The ICO exists to empower you through information.

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

18 July 2024

IC-319452-X2M3

Request

On 12 July 2024 you requested the following information:

1. *Data Breaches and Root Causes:*
    - *From the breaches reported to you, how many have a root cause attributed to poor visibility of data flows within the business?*
    - *From the breaches reported to you, how many have a root cause attributed to the lack of data mapping and the maintenance of an up-to-date Record of Processing Activities (RoPA) and Information Asset Register?*
2. *Anonymous Calls:*
    - *How many anonymous calls has the ICO received that relate to conducting a data mapping exercise and building a RoPA and Information Asset Register?*
3. *Correlation Information:*
    - *Does the ICO have information on the correlation between experiencing a data breach and the lack of visibility of data flows?*
4. *ICO's Internal Processes:*
    - *What process does the ICO have in place to maintain and update its RoPA and Information Asset Register?*
    - *Does the ICO use any software solutions for this process? If so, what software solutions are used?*

For points 1 & 2, please provide a breakdown of company size and industry where possible.

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

Response

We hold information that falls under the scope of your request. However, we are refusing the request because to locate the information requested in entirety would exceed the cost limit set out by section 12 of the Freedom of Information Act 2000 (FOIA).

Section 12(2) of the FOIA states that a public authority is not obliged to confirm or deny if requested information is held if the estimated cost of establishing this would exceed the appropriate cost limit. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 stipulates that the 'appropriate limit' for the ICO is £450. We have determined that £450 would equate to 18 hours work.

It is not possible electronically extract a list of breaches which have '*a root cause attributed to poor visibility of data flows within the business'* or *'a root cause attributed to the lack of data mapping and the maintenance of an up-to-date Record of Processing Activities (RoPA) and Information Asset Register'.* This is because we do not categorise personal data breach cases in this way, nor are our casework systems fully keyword searchable.

Even if they were, data breaches and their underlying causes can be complex, and to categorise these according to your criteria would require us to make a subjective decision in each case based on the evidence available. This would involve manually checking the information recorded on every case.

We hold thousands of personal data breach cases with multiple items attached to each. It is unclear how we could target our searches to narrow down the number of cases we would need to check, as the issues you have identified could, in theory, apply to any data controllers, sectors or incident types.

Assuming it took two minutes to check each personal data breach case we hold (and in many cases it would take longer), it would take over 33 hours just to check 1000 of these cases, which would certainly exceed the 18 hours which would accrue a charge of £450 or less, triggering the provisions of section 12 of the FOIA. On this basis, we are refusing your request.

Advice and assistance

In relation to point 1, we already publish some details about personal data breaches reported to us and this can be broken down by sector. You might also

be interested in the information we publish as part of our data security incident trends, our annual reports and action we've taken.

We have considered how you might refine this part of your request to bring it within the cost limit. We could consider requests limited by time period, sector or organisation, and our data sets (link above) offer some examples of the criteria that can be used to refine our searches. However, any request that requires us to conduct manual searches of large numbers of cases may be refused on the same basis as this request. Furthermore, it is unclear how helpful smaller samples would be in relation to the issues that are of interest to you, unless you want to see how these affect a particular data controller, time period or type of case.

In relation to point 2, we do not record calls in the level of detail that would be required to answer this part of your request. Some information about calls we receive is provided in our annual reports, although this is restricted to the basic details we log such as number received and whether these were from individuals or organisations. We do not categorise calls according to whether or not they are anonymous, nor do we record individual telephone calls in entirety. Where call notes or summaries are made, it is not possible for us to cover all of these using electronic searches, particularly where these relate to specific cases, as we would need to manually check individual case records. This would pose similar challenges to those described above, so any refined request would require more specific parameters to bring it within the cost limit.

In relation to point 3, we do not record information in this way, but would need to check each case manually as described above in order to identify any patterns or correlations as suggested. With this in mind we refer you to the advice on refining your request given in relation to point 1.

In relation to point 4, we don't have a specific written process for maintaining or updating these types of document. In relation to IARs, our Information Management team contact different teams within the ICO annually to prompt reviews and updates, as well as providing guidance and support on recording relevant details. The ROPA is updated as and when required with reference to compliance criteria. We don't have any specific software solutions beyond what we use to produce relevant templates and guidance, and to correspond with any relevant parties.

You might also be interested to know that we have recently published our ROPA in response to another information request here. We have previously disclosed information about our information asset registers here.

If you do decide to refine your request, please note that any request requiring us to manually search large numbers of records is likely to exceed the appropriate limit, and the accuracy of any such searches could not be guaranteed. Consideration can also be given as to whether the value to the public of any resulting information is proportionate to the effort to locate it, particularly given the issues regarding accuracy described.

This concludes our response to your request.

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