Neutral citation number: [2024] UKFTT 00373 (GRC)

Case Reference: EA/2023/0309

First-tier Tribunal
General Regulatory Chamber
Information Rights

Heard by: remotely by video conference
Heard on: 21 November 2023
15 January 2024 (in chambers)
Decision given on: 09 May 2024

Before

TRIBUNAL JUDGE HAZEL OLIVER
TRIBUNAL MEMBER DAVID COOK
TRIBUNAL MEMBER PHEBE MANN

Between

THE LONDON BOROUGH OF HACKNEY

Appellant

and

(1) THE INFORMATION COMMISSIONER
(2) ANKUR BANERJEE

Respondents

Representation:
For the Appellant: John Fitzsimons, counsel
For the Respondent: Sam Fowles, counsel
For the Second Respondent: In person

Decision: The appeal is allowed in part

Substituted Decision Notice:

The Appellant is to provide the Second Respondent with the information which, in accordance with the closed annex to the Tribunal's decision, is not exempt from disclosure and has been agreed between the Appellant and the Information Commissioner, within 28 days of promulgation of this decision.

Failure to comply may result in the Tribunal making written certification of this fact to the Upper Tribunal, in accordance with rule 7A of the First-tier Tribunal (General Regulatory Chamber) Rules and may be dealt with as a contempt of court.

REASONS

Mode of hearing

1. The proceedings were held by video (CVP). All parties joined remotely. The Tribunal was satisfied that it was fair and just to conduct the hearing in this way. The hearing took a full day and so the Tribunal met separately at a later date to discuss and finalise its decision.

Background to Appeal

2. This appeal is against a decision of the Information Commissioner (the "Commissioner") dated 25 May 2023 (IC-179033-S0X6, the "Decision Notice"). The appeal relates to the application of the Freedom of Information Act 2000 ("FOIA"). It concerns information about the Council's Information Asset Register ("IAR") requested from the London Borough of Hackney (the "Council").

3. On 19 March 2022, the Second Respondent (Mr Banerjee) wrote to the Council and requested the following information (the "Request"):

> *"I would like to request the current/latest version of Hackney Council's Information Asset Register (IAR). Before making this request, I carried out a search for this term on hackney.gov.uk as well as https://hackney.moderngov.co.uk/ieDocSea...*
> *Please let me know if you require any clarifications for this request."*

4. The Council responded on 22 April 2022. They confirmed that they held the requested information. However, they withheld the entirety of the IAR under section 31(1)(a) FOIA (law enforcement) and 40(2) FOIA (personal data). Mr Banerjee requested an internal review on 2 May 2022. It appears that the Council has never responded to the review request despite being reminded by the Commissioner.

5. Mr Banerjee complained to the Commissioner on 1 July 2022. The Commissioner issued the Decision Notice on 25 May 2023. The Commissioner decided:

a. The Council was entitled to rely on section 40(2) to withhold the names of individual staff members contained within the IAR.
b. The Council was not entitled to rely on section 31(1)(a) to withhold the IAR. The Commissioner accepted that the potential prejudice relates to the interests within the exemption, and that there is a causal link between disclosure and the prejudice. However, the Commissioner was not persuaded the chance of such prejudice occurring is more than a hypothetical possibility.
c. The Commissioner required the Council to provide Mr Banerjee with a copy of the IAR.

The Appeal and Responses

6. The Council appealed on 21 June 2023. The main grounds of appeal are that the Commissioner erred in concluding that there was only a hypothetical possibility of the prejudice in question occurring. The Council says that section 31(1)(a) is engaged and the information should be withheld under the public interest test.

7. The Commissioner's response maintains that the Decision Notice was correct. The Commissioner says that there is not sufficient likelihood of the prejudice occurring, and the

Council's case relies on hypotheticals and has failed to provide sufficient evidence. The Commissioner also noted that a number of other local authorities publish their IAR, and it is also common for central government departments.

8. Mr Banerjee was joined as a party to the proceedings and submitted a response. He complains of the Council's failure to conduct an internal review. He provides examples of other government departments and local councils which publish their IARs, and refers to a previous decision notice of the Commissioner where he found that section 31(1)(a) was engaged but the IAR of the Department for Digital, Culture, Media & Sport should be disclosed under the public interest test. He says that the Council has not provided compelling evidence why, even if S31(1)(a) is engaged, the IAR could not be released under the public interest test. He also says that section 40 cannot be used to withhold the entire document.

