

Freedom of Information Act 2000 (Section 50)

Decision Notice

Date: 19 July 2010

Public Authority: Chief Constable of Sussex Police
Address: Police Headquarters
Church Lane
Lewes
East Sussex
BN7 2DZ

Summary

The complainant requested copies of documents that a deputy district judge had determined should not be withheld under public interest immunity regulations during the prosecution of protestors against EDO MBM, an arms company. Sussex Police refused to confirm or deny whether it held the information falling within the scope of the request, citing the exemption provided by section 40(5)(b)(i) of the Freedom of Information Act 2000 (the "Act"). The Commissioner finds that confirmation or denial would disclose personal data and that the disclosure of this personal data would be in breach of the first data protection principle. The exemption provided by section 40(5)(b)(i) is therefore engaged and the public authority is not required to take any steps.

The Commissioner's Role

1. The Commissioner's duty is to decide whether a request for information made to a public authority has been dealt with in accordance with the requirements of Part 1 of the Freedom of Information Act 2000 (the "Act"). This Notice sets out his decision.

Background

2. Following protests against EDO MBM, a company that manufactures weapons, an injunction was brought to restrict the activities of protestors. Sussex Police subsequently sought to prosecute a number of individuals for an alleged failure to comply with a notice issued under section 14 of the Public Order Act, which sets out conditions on a public assembly. In the case in question, a deputy district judge ordered the Crown to hand over documents it was withholding under Public Interest Immunity regulations. Owing to the sensitivity of these documents, the Crown decided to withdraw the prosecutions rather than agree to the disclosure.

The Request

3. The complainant submitted the following information request which was received by Sussex Police (the "public authority") on 28 January 2009:

"On 7th February 2006 The Crown abandoned a case alleging breach of section 14 of the public order act against [a named individual] and others. Deputy District Judge Cooper ruled that information she had seen should be in the public domain and would assist defence arguments.

Therefore I request copies of all the documents that the DDJ had sight of that were the subject of her order of disclosure as they clearly on [sic] her view should not be immune to the public interest in their disclosure..."

4. The public authority responded to the request on 20 February 2009. It claimed that, under section 40(5) of the Act, it was not obliged to confirm or deny whether it held the requested information.
5. The complainant requested an internal review on 4 March 2009. On 31 March 2009, the public authority responded with the outcome of its review. This upheld its original decision to refuse the request, citing section 40(5)(b)(i).

6. To support its refusal, the public authority explained that to comply with section 1(1)(a) of the Act – namely, the duty to confirm or deny whether requested information is held – would amount to confirmation to the world that individuals had been the subject of criminal proceedings. This would breach the first data protection principle contained in the Data Protection Act 1998 (DPA).

The Investigation

Scope of the case

7. On 1 May 2009 the complainant contacted the Commissioner to complain about the way his request for information had been handled.

Chronology

8. The Commissioner wrote to the public authority on 23 February 2010. This set out his understanding of the case and asked the public authority to provide supporting arguments if it wished to maintain its reliance on section 40(5) of the Act. The public authority responded to the Commissioner in an email dated 24 March 2010.
9. On 8 April 2010, the Commissioner emailed the public authority for further information in regards to its application of section 40(5) of the Act. This was received on 26 April 2010.

Analysis

Exemption

Section 40(5)(b)(i)

10. Section 40(5)(b)(i) provides that a public authority is not obliged to confirm or deny whether requested information is held if to do so would:
 - constitute a disclosure of personal data, and
 - this disclosure would breach any of the data protection principles or section 10 of the DPA.
11. The Commissioner's analysis of whether the above criteria would be satisfied follows.

Would confirming or denying that the requested information is held constitute a disclosure of personal data?

12. The DPA defines personal information 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 data controller or any person in respect of the individual."

13. In his guidance on the section 40 exemption¹, the Commissioner expanded on what constituted personal data:

"The two main elements of personal data are that information must 'relate to' a living person, and that 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, has them as its main focus or impacts on them in any way."

14. The public authority has argued that the way in which the request is worded clearly indicates that the complainant is seeking information which may or may not show that a named individual was involved in criminal proceedings. Therefore, to comply with section 1(1)(a) of the Act would inevitably disclose information that would significantly relate to that individual.

15. The Commissioner is in agreement with the public authority's analysis, in that confirming or denying whether the requested information is held would constitute a disclosure of personal data

Would disclosure of this personal data breach a data protection principle?

16. In refusing the request, the public authority has claimed that to confirm or deny whether the requested information was held would breach the first data protection principle. This requires that personal data is processed fairly and lawfully and that:

¹http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/personal_information.pdf

- 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.
17. The Commissioner's considerations here focus on the general issue of whether disclosure would be fair to the individual who the complainant has suggested was the subject of court action.

