There shall be no interference by a public authority with the exercise of this right <u>except such as is in accordance with the law</u>*

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 Defendant has not shown that its interference with Mr Bekoe's Article 8 rights was in accordance with the law and therefore it cannot be described as a lawful and legitimate exercise in the balance of rights.

56. For these reasons, I find that the Defendant did misuse private information belonging to Mr Bekoe by accessing details relating to a collection of bank accounts and mortgage accounts associated with Mr Bekoe (and others) in July 2015 without lawful authority.

GDPR

57. The Defendant accepts that there were delays in responding to the DSAR from 19 June 2019. Despite Mr Cunliffe's arguments that some of the late disclosure could not properly be considered as personal data (for example the correspondence relating to processing the DSAR itself) it is clear that the delays in disclosing personal data in violation of the GDPR were ongoing until at least 8 June 2023. This is a significant breach of the GDPR with a delay of almost 4 years in responding effectively to a DSAR.

58. It is clear, both on the inferential basis submitted by Mr de Wilde and on the evidence given by Leila Ridley in particular, that it is likely that there were or are further personal data belonging to the Claimant that have not been disclosed by the Defendant. Although no evidence was provided by the Defendant of the process it would have taken under section 42 of the Care Act, Leila Ridley was able to confirm that certain types of document containing personal data would have been created by the Defendant in circumstances such as this where reports were made to the Police regarding concerns about potential criminal offences and where a credit reference company had been contacted for information about an individual's financial records. I therefore find it likely that further personal data belonging to the Claimant is or was held by the Defendant which has not been disclosed in breach of the GDPR.

59. On the evidence of both Karen Mitchell and Leila Ridley in Court, the legal file would normally have been kept for six years in accordance with the Defendant's data retention policy and this period would have been extended when the Part 8 Claim was made in March 2019. There was no evidence that the failure to disclose the legal file was due to legal professional privilege, rather the Defendant's evidence was that the file had been destroyed or could not be located by the Defendant. Karen Mitchell in her evidence explained that the file reference indicated that it was not a standard housing file but was rather related to safeguarding which would be dealt with by another department. While there was no clear evidence on what exactly happened to the legal file, there was a clear failure to provide adequate security for the Claimant's personal data in breach of the GDPR. Leila Ridley's evidence relating to the likely existence of further data around police reporting and accessing data through Equifax indicates a generally slapdash approach to providing adequate security for he Claimant's personal data.

60. Taking account of the failures to respond adequately to the DSAR, the loss or destruction of the legal file and the failures to provide adequate security to further

personal data, I find that LBI violated Mr Bekoe's GDPR rights under Articles 5, 12 and 15 of the GDPR.

Submissions on Quantum

61. In relation to the misuse of private information claim, Mr de Wilde pointed to the observations of Mann J in ***Gulati v MGN Ltd*** [2015] EWHC 1482 (Ch) at [229 ii)], where the Court held that *"Information about significant private financial matters is also likely to attract a higher degree of privacy, and therefore compensation, than others."*

62. Submissions were made by both parties in relation to the *de minimis* principle In ***TLT v Secretary of State for the Home Department*** [2016] EWHC 2217 (QB) (Mitting J) to create *"a threshold below which damages for "distress" may not be awarded in respect of it"*.

63. Mr de Wilde submitted that, relying on the available comparators in the authorities, an award of damages of £7,500 in respect of the misuse of Mr Bekoe's private information by the Defendant would be appropriate. This, he said, would reflect his loss of control of the information, and the distress which resulted from it. It would also include an element of aggravation. In relation to the GDPR claim, the Claimant sought a total of £6000 comprised of £500 in respect of the delays in compliance with the DSAR, £1500 in respect of the failures to disclose the Further Data, £2000 in respect of the failure to ensure the security of C's personal data, plus an additional amount to reflect the element of aggravation. The Claimant pointed to the distress caused by *"the casual and dismissive approach taken… to my personal data rights".*

64. Mr Cunliffe, in his final submissions, suggested that, in the event that damages were to be awarded, £500 for the misuse of private information and £750 for the GDPR claim would be appropriate if the *de minimis* principle did not apply.

Conclusions on Quantum

65. Compensation is available in the tort of misuse of private information on a wider basis than under the GDPR. In particular, a successful claimant is entitled to damages to compensate them for the loss or diminution of the right to control the use of their private information independently of any distress caused: **Gulati v MGN Ltd**, [45]-[48]; **Lloyd v Google**, [141].

