

Freedom of Information Act 2000 (FOIA)

Decision notice

Date: 25 June 2018

Public Authority: Commissioner of the City of London Police
Address: PO Box 36451
Bishopsgate
London
EC2M 4WNX

Decision (including any steps ordered)

1. The complainant has requested information about a named police investigation. City of London Police (CoLP) would neither confirm nor deny holding the information, citing the exemption at section 40(5) (personal information) of the FOIA.
2. The Commissioner's decision is that CoLP was correct to neither confirm nor deny holding information within the scope of the request by virtue of section 40(5)(b)(i) of the FOIA.

Request and response

3. On 6 November 2017, the complainant wrote to CoLP and requested information in the following terms:

"Between July 14 and December 1, 2010 [name of police officer redacted] was involved with "Operation [name redacted]". In his investigation he found evidence that [suspect's name redacted] was guilty of three counts of money laundering. Would you please send me a copy of all the evidence found by [police officer] that proved [suspect] was guilty of three counts of money laundering".

4. CoLP responded on 12 November 2017. It refused the request, citing the non-disclosure exemption at section 40(2) (personal information) of the FOIA.
5. The complainant requested an internal review, which CoLP provided on 11 January 2018. It revised its position, saying that it would neither confirm nor deny whether it held the information, under section 40(5) of the FOIA.
6. CoLP did not identify to the complainant which sub-section of section 40(5) it was relying on and thus whether it considered she had requested her own personal data or the personal data of third parties. Commenting generally on the application of section 40 of the FOIA, CoLP said that if the information related to her, the complainant should submit a subject access request under the DPA, whereas if the information she was requesting related to third parties, she should obtain a court order.

Scope of the case

7. The complainant contacted the Commissioner on 5 February 2018 to complain about the way her request for information had been handled. She believed that CoLP had evidence that the individual named in her request was guilty of money laundering, but he had never been prosecuted. She said she required the information in order to pass it to a lawyer for advice on whether he could be prosecuted.
8. In correspondence with the Commissioner, although CoLP said that the requested information pertained to third parties, it also stated that it was relying on section 40(5)(a) to neither confirm nor deny whether it held the requested information. This sub-section applies where the information requested is the requester's own personal data.
9. It was not clear to the Commissioner from reading the request and the subsequent correspondence, whether CoLP had in fact intended to cite section 40(5)(b) (which would apply where confirming or denying would breach any of the data protection principles in respect of third parties other than the complainant). On that point, she asked CoLP to clarify who it considered to be the primary data subject for the requested information, as well as for other information to support its position. However, CoLP failed to respond to these enquiries.
10. In the absence of any indication from the complainant that the information relates to her personally, and based on the actual wording of the request, the Commissioner would expect to see section

40(5)(b)(i) cited here, and she has exercised her discretion and treated it as having been cited in this case.

11. Accordingly, the analysis below considers CoLP's application of section 40(5)(b)(i) of the FOIA to neither confirm nor deny holding the requested information.

Reasons for decision

12. Under section 1(1)(a) of the FOIA, a public authority is obliged to advise an applicant whether or not it holds the information they have requested. This is known as the "duty to confirm or deny". However, the duty does not always apply and a public authority may refuse to confirm or deny whether it holds information through reliance on certain exemptions under the FOIA.
13. In this case, CoLP has argued that it is excluded from the duty to confirm or deny by virtue of section 40(5) (personal information) of the FOIA. As set out above, the Commissioner has taken this as being a claim that section 40(5)(b)(i) applies.

Section 40 – personal information

14. Section 40(5)(b)(i) of the FOIA provides that the duty to confirm or deny whether information is held does not arise where confirming or denying would contravene any of the data protection principles set out in the Data Protection Act 1998 ("the DPA"), which was the access regime for personal data at the time of responding to the request.
15. The consequence of section 40(5)(b)(i) is that if a public authority receives a request for information which, if it were held, would be the personal data of a third party (or parties), and its disclosure would breach any of the data protection principles, then it can rely on section 40(5)(b)(i), to refuse to confirm or deny whether or not it holds the requested information.
16. Consideration of section 40(5)(b)(i) involves two steps: first, whether providing the confirmation or denial would involve the disclosure of personal data, and secondly, whether disclosure of that personal data would be in breach of any of the data protection principles.

Is the information personal data?

17. Personal data is defined in section 1 of the DPA as:

"...data which relate to a living individual who can be identified

a) from those data, or

b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intention of the data controller or any other person in respect of the individual."

18. The two main elements of personal data are that the information must 'relate' to a living person and that the person must be identifiable. Information will relate to a person if it is about them, linked to them, has some biographical significance for them, is used to inform decisions affecting them or has them as its main focus.
19. In correspondence with the complainant, CoLP said that complying with her request would place sensitive personal data into the public domain.
20. Sensitive personal data is personal data which falls into one of the categories set out in section 2 of the DPA. The relevant category in this instance is:

"(g) the commission or alleged commission by him of any offence".