Fairness

18. In establishing whether disclosure is fair, the Commissioner will look to balance the consequences of any release of personal data and the reasonable expectation of the data subject with general principles of accountability and transparency.
19. The personal data that would potentially be disclosed here would relate to the named individual in a private capacity. This is significant in that previous decisions issued by the Commissioner have been guided by the principle that information about an individual's private life will deserve more protection than information about someone acting in an official or work capacity.
20. The Commissioner would therefore consider that any individual would have a legitimate expectation that information which may or may not confirm whether they had been the subject of court proceedings would not be released. To disclose this information would, instead, be an unwarranted intrusion into the rights and freedoms of that data subject, given the distress to the data subject that the release of the information could potentially cause.
21. To develop this point, the Commissioner notes that the information in this case falls under section 2(h) of the DPA as it relates to proceedings for any offence committed or alleged to have been committed by the data subject. As such, by its very nature, this has been deemed to be information that individuals regard as the most private information about themselves. Further, as disclosure of this type of information is likely to have a detrimental or distressing effect on the data subject, the Commissioner considers that it would be unfair to disclose the requested information.
22. This view was supported in the Commissioner's decision involving the Ministry of Justice, issued under case reference FS50165494². At paragraph 47 of his decision, the Commissioner expressed his agreement that:

² http://www.ico.gov.uk/upload/documents/decisionnotices/2009/fs_50165494.pdf

"...to reveal to the whole public whether someone was subject to a court case would be unfair. He does not feel that releasing sensitive personal data into the public domain will be fair unless there are exceptional circumstances. He considers that there is a general and reasonable expectation that if someone was to appear in court that the information would not be released to the public domain."

23. In this instance, the Commissioner does not consider that the circumstances of the case would militate against the privacy of the data subject being preserved.

Conclusion

24. As indicated, the Commissioner has taken a clear line that disclosure of personal data relating to an individual in a private capacity should be afforded a high degree of protection, not least because of the sensitive nature of the information in this case. This is based on the Commissioner's understanding that individuals would have a reasonable expectation that information of this kind would not be disclosed.
25. Leading on from these considerations, the Commissioner has determined that to confirm or deny whether the requested information is held would be unfair to the data subject. As disclosure would therefore breach the first data protection principle, section 40(5)(b)(i) is engaged.

The Decision

26. The Commissioner's decision is that the public authority correctly refused the request for information under section 40(5)(b)(i) of the Act.

Steps Required

27. The Commissioner requires no steps to be taken.

Right of Appeal

28. 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,
Arnhem House,
31, Waterloo Way,
LEICESTER,
LE1 8DJ

Tel: 0845 600 0877

Fax: 0116 249 4253

Email: informationtribunal@tribunals.gsi.gov.uk.

Website: www.informationtribunal.gov.uk

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.

Any Notice of Appeal should be served on the Tribunal within 28 (calendar) days of the date on which this Decision Notice is sent.

Dated the 19th day of July 2010

Signed

**David Smith
Deputy Commissioner**

**Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF**

Legal Annex

Freedom of Information Act 2000

Right of Access

Section 1(1) provides that -

Any person making a request for information to a public authority is entitled –

- (a) to be informed in writing by the public authority whether it holds information of the description specified in the request, and
- (b) if that is the case, to have that information communicated to him.

Personal Information

Section 40(1) provides that –

Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.

Section 40(2) provides that –

Any information to which a request for information relates is also exempt information if –

- (a) it constitutes personal data which do not fall within subsection (1), and
- (b) either the first or the second condition below is satisfied.

Section 40(3) provides that –

The first condition is –

- (a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene-
 - (i) any of the data protection principles, or
 - (ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and

- (b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.

Section 40(4) provides that –

The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data).

Section 40(5) provides 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), 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 that 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).

Section 40(6) provides that –

In determining for the purposes of this section whether anything done before 24th October 2007 would contravene any of the data protection principles, the exemptions in Part III of Schedule 8 to the Data Protection Act 1998 shall be disregarded.

Section 40(7) provides that –

In this section-

the data protection principles" means the principles set out in Part I of Schedule 1 to the Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;

"data subject" has the same meaning as in section 1(1) of that Act;

"personal data" has the same meaning as in section 1(1) of that Act."

The Data Protection Act 1998

Interpretative provisions

Section 1(1) provides –

In this Act, unless the context otherwise requires –

“data” means information which –

- (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
- (b) is recorded with the intention that it should be processed by means of such equipment,
- (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or
- (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68;

“data controller” means, subject to subsection (4), a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed;

“data processor”, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller;

“data subject” means an individual who is the subject of personal data;

“personal data” means 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 intentions of the data controller or any other person in respect of the individual;

“processing”, in relation to information or data, means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including –

- (a) organisation, adaptation or alteration of the information or data,
- (b) retrieval, consultation or use of the information or data,
- (c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

“relevant filing system” means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Section 1(2) provides –

In this Act, unless the context otherwise requires –

- (a) “obtaining” or “recording”, in relation to personal data, includes obtaining or recording the information to be contained in the data, and
- (b) “using” or “disclosing”, in relation to personal data, includes using or disclosing the information contained in the data.

Section 1(3) provides –

In determining for the purposes of this Act whether any information is recorded with the intention –

- (a) that it should be processed by means of equipment operation automatically in response to instructions given for that purpose, or
- (b) that it should form part of a relevant filing system,

It is immaterial that it is intended to be so processed or to form part of such a system only after being transferred to a country or territory outside the European Economic Area.

Section 1(4) provides –

Where personal data are processed only for the purposes for which they are required by or under any enactment to be processed, the person on whom the obligation to process the data is imposed by or under that enactment is for the purposes of this Act the data controller.

Section 2 provides –

In this Act “sensitive personal data” means personal data consisting of information as to –

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, such as the disposal of such proceedings or the sentence of any court in such proceedings.

Schedule 1

The Data Protection Principles

1. 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.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.