9. The Council provided replies to both of these responses which maintain its position. The Council says that previous releases of IARs by public authorities are limited and the Council takes a different position as a recent victim of a cyber-attack.

Applicable law

10. The relevant provisions of FOIA are as follows.

> ***1 General right of access to information held by public authorities.***
> *(1) Any person making a request for information to a public authority is entitled—*
> *(a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and*
> *(b) if that is the case, to have that information communicated to him.*
> *……*
> ***2 Effect of the exemptions in Part II.***
> *…….*
> *(2) In respect of any information which is exempt information by virtue of any provision of Part II, section 1(1)(b) does not apply if or to the extent that—*
> *(a) the information is exempt information by virtue of a provision conferring absolute exemption, or*
> *(b) in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.*
> *……..*
> ***31 Law enforcement.***
> *(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—*
> *(a) the prevention or detection of crime…*
> *…….*
> ***58 Determination of appeals***
> *(1) If on an appeal under section 57 the Tribunal considers—*
> *(a) that the notice against which the appeal is brought is not in accordance with the law, or*
> *(b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,*
> *the Tribunal shall allow the appeal or substitute such other notice as could have been served by the Commissioner; and in any other case the Tribunal shall dismiss the appeal.*
> *(2) On such an appeal, the Tribunal may review any finding of fact on which the notice in question was based.*

11. The approach to prejudice-based exemptions was set out in the First Tier Tribunal decision of ***Hogan v Information Commissioner*** [2011] 1 Info LR 588, as approved by the Court of Appeal in ***Department for Work and Pensions v Information Commissioner*** [2017] 1 WLR 1:

a. Firstly, the applicable interests within the relevant exemption must be identified.
b. Secondly, the nature of the prejudice being claimed must be considered. It is for the decision maker to show that there is some causal relationship between the potential disclosure and the prejudice, and that the prejudice is "real, actual or of substance".
c. Thirdly, the likelihood of occurrence of prejudice must be considered. Whether disclosure "would" cause prejudice is question of whether this is more likely than not. To meet the lower threshold of "would be likely to" cause prejudice, the degree of risk must be such that there is a "real and significant risk" of prejudice, or there "may very well" be prejudice, even if this falls short of being more probable than not.

Issues and evidence

12. The Council has confirmed in its open skeleton argument that no issues concerning section 40(2) form the basis of this appeal. This is because the Commissioner agreed that the Council is entitled to rely on s40(2) FOIA with regards to the withholding of names of individual staff members contained within the IAR.

13. The issue is whether the Council was entitled to rely on section 31(1)(a) FOIA to withhold some or all of the IAR. This can be broken down into the following issues:

a. What are the applicable interests within the exemption, i.e. what is the actual harm relied on by the Council?
b. Is there a causal relationship between the disclosure and the prejudice, and is this real, actual or of substance?
c. Would disclosure cause this prejudice, or would it be likely to do so?
d. If section 31(1)(a) is engaged, in all the circumstances of the case, does the public interest in maintaining the exemption outweigh the public interest in disclosing the information?

14. By way of evidence and submissions we had the following, all of which we have taken into account in making our decision:

a. An agreed bundle of open documents.
b. Open and closed witness statements from Robert Miller on behalf of the Council
c. Closed exhibits to Mr Miller's closed witness statement, including the withheld information.
d. An open skeleton argument from the Council.
e. Open and closed skeleton arguments from the Commissioner.
f. Oral submissions from all parties at the hearing.

Open Evidence

15. We had a detailed witness statement from Robert Miller, who is the Strategic Director, Customer and Workplace, at the Council.

