The ICO exists to empower you through information.

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113
ico.org.uk

9 September 2024

Case Reference IC-325393-H7T4

Request

You asked us:

Dear Information Commissioner's Office,

I refer to the story linked below in which it is suggested that Home Office notified the ICO, on or around 2nd May 2024, of a personal data breach relating to corporate systems operated on their behalf by Microsoft.

https://eur03.safelinks.protection.outlook.com/?url=https%3A%2F%2Ftherecord.media%2Frussia-hack-uk-government-home-office-microsoft&data=05%7C02%7Cicoaccessinformation%40ico.org.uk%7C6cea0ff3f2a84230d44408dcbbb51481%7C501293238fab4000adc1c4cfebfa21e6%7C0%7C0%7C638591633614863138%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C0%7C%7C%7C&sdata=DQQIcMJexlILva%2FE41ZkvY0dASqimtg5GTNG5oBX%2BWQ%3D&reserved=0

The story suggests that the ICO previously responded to an FOI request, but did not include any details of your response and you have not yet listed that response on your published FOI pages.

1 - I would therefore be grateful if you would either publish that response in full and provide me with a link to it;

OR

Reply to the following request for information:

Please provide me with a copy of the notification made to the ICO by Home

Office on or around May 2nd 2024 relating to their corporate email services as per the above story.

I would be grateful also for ICO correspondence relating to the decisions not to take further action on this notification, and any supporting information submitted by Home Office ion relation to the notification.

In addition:

2 - Please provide me with a list of any other notifications of personal data breaches in the period 1st November 2023 through to 1st July 2024 from any HM Government and Public Sector Data Controllers (including any parties subject to Part 3 or Part 4 of the Data Protection Act 2018) which relate specifically to personal data processing undertaken on Microsoft Cloud Services.

The include (but are not necessarily limited to):
Microsoft Azure
Microsoft 365
Microsoft Defender and Co-Pilot
Dynamics 365
Microsoft Entra (formerly called Azure Active directory)
Microsoft Teams
Microsoft Exchange Online
Office 365
Windows 365

We received your request on 13 August 2024.

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

Our response

Part 1 of your request

We do not hold that particular FOI response.

From checking our case management system, I can confirm that we have not handled that FOI request you are referring to.

We do hold a case file for the personal data breach ("PDB") incident you are referring to, including the PDB report and the follow-up submission from the Home Office.

Please find the **attached** closure letter from the ICO to the Home Office.

Information withheld

Section 40(2) - third party personal data

You will see that some third party personal data has been redacted in our attachment. In addition, the personal data in the report and submissions from the Home Office is also withheld. Details of the relevant exemptions for them items are found below.

Third-party personal data is exempt under section 40(2) of the FOIA.

Disclosure of this data would break the first principle of data protection - that personal data is processed lawfully, fairly and in a transparent manner.

There is no strong legitimate interest that would override the prejudice that disclosure would cause to the rights and freedoms of the individuals concerned. So we are withholding the information under section 40(2) of the FOIA.

Information withheld – Information from the Home Office

The information submitted by the Home Office to the ICO is exempt information under sections 24, 31 and 38 of the FOIA.

The exempt information is contained in the initial PDB report submitted by the Home Office to the ICO on 2 May 2024, and in their follow-up email response to the ICO on 17 May 2024.

Section 24 – National security

Section 24 of the FOIA states:

"(1) Information which does not fall within section 23(1) is exempt information if exemption from section 1(1)(b) is required for the purpose of safeguarding national security."
…

"(3) A certificate signed by a Minister of the Crown certifying that exemption from section 1(1)(b), or from section 1(1)(a) and (b), is, or at any time was, required for the purpose of safeguarding national security shall, subject to section 60, be conclusive evidence of that fact."

The exemption applies because the details provided by the Home Office go into detailed description about the factors connected to the incident, including security factors. This information could be used for purposes which would pose a cyber security risk to a significant government department.

Section 31 – Law enforcement

Some of the information you have requested is exempt from disclosure under section 31(1)(a), 31(1)(b), and 31(1)(g) of the FOIA.

