

21 August 2024

Reference number: IC-322216-D0M9

Request

You asked us: *"Please can you disclose all information you are able to publish about the recently publicised MoD [Ministry of Defence] payroll databreach. I am particularly interested in the reports submitted to the ICO by the MoD and SSCL [Shared Services Connected Limited] about this incident."*

We received your request on 24 July 2024.

We have handled your request under the Freedom of Information Act 2000 (the FOIA).

Our response

Having conducted a reasonable search of our records, we can confirm that we hold information in the scope of your request. This includes:

- A breach report from the MoD
- A breach report from SSCL
- Subsequent contact with SSCL and the MoD

Any information held is exempt from disclosure under section 44 and section 31 of the FOIA.

Section 44(1)(a) states:

"(1) Information is exempt information if its disclosure (otherwise than under this Act) by the public authority holding it -

(a) is prohibited by or under any enactment"

The enactment in question is the Data Protection Act 2018. Section 132(1) of part 5 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."

Section 132(2) lists circumstances in which a disclosure can be made with lawful authority, however, none of them apply here. As a result, the information is exempt from disclosure.

In relation to section 31, we are relying upon on section 31(1)(g) of the FOIA. We can rely on section 31(1)(g) of the FOIA where disclosure:

"would, or would be likely to, prejudice... the exercise by any public authority of its functions for any of the purposes specified in subsection (2)."

In this case the relevant purposes contained in subsection 31(2) are 31(2)(a) and 31(2)(c) which state:

"(a) the purpose of ascertaining whether any person has failed to comply with the law...

(c) the purpose of ascertaining whether circumstances which would justify regulatory action in pursuance of any enactment exist or may arise ..."

Section 31 is not an absolute exemption, and we must consider the prejudice or harm which may be caused by disclosure. We also have to carry out a public interest test to weigh up the factors in favour of disclosure and those against.

The information you have requested relates to ongoing enquiries into this incident. To release the information you have requested, at this time, could prejudice the ICO's ability to conduct our enquiries into this matter. Disclosure at this stage would discourage our ongoing discussions with the associated parties and may damage our ability to conduct and conclude our enquiries fairly and proportionately.

Disclosure could also jeopardise the ICO's ability to obtain information relating to this case or others in the future, and it is possible that other parties could be

reluctant to engage with the ICO in the future or be more guarded when they do so.

As the regulator, our work into the legislations we oversee is continuous and ongoing and involves liaising with multiple organisations at any one time. Less engagement would make it much harder for us to disseminate and influence good practice in the legislations we oversee, which could potentially lead to a more 'hazardous' data protection landscape.

With this in mind, we have then considered the public interest test for and against disclosure. In this case the public interest factors in disclosing the information are:

- Transparency about whether the associated parties have complied with their data protection obligations.
- Transparency about a high-profile incident.
- Transparency about how the ICO conducts its enquiries.

The factors in withholding the information are:

- The public interest in maintaining organisations' trust and confidence that information they provide to us will be afforded an appropriate level of confidentiality and will not be made public prematurely or, as appropriate, at all.
- The public interest in the ICO being able to maintain a communication channel with all organisations. A lack of, or reduced, communications channels inhibits our work into the legislations we over see which is not in the public interest.
- The public interest in organisations being open and honest in their discussions with the ICO.
- There is a public interest in the ICO being able to act fairly and proportionately. Disclosure of the requested information could undermine our ability to do this.
- The public interest in maintaining the ICO's ability to handle reported breaches as it sees fit.

This concludes our response.

Next steps

You can ask us to review our response. Please let us know in writing if you want us to carry out a review. Please do so within 40 working days.

You can read a copy of our full [review procedure](#) on our website.

If we perform a review but you are still dissatisfied, you can complain to the ICO as regulator of the FOIA. This complaint will be handled just like a complaint made to the ICO about any other public authority.

You can [raise a complaint](#) through our website.

Your information

Our [privacy notice](#) explains what we do with the personal data you provide to us, and sets out [your rights](#). Our [Retention and Disposal Policy](#) details how long we keep information.

Yours sincerely



Information Access Team
Strategic Planning and Transformation
Information Commissioner's Office, Wycliffe House, Water
Lane, Wilmslow, Cheshire SK9 5AF
ico.org.uk twitter.com/iconews
Please consider the environment before printing this email
**For information about what we do with personal data
see our [privacy notice](#)**