16. He covered the following issues in his open witness statement:

a. Mr Miller provided his own professional view on the ongoing and growing threat of organised cybercrime, which he says means that the risks presented by disclosing the Council's IAR in terms of threat actors attempting to exfiltrate sensitive data or attempting to make criminal use of sensitive data previously acquired is more than a hypothetical or remote possibility. He refers to information published by the National Cyber Security Centre and National Crime Agency on growing and increasingly sophisticated threats.

b. Mr Miller says that, in the current geo-political context, there is the real risk of a state actor who intends to cause harm to the UK considering that an attack on local government is a way that they can cause significant disruption to British citizens while remaining below a threshold that might potentially trigger a more serious UK Government response. He refers to a number of well-publicised cyberattacks on other councils. He also provides examples of how threat actors are continuing to develop their techniques and have moved beyond limiting their attack to ransomware to even more sophisticated targeting of sensitive data.

c. Mr Miller led the Council's response to a criminal cyberattack which took place on 11 October 2020. This seriously impacted services which had not been migrated to cloud-based systems. The service areas using those systems had to rely on business continuity and contingency arrangements to minimise disruption to services while the technically complex work to recover systems and data took place. This had a significant impact across a wide range of Council services, with significant and widely reported impacts on residents and businesses. These impacts were felt for years after the attack and continue to be felt today. In addition, the financial impact of the attack on the Council is over £12.5M. There have also been opportunity costs due to diversion of resources to continuity and recovery work, and damage to the Council's reputation.

d. Mr Miller considers the Commissioner's examples of other public bodies who have published their IARs. He says that the information published by both the FCDO (last updated 2019) and Home Office (last updated 2013) is limited and very different from the Council's comprehensive IAR. The search results for IARs provided by the Commissioner only return 32 datasets, of which only 5 relate to UK government and are not marked "not released". He says that the vast majority of departments and agencies do not publish their IARs, and where they do the information published is only a very high-level summary and very different to the comprehensive set of information maintained in the Council's IAR.

e. In relation to the public interest balance, Mr Miller says that the Council has been transparent about both its services and the cyberattack. The Council publishes information about its services and about its data processing (through privacy notices). Mr Miller says that the Council's assessment of risk is that disclosure of the IAR would greatly simplify the work of potential threat actors in targeting the most sensitive data that the Council holds, and that the disclosure would not provide material public benefit in terms of transparency. He sets out the following public interest factors against disclosure:
   - Crime prevention;

- Avoiding the costs (financial, distress, inconvenience, publicity, regulatory) to the Council associated with any cyberattacks;
- Avoiding material and non-material damage to the Council's residents and businesses associated with any cyberattacks;
- Avoiding material and non-material damage to the Council's employees associated with any cyberattacks;
- Preventing any threat to the integrity of the Council's data; and
- Ensuring the Council can continue to comply with its various important statutory duties to provide essential services to its residents and its statutory duties to safeguard their personal data.

17. Mr Banerjee explained his position at the hearing. He does not disagree that the IAR contains sensitive information and could be useful to bad actors, but his issue is whether there is a version with redactions that would be publishable. He is a resident of the Council who was potentially impacted by the cyberattack and wishes to understand the nature and extent of his personal data that may have been impacted. He says that, although the Council's privacy notices contain some detail, they are not specific on what data is held. He also says that the Council's policy on responding to data subject access requests requires a request to be about specific data points. He wants to understand where all data about him could be contained. He is particularly interested in the data elements (e.g. name, address, bank details) and retention periods, especially in the context of the cyberattack. In relation to the public interest, he believes that other data subjects would find this useful, and there is a general public interest in what information is held on data subjects. He says that the FCDO publication achieves this by showing data points and retention periods, which allows data subjects to request information.

Closed Evidence

18. We have seen a copy of the withheld information, together with the closed statement from Mr Miller and other closed exhibits to this statement. We held two closed sessions during the hearing – one to hear evidence from Mr Miller, and one for closed submissions.