We can rely on section 31(1)(a) or 31(1)(b) of the FOIA where discosure:

"would, or would be likely to, prejudice—

(a) the prevention or detection of crime,"

or,

"would, or would be likely to, prejudice—

(b) the apprehension or prosecution of offenders,"

We can rely on section 31(1)(g) 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.

Prejudice test

Disclosure could prejudice the Home Office's ability to investigate and prosecute hostile actors through assistance from law enforcement.

Disclosure could also jeopardise the ICO's ability to obtain information relating to PDBs in the future.

If we create an expectation that incident details will be shared by default in response to requests, then we may discourage the sharing of them details in the first place with the ICO. This would make it harder for us to get open and willing engagement from data controllers about high risk incidents. This would result in a prejudice to our regulatory functions.

Section 38 – Health and safety

Section 38 of the FOIA states:

"(1) Information is exempt information if its disclosure under this Act would, or would be likely to—

(a) endanger the physical or mental health of any individual, or

(b) endanger the safety of any individual."

The exemption applies because disclosure could pose a risk to the welfare of individuals connected to the incident.

Response deadline extension

The exemptions at sections 24, 31 and 38 are not absolute and we will now perform a Public Interest Test (PIT) to decide whether the exemptions fall away or are maintained.

Section 10(3) of the FOIA enables an authority to extend the 20 working day limit up to a 'reasonable' time in any case where it requires more time to determine whether or not the balance of the public interest lies in maintaining an exemption.

The FOIA does not define what might constitute a 'reasonable' extension of time. However, the ICO's view is that an authority should normally take no more than an additional 20 working days to consider the public interest, meaning that the total time spent dealing with the request should not exceed 40 working days.

We will therefore respond to you by 9 October 2024 unless we are in a position to respond earlier. Should we not be in a position to respond by that date we will provide a further update.

Part 2 of your request

We do not have a straightforward way of obtaining the information you have asked for, however I have carried out manual searches to identify the information which is in scope of what you've requested.

Between 1 November 2023 and 1 July 2024, there are seven PDB cases under "Public authority" accounts which contain references to Microsoft Cloud services in their reports or submissions to us.

This information is accurate as of 19 August 2024, which was when I carried out these searches. On our case management system, we have a meta-data category of "Public authority" which we can record against data controller accounts which are public sector (this includes government departments).

Section 31 – List of PDB cases

The case reference numbers for the above-mentioned cases are exempt from disclosure under section 31(1)(g) of the FOIA.

This is with exception to the above-mentioned Home Office case, where some details about the nature of the incident have already been made public.

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.

Prejudice test

We routinely publish datasets of the PDB cases which are reported to us. The datasets contain the case reference numbers, the data controller name, and other administrative details. The incident details of the report are kept out of the datasets.

If we disclose the case reference numbers, then we would be making it possible to identify which data controllers have included references to Microsoft products in their PDB reports to us. Them details are expected to be kept confidential by default, unless there is an overriding justification to put it into the public domain.

Disclosure of PDB details is likely to result in data controllers being reluctant to engage with the ICO in the future.

If there is an expectation that their details will be directly or indirectly revealed to the wider world, it will damage trust in the ICO which will discourage the exchange of information and advice between the ICO and other data controllers, which will make it harder for the ICO to easily get the details we need to deliver effective regulation.

Public interest test

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:

- increased transparency about the nature of PDB reports within the public sector, particularly where they involve products from a high-profile technology company

- increased transparency about the identities and types of data controllers which have undergone incidents that have some connection to Microsoft Cloud services

The factors in withholding the information are:

- the public interest in maintaining organisations' trust and confidence that their reports and their replies to the ICO's enquiries will be afforded an appropriate level of confidentiality

Having considered these factors, we are satisfied that it is appropriate to withhold the information.

There may be cases where data controllers are pro-actively public about their PDB incidents. The ICO is in place to receive the details which they would typically not reveal to the public. This is because we need fuller details to make a proper assessment of the incident and the data controller's security measures.

Although there is a clear public interest in knowing about incidents at public sector data controllers which are processing signficant scopes of personal data and using it to carry out public services, we do consider that there is a stronger public interest in allowing a safe space for the exchange of detailed information about PDB incidents, so that we can put ourselves in the best position to regulate effectively.

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