Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**11 March 2024**
Public Authority:	**The Governing Body of the University of Birmingham**
Address:	**Edgbaston Birmingham B15 2TT**

Decision (including any steps ordered)

1. The complainant has requested information relating to personal data breaches. The University of Birmingham ('the University') refused the entirety of the request under section 31(1)(a) (law enforcement).

2. The Commissioner's decision is that the University was correct to withhold the information it did under section 31(1)(a).

3. The Commissioner does not require further steps.

Request and response

4. On 24 August 2023 the complainant requested:

> "Please could you provide the following details of this record for each breach:
>
> 1. Date and time the breach occurred
>
> 2. Date and time the organisation was made aware of the breach (if different from above)

3. Whether or not the ICO was notified of this breach

4. If the ICO was not notified, the justification for that decision."

5. The University responded on 12 September 2023. It refused to comply with the request, citing section 43(2) (commercial interests).

6. The complainant requested an internal review on the same day.

7. The University provided the outcome to its internal review on 7 November 2023. It upheld its previous position and also introduced a reliance on section 31(1)(a) (law enforcement).

Scope of the case

8. During this investigation, the University withdrew its reliance on section 43(2).

9. Therefore, all that remains is for the Commissioner to determine whether the University is correct to withhold information under section 31(1)(a). The University has applied section 31(1)(a) to the request as a whole.

Reasons for decision

Section 31 – law enforcement

10. Section 31 of FOIA states:

"(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."

11. A public authority doesn't have to have law enforcement responsibilities itself in order to use this exemption; section 31(1)(a) covers all aspects of the prevention and detection of crime, and this is meant to be interpreted broadly.

12. A public authority can apply section 31(1)(a) to withhold any information that would make itself more vulnerable to crime and the University is concerned that disclosure of the requested information would leave it more vulnerable to cyber-attacks.

13. The University has explained:

> "• Disclosure of specific details of every (or, indeed, several) personal data breach would enable a motivated individual to compile datasets and form an opinion on the cybersecurity measures adopted by the University.
>
> • Further, the time and date of each breach would allow a motivated individual to form an opinion on specific patterns of breaches - for example, when during the year more breaches occur – and hence when the University's cybersecurity measures might be more susceptible to attack.
>
> • In addition, knowledge and justification as to whether or not a breach was reported to the ICO creates the opportunity to establish patterns of not only the frequency and regularity of breaches, but also the severity of such breaches."

14. The University is concerned that, put together with information already in the public domain, the withheld information could leave its systems vulnerable to cyber-attacks. The public authority is specifically concerned with an activity called 'footprinting':

> "The University is aware, in particular, of the practice of potential hackers known as 'footprinting': University of Birmingham Edgbaston "Footprinting, also known as fingerprinting, is a methodology used by penetration testers, cybersecurity professionals, and even threat actors to gather information about a target organization to identify potential vulnerabilities. Footprinting is the first step in penetration testing. It involves scanning open ports, mapping network topologies, and collecting information about hosts, their operating systems, IP addresses, and user accounts. This gathered data helps to generate a comprehensive technical blueprint of the target organization."

15. The University is concerned that disclosure would allow a potential hacker to begin mapping its cyber-security processes in this way. The University has shared with the Commissioner a particular example of how this mapping could occur. Whilst the Commissioner doesn't deem it appropriate to replicate this example in this decision notice (because to do so could result in the prejudice that the exemption is specifically trying to avoid), he agrees that the withheld information engages the exemption, on the lower threshold of prejudice.

16. Just because the requested information engages section 31(1)(a) doesn't mean that it can be automatically withheld. The Commissioner must go onto consider where the balance of the public interest lies.

The public interest test

Factors in favour of disclosure

17. In their internal review request, the complainant stated:

> "The university holds extremely sensitive data in some cases and those placing their data in the hands of the university have a right to understand the university's history and past incidents with such data."

18. The Commissioner agrees. There is always a public interest in public authorities being open and transparent in how it protects from, and responds to personal data breaches, and how vulnerable it is to such breaches.

19. The University also recognises this, stating 'The University understands the public interest regarding openness and accountability as to how the University processes data, and that the personal data it holds and processes is safe.'

Factors in favour of maintaining the exemption

20. As the complainant has acknowledged, the University holds sensitive personal data and it's not in the public interest to compromise the public authority's ability to safeguard this information.

21. The Commissioner understands that public organisations, especially Universities, are increasingly being targeted by a significant number of high-risk cyber-attacks. Public organisations are having to become more robust in staying a step ahead of such attacks.

22. Since there is clear evidence of previous cyber-attacks against the University, and since the Commissioner has decided that disclosure could increase the risk of these cyber-attacks further, it must follow that this risk should be mitigated in any way possible.

Balance of the public interest

23. The Commissioner has determined that the balance of the public interest lies in maintaining the exemption in this instance.

24. The Commissioner concurs with the University when it says:

> "The University demonstrates accountability, openness and transparency through its reporting to the ICO as the regulator. If and when a data breach is deemed reportable to the ICO, the University will comply with its legal duty. In that way, the University remains accountable, open and transparent."

25. The complainant is concerned that the University's application of section 31(1)(a) somehow implies that the University 'is effectively admitting to not effectively and appropriately responding to data breaches and putting new protections in place going forward to prevent similar breaches from happening again.'

26. The Commissioner disagrees; he isn't aware of any evidence which indicates that the University is somehow mishandling, or failing to protect, the personal data it processes. Cyber-attacks are becoming increasingly sophisticated and common, which only serves to strengthen the arguments in favour of maintaining the exemption.

27. The complainant is specifically asking for a breakdown of each personal data breach, which is exactly the information that engages section 31(1)(a). However, if the complainant is still concerned, they might wish to request more general information about the University's handling of such breaches.

Right of appeal

28. 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

29. 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.

30. 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

Alice Gradwell
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF