

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 15 September 2016

Public Authority: The Information Commissioner's Office (ICO)

Address: Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Note: This decision notice concerns a complaint made against the Information Commissioner (the Commissioner). The Commissioner is both the regulator of the FOIA and a public authority subject to the FOIA. She is therefore under a duty as regulator to make a formal determination of a complaint made against her as a public authority. It should be noted, however, that the complainant has a right of appeal against the Commissioner's decision, details of which are given at the end of this notice. In this notice the term 'ICO' is used to denote the ICO dealing with the request, and the term 'Commissioner' denotes the ICO dealing with the complaint.

Decision (including any steps ordered)

1. The complainant has requested information relating to an audit of TalkTalk. The ICO refused to disclose the requested information under section 31(1)(g) with subsection (2)(a) and (c) and section 40(2) FOIA.
2. The Commissioner's decision is that the ICO has correctly applied section 31(1)(g) with subsection 2(c) and section 40(2) FOIA to the withheld information.
3. The Commissioner requires no steps to be taken.

Request and response

4. On 20 October 2015 the complainant requested information of the following description:

"The Information Commissioner carried out an audit of TalkTalk, the conclusion of which was announced on the ICO's website on 17th December 2014. The executive summary was not published.

I would like to request the following information.

- 1) The Executive Summary of the Audit Report.
- 2) The full report.
- 3) Any information or correspondence sent by the ICO to TalkTalk as a result of the final report.

Needless to say, I consider that the recent security incident involving TalkTalk, and their public statements that they have not breached the Data Protection Act, substantially shift the public interest in favour of disclosure."

5. On 16 November 2015 the ICO responded. It refused to disclose the information requested at parts 1 and 2 of the request under section 31(1)(g) with subsection (2)(a) and (c) FOIA. It provided the information requested at part 3 of the request but made redactions under section 40(2) FOIA.
6. The complainant requested an internal review on 22 December 2015. The ICO sent the outcome of its internal review on 22 January 2016. It upheld its original position.

Scope of the case

7. The complainant contacted the Commissioner on 5 February 2016 to complain about the way his request for information had been handled.
8. The Commissioner has considered whether the ICO was correct to apply section 31(1)(g) with subsection 2(a) and (c) and section 40(2) FOIA to the withheld information.

Reasons for decision

Parts 1 and 2 of the request

9. The ICO has argued that the withheld information is exempt on the basis of section 31(1)(g) which provides that information is exempt if its disclosure would or would be likely to prejudice the exercise by any public authority of the functions set out in 31(2) of FOIA.
10. The purpose that the ICO has argued would be likely to be prejudiced if the information was disclosed is section 31(2)(a), the purpose of ascertaining whether any person has failed to comply with the law, and section 31(2)(c), ascertaining whether circumstances would justify regulatory action.
11. In this case, in order for section 31(1)(g) of FOIA to be engaged, the ICO must be able to demonstrate that the potential prejudice being argued relates to the interest contained in section 31(2)(a) and/or (c).
12. As with any prejudice based exemption, a public authority may choose to argue for the application of regulation 31(1)(g) on one of two possible limbs – the first requires that prejudice 'would' occur, the second that prejudice 'would be likely' to occur.
13. The ICO has stated that they believe the likelihood of prejudice arising through disclosure is one that is likely to occur, rather than one that would occur. While this limb places a weaker evidential burden on the ICO to discharge, it still requires the ICO to be able to demonstrate that there is a real and significant risk of the prejudice occurring.
14. The Commissioner has considered the application of section 31(1)(g) with subsection (2)(c) in the first instance. He has therefore considered whether the ICO is formally tasked with ascertaining whether circumstances would justify regulatory action.
15. The Commissioner is aware that the ICO has statutory powers to take regulatory action under the Privacy and Electronic Communications Regulations by virtue of Part V and Schedules 6-9 of the Data Protection Act 1998 as amended by Regulation 31 Privacy and Electronic Communication Regulations 2003 and 2011 (PECR).
16. The ICO has argued that it is essential that it is able to carry out its regulatory functions effectively. This includes being able to audit the measures taken by providers of a public electronic communications

- service (service providers) to safeguard the security of that service under PECR.
17. The Commissioner is satisfied that the ICO is formally tasked with ascertaining whether circumstances would justify regulatory action.
 18. The Commissioner has therefore gone on to consider the ICO's arguments as to why it considers disclosure of the withheld information would be likely to prejudice its ability to ascertain whether circumstances would justify regulatory action.
 19. The ICO has argued that its ability to conduct sound audits of service providers would be likely to be prejudiced if they felt constrained from sharing with the ICO full details of the technical and organisational security measures they have taken to safeguard the security of their service because this information might be disclosed into the public domain without their consent.
 20. The ICO considers that disclosure of this type of information, without the consent of the service provider would be likely to have the effect of inhibiting open dialogue between the ICO and the organisations it regulates. In addition it argued, it would be likely to have a negative impact on their co-operation and the free flow of information which enables the ICO to operate most effectively and efficiently.
 21. The ICO confirmed that TalkTalk have recently reported a high profile data security incident to it and it is currently investigating the circumstances of this incident. The ICO acknowledged that there is increased interest in the information requested due to this incident and subsequent media reports. However, it argued that these circumstances heighten the need for it to be able to engage with TalkTalk in an open and frank way.
 22. It summarised that the information requested here is relevant to its ongoing relationship with TalkTalk and the release of this information would be detrimental to the ICO's ability to engage effectively with TalkTalk. It is therefore not appropriate for this information to be disclosed.
 23. Given the nature of the withheld information, and based on the ICO's arguments contained in this Notice, the Commissioner considers that the ICO is formally tasked with ascertaining whether circumstances would justify regulatory action. Its ability to fulfil this function effectively is dependent upon it being able to gather full evidence efficiently whilst investigations are ongoing. The Commissioner therefore accepts that disclosure would be likely to result in the

prejudicial effects to the ICO's purposes described at section 31(2)(c) of FOIA.

24. As section 31 is a qualified exemption, the next step is for the Commissioner to consider whether in all of the circumstances of the case the public interest in maintaining the exemption outweighs the public interest in disclosure.

Public interest test

Arguments in favour of disclosing the information

25. The ICO provided the following arguments in favour of disclosure:

- Increased transparency in the way the ICO conducts its PECR audit function.
- Increased transparency around the technical and organisational security measures it reviews when conducting a PECR audit.
- Increased transparency around the technical and organisational security measures adopted by this particular service provider.

Arguments in favour of maintaining the exemption

26. The ICO provided the following arguments in favour of maintaining the exemption:

- It is vital that it is able to have effective and productive relationships with all the service providers it regulates and that they continue to engage with the ICO in an open, cooperative and collaborative way without fear that information they provide to the ICO or the detail of the ICO's working with them will be made public.
- The ICO works hard to engender useful and productive working relationships with the organisations it regulates and disclosing information they have provided to it, against their wishes, is likely to have a detrimental impact on those relationships.
- The potentially detrimental effect providing details of organisational and technical security strengths and weaknesses identified during a PECR audit engagement might have on the service provider's ability to carry on its services securely.
- The need to meet the service providers' expectations of confidentiality and non-disclosure having ascertained their views on the disclosure of the Audit Report and Executive Summary at

the time of the audit and again as part of considering this information request. As explained in its PECR Guide to Audit:

https://ico.org.uk/media/fpr-organisations/documents/1564/guide_to_ico_pecr_audits.pdf

where an audit is consensual, organisations will be asked for their consent to publish and where it is not provided the ICO will only publish a comment.

- The very strong public interest in the ICO being able to investigate security incidents with confidence that organisations are able to make open and frank disclosures to it as the regulator. In turn, those organisations not being concerned that the ICO will publish their information prematurely, if at all.

Balance of the public interest

27. The Commissioner considers that there is a strong public interest in the ICO operating openly and being accountable in its effectiveness in carrying out its statutory functions, in particular its PECR audit functions, relating to such a high profile incident.
28. The Commissioner does however also consider that there is a strong public interest in not disclosing information which would be likely to impede the ICO's ability to carry out its functions effectively. Particularly as in this case the ICO's investigations are ongoing. This carries such weight as it's important for the ICO to have a good working relationship with Talk Talk and the other organisations it regulates.
29. On balance, the Commissioner considers that the public interest in favour of disclosure is outweighed by the public interest in favour of maintaining the exemption. Section 31(1)(g) with subsection (2)(c) FOIA was correctly applied in this case to the withheld information.
30. As the Commissioner considers that section 31(2)(c) was correctly applied in this case, he has not gone on to consider the application of section 31(2)(a) any further.

Part 3 of the request

Section 40(2)

31. Section 40(2) FOIA provides an exemption for information which is the personal data of an individual other than the applicant, and where one of the conditions listed in regulation 40(3) or 40(4) is satisfied.

32. One of the conditions, listed in section 40(3)(a)(i), is where the disclosure of the information to any member of the public would contravene any of the principles of the DPA.
33. The Commissioner has first considered whether the withheld information would constitute the personal data of third parties.
34. Section 1 of the DPA defines personal data as information which relates to a living individual who can be identified:
 - from that data,
 - or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller.
35. In this instance the information in question is the name of an employee of TalkTalk corresponding with the ICO. The Commissioner does consider that this is information from which the data subject would be identifiable and therefore does constitute personal data.
36. The Commissioner has gone on to consider whether the disclosure of this information would be in breach of the first principle of the DPA. The first principle requires, amongst other things, that the processing of personal data is fair and lawful. The Commissioner has initially considered whether the disclosure would be fair.
37. The ICO explained that whilst the data subject was corresponding with the ICO within a professional capacity, they do not occupy a public facing role as the ICO has confirmed that their name would only be put in the public domain by virtue of this correspondence with the ICO. Furthermore the data subject has refused to provide consent to disclosure. The Commissioner therefore accepts that there would have been a reasonable expectation that the withheld information would not be placed into the public domain.
39. The Commissioner has however gone on to consider whether any of the Schedule 2 conditions can be met, in particular whether there is a legitimate public interest in disclosure which would outweigh the rights of the data subject set out above.
40. The Commissioner does consider however that there is a legitimate public interest in increased transparency in the way the ICO conducts its PECR audit function. However disclosure of the information withheld under section 40(2) FOIA would not meet this legitimate public interest in any significant way.
41. After considering the nature of the withheld information, and the reasonable expectation of the data subject, the Commissioner believes that disclosure under FOIA would be unfair and in breach of the first

principle of the DPA and that any legitimate public interest would not outweigh the rights of the data subject in this case.

42. Therefore the Commissioner considers that section 40(2) FOIA is engaged, and provides an exemption from disclosure.

Right of appeal

43. Either party has the right to appeal against this decision notice to the First-tier Tribunal (Information Rights). Information about the appeals process may be obtained from:

First-tier Tribunal (Information Rights)
GRC & GRP Tribunals,
PO Box 9300,
LEICESTER,
LE1 8DJ

Tel: 0300 1234504

Fax: 0870 739 5836

Email: GRC@hmcts.gsi.gov.uk

Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

44. If you wish to appeal against a decision notice, you can obtain information on how to appeal along with the relevant forms from the Information Tribunal website.
45. Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this decision notice is sent.

Signed

Gemma Garvey
Senior Case Officer
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF