

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 23 April 2013

Public Authority: London Borough of Bexley
Address: Bexley Civic Offices
Broadway
Bexleyheath
Kent DA6 7LB

Decision (including any steps ordered)

1. The complainant has requested information about whether any councillor had been subject to a criminal investigation by the Metropolitan Police and further detail relating to that. The London Borough of Bexley (the "Council") refused to confirm or deny whether it held any information within the scope of this request citing section 40(5) (Unfair processing of personal data) as its basis for doing so. It upheld this position at internal review.
2. The Commissioner's decision is that the Council is entitled to rely on the FOIA provision it has cited.
3. No steps are required.

Request and response

4. On 19 July 2012, the complainant wrote to the Council and requested information in the following terms:

"Are Bexley Council aware of any councillor being the subject of a criminal investigation by the Metropolitan Police in the last 18 months? If so, how many?"
5. The Council responded on 10 September 2012 following the Commissioner's intervention. It refused to confirm or deny whether it held any information within the scope of the request citing the personal data exemption at section 40 as its basis for doing so.
6. Following an internal review the Council wrote to the complainant on 15 October 2012. It upheld its original position.

Scope of the case

7. The complainant had initially contacted the Commissioner on 24 August 2012 to complain about the Council's failure to respond to his request. He received a response as outlined above following the Commissioner's intervention. On 25 October 2012 he wrote to the Commissioner to complain about the way his request for information had been handled. Specifically, he disputed whether the information described in his request was personal data and therefore whether the Council was entitled to rely on section 40(5).
8. The Commissioner has therefore considered whether the Council is entitled to rely on section 40(5) (the personal data exemption) as a basis for refusing to confirm or deny whether it holds information within the scope of the complainant's request.

Reasons for decision

9. The right of access to recorded information under section 1 of FOIA is in two parts. Firstly, a public authority must provide confirmation or denial as to whether it holds any of the information described in a request. Secondly, it must provide that information. Both parts are subject to exemptions. In this case, the Council has argued that it is not obliged to provide confirmation or denial because the exemption at section 40(5) applies.
10. Section 40(5) states that:

"The duty to confirm or deny-

(a) does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1) [the requester's personal data], and

(b) does not arise in relation to other information if or to the extent that either

(i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of the Act were disregarded, or

(ii) by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed)."

11. The Council argues that section 40(5)(b)(i) applies because, in its view, it would contravene the first data protection principle of the Data Protection Act ("DPA") if it were to provide confirmation or denial as to whether it holds the information described in the request.
12. The first data protection principle of the DPA states that:

"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions in Schedule 2 is met, and in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."
13. The complainant argues that the requested information is not personal data. Where information is not personal data, the provisions of the Data Protection Act (DPA) do not apply to it and, consequently, section 40 of the FOIA cannot apply.
14. This notice will now look at whether the requested information would be personal data if it were held and, where it would be, whether providing confirmation or denial as to whether it is held would contravene the DPA.

Would the requested information, if held, be personal data?

15. The term "personal data" is defined specifically in the DPA.¹ In determining whether information is personal data, the Commissioner has referred to his own guidance and considered the nature of the requested information.² In general terms, personal data is information which relates to a living, identifiable individual and which is biographically significant about them.
16. Under the requirements of the DPA, personal data must be processed in accordance with the data protection principles of the DPA. The Council has argued that the information described in the request would, if held, be personal data and that confirming or denying it is

¹ <http://www.legislation.gov.uk/ukpga/1998/29/contents>

²

http://www.ico.gov.uk/for_organisations/data_protection/the_guide/key_definitions.aspx

held would be unfair and thus in breach of the first data protection principle of the DPA.

17. The complainant has argued that he does not want information about specific individuals but instead he wants information about the number of councillors that have been the subject of a criminal investigation by Metropolitan Police in the last 18 months.
18. The Council's position is that it must adopt a consistent approach in responding to questions about whether or not it holds records about criminal investigations into identifiable individuals – it must refuse to provide confirmation or denial. If it does not adopt a consistent approach, that would give rise to a contravention of the first data protection principle.
19. The right of access to information under FOIA is the right of access to recorded information. In practical terms, if the Council is obliged to provide confirmation or denial that it holds recorded information, such confirmation or denial would take one of the following forms:
 - No, we do not hold any recorded information showing our awareness as to whether any councillor has been the subject of a criminal investigation by the Metropolitan Police in the last 18 months.
 - Yes, we do hold recorded information showing our awareness as to whether any councillor has been the subject of a criminal investigation by the Metropolitan Police in the last 18 months. However, we are not obliged to give it to you because it is exempt.
 - Yes, we do hold recorded information showing our awareness as to whether any councillor has been the subject of a criminal investigation by the Metropolitan Police in the last 18 months and the number is [X].
20. As can be seen, arguably, at least one of the above scenarios would not give rise to a negative outcome for any of the councillors. The Commissioner accepts that, from that narrow perspective, it can be difficult to understand why the Council believes it must take a consistent approach.
21. In the first scenario, personal data about all of the councillors as identifiable individuals would be disclosed – the Council would disclose that none of them has been the subject of a criminal investigation by the Metropolitan Police in the last 18 months.
22. In the second scenario, there are two possible conclusions that can be drawn from such a response. Firstly, the reader could conclude