21. Having had particular regard to the wording of the request, which includes a criminal allegation against a named individual, the Commissioner is satisfied that the requested information comprises sensitive personal data about a third party. This is because the requested information, if held, relates to a criminal allegation against the individual named in the request.
22. Accordingly, the Commissioner considers that if CoLP confirmed or denied holding the requested information it would constitute a disclosure of sensitive personal data relating to the data subject named in the request. This is because the act of confirming or denying whether the requested information is held would disclose to the requester, and to the world at large, whether or not CoLP had conducted a criminal investigation into the criminal allegations set out in the request.
23. Having accepted that the request is for the sensitive personal data of an individual other than the applicant, and that the act of confirming or denying would involve the disclosure of sensitive personal data, the Commissioner must go on to consider whether this disclosure would contravene any of the data protection principles.
24. CoLP has indicated, and the Commissioner agrees, that the first data protection principle is relevant in the circumstances of this case.

Would confirmation or denial breach the first data protection principle?

25. The first data protection principle states -

"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless -

(a) at least one of the conditions in Schedule 2 is met, and

(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

26. In the case of a FOIA request, personal data is processed when it is disclosed in response to the request. This means that the information can only be disclosed if to do so would be fair, lawful and would meet one of the DPA Schedule 2 conditions and, in this case, one of the Schedule 3 conditions. If disclosure would fail to satisfy any one of these criteria, then the information is exempt from disclosure.

27. The Commissioner has first considered whether the disclosure which would take place as a result of confirming or denying whether information was held, would be fair to the data subject in question.

28. In considering whether a disclosure of personal information is fair, the Commissioner takes into account the following factors:

- the data subject's reasonable expectations of what would happen to their information;
- the consequences of disclosure (if it would cause any unnecessary or unjustified damage or distress to the individual concerned); and
- any legitimate interests in the public having access to the information and the balance between these and the rights and freedoms of the individuals who are the data subjects.

29. The Commissioner recognises that members of the public have an instinctive expectation that a police force, in its role as a responsible data controller, will not disclose sensitive information about them (including whether or not they have been the subject of a criminal investigation) and that it will respect their confidentiality.

30. Furthermore, the Commissioner considers that, in most cases, the very nature of sensitive personal data means it is more likely that disclosing it will be unfair. The reasonable expectation of the data subject is likely to be that such information would not be disclosed in response to an FOIA request and that the consequences of any disclosure could be damaging or distressing to them.

31. In light of the above, the Commissioner considers that information relating to criminal allegations and investigations, if held, will carry a strong general expectation of privacy for the parties concerned.
32. As to the consequences of disclosure upon a data subject, the question – in respect of fairness - is whether disclosure would be likely to result in unwarranted damage or distress to that individual.
33. When considering the consequences of disclosure on a data subject, the Commissioner will take into account the nature of the withheld information. She will also take into account the fact that, as set out in paragraph 22, above, disclosure under the FOIA is effectively a disclosure to the world at large, without conditions or controls.
34. Given the nature and timeframe of the request in this case, and the sensitivity of the subject matter, the Commissioner considers that disclosure by way of confirmation or denial would constitute an invasion of the data subject's privacy, and the consequences of any disclosure could cause them damage and distress.
35. Notwithstanding a data subject's reasonable expectations or any damage or distress caused, it may still be fair to disclose information, or in this case confirm or deny that information is held, if there is an overriding legitimate interest in disclosure. Under the first principle, the disclosure of the information must be fair to the data subject, but assessing fairness involves balancing their rights and freedoms against the legitimate interest in disclosure to the public and the private interests of the requester.
36. This is a different balancing exercise than the normal public interest test carried out in relation to exemptions listed under section 2(3) of the FOIA. Given the importance of protecting a data subject's personal data the Commissioner's 'default position' is in favour of protecting the privacy of the individual. The legitimate interest in confirming or denying that information is held must outweigh the public interest in protecting the rights and freedoms of the data subject if providing confirmation or denial is to be considered fair.
37. Examples of a legitimate public interest in disclosure include the general public interest in transparency, the public's interest in the issue the information relates to and any public interest in disclosing the specific information.
38. The complainant has not explained to the Commissioner any specific private interests that would be served by compliance with the request. However, the Commissioner understands from correspondence with the complainant in other cases that she alleges that the data subject

defrauded her husband of their life savings, but she has repeatedly failed to provide information capable of verifying this claim to CoLP. Consequently, the Commissioner has not accorded any weight to the complainant's presumed interests when balancing them against the privacy rights of the data subject. In any case, the appropriate procedure for anyone who considers themselves to be the victim of a crime is to report it to the police, and to allow them to take it forward.

Conclusion

39. In considering whether the exemption at section 40(5)(b)(i) of the FOIA was correctly applied in this case, the Commissioner has taken into account that disclosure under the FOIA should be considered in its widest sense – which is to the public at large.
40. With due regard to the nature and age of the requested information, the reasonable expectations of the data subject and the potential impact on them if the existence of their personal data in the context of a criminal investigation was to be confirmed or denied, the Commissioner considers that it would be unfair to do so.
41. The Commissioner is satisfied that confirming or denying that the requested information is held would not only be an unwarranted intrusion of the data subjects privacy but could potentially cause unnecessary and unjustified distress to the individual named in the request. She considers these arguments outweigh any legitimate interest in disclosure.
42. Accordingly, she considers that the exemption provided by section 40(5)(b)(i) is engaged and that CoLP was therefore not obliged to confirm or deny whether it held the information requested by the complainant.
43. As the Commissioner has determined that it would be unfair to confirm or deny that the information is held, it has not been necessary to go on to consider whether this is lawful or whether one of the schedule 2 or schedule 3 DPA conditions is met.

Right of appeal

44. 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

45. 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.
46. 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

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