ICO Disclosure Log
Response to Request

Reference: IRQ0548264
Date of response: 08/08/2014

Request

Via Twitter:

Please provide details of the "non-trivial data security incident" ICO had in the last 12mnths

Response

Further to our acknowledgement of 23 July 2014 we can now respond to your request for information dated 16 July 2014.

As you know we have dealt with your request in accordance with your 'right to know' under section 1(1) of the Freedom of Information Act 2000 (FOIA), which entitles you to be provided with a copy of any information 'held' by a public authority, unless an appropriate exemption applies.

Request

In your tweet of 16 July you asked *"Please provide details of the "non-trivial data security incident" ICO had in the last 12mnths…"*.

Reference to the data security incident you refer to was included at page 46 of the Information Commissioner's annual report for 2013/14, which was published on 15 July and can now be accessed via our website here. This states:

"There has been one non-trivial data security incident. The incident was treated as a self reported breach. It was investigated and

treated no differently from similar incidents reported to us by others. We also conducted an internal investigation.

It was concluded that the likelihood of damage or distress to any affected data subjects was low and that it did not amount to a serious breach of the Data Protection Act. A full investigation was carried out with recommendations made and adopted. The internal investigation was also concluded."

Our associated press statement relating to this breach reads as follows:

"This incident was treated as a self-reported breach, and was investigated in the same way we would handle any similar incidents reported to us by others.

It was concluded that it did not amount to a serious breach of the Data Protection Act, and the internal investigation was concluded.

We are unable to provide details of the breach at this stage, as the information is linked to an ongoing criminal investigation."

Information Held/ Withheld

We have carefully considered for disclosure all the information we hold which relates to this data security breach. However, we are unable to provide any of it to you for the following reasons.

Firstly, we are withholding much of this information in reliance on section 30 of the FOIA, which concerns investigations and proceedings conducted by public authorities.

Specifically, section 30(1) of the FOIA states:

30(1) Information held by a public authority is exempt information if it has at any time been held by the authority for the purposes of –

(a) any investigation which the public authority has a duty to conduct with a view to it being ascertained -
(i) whether a person shall be charged with an offence, or
(ii) whether a person charged with an offence is guilty of it,
(b) any investigation which is conducted by the authority and in the circumstances may lead to a decision by the authority to institute criminal proceedings which the authority has power to conduct, or
(c) any criminal proceedings which the authority has power to conduct'

These purposes apply when the Information Commissioner has determined whether a criminal offence has been committed under any of the information acts he regulates, and whether to take action.

As we have already explained, the information relating to the breach is subject to an ongoing criminal investigation, and as such the exemptions at s30(1)(a)(i) and 30(1)(b) are both engaged. Section 30(1) is a class based exemption, rather than prejudice based, so we do not need to consider any prejudice in disclosing the information you have requested. However, we do have to balance the public interest, that is we must consider whether the public interest favours withholding or disclosing the information you have asked for.

In this case, and at this time, the factors in favour of disclosing this information are:

- Transparency about the way in which the ICO as a data controller ensures the security of the information it holds and processes
- Assurance that this breach was correctly and fully investigated by the ICO and that any recommendations made were acted upon and implemented
- Greater scrutiny of the ICO investigation process, in relation to this or other investigations into possible offences

The factors in favour of withholding this information are:

- Protecting the ability of the ICO as statutory regulator and the authority with the power to conduct such investigations to do so as it sees fit, without external factors prejudicing a particular case
- Maintaining the confidentiality of information and evidence considered as part of the criminal proceedings
- Ensuring that individuals are not deterred or inhibited from participating fully and candidly with the investigation process, either as part of this or future investigations

We find that the balance of public interest lies with maintaining the exemption. It is of the utmost importance that ICO is able to carry out its statutory duty and conduct investigations into potential criminal offences confident that information will not be inappropriately disclosed.

Secondly, some of the information has been withheld in reliance on the exemption at s40(2) of the FOIA, which states:

"Any information to which a request for information relates is … exempt information if … it constitutes personal data … and … the disclosure of the information to a member of the public … would contravene any of the data protection principles".

The information we hold relating to the data security breach does include references to members of staff at the ICO. This personal information is exempt from disclosure under section 40(2) which, by virtue of section 40(3)(a)(i), allows a public authority to withhold information from a response to a request under the FOIA when the information requested is personal data relating to someone other than the requestor, and its disclosure would contravene one of the Data Protection principles.

We consider that none of the individuals referred to in this information would anticipate or expect their details to be disclosed to anyone outside the ICO. Therefore, we consider that such a disclosure would be unfair and in breach of the first Data Protection principle which states that *"Personal data shall be processed fairly and lawfully …".* It is for this reason that it is being withheld you in reliance on section 40(2) of the FOIA.

Advice and assistance

Although we are unable to disclose any of the information relating to this data security breach at this time, it may be helpful to try to explain our actions following the 'non-trivial data security breach'.

As the notice in our annual report confirms, we reported the data security breach to the ICO as a regulator. The incident was then investigated by the ICO in the same way as any other incidents reported by a data controller.

We considered the ICO's published guidance for data controllers 'Notification of data security breaches to the ICO', which is available here.

As this data security incident relates to an ongoing criminal investigation it is highly unlikely that any further comments will be made by the ICO regarding this breach until that criminal investigation is complete. At that time, however, it is likely the ICO will make a clear public statement about what occurred and the action taken.

Review Procedure

If you are dissatisfied with this response and wish to request a review of our decision or make a complaint about how your request has been handled you should write to the Information Access Team at the address below or e-mail accessicoinformation@ico.org.uk.

Your request for internal review should be submitted to us within 40 working days of receipt by you of this response. Any such request received after this time will only be considered at the discretion of the Commissioner.

If having exhausted the review process you are not content that your request or review has been dealt with correctly, you have a further right of appeal to this office in our capacity as the statutory complaint handler under the legislation. To make such an application, please write to our Customer Contact Team at the address given or visit our website if you wish to make a complaint under either the Freedom of Information Act or Environmental Information Regulations.

A copy of our review procedure can be accessed from our website here.