that the Council holds a record showing that that one or more of the councillors has been the subject of a criminal investigation by the Metropolitan Police in the last 18 months. Where the Council did not disclose an actual figure, this confirmation would, nevertheless, still reveal that at least one of their number has been under investigation. This, of itself, constitutes personal data about all of the councillors because it would reveal that at least one of them could be the subject of this information.

23. The second possible conclusion from the second scenario is that although the Council holds a record of its awareness as to whether any councillor has been the subject of a criminal investigation by the Metropolitan Police in the last 18 months, that record shows the figure "zero".
24. The Commissioner would observe, in passing however, that it is highly improbable that the Council keeps records so precise as to note whether or not any of the councillors has been the subject of a criminal investigation by the Metropolitan Police such that the record might show "zero", given that this would be such an unusual event. If any record is held at all, it would only be likely to exist where it shows that one or more councillors is/are, in fact, under criminal investigation by the Metropolitan Police or any other law enforcement body.
25. Turning now to the third scenario, where the Council confirms it holds information and provides the number of councillors to whom it relates, the question arises as to whether any of the councillors could then be identified.

Could individuals be identified simply from confirmation that information is held?

26. According to its own website, there are 63 councillors at the Council (3 per each of the 21 wards).³ In the Commissioner's view, were the Council to confirm it held information, regardless of whether it went on to provide the figure in question, it would be relatively straightforward, using local knowledge, for anyone to identify which councillor or councillors from this Council the figure applied to. In reaching this view, the Commissioner has had particular regard for his own technical guidance which states:

"When considering identifiability it should be assumed that you are not looking just at the means reasonably likely to be used by the ordinary man in the street, but also the means that are likely to be

³ <http://www.bexley.gov.uk/index.aspx?articleid=421>

used by a determined person with a particular reason to want to identify individuals. Examples would include investigative journalists, estranged partners, stalkers, or industrial spies".⁴

27. In the Commissioner's view, given the public role undertaken by councillors and their close relationship with the local community, it would be relatively easy for a determined person, particularly with local knowledge, to identify which councillor(s) the information related to. The Commissioner has had regard to the circumstances of this case in reaching this view.
28. Where the Council went on to provide the number (as in the third scenario) it would, in the Commissioner's view be even easier to identify which councillor or councillors this information related to.
29. The Commissioner would add that even if the Council gave only the minimum amount of information, e.g., confirmation that it held something about one or more of the councillors, this would put all the councillors under a cloud of public suspicion. It would disclose that one or more of their number was the subject of an allegation of criminality.
30. The Commissioner would also note that where a councillor or councillors has/have been the subject of a criminal investigation in the past 18 months that would constitute an unproven allegation until such time as the individual or individuals were prosecuted after the conclusion of the due process of law. Such information (regardless of whether it was proven or not) would therefore be sensitive personal data within the meaning of section 2 of the DPA (see note 1). As noted above, the DPA imposes extra rules about the processing of sensitive personal data which must be satisfied before personal data can be processed.
31. The Commissioner has set out the above three scenarios to illustrate the dilemma facing the Council. As noted above, not all the scenarios would result in obvious detriment for any of the councillors. However, if the Council were to only provide confirmation or denial where that did not give rise to harm to any of the councillors (for example, the first scenario), a subsequent refusal to provide confirmation or denial could reasonably be construed as confirmation that it did hold such personal data about one or more of the councillors. This would, in effect, involve the disclosure of personal data about all the

4

http://www.ico.org.uk/for_organisations/data_protection/the_guide/~media/documents/library/Data_Protection/Detailed_specialist_guides/PERSONAL_DATA_FLOWCHART_V1_WITH_PREFACE001.ashx

councillors. The fact that it would not be an accurate disclosure about all of them (unless they were all the subject of a criminal investigation) is not relevant. Section 40 relates to the disclosure under FOIA of personal data, not the disclosure of accurate personal data, although accuracy can be a factor in considering fairness.

32. The Commissioner concludes therefore that the Council is seeking to adopt a consistent approach by refusing to provide confirmation or denial because to do otherwise could involve the disclosure of personal data – it would tell the public that it holds something within the scope of the request about one or more of the councillors.
33. Having concluded that any approach other than a consistent refusal to provide confirmation or denial would reveal something about one or more of the councillors, the Commissioner then considered whether providing such confirmation or denial would be unfair.

