Reference: IC-270452-F8X2

Freedom of Information Act 2000 (FOIA)

Decision notice

Date:	**17 April 2024**
Public Authority:	**Information Commissioner**
Address:	**Wycliffe House** **Water Lane** **Wilmslow** **Cheshire SK9 5AF**

Decision (including any steps ordered)

1. The complainant has requested information relating to a personal data breach (PDB) investigation. The Information Commissioner's Office (ICO) provided some information within scope of the request but refused to provide the remaining information citing section 44(1)(a) FOIA (prohibitions on disclosure).

2. The Commissioner's decision is that the ICO is entitled to rely section 44(1)(a) to withhold the requested information.

3. The Commissioner does not require further steps.

Jurisdiction and Nomenclature

4. This decision notice concerns a complaint made against the Information Commissioner. The Information Commissioner is both the regulator of the FOIA and a public authority subject to the FOIA. They are therefore under a duty, as regulator, to make a formal determination of a complaint made against them in their capacity as a public authority – a duty confirmed by the First Tier Tribunal. It should be noted however that the complainant has a right of appeal against the Commissioner's decision, details of which are given at the end of this notice.

5. This notice uses the term "the ICO" to refer to the Information Commissioner dealing with the request and dealing with previous

complaints brought under the FOIA. It uses the term "the Commissioner" when referring to the Information Commissioner dealing with this particular complaint.

Request and response

6. On 22 August 2023, the complainant wrote to the ICO and requested information in the following terms:

"if you would confirm whether or not your investigations are now complete. If so, I would be grateful if you would confirm whether or not you found that Marie Stopes/MSI Reproductive Choices and/or Stor-a-file were, at the time of the data breach, complying with the necessary data protection legislation and processing affected individuals' personal data lawfully."

7. The ICO responded on 31 August 2023 and confirmed that a data breach report relating to a cyber breach in September 2021 had been received, and subsequently investigated. The investigation concluded on 23 December 2021. The outcome was logged as 'No Further Action', implying that it was unlikely that the legislation the ICO oversees had been contravened by the reporting data controller.

8. The complainant requested an internal review and also requested some further information.

9. In its response the ICO acknowledged that it had not provided information relating to the Stor-a-File investigation but noted that it was provided on 11 October 2023 along with an apology for the omission. The ICO was therefore satisfied that all the requested information had been provided.

10. On 12 October 2023 the complainant made a follow-up request:

"Irrespective of whether or not you are taking any regulatory action, I just want to know what happened. Put simply, how did the hackers gain access to my personal information? How were they able to steal the information from Stor-a-File's IT systems?

I also then want to know, again irrespective of whether or not you are taking any regulatory action, whether you consider that MSI RC and Stor-a-File complied with the relevant data protection law? …it is important to understand whether you, as the independent regulator for data protection charged with upholding information rights in the public interest, consider that there were any failures by MSI RC and Stor-a-File that allowed the hackers to access personal data."

11. On 25 October 2023 the ICO responded and provided the closure letters to each of the reporting parties and some additional explanatory information. It withheld some personal data under Section 40(2) FOIA as well as additional information under Section 44 of the FOIA.

12. In their complaint to the Commissioner the complainant stated that they did not consider the ICO's responses to be adequate and had not addressed all their concerns.

13. They also raised a number of issues relating to adequacy of security measures at the time of the breach and contested that it was a 'limited data breach' as they believed it had affected thousands of individuals causing a great deal of anxiety and distress.

14. The complainant did not accept that the ICO could not provide further information relating to their request.

Scope of the case

15. The Commissioner considers that the scope of his investigation is to be to determine whether the ICO is entitled to rely on section 44(1)(a) FOIA as a basis for withholding any remaining information.

Reasons for decision

16. Section 44(1) of the FOIA provides an exemption from disclosure for any information whose disclosure would either be otherwise prohibited by another piece of legislation or would constitute a contempt of court.

17. In this particular case, the ICO is relying on section 132 of the DPA2018 as the statutory bar preventing disclosure. Section 132(1) of that Act states that:

    "A person who is or has been the Commissioner, or a member of the Commissioner's staff or an agent of the Commissioner, must not disclose information which—

    (a) has been obtained by, or provided to, the Commissioner in the course of, or for the purposes of, the discharging of the Commissioner's functions,

    (b) relates to an identified or identifiable individual or business, and

    (c) is not available to the public from other sources at the time of the disclosure and has not previously been available to the public from other sources, unless the disclosure is made with lawful authority."

18. Section 44 of FOIA allows a public authority to withhold information whose publication outside of FOIA would be prohibited by law.

19. Section 132 of the Data Protection Act 2018 (DPA2018) makes it a criminal offence for any person to disclose identifiable in contravention of section 132(1).

20. It is common ground between the parties that the withheld information was provided to the ICO for the purpose of the discharge of one of the ICO's functions: namely to investigate personal data breaches. Therefore the DPA2018 would prevent this information being disclosed unless a lawful gateway to disclose applied.

21. Section 132(2) of the DPA2018 originally set out six possible gateways through which disclosure could take place with lawful authority:

    For the purposes of subsection (1), a disclosure is made with lawful authority only if and to the extent that—

    (a) the disclosure was made with the consent of the individual or of the person for the time being carrying on the business,

    (b) the information was obtained or provided as described in subsection (1)(a) for the purpose of its being made available to the public (in whatever manner),

    (c) the disclosure was made for the purposes of, and is necessary for, the discharge of one or more of the Commissioner's functions,

    (d) the disclosure was made for the purposes of, and is necessary for, the discharge of an EU obligation[1],

    (e) the disclosure was made for the purposes of criminal or civil proceedings, however arising, or

    (f) having regard to the rights, freedoms and legitimate interests of any person, the disclosure was necessary in the public interest.

22. As noted above, the information was not provided with a view to it being published and therefore gateway (b) cannot apply either. The lawful gateways set out in section 132(2) are intended to set out a limited number of circumstances in which it will not be a criminal offence for the public authority to disclose certain information. Those gateways should thus be read restrictively.

[1] repealed on 31 December 2020 as part of the UK's withdrawal from the European Union

23. If the ICO were to publish the information on its website, it would not be doing so for the purpose of criminal or civil proceedings (unless a specific court order had been made requiring publication). The "proceedings" gateway will only apply to a restricted disclosure made, during the course of criminal or civil proceedings, to one of the other parties, or to the court itself. This is not such a disclosure and therefore this specific gateway would not provide lawful authority.

24. The Commissioner is also satisfied that disclosure is not necessary to satisfy the public interest. Although the complainant has stated that the breach affected a significant number of individuals, whilst legitimate, is unlikely to be of significant interest to the wider world. He is further satisfied that the public interest is satisfied to a degree by the fact that the ICO carried out an investigation into the PDB and provided the outcome to the complainant.

25. As there is no lawful gateway through which this information could be disclosed, it follows that section 132 of the Data Protection Act 2018 prohibits its disclosure and the information is thus exempt under section 44(1)(a).

Right of appeal

26. 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

27. 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.

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

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