# Freedom of Information Act 2000 (Section 50)

## Decision Notice

**Date: 15 March 2010**

**Public Authority:** Chief Constable of Kent Police
**Address:** Kent Police Headquarters
Sutton Road
Maidstone
Kent
ME15 9BZ

## Summary

The complainant requested the names, ranks and collar numbers of the police officers involved in making an arrest of a photographer, under the powers contained in section 44 of the Prevention of Terrorism Act 2000. The public authority refused the request under section 40(2) of the Freedom of Information Act 2000, claiming that the information was sensitive personal data and should not be disclosed. The Commissioner finds that, in the circumstances that the request was made, disclosure of the requested information would breach the first data protection principle. The exemption provided by section 40(2) 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. On 8 July 2009, two police officers and a police community support officer of Kent Police (the "public authority") arrested a photographer

under the provisions contained in section 44 of the Prevention of Terrorism Act 2000. The photographer subsequently placed a photograph of two of the officers on his blog, and posted a copy of his letter of complaint to the public authority's Professional Standards Department. This identified the police officers who he believed had behaved inappropriately in making his arrest.

3. In agreement with the public authority, the photographer agreed to remove any identification of the police officers from his blog, including blurring the faces of the officers in the photograph, while the Professional Standards investigation was underway.

## The Request

4. In correspondence dated 2 August 2009, the complainant requested the following:

*"…the names, ranks and collar numbers of the police officers who intercepted and arrested* [the photographer] *on 8 July 2009 on Chatham High Street at around 12.30pm."*

5. The public authority responded by letter on 18 August 2009. It stated that, in most circumstances, its response would be to refuse to confirm or deny whether any information in relation to the arrest existed, as to do so would in itself disclose the sensitive personal information that an individual had been involved in an alleged offence.

6. However, since the individual had placed this information in the public domain of his own volition, the public authority considered it would be unreasonable to take this approach. It therefore confirmed that the incident had resulted in an official complaint being submitted. However, it decided that it would be unfair for the purposes of the first data protection principle to release the names of the officers involved because it would identify employees who were the subject of a complaint. It therefore refused the request pursuant to section 40(2) of the Act.

7. The complainant requested an internal review on 23 August 2009. Among other points, the complainant stated that where police officers have found to have broken the law, the naming of the officers would act as a powerful deterrent. The public authority replied with the outcome of its review on 15 September 2009. This upheld the public authority's original decision to refuse the request under section 40(2).

8. Although not part of its standard complaints procedure, the complainant asked the public authority on 11 October 2009 to conduct a fresh review on the basis of advice given in another case by the Commissioner. The public authority carried out a review as instructed but maintained, in its correspondence of 29 October 2009, that section 40(2) did apply.

## The Investigation

---

### Scope of the case

9. On 25 November 2009, the complainant contacted the Commissioner to complain about the way his request for information had been handled. The complainant specifically asked the Commissioner to consider whether the public authority was entitled to rely on section 40(2) of the Act to refuse his request.

### Chronology

10. The Commissioner wrote to the public authority on 25 January 2010, setting out his understanding of the case. He went on to offer his preliminary view that police officers, who were in direct contact with the general public, should have a greater expectation that their personal data would be disclosed. The Commissioner therefore invited the public authority to release the requested information.

11. In its letter of 8 February 2010, the public authority declined the Commissioner's invitation, being firmly of the belief that previous decisions issued by the Commissioner supported its position.

12. Following receipt of this correspondence, the Commissioner telephoned the public authority on 17 February 2010 to seek further clarification on the nature of the arrest. During the conversation, the public authority directed the Commissioner to the Information Tribunal's decision in *David Young v the Information Commissioner (EA/2009/57 & 2009/89)*, indicating that its position was analogous to its own.

13. On 23 February 2010, the complainant emailed the Commissioner to direct him to the blog of the arrested photographer, particularly his posts of 25 November 2009 and 11 December 2009, which illustrated developments in the complaint being investigated by the Professional Standards Department.

14. The Commissioner responded to the complainant on 2 March 2010. He acknowledged that, according to the blog, the photographer in question

had received a letter from the Professional Standards Department which confirmed its finding that his complaint had been recorded as proven. However, the Commissioner informed the complainant that his investigation could only examine the circumstances of the case as they stood at the time of the request. Therefore, these developments could not be included in the scope of his considerations.

## Analysis

---

### Exemptions

### Section 40(2) of the Act

15. Section 40(2) of the Act provides an exemption for information which is the personal data of any third party. In order for the public authority to rely on section 40(2) in this case, it would have to be satisfied that:

- the requested information was the personal data of the police officers in question; and
- disclosure of that information would contravene a data protection principle contained in the Data Protection Act 1998 (the "DPA").

16. The Commissioner addresses each of these points in turn.

### Is the requested information personal data?

17. The complainant has requested the names, ranks and collar numbers of police officers. The Commissioner is satisfied that this information is clearly about identifiable individuals and is biographical in a significant sense. He therefore accepts that the withheld information would constitute personal data for the purposes of the DPA.

### Would disclosure contravene a data protection principle?

18. The public authority has argued that the release of the requested information would breach the first data protection principle, which requires the processing of personal data to be both fair and lawful. The Commissioner's considerations here focus on the general issue of whether disclosure would be fair to the police officers who are the focus of the request.

*Fairness*

19. In establishing whether disclosure is fair, the Commissioner has balanced the consequences of any release of personal data and the

reasonable expectations of the data subjects with general principles of accountability and transparency.

20. In his guidance, entitled *"When should names be disclosed"*[1], the Commissioner set out the following factors to guide whether a public authority should consent to the release of information identifying an individual:

    1. Does the information requested relate primarily to the person's public function rather than their private life?
    2. Should the individual expect their role to be subject to public scrutiny? You should consider:

        - how senior they are;
        - whether they have a public profile; and
        - whether their role requires a significant level of personal judgment and individual responsibility.

21. The Commissioner has no doubt that the requested information refers to individuals acting in an official capacity, that is in making an arrest of an individual under the powers contained in the Prevention of Terrorism Act 2000. It is also clear that a police officer has a prominent role in a community and holds considerable powers in maintaining and enforcing public order, as evidenced by the arrest itself. Therefore, while the position may not be considered a senior-ranking role and may therefore have a greater expectation to privacy than, say, a Chief Constable, nevertheless the Commissioner considers that an officer would exercise a high level of personal judgment, and would bear significant responsibilities, in the course of his or her duties.

22. In light of these factors, the Commissioner would normally take the view that an officer, who in any case has direct contact with the general public and would be displaying their collar number when on patrol or other official business, should expect to be subject to a high degree of scrutiny.

23. Yet, when weighing up what an appropriate level of scrutiny would be, the Commissioner accepts that there is an objectively reasonable expectation that anyone's personnel or disciplinary records will remain private. The Commissioner has therefore acknowledged the need in this instance to consider the context in which disclosure would take place and what the possible ramifications of disclosure would be.

[1] The guidance can be accessed at:
http://www.ico.gov.uk/upload/documents/library/freedom_of_information/practical_application/whenshouldnamesbedisclosed.pdf

24. In the previously referenced blog, which is freely accessible, the author states that a letter of complaint had been sent to the public authority's Professional Standards Department and included a copy of the said letter on his web-page. By requiring disclosure, the Commissioner would, in effect, be identifying the officers who had been the subject of a complaint.

25. In its decision involving *David Young v the Information Commissioner (EA/2009/57 & 2009/89)*, the Information Tribunal remarked that:

> "[police] *officers can in general reasonably expect that the mere existence of complaints about them will not be the subject of public disclosure. Such disclosure would therefore prejudice their rights and/or legitimate interests and we consider that such prejudice would be sufficient to make disclosure 'unwarranted' in these cases."*

26. In accordance with the Tribunal's findings, the Commissioner is of the opinion that the release of the requested information would be unfair to the data-subjects. As disclosure would therefore not meet the conditions set out in the first data protection principle, he considers the exemption provided by section 40(2) to be engaged.

27. The Commissioner would note that, in coming to this decision, he has no knowledge of whether the author has agreed to remove the names of the police officers from his blog in perpetuity. He is therefore conscious that the requested information may be placed in the public domain irrespective of what decision is made in this notice.

28. Nevertheless, as a regulator of both the Act and the DPA, the Commissioner is mindful of his responsibilities to ensure, as far as he is able, that information is processed in accordance with the legislation. He has therefore concentrated on whether the identities of the police officers should be disclosed under the Act and considered the issue of possible disclosure outside the legislation as extraneous to his decision.

29. The Commissioner would also note that his decision does not give carte blanche for a police force, or any authority, to refuse to disclose the identity of an individual simply on the basis that they may be the subject of a complaint at a later date. Instead, he would stress that each case must be judged on the facts as they stand at the time of a request.

## The Decision

30. The Commissioner's decision is that the public authority dealt with the request for information in accordance with the Act.

## Steps Required

31. The Commissioner requires no steps to be taken.

**Right of Appeal**

32. 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 served.

**Dated the 15th day of March 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(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.

### 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.

Schedule 2

Conditions relevant for purposes of the first principle: processing of any personal data

1. The data subject has given his consent to the processing.

2. The processing is necessary –

(a) for the performance of a contract to which the data subject is a party, or
(b) for the taking of steps at the request of the data subject with a view to entering into a contract.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by the contract.

4. The processing is necessary in order to protect the vital interests of the data subject.

5. The processing is necessary –

(a) for the administration of justice,
(b) for the exercise of any functions conferred on any person by or under any enactment,

(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6. (1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.