66. I note the observations of the Supreme Court in ***Lloyd v Google LLC*** [2021] UKSC 50; [2022] AC 1217 at [153] (Lord Leggatt JSC) as to the need for a breach of the DPA 1998 to cross a *"threshold of seriousness"*. However, I am satisfied that the threshold is crossed in this case as the underlying issue relates to a comprehensive collection of the Claimant's financial information (***Gulati v MGN Ltd*** [2015] EWHC 1482 (Ch) at [229 ii)]) and therefore I do not need to consider the further submissions made about the current application of the *de minimis* principle.

67. While this claim is brought under the heads of both misuse of private information and breach of GDPR, there is significant overlap in terms of the impact of both aspects of the claim on the Claimant. The GDPR claim comes, in essence, from his efforts to

uncover and challenge the misuse of private information. He gave evidence as to the distress caused by both the misuse of private information and the violation of his GDPR rights, but it is very difficult to unpick the nature of that distress in a meaningful way between the two claims. In the circumstances, with both claims taking place against the backdrop of ongoing litigation and continued delays in disclosure up until the week before trial, I believe that it is most appropriate to consider damages for both claims together as a single figure.

68. I take account of Mann J's analysis in ***Gulati*** at [205] where he considered the question of aggravated damages in claims for misuse of private information, holding that the following was established by Underhill J in ***Commissioner of Police for the Metropolis v Shaw*** [2012] ICR 464:

> *"(i) It reiterates that the damages are compensatory, not punitive.*
>
> *(ii) They are, at least usually, an aspect of injury to feelings. The aggravating factors cause greater hurt, and thus increase the damages.*
>
> *(iii) There are typically three aspects of conduct of the defendant which are capable of triggering an aggravated damages award - the manner in which the wrong was committed, motive and subsequent conduct.*
>
> *(iv) The third of those factors can include the manner in which the trial (and a fortiori the litigation as a whole) is conducted by the defendant.*
>
> *(v) A separate figure for aggravated damages can be given; or it can be wrapped up in one overall figure. Underhill J tended to favour the latter course."*

69. I find that the third factor, the subsequent conduct of the Defendant, in this case, is sufficient to trigger aggravated damages. The way that the trial and the litigation as a whole has been conducted by the Defendant has revealed a lack of respect for legal requirements related to privacy and data protection. Repeated failure to disclose key information, disclosure at the final hour, two working days before the trial, and the absence of any clear evidence to support or substantiate Defence submissions relating to alleged fraud have clearly aggravated the distress caused to the Claimant. To be clear, it is not the assertion of a Defence in this case which triggers aggravated damages but rather the absolute failure to evidence it along with the continued unjustified shape shifting of the basis of the defence which continued right up until Mr Cunliffe's final submissions at trial.

70. Adopting the approach favoured by Underhill J in ***Commissioner of Police for the Metropolis v Shaw*** [2012] ICR 464, I find that the aggravated nature of the damages should be wrapped up in one overall figure.

71. It is difficult to identify an exact comparator to this case for the purposes of assessing quantum, most of the cases identified involve publication of private information or breach of confidence, neither of which is relevant in this Claim. The facts in ***Ali v Chief Constable of Bedfordshire*** [2023] EWHC 938 (KB) (Chamberlain J) are quite different to this case. But I note that, in awarding the Claimant £3000 in compensation for distress under the GDPR, the Judge held that, were it necessary to do so he would have awarded the same amount "as compensation for loss of the right to control the information", at [53]. In ***Gulati***, where the exact nature and extent of activities undertaken by private investigators that amounted to misuse of private information was not known, the awards ranged from £3,000 to £10,000 reflecting the inferred scale of the intrusion.

72. It is difficult to break down specific heads of distress. I am not persuaded by Mr. Cunliffe's argument that these awards should be calculated on the basis of a particular amount per instance of intrusion with reference to ***Gulati***. Rather, the authorities give some overall guidance as to damages taking account of the seriousness and extent of the misuse of private information and its likely impact. While I note Mr de Wilde's submissions regarding separate heads of damage for the discrete elements of GDPR breach, the overlapping and ongoing nature of the separate Claims and different elements of GDPR breach leads me to the conclusion that an overall combined figure for damages would be the most appropriate course in this case.

73. In this case, taking account of the misuse of private information, the loss of the right to control the information and the level of distress caused by the GDPR breaches along with the aggravating factors, I award an overall figure of £6000 for damages.

Result

74. The claims for misuse of private information and breach of GDPR succeed. There will be judgment for the claimant in the sum of £6000.