Would providing confirmation or denial be unfair

34. In deciding whether providing confirmation or denial would be unfair, and thus breach the first data protection principle, the Commissioner takes into account a range of factors including:
 - The reasonable expectations of the individual in terms of what would happen to their personal data. Such expectations could be shaped by:
 - what the public authority may have told them about what would happen to their personal data;
 - their general expectations of privacy, including the effect of Article 8 of the European Convention on Human Rights;
 - the nature or content of the information itself;
 - the circumstances in which the personal data was obtained;
 - particular circumstances of the case, e.g. established custom or practice within the public authority; and whether the individual consented to their personal data being disclosed or conversely whether they explicitly refused.
 - The consequences of confirmation or denial, i.e. what damage or distress would the individual suffer if confirmation or denial was provided? In consideration of this factor, the Commissioner may take into account
 - whether information of the nature requested is already in the public domain;
 - if so, the source of such a disclosure; and

- even if the information has previously been in the public domain does the passage of time mean that disclosure now could still cause damage or distress?
35. Furthermore, notwithstanding an individual's reasonable expectations or any damage or distress caused to them by confirmation or denial, it may still be fair to provide that confirmation or denial if it can be argued that there is a more compelling and legitimate interest in doing so.
36. In considering 'legitimate interests' in order to establish if there is such a compelling reason for confirmation or denial, such interests can include broad general principles of accountability and transparency for their own sakes as well as case specific interests. In balancing these legitimate interests with the rights of the individual in question, it is also important to consider a proportionate approach, i.e. it may still be possible to meet the legitimate interest by partial confirmation or denial in relation to some of the requested information rather than viewing confirmation or denial as an all or nothing matter.
37. As noted above, the processing of sensitive personal data under the FOIA must be fair and lawful and must be in accordance with one of the conditions of Schedule 2 of the DPA (as well as one of the conditions of Schedule 3 of the DPA) (see Note 1).
38. If one of the two limbs of the first data protection principle of the DPA cannot be satisfied, the provision of confirmation or denial would contravene that data protection principle. A public authority would therefore be entitled to rely on section 40(5) as a basis for refusing to provide confirmation or denial.

The complainant's arguments

39. The complainant drew attention to on-line articles regarding one of the councillors to indicate that certain information was in the public domain.

The Council's arguments

40. The Council set out detailed arguments as to why it was entitled to rely on section 40(5) as a basis for refusing to confirm or deny whether it held any of the requested information. The Commissioner does not propose to reproduce them on the face of this notice in order to avoid providing a response to the complainant's request via this notice.

41. However, the Commissioner can highlight some of the points raised by the Council:
- Although there are on-line articles available around this general topic, these articles contain unsubstantiated allegations.
 - It must have regard for its duties under the Human Rights Act when considering matters of privacy relating to councillors.
 - Providing a response would involve the processing of personal data that was outside the reasonable expectations of the councillors.

The Commissioner's conclusion

42. When considering any of the exemptions within section 40, the Commissioner focusses on fairness – would it be fair in all the circumstances of this case to provide confirmation or denial as to whether it holds the requested information? Where the information in question is sensitive personal data, one of the conditions in Schedule 3 of the DPA must also be satisfied to permit confirmation or denial without breaching the first data protection principle of the DPA. To meet one of the conditions described in Schedule 3 constitutes a very high test for processing. This reflects the sensitivity of the information in question.
43. The Commissioner thinks that where information is sensitive personal data, the data subject (in this case, any of the councillors) has a greater expectation of confidentiality. The Commissioner also thinks that such an expectation is both reasonable and legitimate given the type of information in question. In this case, the information, if held, would be about allegations of criminality.
44. Where a person has allegations of criminality made against them, particularly in a high profile case, a certain amount of information will inevitably be put into the public domain about them as part of the process of law enforcement and as a consequence of media reports, particularly if the matter goes to court. However, that is not the case here because the Commissioner is only aware of unsubstantiated allegations that the complainant has drawn to his attention. The fact that unsubstantiated allegations have been put into the public domain, does not, in the Commissioner's view, add weight to the argument in favour of providing confirmation or denial.
45. In light of the above, the Commissioner has concluded that the provision of confirmation or denial in this case would be unfair and wholly outside the reasonable expectations of any of the councillors.

46. For completeness, the Commissioner has also considered whether it would be possible to satisfy a DPA Schedule 3 condition in order to allow the provision of confirmation or denial. He has concluded that it would not.

Right of appeal

47. 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: 0116 249 4253

Email: informationtribunal@hmcts.gsi.gov.uk

Website: www.justice.gov.uk/guidance/courts-and-tribunals/tribunals/information-rights/index.htm

48. 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.
49. 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

Alexander Ganotis
Group Manager – Complaints Resolution
Information Commissioner’s Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF