25 September 2023

Case Reference IC-254210-Y5V1

Your request

You asked us for the following:

"*1 The total number of GDPR / Data protection breaches reported to the ICO by the PSNI in the last two years, up to and including 25 August 2023?*

2 The total number of GDPR / Data protection breaches reported to the ICO by the PSNI, which resulted in action being taken, in the last six years, up to and including 25 August 2023?

3 Please provide copies of the reports and/or summary of each case where advice has been given or action has been taken. (I understand the redaction of sensitive information such as officer names or identifiable information may be required.)

4 Please show any correspondence between the ICO and the PSNI in the three years, up to and including 25 August 2023, relating to FOIA compliance and data management not related to individual reported breaches."

Where your questions satisfy the criteria of a valid information request, we have considered your request under the Freedom of Information Act 2000 (FOIA).

Our response

We can confirm that we hold information within scope of your request as follows:

1. Between 26 August 2021 and 25 August 2023 we have received 30 personal data breach reports from PSNI.

2. Our records for personal data breach reports held date from January 2019. For that period we hold records for 52 breach referrals. None of these resulted in formal regulatory action, though three cases remain open.

   The ICO has issued a reprimands to PSNI on 14 March 2019 and a Notice of Intent to issue a reprimand on 27 July 2023.

The ICO has recently carried out a consensual audit of PSNI. You can find the executive summary of the report here.

Regarding parts 3&4 of your request:

It is likely that the ICO will have given some advice to PSNI for most if not every breach received. We are also processing information in relation to over 160 data protection and FOI complaints about PSNI, many of which are likely to have involved the exchanging of advice. The advice may well have been generic and at any rate will likely reflect the general advice we give on our website regarding data protection compliance.

The ICO does engage with PSNI on a regular basis regarding its compliance with both data protection and freedom of information legislation, both in terms of general compliance as well as in relation to individual items of casework. The ICO has also engaged substantively with PSNI regarding the recent consensual audit it undertook.

However, this information is exempt under sections 31 of the FOIA. We shall now explain our reliance on this exemption, but in summary we consider it to be prejudicial to the pursuance of our current investigation into the recent high profile breach reported by PSNI to engage with them on the disclosure of the information you have requested or for the ICO to consider such a disclosure until the investigation is concluded.

Section 31

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 …"

The information contained in any advice we have given to PSNI and any correspondence shared with them from the ICO clearly

constitutes our law enforcement and regulatory functions.

In order to decide what information is disclosable, the ICO would have to consult with PSNI on every piece of correspondence, as well as check that the advice it has given in scope of part 3 of your request did not itself reveal information provided by PSNI – which then would have to be consulted on. Please note that it is a criminal offense under section 132 of the Data Protection Act for any member of ICO staff to disclose information supplied by an organisation for regulatory functions without 'lawful authority', which usually involves seeking consent from said organisation. Moreover, the ICO would also need to seek the opinion of internal staff in various departments to check that any outgoing information would not prejudice the pursuance of current investigations and/or engagement with PSNI.

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.

Our investigation into the recently reported high profile data breach from PSNI is still ongoing. To release the information you have requested, despite the fact that it may not directly relate to the breach itself, could prejudice the ICO's ability to conduct the investigation in an appropriate manner. Disclosure at this stage of any information regarding compliance discussions with PSNI would discourage our ongoing discussions between the ICO and PSNI and may damage our ability to conduct and conclude the investigation fairly and proportionately.

This is especially the case with our engagement with PSNI regarding the recently completed audit, which may also involve information relevant to the breach and its investigation. However, consulting with PSNI on the disclosure of *any* of our correspondence would likely distract them, and the ICO, from the principle task of mitigating and resolving the issues revealed in the data breach.

Disclosure could also jeopardise the ICO's ability to obtain information relating to this case or others in the future.

Disclosure is likely to result in other parties being reluctant to engage with the ICO in the future.

The Public Interest Test for Section 31

In this case the public interest factors in disclosing the information are:

- increased transparency in the way in PSNI has engaged with the ICO regarding its compliance with information legislation
- increased transparency in the way in which the ICO conducts its regulatory activity.

The factors in withholding the information are:

- the public interest in maintaining organisations' trust and confidence that their replies to the ICO's enquiries will be afforded an appropriate level of confidentiality;
- the public interest in allowing both parties (the ICO and PSNI) to prioritise engagement regarding the high profile breach of sensitive data without the distraction of considering, discussing and disclosing or exempting related and unrelated information
- the public interest in organisations being open and honest in their correspondence with the ICO without fear that their comments will be made public prematurely or, as appropriate, at all; and
- the public interest in maintaining the ICO's ability to conduct its regulatory activity as it sees fit

Having considered these factors, we are satisfied that it is appropriate to withhold the information. However, once the investigation into the recent breach is fully concluded it is likely that the public interest would shift and we would be able to freely consult with PSNI on the disclosure of the requested information. Any regulatory outcome of the current investigation is likely to be published on our website.

This concludes our response.

We hope you find this information helpful.