Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 10 November 2022

Public Authority: London Borough of Hackney
Address: Town Hall
Mare Street
London
E8 1EA

Decision (including any steps ordered)

1. The complainant submitted an information request to London Borough of Hackney ("the Council") relating to the cyber-attack of October 2020.

2. The Commissioner's decision is that the Council was entitled to rely on section 31(1)(a) of FOIA to withhold the requested information. As the Commissioner considers that this applies to all of the requested information, he has not gone on to consider the Council's application of section 31(1)(g) by virtue of section 31(2)(i).

3. The Commissioner does not require any further steps.

Request and response

4. On 7 July 2021, the complainant made the following request for information under FOIA:

> "Please may I have the following data, which all relates to the cyber attack against Hackney Council in October 2020:
>
> 1) Exactly what council services were affected by the initial hack?
>
> 2) Exactly what services have been recovered / are now back up and running and are fully operational (as of the time of the response to this FOI)?
>
> 3) How many users had their data potentially exposed by the hack?
>
> 4) How many users has the council identified so far that had their personal data leaked as a result of the hack?
>
> 5) At the time of the cyber attack, did the council have a backup system in place in case of a cyber attack?
>
> 6) How much was spent annually on cyber security by the council before the cyber attack?
>
> 7) How much is the council now spending annually on cyber security?
>
> 8) How much money does the council estimate it has lost as a result of the damage from the cyber attack?."

5. The Council responded on 9 August 2021 stating that it withheld the information under Section 31(1)(a) of FOIA (prevention or detection of crime).

6. On 5 September 2021, the complainant requested an internal review. The Council provided the complainant with its response to the internal review request on 3 March 2022 in which it upheld its response and also sought to apply section 31(1)(g) by virtue of section 31(2)(i) of FOIA.

Reasons for decision

Section 31- the prevention and detection of crime

7. Section 31(1)(a) of FOIA provides that any information to which a request for information relates is exempt information if its disclosure under this Act, would, or would be likely to prejudice the prevention or detection of crime.

8. In order for section 31 to be engaged, the following criteria must be met:

   • the actual harm which the public authority claims would, or would be likely to, occur if the withheld information was disclosed has to relate to the applicable interests within the relevant exemption (in this case, the prevention or detection of crime);

   • the public authority must be able to demonstrate that some causal relationship exists between the potential disclosure of the information being withheld and the prejudice which the exemption is designed to protect. Furthermore, the resultant prejudice which is alleged must be real, actual or of substance; and,

   • it is necessary to establish whether the level of likelihood of prejudice being relied upon by the public authority is met – ie disclosure 'would be likely' to result in prejudice or disclosure 'would' result in prejudice.

9. In decision notice IC-106031-D4Y0[1], the Commissioner found that the Council was correct to rely on section 31(1)(a) to withhold information relating to the cyber attack of 2020. In paragraphs 17-21 he set out why the exemption was engaged. The present request is for information relating to the same cyber-attack and is therefore caught by the same reasons as set out in paragraphs 17-21 in the above decision notice.

10. The Commissioner is aware that the Council has subsequently released further information regarding the cyber-attack in a television interview aired in July 2022.

[1] https://ico.org.uk/media/action-weve-taken/decision-notices/2022/4020736/ic-106031-d4y0.pdf

11. When considering whether the public interest test favours maintaining the exemption or disclosing the requested information, the Council has stated that is strives to be an "open and transparent authority", but in some circumstances it cannot responsibly release the requested information. However, it hoped that it could address this need via the investigation into the cyber-attack conducted by the Commissioner. In providing reasons in favour of maintaining the exemption, the Council stated that the investigation was ongoing, and that as the information requested was not in the public domain then disclosure would endanger the physical or mental health or safety of an individual.

12. The Commissioner considers there is a public interest in the Council being open and transparent and of the need to inform service users how their service had been affected. However, he also accepts the concerns around disclosing security arrangements regarding an ongoing investigation and the Council's duty to protect the physical or mental health or safety of any individual including data subjects affected by the cyber-attack. As such the Commissioner is satisfied that, in this case, the public interest test favours maintaining the exemption.

13. The Commissioner's decision is that the Council is entitled to rely on section 31(1)(a) of FOIA to withhold the requested information.

Other matters

14. There is no obligation under FOIA for a public authority to provide an internal review process. However, it is good practice to do so and, where an authority chooses to offer one, the section 45 Code of Practice sets out, in general terms, the procedure that should be followed. The code states that reviews should be conducted promptly and within reasonable timescales. The Commissioner has interpreted this to mean that internal reviews should take no longer than 20 working days in most cases, or 40 in exceptional circumstances.

15. In this case the complainant requested an internal review on 5 September 2021 and the Council provided the outcome of its review on 3 March 2022, nearly six months later.

16. The Commissioner understands the difficulties the Council would have experienced during the Covid-19 pandemic and a cyber security incident. Nevertheless, he would like to take this opportunity to remind the Council of its responsibilities in carrying out an internal review within the guidelines of the Code of Practice.

Right of appeal

17. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

    First-tier Tribunal (Information Rights)
    GRC & GRP Tribunals,
    PO Box 9300,
    LEICESTER,
    LE1 8DJ

    Tel: 0203 936 8963
    Fax: 0870 739 5836
    Email: grc@justice.gov.uk
    Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

18. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.

19. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed

Phillip Angell
Group Manager
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF