

Case reference RCC0573369

I write further to your email of 26 February 2015, requesting a review of the decision set out in the response to you dated 25 February. This review will consider the handling of your request of 30 January (ref IRQ0569536) and in particular the application of section 31(1)(g) of the Freedom of Information Act 2000 (FOIA) and the consideration of the public interest. Although your email appears to focus on the application of section 31, for completeness I will also review the decision to withhold some information under section 40 FOIA.

I am principal adviser in Performance Improvement and can confirm that I have had no prior involvement in the handling of this request.

Your request for review and the points raised is set out below; this is followed by my internal review findings:-

"I write with a request for an internal review of the decision to refuse to release information to me under the Freedom of Information Act.

As is clear, the requested information relates to one of the most serious data breaches the public has been told about.

Indeed, the ICO's own emails refer to the case as "so high profile and politically sensitive".

The arguments put forward by the ICO for non-disclosure are general, in that they refer to the public interest of protecting process. They are not specific to this "high profile and politically sensitive case". Indeed, the ICO has failed to identify any specific harm that would be caused by releasing this specific information. As the ICO's own guidance on FOIA exemptions makes clear, authorities must provide reasons why the specific information would cause harm, rather than putting forward general arguments in favour of trying to protect process.

It has to be pointed out that the ICO very rarely produces reports on such serious data breaches. It often provides a press release with the details of any penalty but rarely provides transparency surrounding the investigative processes and decisions which led to the penalties. This is a case which requires maximum transparency. The public interest is better served by disclosure of information capable of informing the public further about this "high profile and politically sensitive" case.

The public must have confidence that the regulator in this area isn't "weak and defensive" - as its emails show it was worried about appearing in the context of being unable to answer questions about the breach.

It will also provide the public with details of what the MoJ told the ICO about this breach. It is of note that it took the MoJ two weeks to alert the ICO to the breach. This is confirmed by the MoJ's disclosure that it found out the discs were missing on January 8 and an ICO press response that it

was contacted about it on January 22. The information may show what the ICO has done about it since then. The information may also demonstrate why the ICO didn't inform the Mail on Sunday that information on two other high profile cases was also missing. It may also show why there was apparent surprise that Number 10 had commented on the story.

It is also worth noting that disclosure of the requested information is not capable of prejudicing the outcome. It is up to the ICO to decide if there should be a CMP. There is no judge and jury.

I look forward to the ICO being fully transparent about this high profile and politically sensitive case."

I have carefully considered the points you make and also carefully reviewed and considered all of the information held falling within the scope of your request including that which has already been disclosed. My findings are as follows.

In relation to the information which has been redacted from the disclosed information as not being within the scope of your request I agree with that decision.

In relation to the redactions made under section 40(2) FOIA, third party personal data, by virtue of section of section 40(3)(a)(i), I find that disclosure of this information, with the exception of the content of one email, would be a breach of the first principle of the Data Protection Act 1998 (DPA).

The email to which I refer is an unsolicited email from a third party sent to Christopher Graham on 30 January, in response to the BBC news report concerning the data loss by Ministry of Justice. The content of this email is now disclosed in full (attached) with the exception of the personal data of the third party, ie name and contact details redacted under section 40(2) FOIA.

I turn now to the application of section 31(1)(g) FOIA. The vast majority of information held in relation to your request, apart from a small amount of personal data which has been redacted, has already been disclosed. Section 31(1)(g) has been applied in relation to one further document. As stated above, I have carefully reviewed this information and considered its content. My finding in relation to the information contained in this document is that section 31(1)(g) is engaged by virtue of the purposes referred to in section 31(2)(a) and (c). I will explain in more detail below.

Section 31(1)(g) is a qualified exemption so I have also had to consider whether in all the circumstances of this case the public interest in maintaining the exemption outweighs the public interest in disclosure. For the reasons set out below you will see that I have concluded that it does.

The exemption.

Section 31(1)(g) provides that:

Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice-

(g) the exercise by any public authority of its functions for any of the purposes specified in subsection (2)

Section 31(2)(a) and (c) provides that:

The purposes referred to in subsection (1)(g) to (i) are-

(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 ICO exercises a number of statutory functions for the purpose of ascertaining whether a public authority/data controller has failed to comply with the law and/or for the purpose of ascertaining whether circumstances exist or may arise which would justify regulatory action in relation to relevant legislation.

A considerable proportion of the ICO's regulatory work is concerned with ascertaining whether public authorities/data controllers have complied with the statutory requirements placed upon them by both the DPA and FOIA.

Clearly the information you have requested relating to, as you state in your request, "an alleged data breach" is information which the ICO needs to consider in determining whether a data controller has breached the DPA. It follows therefore that the purposes referred to in subsection (a) and (c) above apply in relation to this information. Disclosure of this information in relation to the ICO's regulatory work, particularly in relation to a live case would, in my opinion, be likely to prejudice the ICO's regulatory functions. It is also my opinion that disclosure would have the effect of inhibiting open dialogue between the ICO and public authorities/data controllers.

In order to carry out a cost effective, timely and efficient regulatory function the ICO must maintain the trust and confidence of the public authorities/data controllers it regulates to ensure their co-operation. The best way to achieve this is by informal, open, voluntary and uninhibited exchange of information with these public authorities/data controllers. In my opinion this informal exchange of information and co-operation by public authorities/data controllers would be likely to be adversely affected if details of their failings, as discussed in those informal exchanges, were routinely made public. The consequence of this would be that the ICO would be unable to provide an appropriate level of service and its

regulatory functions would be prejudiced. It is my view that disclosure of the withheld information would be likely to prejudice the ability of the ICO to carry out its regulatory functions of monitoring the performance of public authorities to ensure compliance with the relevant law. It would be likely to prejudice the exchange of information between the ICO and public authorities/data controllers which would become more guarded and cautious in proactively providing information if they thought it would be disclosed. This would in turn be likely to prejudice the effectiveness of the ICO's regulatory processes.

For the reasons set out above I have concluded that section 31(1)(g) is engaged, in that disclosure of the requested information would be likely to prejudice the ICO's regulatory functions. I have therefore gone on to consider whether the public interest arguments lie in favour of disclosure or in favour of maintaining the exemption.

In addition to the factors set out by my colleague Janine Gregory in her response to you, I have also considered the following matters.

Public interest in favour of disclosure.

There is a clear public interest in the ICO being open and transparent in the way it monitors the performance of public authorities/data controllers in relation to their duties and responsibilities under the relevant legislation. Such openness and transparency helps to promote public awareness and understanding of the ICO regulatory functions.

Further information about the way the ICO monitors the performance of specific public authorities/data controllers would be of interest to those members of the public who have a particular interest in those public authorities/data controllers. This might be because they already have been personally affected by the decision or actions of a particular public authority/data controller or because the particular public authority/data controller has already attracted media attention as a result of its failings. There is also a public interest in the ICO publishing information which would help to demonstrate that it is complying with its statutory duties by overseeing the performance of public authorities/data controllers with reference to the relevant legislation. The publication of this information would be evidence that the ICO is providing an appropriate standard and quality of public service and would demonstrate accountability.

Disclosure of the information could provide fuller evidence as to whether the ICO was exercising its regulatory functions efficiently and effectively.

In addition you state in your email requesting a review that the ICO rarely reports on serious data breaches, that this is a case which requires maximum transparency and that the public interest is better served by

disclosure of information capable of informing the public further about this “high profile and politically sensitive case”.

Public interest in favour of maintaining the exemption.

There is a public interest in the ICO complying with the law. For example, there is expectation that it will comply with section 59(1)(a) of the Data Protection Act 1998 (DPA) by ensuring that the details it receives about public authorities/data controllers in the course of its investigations remain confidential. Section 59(1)(a) states, subject to certain conditions applying:

'No person who is or has been the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner shall disclose any information which – (a) has been obtained by, or furnished to, the Commissioner under the purposes of the information Acts'.

In the light of section 59(1)(a) of the DPA there is generally an expectation on the part of public authorities/data controllers that the information they disclose to the ICO will not normally be disclosed. If the ICO were to routinely disclose all such information in every case this would inevitably hinder the flow of information in the future. This in turn would prejudice the effectiveness and efficiency of the ICO's regulatory functions.

There is a public interest in the ICO providing a cost effective, timely and efficient regulatory function of public authorities/data controllers through co-operation and open dialogue to ensure compliance with the relevant legislation. To do this the ICO must maintain the trust and confidence of the public authorities/data controllers it regulates and ensure their co-operation is maintained. This is best achieved by an informal, open, voluntary and uninhibited exchange of information with public authorities/data controllers. I consider that co-operation from public authorities/data controllers may be adversely affected if details of their failings were to be made public. This would in turn prejudice the ICO's ability to deliver the levels of service required of it. For example, if the ICO could no longer rely on the informal co-operation of authorities it might be forced to resort to regulatory intervention such as the use of Information Notices (under section 51 (1) of the Act) more often. Use of such measures would divert staff resource, and may have a cost implication for the ICO. This would have a detrimental impact upon the level of service the ICO is able to provide to the public it serves. In addition, in my opinion, recourse to these powers would, as an alternative to informal discussions, make the process of engagement with public authorities more drawn out and less effective by reducing open dialogue.

There is a public interest in having an effective and efficient regulator of

public authorities/data controllers to ensure compliance with the relevant law.

There is also public interest in encouraging public authorities/data controllers in being open and honest about any difficulties they are experiencing, without fear that any such issues will be made public prematurely, or (where appropriate) at all. In my opinion disclosure of the withheld information may dissuade authorities/data controllers from being open and honest with it going forward. For example, public authorities/data controllers may no longer proactively approach the ICO about the problems they are facing, prejudicing its ability to promote observance of the relevant legislation.

Having considered the public interest arguments both for and against disclosure I am not satisfied that there is sufficient weight within the arguments to favour disclosure. In my opinion maintaining an informal process for the gathering of information, in connection with compliance with both DPA and FOIA is essential to maintaining the ICO's role as an effective and efficient regulator of the legislation. To disclose the withheld information would erode this facility which would place undue strain on available resources and undermine the ability of the ICO to monitor activity and influence behaviour. In light of the above I find that the public interest in maintaining the exemption in section 31(1)(g) outweighs the public interest in disclosure.

Finally, I note in your email requesting an internal review you make reference to "weak and defensive" and on four separate occasions "high profile and sensitive". These phrases, it should be borne in mind, were part of a consideration about the merits of accepting an interview bid with Radio 4's PM. Clearly the request in relation to an "alleged data breach" following the MoJ statement would be considered high profile and politically sensitive, however, the reference to "weak and defensive" relates to a possible perception that due to being unable to discuss specifics during our investigation, accepting the bid and only being able to focus on our basic message could be misconstrued.

I hope that you find this helpful. However if you are dissatisfied with the outcome of this review you may make a section 50 complaint to the ICO.

How to complain

Information on how to complain is available on the ICO website at:

http://www.ico.gov.uk/complaints/freedom_of_information.aspx

By post: If your supporting evidence is in hard copy, you can fill in the Word version of our complaint form, print it out and post it to us with

your supporting evidence. A printable Freedom of Information Act complaints form is available from the ICO website. Please send to:

First Contact Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

By email: If all your supporting evidence is available electronically, you can fill in our online complaint form. Important: information included in the form, and any supporting evidence will be sent to us by email.