

11 November 2024

Case Reference IC-337685-P7W1

Request

You asked us:

"Under the Freedom of Information Act 2000, I would like to know the following:

- 1. The number of data breaches reported using the 'Report a personal data breach' form.*
- 2. The number of these reports where the "Yes" box was ticked in answer to the question 'Is the personal data breach likely to result in a high risk to data subjects'?*
- 3. The number of these reports where the respondent ticked the box "We have determined that we are unable to restore the personal data to the same state it was shortly prior to the incident, ie backups failed, no current backup, backup encrypted etc" in response to the question '(Cyber incidents only) Recovery time'.*

I would like this data broken down for each of the last 3 years with an September 30 year end date. If this is not possible then please use the year-end used internally by the organisation."

We received your request on 14 October 2024.

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

Our response

We can confirm we hold information that falls in scope of your request.

However, finding and extracting the full extent of information would exceed the cost limit set out by section 12 of the Freedom of Information Act 2000 (FOIA).

This means we are not obliged to comply with your request.

The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 states that the 'appropriate limit' for the ICO is £450. We have determined that £450 would equate to 18 hours work.

Please see below for further details.

Details

When the ICO receives a Personal Data Breach ("PDB") notification from an organisation which has used the online form, we then set it up as a PDB case on our case management system.

There are elements of information which are able to be extracted from PDB forms for reporting purposes (to get an overview of PDB casework). Those elements contribute to detailed Excel casework reports which give us a comprehensive overview of PDB cases (eg reference numbers and case outcomes).

Some elements of information are not able to be rendered into a report. Unfortunately, the elements which you have specified in your request are examples of this.

The PDB reporting form does indeed let organisations tell us whether there is a high risk to data subjects (living individuals), and lets them tell us whether they have been unable to restore the personal data to how it was before the incident.

These elements of information are not elements which we can run automated reports on.

This means that to find and extract the information you have requested in questions two and three, we would have to manually check through all PDB cases in scope of the date range. I have provided the case figures below to demonstrate why this is an issue here.

Note - PDB "Request Channel"

In our PDB casework overview reports, we don't have an actual, direct category for recording whether a case was reported using the PDB form. However, we do have a "Request Channel" category, and in this category, we can select whether the channel for the PDB case was "Online."

Essentially, this probably means that any PDB case with a "Request Channel" recorded as "Online" should be a PDB case which has been reported to the ICO using the PDB online form.

Casework Figures

The below figures are based on the casework report for all PDB cases we currently have logged on our case management system.

Please note that some cases will have been deleted in line with our retention policy, so older cases may be missing from the figures below. These figures are correct as of today's date (11 November 2024).

The data for each period covers the year beginning on 1 October and ending on 30 September.

	Year		
	Oct 2021 - Sep 2022	Oct 2022 - Sep 2023	Oct 2023 - Sep 2024
PDB cases received "Online"	8	5912	11,766
"Cyber" cases received "Online"	1	2020	3134

Summary

To carry out the search for PDB cases which have been marked as high risk by the organisation, and to carry out the search for PDB cases where personal data hasn't been restored by the organisation, we would firstly need to filter all possible cases in scope of your request by using the PDB casework report.

We would then need to search our case management system using the case references in the report to find the relevant cases.

We would then need to search for the PDB form on the case, and find the relevant sections in there.

Realistically, we would have to allow up to five minutes searching time per case. Unfortunately, you can see that due to the volume of cases, this search would far exceed the cost limit for a FOIA request.

Advice and assistance

You may wish to narrow your request to information about PDB "Cyber" cases, reported "Online," for a particular **sector or sub-sector**. The number of cases in scope of the request may still be high, but depending on which sector was of particular interest, the scope of information could be significantly reduced which could keep the request within the FOIA cost limit.

You may wish to alter your request so that it aligns with the categories in our casework reports. We can easily filter information in our report based on the categories in there. Here are some examples of the categories:

- Request Channel
- Closure Channel
- Incident Type
- Decision (decision by the ICO about the PDB case)
- Cyber Incident (Yes/No)
- Number Affected (people)
- Data Subjects (type of people involved, eg Customers / Employees / Patients / Users / Students / Vulnerable Adults)
- Data Types (Basic personal identifiers / Health data / Criminal convictions/offences / Economic and financial data)
- Further Investigation Required

You may wish to narrow the scope to the number of "Cyber" cases where "Further Investigation Required" has been selected, as these cases would probably be more likely to relate to higher risk incidents (relating back to question two of your request).

We would need to consider if it is in the public interest for us to dedicate the resources necessary to carry out this kind of search, or whether it represents an unreasonable burden on us as a public authority.

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](#)