19. The following is a gist of the closed sessions. An oral gist of the closed evidence session was also provided to Mr Banerjee during the hearing.

a. The Tribunal began its closed evidence session by hearing evidence from Mr Miller concerning the material set out in his closed witness statement. Mr Fitzsimons asked Mr Miller a number of questions supplemental to his statement and Mr Miller explained the nature and purpose of an IAR, the risk picture concerning cyberattacks generally and more specifically the Council, the risks he associates with the IAR being made public, and the likelihood of that risk occurring. Mr Miller also explained his view that if s31(1)(a) is engaged, the public interest in withholding the information outweighs the public interest in disclosing it.

b. Mr Fowles then asked Mr Miller a series of specific questions about certain information contained within the IAR. He undertook a comparative exercise with Mr Miller where Mr Miller was asked to compare the contents of the Council's IAR with that of the FCDO and the Home Office in the new open bundle. He also challenged Mr Miller on the evidential basis he was advancing to support his risk assessment.

c. Judge Oliver also asked a number of questions and it was discussed which columns and rows, if any, of the IAR could be redacted and if so, how a redacted version could be published. Tribunal Member Cook asked Mr Miller to explain in more detail the nature and fallout from the cyberattack in 2020. Tribunal Member Mann also asked a further question arising from Mr Miller's risk assessment.

d. During the closed submissions session, we heard submissions from Mr Fowles about whether the exemption was engaged and what information from the IAR should be disclosed, with reference to specific columns and items in the IAR and the closed evidence. Mr Fitzsimons responded to these submissions. The Tribunal also discussed with both counsel the options for making its decision.

Discussion and Conclusions

20. In accordance with section 58 of FOIA, our role is to consider whether the Commissioner's Decision Notice was in accordance with the law. As set out in section 58(2), we may review any finding of fact on which the notice in question was based. This means that we can review all of the evidence provided to us and make our own decision. We deal in turn with the issues.

21. ***What are the applicable interests within the exemption, i.e. what is the actual harm relied on by the Council?*** The harm relied on by the Council is the risk that disclosure of this information would aid potential cyberattacks and enable attackers to identify potential targets. This is not in dispute. It would clearly prejudice the prevention of crime as cyberattacks are unlawful.

22. ***Is there a causal relationship between the disclosure and the prejudice, and is this real, actual or of substance?*** The Commissioner accepted in his decision that the potential prejudice to the prevention of unlawful cyberattacks relates to the interests that section 31(1)(a) is designed to protect, and we agree. The Commissioner also accepted that the threats from cyberattacks are real, and additional disclosed information could in theory allow better targeting of attacks. We agree that it is plausible to argue that there is a causal link between disclosure of the information and the increased risk of cyberattacks, meaning that the prejudice if the IAR were to be disclosed is real, actual and of substance.

23. ***Would disclosure cause this prejudice, or would it be likely to do so?*** The Council relies on the lower "would be likely to" threshold. This means the risk does not need to be more probable than not, but there does need to be a "real and significant risk" of prejudice. This is the key issue in dispute between the Council and the Commissioner.

24. The Council says that the evidence from Mr Miller has demonstrated that the Council's case does not rely on hypotheticals. There is a developing cyber threat environment and increase in attacks on local authorities. The evidence shows that most public bodies do not publish their IARs, and the examples given by the Commissioner do not contain the same detail as the Council's IAR. The Council takes the view that those who have published IARs (such as Cheshire East Council) have exposed themselves to significant risks. The Council's response to the reply from Mr Banerjee explains how this would allow potential attackers to target the most sensitive data and also reveal that they will be able to obtain all financial details about that council. There is also the context and ongoing impact of the 2020 cyberattack which is explained in closed evidence.

25. The Commissioner says that the Council has shown a general threat from hacking and that some of the IAR information is sensitive, but it is only speculation that the IAR would be meaningful

to a hacker. The Commissioner's position is that Mr Miller's evidence does not establish a causal connection between disclosure and the risk of a cyberattack. He says that the Council should take a granular approach of analysing the information fully, rather than taking a blanket approach of withholding all of the information, even when a large data set is involved. The public authority is required to carry out the exercise of separating out the disclosable information. This can be published as a separate set of information, as FOIA does not require publication of the full IAR with redactions shown.

26. As set out above, Mr Banerjee accepts that some of the information in the IAR could be useful to bad actors, but he believes it would nevertheless be possible to publish a version with redactions.

27. In closed session the positions of the Commissioner and the Council came slightly closer together after we had viewed the withheld information. The Commissioner had identified eight categories of information, and took the position that six of these should be disclosed (rather than the full IAR). The Council accepted that they should look at the information in a more granular way. We consider this in more detail in the closed annex to this decision.

