Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
T. 0303 123 1113 F. 01625 524510

2 August 2023

IC-245917-W7Z9

**Request**

You asked us:

*"I would like to receive all commercial data security incident reports dating back to Jan 2013.*

*If such a data points can be included, I would like to identify whether incidents were deemed to have been caused by improper or inadequate storage of data. I also have interest in the estimated costs to businesses as a result of incidents.*

*If accessible to the public, I would like to identify locations, as accurately as possible (by town or county, for example) of reported incidents."*

Your request has been handled under the Freedom of Information Act 2000 (the FOIA). As you are probably aware, this legislation provides public access to recorded information held by a public authority unless an appropriate exemption applies.

**Our response**

I am refusing the Freedom of Information request you have made because the amount of work involved in complying with it would place a grossly oppressive burden on our resources, meaning that we are able to rely on Section 14 (1) of the FOIA.

Section 14 (1) FOIA states that:

*'14.—(1) Section 1(1) does not oblige a public authority to comply with a request for information if the request is vexatious.'*

The ICO's guidance explains that:

*"A single request taken in isolation, …….may be vexatious solely on the grounds of burden. That is, where complying with the request would place a grossly oppressive burden on your resources which outweighs any value or serious purpose the request may have."*

While we do not doubt that you have a genuine interest in the information you have requested, we have determined that the burden placed on our resources in complying with this request would outweigh the public interest in the requested information.

Our guidance further provides that, in order to refuse to respond to a request under s.14(1) due to burden alone, we should be able to establish firstly that the requested information is voluminous, secondly that we have real concerns about exempt information being contained within it, and thirdly that the exempt material is scattered throughout and cannot be easily isolated. I have provided further explanation of our consideration of this below.

Firstly, the ICO regularly disposes of records in line with our Retention and Dispoal Policy. Our policy states that we dispose of personal data breach (PDB) reports after 2 yesrs in cases where no regulatory action was taken, or 6 years in cases where regulatory action was taken. This means that we do not hold PDB records dating back to 2013.

As reported in our Annual Report, more that 9000 PDBs are reported to the ICO every year. In order to disclose a breach report, we would need to contact each organisation that reported a breach about the material contained in the report and whether or not it was appropriate for disclosure under FOIA. As you are likely aware, disclosure under FOIA is considered disclosure to the wider world.

Many PDB reports include sensitive information about the organisations involved that would prejudicial to disclose to the wider world. This means that in many, if not most, cases, we would be unable to disclose the reports. The drain on resources to contact the many thousands of organisations about their PDB reports would outweigh the amount of information that we would actually be able to disclose.

Our guidance states that the threshold for applying s.14 FOIA on the basis of burden is a higher one than for s.12 FOIA, which allows a public authority to refuse to comply with a request if the necessary searches involved in doing so would take longer than 18 hours. We are relying on s.14 here because the

burden is related to the time required for reviewing and redacting the relevant information, rather than searching for information that may be in scope.

Our casework system records the organisation that submitting a PBD, the date of submission, and the outcome of our review of the report. We record what sector each organisation is, but we do not record if they are commercial business. Our system also does not record the nature of the breach. This means that we would have to manually check every PDB to identify if the organisation is a commercial business and the cause of the breach.

We estimate that checking a report manually takes an average of 3.5 minutes. In the 2022-23 financial year, the ICO received 9146 PDB reports. This means it would take 533.5 hours to find the information you requested for one financial year alone. This far exceeds the 18 hour limit to search for information detailed above. This also does not include the time it would take us to contact each organisation that submitted a PDB.

We therefore advise that we are refusing to comply with this request under s.14(1) of the FOIA.

However, we do proactively publish related information related to your queries. We publish quarterly data sets of all the PDB reports we receive. These reports include the name of each organisation, the sector, and the outcome of our investigation into their PDB.

We also publish information on data security incident trends. This page provides more accessible ways to explore information about PDBs reported to the ICO.

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 here.

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 set out your rights. Our retention schedule can be found here.

Yours sincerely

Information Access Team
Risk and Governance Department, Corporate Strategy and Planning Service
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**