28. We find that some, but not all, of the information in the IAR would be likely to cause the prejudice. This is based on the ongoing and growing threat of organised cybercrime. It is also based on the context of what happened with the 2020 cyberattack on the Council, which is discussed in more detail in the closed annex. The Council concedes that it should have taken a more granular approach to disclosure of the information. We agree. We considered the content of the IAR in the closed hearing, and find that much of the information could be disclosed without being likely to cause prejudice to prevention of cyberattacks. However, some of the information does meet this test. We have explained the detail of our reasoning in the closed annex, as doing so in the open decision would reveal the content of the withheld information.

29. We have identified principles for categories of information that can be withheld and asked the Council and the Commissioner to agree a version of the IAR that can be disclosed based on these principles. We are not able to provide full details of our reasoning in the open decision. In the closed annex, we explain the reasoning in full and provide some indications as to how these principles should be applied to the IAR. We can set out here the following broad principles for information that should be withheld:

a. All personal data (exempt under section 40(2) FOIA) – as already agreed by the parties.
b. All information about location of electronic storage of data (exempt under section 31(1)(a) FOIA).
c. All information which indicates specifically that personal data or special category personal data is held (exempt under section 31(1)(a) FOIA).

30. ***If section 31(1)(a) is engaged, in all the circumstances of the case, does the public interest in maintaining the exemption outweigh the public interest in disclosing the information?*** We have found that disclosure of certain types of information would be likely to increase the risk of cyberattacks and so prejudice the Council's ability to prevent such attacks. We therefore need to consider whether this information should nevertheless be disclosed under FOIA under the public interest test.

31. The Council accepts that there are important factors in favour of disclosure, including those of transparency and accountability. However, they say this interest is reduced due to much of the information being already available online. The Council says it has been as transparent as possible within the constraints of the need for appropriate cyber security. The Council relies on the list of significant public interest harms set out in Mr Miller's evidence, the most important being the Council's ability to provide essential services. The Council also relies on further harms including the "mosaic effect" as identified in closed evidence. The Council says that these various harms plainly outweigh the limited public interest in disclosing the disputed information.

32. The Commissioner recognises that there is a public interest in ensuring personal data held by public authorities is protected, but this interest is reduced if the likelihood of prejudice is marginal. Transparency helps the public to see that government (including local government) takes decisions that are in the best interests of the public, and the Council has wrongly assumed that it must withhold information from the public in order to protect them from hackers. Citizens can be better informed by knowing what information is held by the Council, exercising any rights under the UKGDPR, and scrutinising the steps taken by the Council to protect information. The Council has not given enough weight to citizen agency. The Commissioner also says that the key information is the description of information held, which has been published by high profile government departments without any evidence of negative impacts.

33. Mr Banerjee makes a similar point to the Commissioner – that he and other citizens want transparency about the specific types of data that is held about them by the Council, particularly in light of the 2020 cyberattack.

34. We acknowledge the importance of transparency. We take the point of both the Commissioner and Mr Banerjee that there is significant public interest in citizens knowing specifically what types of data are held about them, particularly in light of the cyberattack, so that the Council's actions can be scrutinised.

35. We have taken a more limited view than the Council on which information can be withheld. This does not include basic descriptions of the data held, and so publication of this information will go a considerable way towards meeting the public interest in transparency. For the information which can be withheld, there is a significant public interest in doing so in order to prevent future cyberattacks. There are a number of harms caused by cyberattacks which there is important public interest in avoiding, as explained by Mr Miller in his witness statement. These include preventing harm to residents and businesses, and ensuring that the Council can provide its essential services. We have also considered specific public interest harms relating to the 2020 cyberattack, as explained in the closed annex. Having considered all of these public interests together, we therefore find that the public interest in maintaining the exemption outweigh the public interest in disclosing the information.

36. We allow the appeal in part and issue the Substituted Decision Notice set out at the start of this decision.

37. The issuing of this decision has been delayed while the Council and Commissioner agreed a final version of the information for disclosure. There were also issues with the readability of this document when it was provided to the Tribunal, which has caused a further delay. The Council should ensure that the information is provided to the Appellant in a fully readable format.

Signed Judge Hazel Oliver Date: 8 May 2024